THE HIRING GUIDE:
Cybersecurity in Manufacturing

Updated June 2021

Change Record

DATE	SECTIONS	DESCRIPTION
October 8, 2020	Sucess Profiles Career Pathways	Manufacturing Cybersecurity Systems Operator was added as a career pathway (p. 66) & success profile (p.99).
June 21, 2021	Sucess Profiles Career Pathways	Manufacturing Cybersecurity AI Engineer was added as a career pathway (p. 67) & success profile (p. 107). Manufacturing Cybersecurity Analyst was added as a career pathway (p. 70) & success profile (p. 117).

Table of Contents

Acknowledgments

In addition to thanking our many colleagues at MxD, ManpowerGroup, other institutes, other employers and intermediaries, and workforce organizations in our network with who we had conversations on the Cyber[ME] project, we would like to formally acknowledge the sponsors, project team and formal contributor/reviewers.

Specific content of the presented Now and Next outputs (work domains, roles taxonomy, role profiles and certain sub-lists for prioritized work) have been peer reviewed by various combinations of the listed contributors. The views expressed for the broader narrative and other extended derivative outputs of the broader taxonomy work are those of the authors and their respective organizations.

Authors	Lory Antonucci – Manufacturing Solutions, ManpowerGroup Michael Garamoni - MxD	Rebekah Kowalski – Manufacturing Solutions, ManpowerGroup
Executive Sponsors	Chandra Brown- MxD Rebekah Kowalski – Manufacturing Solutions, ManpowerGroup Federico Sciammarella, PhD – MxD	Lizabeth Stuck - MxD Michael Stuhl - Manpower North America, ManpowerGroup
Project Core Team	Akin Akinbosoye – MxD Patricia Fields - Experis, ManpowerGroup	Christine Koprowski - Manpower Manufacturing, Manpower Group Charles Pritzl - Experis, ManpowerGroup
Reviewers	Guillaume Deudon – Dow Matt Jeffries – U.S. Navy Charlie Lewis – McKinsey and Company Dan Rozinski – Dow	Scott Sommer - International Academy of Automation Engineering Baijian Yang, PhD – Purdue University Chuck Zelnio – John Deere
Contributors	Nilanjan Banerjee, PhD – University of Maryland-Baltimore County Alethe Denis – ManpowerGroup Solutions Raleen Gagnon – ManpowerGroup Solutions Nathan Hartman, PhD – Purdue University John Livingston – Verve Industrial Solutions Adeeb Mahmood – Siemens USA Jose Medina Cruz – University of Illinois at Urbana-Champaign, Critical Infrastructure Resilience Institute	Marian Merritt – National Initiative for Cybersecurity Education David Palomo – Textron Cesar Pena – MxD Jordan Segue - Siemens Industry Andrea Whitesell – University of Illinois at Urbana-Champaign, Critical Infrastructure Resilience Institute
Supplemental Reviewers	Voula Colburn – MxD Tony Del Sesto – MxD Elliot Forsyth – Michigan Manufacturing Technology Center Mike Gahn – Rolls-Royce Katherine Fu, PhD – Georgia Institute of Technology Anthony Holden - U.S. Army Mike Hourigan – International Academy of Automation Engineering Paul Huang – Office of Naval Research Malcolm Jeffers – International Academy of Automation Engineering	Romina Lara – MxD Joe Nesmith – ManpowerGroup Public Sector Jennie Parr Kirchner – ManpowerGroup Jennifer Pilat – MxD Chris Saldana, PhD – Georgia Institute of Technology John Sands, PhD – Moraine Valley Community College Alyssa Sullivan – MxD Pat Toth – NIST, Manufacturing Extension Partnership Katia Valenzuela – MxD Michael Yucuis – MxD

The Hiring Guide: Cybersecurity in Manufacturing. Antonucci, L., Garamoni, M., Kowalski, R. (2020).
We welcome a conversation!

The Challenge

Manufacturing enterprises face increasing challenges and threats to secure their information and physical assets throughout the product life cycle. From design and manufacturing through consumer/field use and operations there are privacy and security concerns for the physical and virtual assets that make up the process and the product. Manufacturers - from large consumer and military industrialists to specialty medical device and consumer products makers - also face industry specific needs including sector practices, regulatory demands, and standards adoptions; lagging supply chain cybersecurity practice adoption, investment and maturity variances and other business factors drive increasing demands for improved cybersecurity practices.

Sharing current and future cybersecurity skill needs with other industries, manufacturers compete with other market segments for a cyber-capable workforce across several business and technical work areas. Previous and ongoing cyber workforce development initiatives in the public and private sector provide foundational resources to guide workforce planning and development but more manufacturing-specific guidance is needed. Here at the start of a new decade, the gap has only widened, and the needs to secure the talent has increased.

- **What is driving this urgent need?**
- **What is the future cyber workforce and its capabilities?** What specific roles need be developed, hired and employed for success and cyber resiliency for manufacturing? What career paths are representative of the opportunities for solid and varied careers as the workforce for Manufacturing cyber excellence is hardened just as the other assets in Manufacturing need be steeled against the challenges and threats?
- **Where is the workforce of tomorrow today?**
- **Who and what enables the cyber workforce?**

Our framework establishes the “now and next” view of the critical work required of cybersecurity workers in business and technical areas of manufacturing; it also profiles what value those roles bring to the manufacturing enterprise and ecosystem. The taxonomy work leverages and learns from the National Institute for Standards and Technology (NIST) and National Initiative for Cyber Education (NICE) frameworks and other cyber workforce research most from the government arena, since many of those are essential and relevant. Yet there is a need to represent the legacy of production, and the future practices and potentials of modern manufacturing.

Our framework and the related tools produced in this project bring fundamental definition across the digital manufacturing enterprise. This means our view is wide in scope and has unique roles as well as conventional areas. Some bring certain business functions into the cybersecurity fold: who knew about smart contracts in purchasing 20 years ago? When did IoT Device Engineers become part of the Product Security team?

Risk intelligence, alignment and governance in 2020 and beyond requires engaging and expecting the participation of many functions not previously thought to be part of something “technical” like cybersecurity. Securing the full life cycle of designs, materials, processes, plants, products and more brings on board Supply Chain and Procurement staff and Product Managers. And many more roles even in conventional information technology now have a specific and identifiable set of tasks and tools as they contribute to Secure by Design, secure from the start.

The connected, digital operating environment and place where life takes place asks many to play a significant role in securing the assets of manufacturers, their employees and customers, and other stakeholders.

A changing environment as major as the one that we are seeing broadly in digital technology, society, and business is one that affects the entire manufacturing enterprise. It requires many roles in the workforce to be part of the **cyber in manufacturing enterprise (Cyber^{ME})** workforce.

This project was completed under the Cooperative Agreement W31P4Q-14-2-0001, between Army Contracting Command – Redstone and UI LABS on behalf of the Digital Manufacturing and Design Innovation Institute. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Department of the Army.

This effort between MxD, the Manufacturing USA digital manufacturing institute, and ManpowerGroup (NYSE: MAN) has produced a manufacturing centric view of the cybersecurity workforce needed to enable cybersecurity capability and resiliency at small, medium and large manufacturers. Views of today's challenges and tomorrow's horizons have been considered as several key workforce tools have been created. These tools and ongoing work on evolving the cyber workforce can serve as a manufacturing specific primer for industry, individuals, academia, government and workforce development as they meet the related workforce challenges.

MxD brings together the public and private sector– including academia, students, startups, nonprofits, and government stakeholders – on technical and workforce development projects. The institute engages in research and policy efforts, as well as in promoting the new digital enterprise, connected factory of the future and new data-centric manufacturing enterprise connected by the digital thread.

A leader in innovative workforce solutions space, ManpowerGroup Joined MxD in this effort following up on its 2017 Digital Manufacturing Workforce Taxonomy project with MxD's predecessor, the Digital Manufacturing Design Innovation Institute.

The Hiring Guide project engaged experts from over 25 industry, academic, workforce development, and government organizations to identify the Cyber^{ME} workspace and the work roles needed now and into the future. The project efforts defined work domains, created representative career paths and success profiles, and updated key supply/demand views. The picture of the cyber in manufacturing workforce presented herein can be used to facilitate many future conversations needed to address the actual recruitment, development and progression of the cyber warriors needed in manufacturing.

The pivotal success factors in building a taxonomy are to describe and classify; then group by meaningful and differentiating characteristics; and then classify consistently resulting in a reliable structure for organizing and understanding the scope of interest. The Cyber^{ME} job roles taxonomy structure is at the center of a set of meaningful tools and thought leadership contained in the Hiring Guide to organize the work, workers, and work environment of the cybersecurity in manufacturing ecosystem.

Common Considerations for Small, Mid-Size and Large Manufacturers

What range of identified cyber needs and project assets will support all manufacturers, whether small, mid-size or large?. While the Hiring Guide assets can't be a universal prescription for all manufacturers as a specific intact set; they can be a "dictionary" of accessible roles and selected targets to write each organization's cyber workforce story.

The goal was to provide a common toolset that enables all manufacturers and workforce partners to see examples of major cyber needs and opportunities. For smaller to mid-size manufacturers, while there may not yet be an immediate or full time need for certain roles, an understanding that some roles may be part of their prime manufacturers' workforce is important. We aimed to produce resources that smaller organizations can use to understand what roles they may need from vendors and partners as well as to attract developmental roles to their organization as part of the larger, sustainable cyber workforce system.

Awareness of the broad set of tools provided in the Hiring Guide, for manufacturers of all sizes, accommodates these understandings:

- Smaller companies may consolidate several roles into one or two positions; while they may not need the same volume or number of people in any role, they will still need most of the role outputs.
- Companies of all sizes may choose - for many reasons – to supplement in-house positions with additional contractor, consultant, or temporary staff. Whether or not the position is internal, many of the roles addressed are part of their overall needed capability.

PATHS

Paths

This section answers What is the future cyber workforce and its capabilities?

Several key project outputs in this section are the core of the taxonomy work: domains, roles, and views of the roles via impacts, stages, highlighted roles, critical roles, and transitioning roles. All of these outputs and tools are 'paths' to the workforce and have been developed to answer that overarching question: what is the future cyber workforce in manufacturing and its capabilities?

This section also contains derivative efforts from the domains and roles. Once domains and roles were determined and characterized, the project team and reviewers determined some prioritization of interest and generalized need – a 'first look" type of designation. With those initial views came 40 roles to highlight, 3 success profiles developed from the first 30 critical roles list; 8 themes of career paths developed, each with a representative sample; and four personas representing potential candidates provided to kickstart recruiting conversations.

Taxonomy Structure: Content Previews

Drivers

The important business, social, technical and geo – political factors causing the increased focus on cybersecurity for manufacturing at this time. Specific drivers influence needs and as a result, the solutions for the time and state.

Work Domains

Work domains – also high level areas of knowledge and skill - describing the performances and capabilities that need to be demonstrated for success and resiliency of the Cybersecurity[ME].

Role vs. Jobs

This is the primary orientation of the taxonomy work. Structuring and focusing on roles versus positions in the taxonomy accommodates the diverse business and workforce environments. Identifying and developing roles allows for single or multiple roles together as the job when building out positions specific to each employer.

Role Impacts

Role impacts are segmented by timing and life cycle of when they emerge or are often best positioned . The timing and cadence of roles and related work team and organizational designs, can help advance or change overall capability. In turn, this helps achieve the employer's evolving business and workforce progression needs.

Role Stages

Role stages are defined in terms of the maturity of the role and its uniqueness to the field of cybersecurity. Stages include previous roles that have been updated and changed by cybersecurity, those that are native to cybersecurity and those that may emerge in the future.

Transition Roles

A designation of approximately 50 identified roles that are destinations for transitioning workers. With upskilling, additional experience, or formal education or certifications, these destination roles may be achievable with 2 years or less of additional development.

Highlighted Roles

A designation of approximately 40 identified roles that showcase the overall scope and type of needs addressed by the taxonomy. These roles also illustrate work that will contribute greatly to cybersecurity success and/ or represent major shifts in the workforce or manufacturer.

Critical Roles

A designation of approximately 30 identified roles that are positioned as early focus for employers, educators, government and the workforce. Seen as important to the ecosystem for a number of reasons, these roles are not the only critical roles, but a solid set of the "first critical" roles to consider.

Note: For some of the outputs such as role lists, the lists are presented in line in this section. For most of the other outputs (profiles, paths, personas), there is an introduction in this section and a reference to the appendix for the complete output.

Overview of Work Domains

Domains are commonly known as a body of knowledge or, more practically, an area of expertise. For our purposes with the workforce and roles taxonomy efforts, we create work domains. Defining the work domains is one of the most foundational steps. Having the domains aligned to business, technical and capability needs is necessary to organize and specify the workforce performances and outputs and align them to key functions and roles.

Identifying the work domains serves to answer:

- What are the work areas for a manufacturer that deliver cybersecurity outputs and performances, and are needed for successful cybersecurity capability?
- What subareas can be defined?
- Which domains are common to any enterprise gaining cybersecurity capacity and capability but are also present in manufacturing?
- Which are unique to manufacturing or oriented towards manufacturing, even if also shared with another sector's cybersecurity capability?

The NIST Cybersecurity Framework and the NICE Workforce Framework are two indispensable resources in the cybersecurity industry and workforce development world. They have been leveraged in this taxonomy work.

In the NIST framework, there are five major stages and over 20 next level activities. The NIST Framework provides a common organizing structure for cybersecurity practices by assembling standards, guidelines, and other control system elements, but the framework does not provide work roles. The NICE Framework is where the initial mapping and connection to specific work roles begins by defining common cybersecurity functions and areas of cybersecurity work, including 52 roles with alignment to Standard Occupational Classification jobs. These roles to date from NICE have been industry agnostic but have skewed towards generic risk, solid overall cybersecurity management, and conventional network and software-oriented cybersecurity activities.

The MxD Cyber^{ME} Taxonomy leverages the 52 NICE roles and builds from there considering the key themes and priorities that formed the project charter. Those key themes include a taxonomy that:

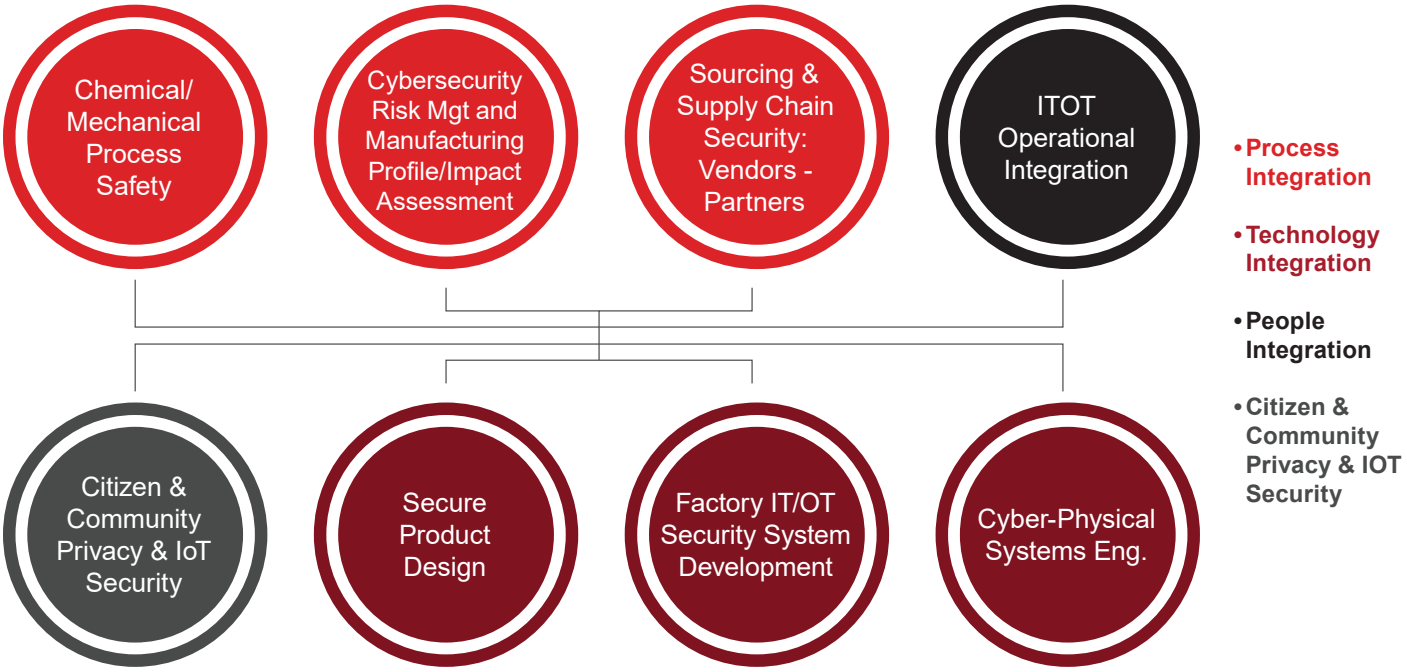
1. Is manufacturing centric and manufacturing applicable; this didn't mean creating a taxonomy 100% unique to manufacturing but one that was clearly defined in the context of manufacturing cybersecurity needs and practices.
2. Focuses on roles and not jobs, to allow for maximum flexibility and realities of how jobs are designed and deployed.
3. Reaches across the enterprise, beyond conventional technology and beyond only a network focus or, in the case of manufacturing, beyond a production focus into other organizational functions wherever critical work is performed that enables or delivers cybersecurity capabilities.
4. Specifies roles and work enough to allow for flexibility in small, medium and large manufacturers; provides the ability to build collections of roles into jobs that meet the maturity and scale of the company.
5. Provides enough specificity to build derivative project tools for career planning, curriculum design, hiring, etc.

Seven primary Cyber^{ME} domains have been identified. In turn, these 7 domains were further detailed into 35 subdomains. Extending from and having some clear relationships to the NIST and NICE frameworks to date, all of these Cyber^{ME} domains and subdomains are defined and oriented towards the practice of cybersecurity in manufacturing.

The following section of Paths (Pathways) of this consolidated deliverable presents the primary outputs as shown above as well as several extended outputs from the taxonomy work. There one will find the drivers, domains, views of the roles in the taxonomy, sample career paths, recruiting personas, and success profiles. In the People section, the supply/demand insights and data are provided. In the Partners section is the map of the ecosystem, a discussion on some key connections and general calls to action.

Overview of Work Domains

Positioning Manufacturing Specific Focus Hubs for Cyber[ME]



Along with the NIST/NICE frameworks, the drivers, and the core themes, the Hubs influenced the domain and subdomain framework development to the greatest degree.

Process Integration	Manufacturers have unique operations. Applying practices from other industries will only work so much. Specific industry practices and related security concerns for human, facility, material, process and product safety is essential. These will vary by manufacturing sectors and individual organizations specific to their footprint and focus, but each will have a profile and related security risks. Manufacturing has probably the most complex and distributed supply chains including national defense and critical infrastructure. The just-in-time and segmenting core capability production strategies of recent decades have driven the importance and criticality of supply chain cybersecurity.
Technology Integration	Growing interconnectedness of IT and OT is a hallmark issue for manufacturing security. This includes legacy factory and production environments, the development of security software and systems and retrofitting where necessary. As manufacturers modernize, embrace IoT, and connect to larger mega-structures (see later Smart Cities/Smart grid references), there will continue to be a rise in the engineering of more complex and larger scale cyber-physical systems. Across the entire product life cycle, approaching security as being “designed-in” vs. “bolted-on” post-production represents a key manufacturing transformation.
People Integration	The convergence requirement between IT and OT cybersecurity in manufacturing is focused on the everyday functional operations between the two disciplines and the need to converge their ongoing cybersecurity governance, compliance, resourcing, practices and operations.
Citizen & Community Privacy/ IoT Security	As more personal information is accessed, collected and shared via IoT devices and advanced or assisted automation merges with everyday life, it’s essential for manufacturers to address the role of individuals’ privacy and safety concerns. From ethics to liability, this is a necessary hub for the makers of modern life.

The first map outlines the seven Cyber^ME domains.

Cyber^ME Domain Maps

Themes: Enterprise, not just factory. Ecosystem, not just enterprise. It's not only the cybersecurity analysts role. Process and product. Before, during and after. Future horizons with maybe fewer not more options…

The seven domains defined cover both the NIST framework and a manufacturing-centric view beyond the NIST framework to achieve a goal of the project – a fuller view of cybersecurity for manufacturers inclusive of these more specific themes:

1. **Cybersecurity in manufacturing is the responsibility of the entire enterprise** and is inclusive of work domains across the company and, while essential, not just focused on securing the factory or only involving primarily the conventional corporate information technology area.
2. Cybersecurity in manufacturing is even beyond the enterprise and actually a **responsibility of the manufacturing ecosystem, not just the enterprise.** The domains, subdomains, associated roles, and later ecosystem map (Section 4: Partners) recognize first that inclusion of the supply chain is mandatory and that vendors and third parties are a key part of the workforce delivery of cybersecurity capabilities. No examples of self-contained manufacturing companies were identified in our research.
3. There are **many areas and subareas in all manufacturing organizations that have a role, literally, in manufacturing cybersecurity.** While white hats and ethical hackers, or vulnerability specialists and cybersecurity analysts are commonly known cybersecurity roles, the span of involved roles goes well beyond those well-established jobs. Cyber is not only the cybersecurity analyst's role. From cybersecurity accountants to cybersecurity recruiting specialists and IoT Device Engineers and Incident Response Managers, there is a large contingent of Cyber^ME roles. Having diverse subdomain home bases for those varied roles was mandatory for the domain view.
4. A domain view in manufacturing has to **accommodate both the process view – the process of manufacturing, and the product view, the further life cycle of the use of the manufactured goods** that have connectivity and therefore have cybersecurity needs and roles to service those product tasks
5. A domain view also has to **consider enabling domains before, during and after cyber is practiced.** Domains such as Readiness & Development and R&D and Innovation, and roles from Workforce Planning Manager to Researchers and Standards Developers are included to establish that there is a pipeline for innovation outputs and talent outputs, and a life cycle for the recruiting, development and upskilling of that talent.

CyberME Domain and Sub-domains

The next level of the graphic provides more detail, outlining some of the sub work functions that align within the domains.

Readiness & Development	• Education / Development / Training • Exercise & Testing • Recruitment & Staffing
Business & Technical Alignment	• Cybersecurity Emergency Response Management • Culture Change & Transformation • Enterprise Risk Management & Manufacturing Target Profile • Financial Assurance • Leadership, Governance & Policy Management • Secure Design & Secure Product Management • Security Operations • Smart Factory – Smart Cities Strategy • User & Consumer Support
Information Technologies and Integration	• Application Management & Security • Cloud/Edge Computing & Security • Data & Information Management & Security • Integration & Convergence • Intrusion Detection • Network Management & Security • Systems Management & Security (Secure Systems Development)
Operating Technologies and Integration	• Application Management & Security • Cloud/Edge Computing & Security • Data & Information Management & Security • Integration & Convergence • Intrusion Detection • Network Management & Security • Systems Management & Security (Secure Systems Development)
Supply Network and Partnering	• Application Management & Security • Cloud/Edge Computing & Security • Data & Information Management & Security • Integration & Convergence • Intrusion Detection • Network Management & Security • Systems Management & Security (Secure Systems Development)
Compliance, Legal & Forensics	• Forensics & Investigations • Legal • Regulatory & Compliance • Risk Mitigation Program Management (Business Continuity, Disaster Recovery, Information Security, etc.)
Cyber R&D and Innovation	• R&D • Innovation

Domain Descriptions

- Education / Development / Training
- Exercise & Testing
- Recruitment & Staffing

Work Domain: Readiness & Development

The **Readiness & Development** domain can be thought of as an initial or foundational domain if one considers the life cycle of cybersecurity talent. In this domain is where the essential roles that address cybersecurity talent management, human capital, and readiness of the cybersecurity workforce are most directly considered. It covers recruitment and staffing support – including an often mentioned need to have specialized cyber-familiar recruiters and workforce planners – to those involved in development and training of the large incoming cyber workforce. It is also home to the somewhat specific and modernized versions of the practice teams that are well-known to various military, civic and industry incident response teams who use team/role play structures to practice scenario based 'challenge' exercises.

- Cybersecurity Emergency Response Management
- Culture Change & Transformation
- Enterprise Risk Management & Manufacturing Target Profile
- Financial Assurance
- Leadership, Governance & Policy Management
- Secure Design & Secure Product Management
- Security Operations
- Smart Factory - Smart Cities Strategy
- User & Consumer Support

Work Domain: Business & Technical Alignment, Governance and Response

The Business & Technical Alignment, Governance and Response domain is the domain that recognizes the organizational-level business connections and overarching shared commitment to cybersecurity that is needed across the enterprise to prepare and respond to cyber risks. Leadership, governance, enterprise risk management and other administrative functions are combined here to reinforce the alignment necessary for resourcing, accountability, culture change and overall cybersecurity success. This includes security operations management, and emergency response leadership and roles for a unified front before breaches during active monitoring, during breaches and for any resulting response management. A key distinction of this phase is the inclusion of product design leadership that anchors the Secure by Design approach to build in security from the start and then throughout the product life cycle. Also part of this "secure from the start" mentality is the "smart factory-smart cities" design work area, an essential foundation for safe, secure industrial systems that are part of our increasingly connected life.

Domain Descriptions

- Application Management & Security
- Cloud/Edge Computing & Security
- Data & Information Management & Security
- Integration & Convergence
- Intrusion Detection
- Network Management & Security
- Systems Management & Security (Secure Systems Development)

Work Domain: Information Technologies & Integrations

Information Technologies & Integrations is the domain that covers the "soft information" side of data and communications technologies: IT infrastructure, technologies, systems and network capabilities including development, operations and ongoing security management. Many of the functions and related roles in this domain will be modernized versions of conventional IT roles, now updated both for new technologies – think cloud, edge, IoT – and it is also home to some of the well-known cyber native roles and functionality with the Intrusion Detection function and roles here. (Remember other related Security Operations Management is in the Business Alignment, Leadership and Governance domain). A cornerstone of this domain is the Secure Systems Development focus, carrying forward the Secure from the Start mindset applied into app and systems development. This domain also has a shared subdomain with the OT domain: they each have Integration and Convergence and have parallel roles of the IT/OT Integration Engineer in recognition of the important efforts to operationally align and connect these two domains for cybersecurity success.

- Automation & Controls
- Cyber-Physical Asset Management
- Industrial Controls Security
- Infrastructure Management
- Integration & Convergence
- Mechatronics
- Physical Systems & Facility Security

Work Domain: Operating Technologies & Integration

Operating Technologies & Integrations is the domain that covers the cybersecurity associated work areas managing production hardware, plant and physical facilities, and physical systems and technologies that aid in the physical execution of manufacturing, processing, assembly or operation of a product. Operating Technologies in mind for cybersecurity include digitally controlled/sensed equipment and cell/platform assemblies, shop floor tools/systems/software, automation and controls, infrastructure systems, and robotics and other automation assistance used to optimize production and product quality. An added dimension is the inclusion of the physical functionality of all IoT products which have their own operating technologies in the sense of hardware/device security. Operating Technologies and its oft-cited rival, Informational Technologies, are actually positioned as kindred domains. Together they are the apex of cybersecurity in manufacturing, bringing together the physical and digital realms for secure, safe and optimal performance. To both was added the sub-domain of Integration and Convergence and the shared role of the IT/OT Integration Engineer.

Domain Descriptions

- Contracts & Procurement
- Supply Network Management
- Vendor Integration

Work Domain: Supply Networking and Partnering

Supply Networking and Partnering is the domain where security considerations of the direct supply network, contracts and procurement roles and the integration of vendors/vendor systems is considered. A manufacturer is only as secure as the weakest link in their supply chain, and supply chains are an increasing target of cybersecurity threats and vulnerabilities. For many manufacturers who are part of the Defense contracting system, their status and the related cyber requirements of DFARS are a primary security consideration and often drive their cybersecurity practices and workforce needs. Also creating demand for some roles in this domain is the substantial dependence of manufacturers (and other industries) on vendor partners in the delivery of cybersecurity capabilities and expertise. A greater level of data connectivity within the Supply Network enables real time supply chain optimization, but with that increased risk management when it comes to secure data and communications. Also in the contracts and procurement sub-domain is the inclusion of Smart Contracts, an increasing use of electronic contract management and fulfillment contract management systems secured by block chain and other distributive computing practices. Secure transactions increase, fraudulent performance decreases and automation of many of the administrative aspects of vendor and contract management are supported by the cybersecure practice of smart contracting.

- Forensics & Investigations
- Legal
- Regulatory & Compliance
- Risk Mitigation Program Management (Business Continuity, Disaster Recovery Information Security, etc.)

Work Domain: Compliance, Legal & Forensics

Compliance, Legal & Forensics is the work domain most aligned to formal internal and external legal and regulatory interactions and outputs. As the impacts and types of cybercrimes and disruptions increase exponentially, there is even more movement to investigate, assign causality, prosecute where possible and learn more about the actors, vectors and targets to mitigate future risks. Standards and compliance expectations come from both internal and external sources – from the board of trustees to the DoD. Internal compliance and supply chain compliance intersect here as well along with other Risk Program management roles. A frequent career path in cybersecurity is known to be between law enforcement and commercial/private sector cybersecurity. Not only is there good skill adjacency, there is direct agency and legal experience that can be leveraged here between manufacturers and public/government sector employment/roles.

Introduction to the Roles

The main purpose of the taxonomy is to provide a structure that defines and classifies the work that is being done in Cyber[ME] and to enable the workforce development goals of the manufacturing ecosystem: industry, individuals, academia, workforce and community development, and government. Drawing on the NICE roles, role research from several other federal agencies, O*NET and proprietary and public jobs data bases, as well as original design and applied research, the project team and reviewers ultimately identified 247 roles across the domains that have at least a quarter of their role responsible for dedicated cybersecurity tasks, outputs, decisions or the application of cybersecurity related knowledge

Our priority focus is on roles - a cluster of related duties, skills, or knowledge that contributes to key outcomes of a work effort. Roles represent the “assemblies” of skills, knowledge and outputs that optimally enable cybersecurity in the manufacturing ecosystem overall and within a manufacturer most directly. This focus on identifying roles rather than jobs is an important distinction. The US manufacturing industry is diverse, encompassing a variety of work environments. These roles are seen as critical to the success of manufacturing enterprises. Each manufacturing organization will need different sets or combinations of these roles on different timelines depending on their life cycle and their business focus.

Jobs are one or more roles tied together to meet a need or focus of an organization and managed as a position for one or more people to do. Organizations can assemble roles into jobs as needed. A role can be an entire job and often is an entire job, especially in larger organizations; other organizations will combine roles, especially in early stages or where the volume of work does not require dedicated positions. Roles can and often still are mapped to many of our public and private workforce resources that are labeled as “jobs”.

In the end, the purpose of the taxonomy is to provide essentially a dictionary of possible roles; each organization writes its own cyber workforce and jobs story using this dictionary.

247 Cyber[ME] Roles Identified & Mapped to the Technical Domains

The roles are grouped by the domain and then by the subdomain. They are also described in terms of role impacts, role stage, and whether the role is a Highlighted, First 20 Critical or Transition role. Each of those distinctions are meant to be helpful in understand the value and cadence of developing and investing in a workforce with those skills and scopes of work.

Before the view of the roles by domains, a key question: Why so many roles?

Admittedly, the taxonomy is expansive.

Several factors contributed to the detail and scope.

1. **Cyber is everyone's job.** There are more people involved in cyber resiliency and effectiveness, and more people have some responsibility to produce cyber outputs and/or apply cyber knowledge. This automatically opens up the range of roles.

2. **Span of functions is wider.** The scope of the taxonomy was by necessity and design meant to achieve fuller coverage of business, business-technical and technical roles. We didn't leave out HR or finance completely. We included external partner key roles.

3. **Used a lower threshold.** We used a generalized threshold of 25% of a workload/work design to qualify for inclusion. That is a lower threshold than DM&D which was a 50% threshold of digital work/tools/knowledge for inclusion. The lower threshold is an acceptance of the fact that a small behavior can produce a large cyber risk/impact.

4. **Comparatively, NICE identifies macro jobs.** In comparison, the NIST/NICE positions are not roles but jobs, macro jobs and more generalists. Considering the newness of cyber roles generally, and the wider needs, the use of more micro roles enables flexibility and applicability.

5. **Cyber jobs/roles/work is newer.** There is less industry standardization or normative role design to date in cybersecurity. On the way to figuring it out, companies often have to combine or create custom positions.

6. **Modularity allows flexible design.** Jobs classifications available to workforce developers and employers is very helpful in certain ways, but not as helpful as roles that can be assembled and combined, building up to jobs and positions when needed. This allows for accommodating size and maturity flexibility. (See below as well).

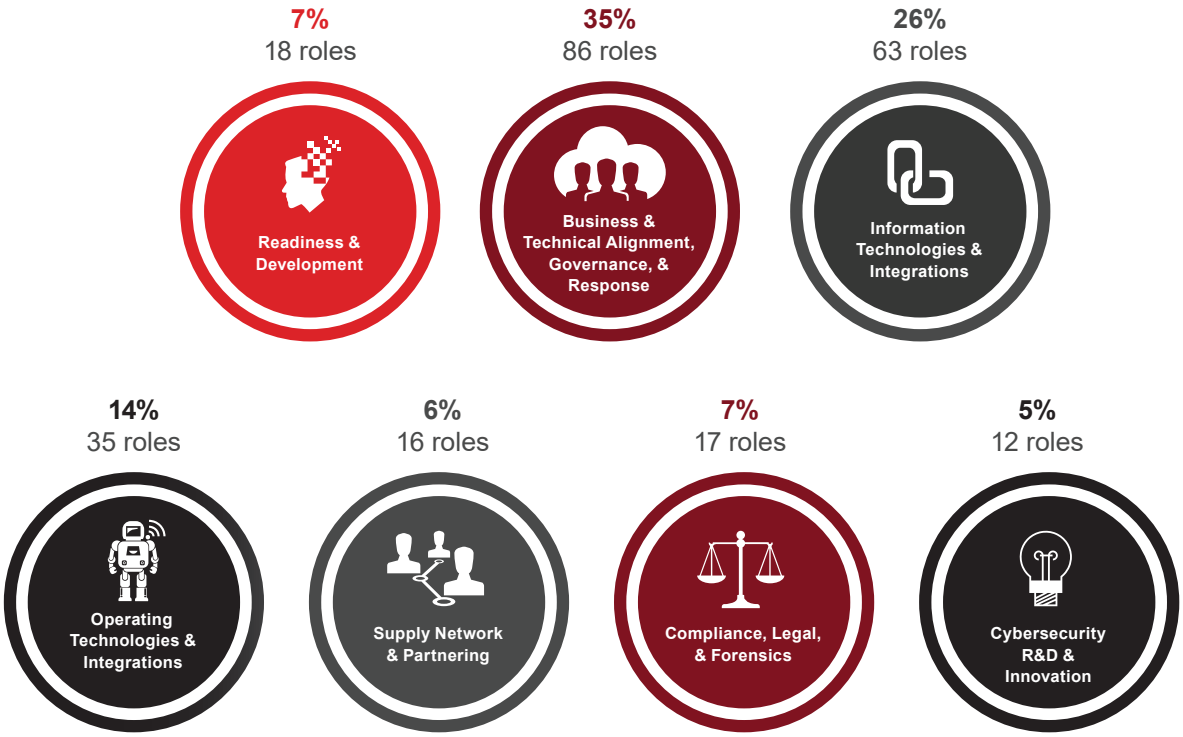
7. **More actually allows for less in job design.** Small to mid-size manufacturers will benefit from the detail and availability of the broader array when it comes to their assembly of roles. They can be more specific about workforce planning, job design, and recruiting that meet their needs, which sometimes will be more narrow and sometimes could be broader or more generalized.

The roles are grouped in fairly understandable and manageable numbers. With a bit of review and familiarity, the breadth should well serve manufacturers of various sizes and types in their workforce efforts.

Cyber[ME] Work Domains

Role Distribution (% of 247 total roles)

Below is the distribution of the roles across the domains. Business Alignment and Governance draws the largest number of roles, with Information Technology second, and Operational Technologies roles the third most frequent home domain.



Roles by Domains

The following sub-sections present the community of 247 roles through lists of roles by domain. Later views will present sub-lists of the community of Cyber[ME] roles using the other filters of role impact and other descriptors (highlighted, transition, critical, etc.).

Welcome to the Cyber[ME] Community of Roles!

Business Alignment and Governance Domain

This domain holds 86 Cyber[ME] roles, approximately 35% of the total.

Domain	Subdomain	Cyber Role
Business & Technical Alignment	Culture Change and Transformation	Cybersecurity Awareness Communications Specialist Cybersecurity Knowledge Bank Manager DevSecOps Transformation Leader Digital Transformation Advisor Enterprise Cybersecurity Culture Change Management Specialist Security Evangelist Security Program Management Office (SPMO) Leader
	Cybersecurity Emergency Response Management	Agency Response Coordinator Breach Response Analyst Breach Response Manager Corporate Crisis Management Leader Disaster Recovery Coordinator Incident Analyst Incident Communication Facilitator Incident Containment Responder Incident Historian/Archivist Incident Responder Incident Response Manager Incident Specialist (Specific Actor, Vector, Target) Incident Task Force Leader Site/Plant/Regional Emergency Response Leader
	Enterprise Risk Management and Mfg Target Profile	Business Continuity Consultant Business Impact Analyst Chief Risk Officer Cybersecurity Assessor/Planner-Manufacturing Profile Cybersecurity Insurance Specialist Cybersecurity Risk Manager Governance Compliance & Risk Manager Lead Internal Auditor Risk Advisor
	Financial Assurance	Cryptocurrency Accountant Cybersecurity Accountant Cybersecurity Economist
	Leadership, Governance and Policy Management	AI Ethics Advisor Anti-Counterfeiting Advisor Chief Executive Officer (CEO) Chief Information Officer (CIO) Chief Information Security Convergence Officer (CISO/CISCO) Chief Security Officer (CSO) Company Owner (SMM) Cyber Policy Analyst Cybersecurity Ethicist Cybersecurity Governance Business Analyst Data Privacy Officer Information Systems Security Officer (ISSO) Internal Manufacturing Cybersecurity Standards Developer Manufacturing Operations Senior Leader Plant Manager/Site Manager Privacy Policy Analyst Program Manager Project Manager Security Director

Domain	Subdomain	Cyber Role
	Secure Design and Secure Product Management	Autonomous Device Security Engineer Chip Hardware Internals Security Engineer Embedded Code Developer – Security Focused IoT (Internet of Things) Security Specialist Mobile Security Engineer Mobile Security Technician Personally Identifiable Information (PII) Advisor Product Designer Product Security Engineer Product Specialist Quality Assurance Specialist Secure Design Product Life Cycle Manager
	Security Operations	Cybersecurity Analyst Security Auditor Security Operations Center (SOC) Analyst Security Operations Center (SOC) Engineer Security Operations Center (SOC) Manager SOC Operations Analyst (Cybersecurity Analyst) SOC Operations Lead SOC Operations Specialist
	Smart Factories, Smart Cities	Smart Factory Architect Smart Factory Designer Smart Grid Security Engineer
	Smart Factory, Smart Cities Strategies	Autonomous Factory Engineer Secure Smart Factory-Smart Grid (Meta Systems) Engineer
	User and Consumer Support	Application Security Support Representative Citizen Security Smart Grid Sentinel End Consumer/Customer (Products) End User/Customer (Systems) Personal Privacy and Data Guardian Personally Identifiable Information (PII) Advocate Personally Identifiable Information (PII) Customer Support Representative
		All Employees All Managers

Information Technologies & Integration

This domain holds 63 Cyber[ME] roles, approximately 26% of the total.

Domain	Subdomain	Cyber Role
Information Technologies and Integration	Application Management and Security	Application Security Administrator Application Security Architect Application Security Developer Application Security Engineer Application Security Specialist
	Cloud/Edge Computing and Security	Cloud Security Architect Cloud Security Engineer Cloud Security Specialist Edge Device Engineer
	Data and Information Management and Security	Client/Server Analyst Data Architect Data Loss Prevention (DLP) Analyst Data Loss Prevention (DLP) Auditor Data Loss Prevention (DLP) Engineer Data Owner Data Security Analyst Data Warehousing Archiving Specialist (Data Custodian) Database Administrator IoT (Internet of Things) Data Manager
	Integration and Convergence	Cybersecurity IT/OT Integration Engineer IoT (Internet of Things) Communications Architect
	Intrusion Detection	Cryptanalyst Cybersecurity Intelligence Specialist Firewall (Network Access Control) Analyst Intrusion Detection Analyst Malware Analyst Virus and Malicious Code Technician Vulnerability Assessor Vulnerability Manager Vulnerability Specialist
	Network Management and Security	Enterprise Encryption Engineer Linux Administrator MS Exchange Administrator Network Administrator Network Redundancy Engineer Network Security Administrator Network Security Advisor Network Security Architect Network Security Engineer Network Security Operator Network Specialist Windows Administrator
	Systems Management & Security (Secure Systems Development)	Biometrics Engineer Blockchain Developer Blockchain Engineer Cryptography Analyst Cybersecurity Artificial Intelligence Engineer Cybersecurity Artificial Intelligence Specialist Cybersecurity Artificial Intelligence Trainer Cybersecurity Scrum Master Cybersecurity Systems Testing and Evaluation Specialist Machine Learning Specialist Penetration Tester/Ethical Hacker (Operational) Public Key Infrastructure (PKI) Analyst Public Key Infrastructure (PKI) Engineer Secure Software Developer Secure Systems Developer Security Systems Architect Source Code Auditor System Administrator Systems Architect Systems Engineer Technical Support Specialist

Operating Technologies & Integration

This domain holds 35 Cyber[ME] roles, approximately 14% of the total.

Domain	Subdomain	Cyber Role
 Operating Technologies and Integration	Automation and Controls	Autonomous Plant Remote Manager Autonomous Remote Plant Operator Cybersecurity Systems Operator Factory Automation Engineer Factory Automation Manager Hardware Engineer Industrial (Process) Automation Engineer Industrial Control Engineer Industrial Controls System Specialist Industrial Process Automation Support Specialist Industrial Process Management Manager Instrumentation/Sensor Engineer Manufacturing Execution System (MES) Engineer Manufacturing Execution System (MES) Support Specialist
	Cyber-Physical Asset Management Industrial Controls Security	Cyber-Physical Asset Controller Cybersecurity Operations Specialist Chip Hardware Internals Security Architect Distributed Control Systems Analyst Distributed Controls Systems Engineer Hardware Engineer Industrial Control Network Security Architect Industrial Control Systems Analyst Industrial Controls Network Security Analyst Industrial Controls Network Security Engineer Supervisory Controls and Data Acquisition (SCADA) Engineer Supervisory Controls and Data Acquisition (SCADA) Security Analyst
	Infrastructure Management	Infrastructure Administrator Infrastructure Engineer Infrastructure Lead Infrastructure Security Architect Infrastructure Specialist Technician
	Integration and Convergence	Cybersecurity IT/OT Integration Engineer
	Mechatronics	Mechatronics Engineer
	Physical Systems and Facilities Security	Physical Security Administrator Site Emergency Services and Security Leader

Compliance, Legal, & Forensics

This domain holds a total of 17 Cyber[ME] roles, approximately 7% of the community

Domain	Subdomain	Cyber Role
Compliance, Legal & Forensics	Forensics and Investigations	Cybercrimes Investigations Coordinator Cybersecurity Forensics Engineer Digital Forensics Analyst Endpoint Forensics Specialist Network Forensics Specialist Psychologist
	Legal	Chief Legal Officer/Legal Advisor Intellectual Property Manager
	Regulatory and Compliance	Compliance Administrator Compliance Analyst
	Risk Mitigation Program Management	Compliance Manager IT/OT Cybersecurity Compliance Auditor Public Policy Advisor BC/DR/IS Manager BC/DR/IS Planner Data Recovery Specialist Disaster Recovery Coordinator

Cyber R&D

This domain holds a total of 12 Cyber[ME] roles, approximately 5% of the community

Domain	Subdomain	Cyber Role
Cyber R&D and Innovation	Innovation	Industrial Systems/Operational Technology Security Advisor Internal Cybersecurity Futurist Manufacturing Industry Cybersecurity Standards Developer National Secure Platform Architect National Secure Platform Auditor National Secure Technology Advisor Sentient Agent Monitor
	R&D	Cybersecurity Research Analyst/Technical Writer Manufacturing Cyber Security Researcher and Advisor Manufacturing Cybersecurity R&D Specialist Socio-Cyber Resilience Researcher and Advisor Technology Researcher

Readiness & Development

This domain holds a total of 18 roles, approximately 7% of the roles.

Domain	Subdomain	Cyber Role
Readiness & Development	Education/Development/ Training	Curriculum Developer/Planner Cybersecurity Instructor/Cybersecurity Faculty Cybersecurity K-12 Teacher Cybersecurity User Trainer/Coach Cybersecurity Workforce Developer
	Exercise and Testing	Blue Team Member (Defender) Cyber Exercise Developer Cyber Exercise Evaluator Cyber Exercise Facilitator IT/OT White Hat /Ethical Hacker (Exercise Role) Purple Team Member (Collaboration Coach) Red Team Member (Attacker) Tiger Team Member (Team of Testing Experts) Wireless Tester
	Recruitment and Staffing	Cybersecurity Recruiting Specialist Cybersecurity Workforce Manager Cybersecurity Workforce Planner Incident Task Force Resourcer

Supply Networking & Partnering

This domain holds a total of 16 Cyber[ME] roles, approximately 6% of the roles.

Domain	Subdomain	Cyber Role
 Supply Network and Partnering	Contracts and Procurement	Procurement Manager Smart Contract Advisor Smart Contract Reviewer
	Supply Network Management	International Compliance Manager International Supply Chain Manager Logistics Compliance Analyst Procurement Cybersecurity Advisor Supply Network Cybersecurity Compliance Auditor Supply Network Cybersecurity Compliance Manager Supply Network Global Compliance Manager
	Vendor Integration	Cybersecurity Partner Integration Planner Cybersecurity Solutions Sales Engineer Cybersecurity Strategic Solutions Advisor Electronic Data Interchange (EDI) Analyst Security Sales Account Manager Vendor/Alliance Collaboration Coordinator

Role Stages

Background

With the broader community established, we can look at other characteristics of the Taxonomy that provide richness to how the workforce is changing and evolving.

We have considered how the roles in the Cyber[ME] Community Map are reflective of evolving technologies. While it was not in scope to define the generations of technologies used by each role, it was possible to apply a more generalized view of the maturity of the various roles.

Three stages were established:

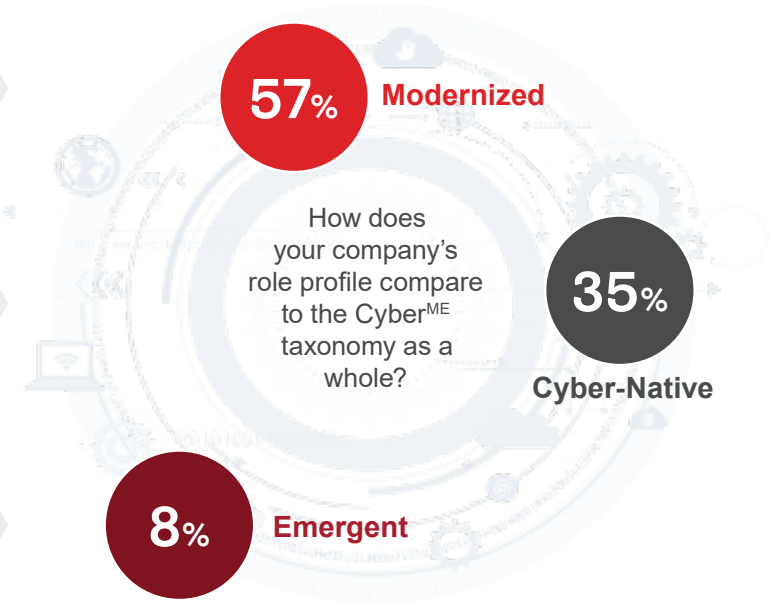
- Modernized
- Cyber-Native
- Emergent

The following graphic briefly defines the stages.

Modernized
Add cybersecurity capabilities, duties and outputs to established yet updated business and/or technical roles.

Cyber-Native
Developed to date mostly as part of cybersecurity's functional growth.

Emergent
Emerging from today's newest practices and/or possible with some of tomorrow's horizons.



Over half of the roles are actually existing roles that have been modernized, updated, or retooled to address cyber skills needs; only 8% are listed as emergent, potentially on the horizon as tomorrow's newest jobs. Fully a third of the taxonomy (35%) can be seen as cyber native: they are primarily roles that are native to cybersecurity and they exist today. Their scale and population, and their supply and demand are dependent on whether they are pioneer, keystone or producer roles, and on how mature are the manufacturers who employ them.

Consideration of Role Impact

Another way that each role of the taxonomy is defined is through the impact that role has on the development and evolution of the cybersecurity workforce and the cyber capability. The impacts consider the relationships of the roles to each other in terms of when they often appear – earlier or later as an organization matures its cybersecurity focus - and the relationship to the organization in terms of general impact.

As part of the ManpowerGroup workforce transformation approach, three initial types of impact are identified: pioneer, keystone, and producer. Looking at the broad taxonomy with this lens should help companies as they examine the blend of capabilities they need based on where the company is its evolution and where it wants to move to in its cybersecurity organization and capability. Identifying each role in this way makes possible discussion of:

- Which roles serve which purpose in terms of order or cadence when examining or planning a workforce overall?
- Which roles help sooner in a transformation?
- Which roles are more able to jumpstart the overall cybersecurity capability within an organization?
- Which roles evolve to be 'workforce valves' to enable the flow of work and information?
- Which roles offer specialization and generalization at scale?

As shown in the graphic below, three types of roles emerged – each with important contributions from a workforce planning perspective.

Role Impacts: Cyber^{ME} Distribution

Pioneer 27%

- Emerge early; pave the way
- Establish primary cyber capabilities
- Play broad roles initially
- Strategic generalists
- Roles often advance into specialties

Example Roles

- Smart Factory Designer
- Compliance Manager
- Data Security Analyst
- SOC Operations Analyst
- System Administrator
- Cybersecurity Recruiting Specialist
- White Hat/Ethical Hacker

Keystone 23%

- High impact on growth & performance
- Central hub of workflow, process, & direction
- Provide/direct key resources & information
- Support other roles & facilitate output

Example Roles

- Chief Risk Officer
- Cloud Security Architect
- Incident Containment Responder
- Personally Identifiable Information Advisor
- Socio-cyber Resilience Researcher & Advisor:

Producer 50%

- Represent specialties
- Enable scale
- All levels
- Responsible for continuous work output
- Convert key resources into outcomes

Example Roles

- All Employees
- Cybersecurity Accountant
- Cybersecurity AI Engineer
- Distributed Controls Systems Engineer
- Endpoint Forensics Specialist
- Network Administrator
- Purple Team Member
- SCADA Security Analyst

Considering the Pioneer, Keystone and Producer role types – all important and required in a Cyber[ME] organization, or any organization – should inform an owner's or leader/planner's view of what capabilities to hire, develop, or position as business and talent planning occur. As companies are executing on their business plans to advance Cyber[ME], this framework of role impact should become key language and method for considering what roles to grow, position, or leverage to achieve business goals.

Each impact type and their set of roles is listed below.

Cyber[ME] Pioneers

As we worked across the broad view of Cyber[ME] activity and outputs, some roles appeared as important initial sets of capabilities and outputs. Pioneer roles are just that – roles that emerge early as foundational when looking at a large work area. Pioneer roles in Cyber[ME] establish primary cybersecurity capabilities and play broader roles initially that can lead to other related yet more specialized roles. These pioneer roles may be roles that organizations develop and hire for earlier in the workforce planning, or roles that evolve faster and appear to take on large amounts of early effort to build out company capability. People in these roles themselves tend to learn and evolve rapidly as their roles can consist of both generalized and specialized responsibilities. These roles expand or refine quickly as the organization matures and grows. Slightly more than one quarter of the Cyber[ME] Role Community (27%) is comprised of these forerunner roles.

Role Impact	Domain	Cyber Role	Role Stages
	Business & Technical Alignment	Breach Response Manager	Cyber Native
		Business Continuity Consultant	Modernized
		Business Impact Analyst	Modernized
		Corporate Crisis Management Leader	Modernized
		Cyber Policy Analyst	Cyber Native
		Cybersecurity Economist	Cyber Native
		Digital Transformation Advisor	Modernized
		Disaster Recovery Coordinator	Modernized
		Enterprise Cybersecurity Culture Change Management Specialist	Modernized
		Incident Response Manager	Modernized
		Internal Manufacturing Cybersecurity Standards Developer	Modernized
		IoT (Internet of Things) Security Specialist	Cyber Native
		Lead Internal Auditor	Modernized
		Mobile Security Engineer	Cyber Native
		Risk Advisor	Modernized
		Security Evangelist	Cyber Native
		Security Operations Center (SOC) Analyst	Cyber Native
		Security Program Management Office (SPMO) Leader	Modernized
		Smart Factory Architect	Emergent
		Smart Factory Designer	Emergent
		Smart Grid Security Engineer	Emergent
		SOC Operations Analyst (Cybersecurity Analyst)	Cyber Native
		SOC Operations Lead	Cyber Native
	Compliance, Legal & Forensics Cyber R&D and Innovation	BC/DR/IS Planner	Modernized
		Compliance Manager	Modernized
		Psychologist	Modernized
		Industrial Systems/Operational Technology Security Advisor	Modernized
		Manufacturing Cybersecurity Researcher and Advisor	Cyber Native
		National Secure Platform Auditor	Emergent

	Information Technologies and Integration	Cloud Security Engineer	Cyber Native
		Cybersecurity Artificial Intelligence Specialist	Cyber Native
		Cybersecurity Intelligence Specialist	Cyber Native
		Data Loss Prevention (DLP) Analyst	Cyber Native
		Data Security Analyst	Modernized
		Firewall (Network Access Control) Analyst	Cyber Native
		Intrusion Detection Analyst	Cyber Native
		Malware Analyst	Cyber Native
		Network Security Administrator	Cyber Native
		Network Security Architect	Cyber Native
		Network Security Operator	Cyber Native
		Penetration Tester/Ethical Hacker (Operational)	Cyber Native
		Secure Software Developer	Modernized
		Secure Systems Developer	Modernized
		Source Code Auditor	Modernized
		System Administrator	Modernized
		Systems Architect	Modernized
		Systems Engineer	Modernized
	Operating Technologies and Integration	Cyber-Physical Asset Controller	Modernized
		Cybersecurity IT/OT Integration Engineer	Modernized
		Cybersecurity Operations Specialist	Cyber Native
		Cybersecurity Systems Operator	Modernized
		Factory Automation Engineer	Modernized
		Hardware Engineer	Modernized
		Industrial (Process) Automation Engineer	Modernized
		Industrial Control Engineer	Modernized
		Industrial Control Systems Analyst	Modernized
		Infrastructure Engineer	Modernized
		Infrastructure Lead	Modernized
		Supervisory Controls and Data Acquisition (SCADA) Engineer	Modernized
	Readiness & Development	Cybersecurity Instructor/Cybersecurity Faculty	Modernized
		Incident Task Force Resourcer	Modernized
		IT/OT White Hat /Ethical Hacker (Exercise Role)	Cyber Native
	Supply Network and Partnering	Cybersecurity Partner Integration Planner	Modernized
		Security Sales Account Manager	Modernized
		Supply Network Cybersecurity Compliance Manager	Cyber Native
		Supply Network Global Compliance Manager	Modernized
		Vendor/Alliance Collaboration Coordinator	Modernized

Cyber^{ME} Keystones

Working across the broad view of Cyber^{ME} activity, some roles appear as important sets of capabilities and outputs that also have a pivotal place in the flow or influence on the work volumes and outputs of others and the broader processes.

While all roles have that to some extent, some roles play an even stronger position in the expansion of roles around them. These roles are called Keystone roles. Keystone roles are a smaller, less frequent group within a large body of work compared to their pioneer and producer counterparts. Approximately 23% of the defined roles in the Cyber^{ME} taxonomy are Keystone roles.

However, even when smaller in number (how many serve in that role or how many a manufacturer may need), these roles usually exert a high impact on the growth and performance of digital manufacturing and design overall. They support the other types of roles and facilitate their output often by creating outputs that increase the demand for other roles and guide their impact; they provide or direct key resources and information even more than other roles, all positioning the keystone category as the central hub of workflow and direction for an organization. These keystone roles are in central positions of key processes and workflows.

Role Impact	Domain	Cyber Role	Role Stages
	Business & Technical Alignment	AI Ethics Advisor	Modernized
		Anti-Counterfeiting Advisor	Modernized
		Autonomous Factory Engineer	Emergent
		Chief Executive Officer (CEO)	Modernized
		Chief Information Officer (CIO)	Modernized
		Chief Information Security Convergence Officer (CISO/CISCO)	Cyber Native
		Chief Risk Officer	Modernized
		Chief Security Officer (CSO)	Cyber Native
		Chip Hardware Internals Security Engineer	Cyber Native
		Company Owner (SMM)	Modernized
		Cybersecurity Assessor/Planner-Manufacturing Profile	Cyber Native
		Cybersecurity Ethicist	Cyber Native
		Cybersecurity Risk Manager	Cyber Native
		Data Privacy Officer	Cyber Native
		DevSecOps Transformation Leader	Modernized
		Governance Compliance & Risk Manager	Modernized
		Incident Containment Responder	Modernized
		Incident Task Force Leader	Modernized
		Information Systems Security Officer (ISSO)	Cyber Native
		Manufacturing Operations Senior Leader	Modernized
		Personally Identifiable Information (PII) Advisor	Cyber Native
		Plant Manager/Site Manager	Modernized
		Product Security Engineer	Cyber Native
		Secure Design Product Life Cycle Manager	Modernized
		Secure Smart Factory-Smart Grid (Meta Systems) Engineer	Emergent
		Security Director	Modernized
		Security Operations Center (SOC) Manager	Cyber Native
	Compliance, Legal & Forensics	Chief Legal Officer/Legal Advisor	Modernized
		Intellectual Property Manager	Modernized
		IT/OT Cybersecurity Compliance Auditor	Cyber Native
	Cyber R&D and Innovation	Internal Cybersecurity Futurist	Emergent
		Manufacturing Cybersecurity R&D Specialist	Cyber Native
		Manufacturing Industry Cybersecurity Standards Developer	Cyber Native
		National Secure Platform Architect	Emergent
		National Secure Technology Advisor	Emergent
		Socio-Cyber Resilience Researcher and Advisor	Emergent
	Information Technologies and Integration	Application Security Architect	Cyber Native
		Cloud Security Architect	Cyber Native
		Cryptanalyst	Modernized
		Cybersecurity IT/OT Integration Engineer	Modernized
		Data Loss Prevention (DLP) Auditor	Cyber Native
		Data Owner	Modernized
		Edge Device Engineer	Emergent
		Enterprise Encryption Engineer	Cyber Native
		IoT (Internet of Things) Communications Architect	Cyber Native
		Public Key Infrastructure (PKI) Engineer	Cyber Native
		Security Systems Architect	Cyber Native
	Operating Technologies and Integration	Chip Hardware Internals Security Architect	Cyber Native
		Factory Automation Manager	Modernized
		Infrastructure Security Architect	Modernized
	Readiness & Development	Cybersecurity Workforce Planner	Modernized
	Supply Network and Partnering	Cybersecurity Solutions Sales Engineer	Cyber Native
		Cybersecurity Strategic Solutions Advisor	Cyber Native
		Procurement Cybersecurity Advisor	Modernized
		Smart Contract Advisor	Emergent
		Smart Contract Reviewer	Emergent
		Supply Network Cybersecurity Compliance Auditor	

Cyber^{ME} Producers

Half of roles (50%) are known as Producer roles. In any broad community of related workers, some roles are responsible for producing the group/company's major accomplishments and output. These are the roles that are usually larger in number and through their work they elevate the volume of output that the overall organization accomplishes and often increase the specialization and maturity of roles.

The size of the workforce in these roles is a business factor for each manufacturer based on their size and their "niche" or area of business across the manufacturing life cycle. Producers can be at any level or any type (technician to engineer to manager, etc.). In their work, they magnify and amplify the resources given. These essential functions, across any domain where some are more specialized and others more generalized, are responsible for much of the continuous work output of a manufacturer – they convert key resources into outcomes for the business and produce the lion's share of the overall operational value. Producers enable the enterprise or the entire ecosystem to flourish by expanding and optimizing resources through both generalist and specialist role making.

Role Impact	Domain	Cyber Role	Role Stages
	Business & Technical Alignment	Agency Response Coordinator	Modernized
		All Employees	Modernized
		All Managers	Modernized
		Application Security Support Representative	Cyber Native
		Autonomous Device Security Engineer	Emergent
		Breach Response Analyst	Cyber Native
		Citizen Security Smart Grid Sentinel	Emergent
		Cryptocurrency Accountant	Cyber Native
		Cybersecurity Accountant	Modernized
		Cybersecurity Analyst	Modernized
		Cybersecurity Awareness Communications Specialist	Modernized
		Cybersecurity Governance Business Analyst	Modernized
		Cybersecurity Insurance Specialist	Emergent
		Cybersecurity Knowledge Bank Manager	Modernized
		Embedded Code Developer – Security Focused	Cyber Native
		End Consumer/Customer (Products)	
		End User/Customer (Systems)	
		Incident Analyst	Cyber Native
		Incident Communication Facilitator	Modernized
		Incident Historian/Archivist	Cyber Native
		Incident Responder	Cyber Native
		Incident Specialist (Specific Actor, Vector, Target)	Cyber Native
		Mobile Security Technician	Cyber Native
		Personal Privacy and Data Guardian	Cyber Native
		Personally Identifiable Information (PII) Advocate	Cyber Native
		Personally Identifiable Information (PII) Customer Support Representative	Cyber Native
		Privacy Policy Analyst	Modernized
		Product Designer	Modernized
		Product Specialist	Modernized
		Program Manager	Modernized
		Project Manager	Modernized
		Quality Assurance Specialist	Modernized
		Security Auditor	Modernized
		Security Operations Center (SOC) Engineer	Cyber Native
		Site/Plant/Regional Emergency Response Leader	Modernized
		SOC Operations Specialist	Modernized

	Compliance, Legal & Forensics	BC/DR/IS Manager	Modernized
		Compliance Administrator	Modernized
		Compliance Analyst	Modernized
		Cybercrimes Investigations Coordinator	Cyber Native
		Cybersecurity Forensics Engineer	Cyber Native
		Data Recovery Specialist	Modernized
		Digital Forensics Analyst	Cyber Native
		Disaster Recovery Coordinator	Modernized
		Endpoint Forensics Specialist	Cyber Native
		Network Forensics Specialist	Cyber Native
		Public Policy Advisor	Modernized
		Cybersecurity Research Analyst/Technical Writer	Modernized
	Cyber R&D and Innovation	Sentient Agent Monitor	Emergent
		Technology Researcher	Modernized
	Information Technologies and Integration	Application Security Administrator	Cyber Native
		Application Security Developer	Modernized
		Application Security Engineer	Modernized
		Application Security Specialist	Cyber Native
		Biometrics Engineer	Cyber Native
		Blockchain Developer	Emergent
		Blockchain Engineer	Emergent
		Client/Server Analyst	Modernized
		Cloud Security Specialist	Cyber Native
		Cryptography Analyst	Modernized
		Cybersecurity Artificial Intelligence Engineer	Cyber Native
		Cybersecurity Artificial Intelligence Trainer	Cyber Native
		Cybersecurity Scrum Master	Modernized
		Cybersecurity Systems Testing and Evaluation Specialist	Cyber Native
		Data Architect	Modernized
		Data Loss Prevention (DLP) Engineer	Cyber Native
		Data Warehousing Archiving Specialist (Data Custodian)	Modernized
		Database Administrator	Modernized
		IoT (Internet of Things) Data Manager	Cyber Native
		Linux Administrator	Modernized
		Machine Learning Specialist	Cyber Native
		MS Exchange Administrator	Modernized
		Network Administrator	Modernized
		Network Redundancy Engineer	Modernized
		Network Security Advisor	Cyber Native
		Network Security Engineer	Cyber Native
		Network Specialist	Modernized
		Public Key Infrastructure (PKI) Analyst	Cyber Native
		Technical Support Specialist	Modernized
		Virus and Malicious Code Technician	Cyber Native
		Vulnerability Assessor	Cyber Native
		Vulnerability Manager	Cyber Native
		Vulnerability Specialist	Cyber Native
		Windows Administrator	Modernized

	Operating Technologies and Integration	Autonomous Plant Remote Manager	Emergent
		Autonomous Remote Plant Operator	Modernized
		Distributed Control Systems Analyst	Modernized
		Distributed Controls Systems Engineer	Modernized
		Hardware Engineer	Modernized
		Industrial Control Network Security Architect	Modernized
		Industrial Controls Network Security Analyst	Modernized
		Industrial Controls Network Security Engineer	Modernized
		Industrial Controls System Specialist	Modernized
		Industrial Process Automation Support Specialist	Modernized
		Industrial Process Management Manager	Modernized
		Infrastructure Administrator	Modernized
		Infrastructure Specialist Technician	Modernized
		Instrumentation/Sensor Engineer	Modernized
		Manufacturing Execution System (MES) Engineer	Modernized
		Manufacturing Execution System (MES) Support Specialist	Modernized
		Mechatronics Engineer	Modernized
		Physical Security Administrator	Modernized
		Site Emergency Services and Security Leader	Modernized
		Supervisory Controls and Data Acquisition (SCADA) Security Analyst	Modernized
	Readiness & Development	Blue Team Member (Defender)	Cyber Native
		Curriculum Developer/Planner	Modernized
		Cyber Exercise Developer	Modernized
		Cyber Exercise Evaluator	Modernized
		Cyber Exercise Facilitator	Modernized
		Cybersecurity K-12 Teacher	Modernized
		Cybersecurity Recruiting Specialist	Modernized
		Cybersecurity User Trainer/Coach	Modernized
		Cybersecurity Workforce Developer	Modernized
		Cybersecurity Workforce Manager	Modernized
		Purple Team Member (Collaboration Coach)	Cyber Native
		Red Team Member (Attacker)	Cyber Native
		Tiger Team Member (Team of Testing Experts)	Modernized
		Wireless Tester	Modernized
	Supply Network and Partnering	Electronic Data Interchange (EDI) Analyst	Modernized
		International Compliance Manager	Modernized
		International Supply Chain Manager	Modernized
		Logistics Compliance Analyst	Modernized
		Procurement Manager	Modernized

Community Map of Roles:
Bringing it All Together

The Community Map of Roles is a way of visualizing the entire listing of the 247 roles identified for the Cyber[ME]. This is the collective view of how the domains and the roles assemble together as a community of workers and capabilities.

In the key to the map below, the pattern of information is shown. Coming from the center of the map and connected by a single word that summarizes the purpose of the domain, is the “circuit branch” of each domain. Each domain has subdomain sections with the roles of that subdomain listed. All seven domains are presented, appearing clockwise from Readiness (prepare) through the other domains to R&D (improve).

On the following page is a full map of the 247 roles (For hard copy viewers, see Appendix B for the role map in an enlarged format for easier reading)

R&D
- Cybersecurity Research Analyst/Technical Writer
- Manufacturing Cybersecurity R&D Specialist
- Manufacturing Cybersecurity Researcher & Advisor
- Socio-Cyber Resilience Researcher & Advisor
- Technology Researcher

Innovation
- Industrial Systems/Operational Technology Security Advisor
- Internal Cybersecurity Futurist
- Manufacturing Industry Cybersecurity Standards Developer
- National Secure Platform Architect
- National Secure Platform Auditor
- National Secure Technology Advisor
- Sentient Agent Monitor

Cybersecurity R&D & Innovation

Forensics & Investigations
- Cybercrimes Investigations Coordinator
- Cybersecurity Forensics Engineer
- Digital Forensics Analyst
- Endpoint Forensics Specialist
- Network Forensics Specialist
- Psychologist

Risk Mitigation Program Management (Business Continuity, Disaster Recovery, Information Security)
- BC/DR/IS Manager
- BC/DR/IS Planner
- Data Recovery Specialist
- Disaster Recovery Coordinator

Regulatory & Compliance
- Compliance Administrator
- Compliance Analyst
- Compliance Manager
- IT/OT Cybersecurity Compliance Auditor
- Public Policy Advisor

Legal
- Chief Legal Officer/ Legal Advisor
- Intellectual Property Manager

Compliance, Legal, & Forensics

Supply Network & Partnering

Vendor Integration
- Electronic Data Interchange (EDI) Analyst
- Cybersecurity Partner Integration Planner
- Cybersecurity Solutions Sales Engineer
- Cybersecurity Strategic Solutions Advisor
- Vendor/Alliance Collaboration Coordinator
- Security Sales Account Manager

Supply Network Management
- International Compliance Manager
- International Supply Chain Manager
- Logistics Compliance Analyst
- Procurement Cybersecurity Advisor
- Supply Network Cybersecurity Compliance Auditor
- Supply Network Cybersecurity Compliance Manager
- Supply Network Global Compliance Manager

Contracts & Procurement
- Procurement Manager
- Smart Contract Advisor
- Smart Contract Reviewer
- Manager
- Supply Network Global Compliance Manager

Readiness & Development

Recruitment & Staffing
- Cybersecurity Recruiting Specialist
- Cybersecurity Workforce Manager
- Cybersecurity Workforce Planner
- Incident Task Force Resourcer

Education / Development / Training
- Curriculum Developer/Planner
- Cybersecurity Instructor/Cybersecurity Faculty
- Cybersecurity K-12 Teacher
- Cybersecurity User Trainer/Coach
- Cybersecurity Workforce Developer

Exercise & Testing
- Blue Team Member (Defender)
- Cybersecurity Exercise Developer
- Cybersecurity Exercise Evaluator
- Cybersecurity Exercise Facilitator
- IT/OT White Hat / Ethical Hacker (Exercise Role)
- Purple Team Member (Collaboration Coach)
- Red Team Member (Attacker)
- Tiger Team Member (team of testing experts)
- Wireless Tester

Improve > Prepare > Align > Core IT > Converge

CyberME Community of Roles Map

Assure > Partner > Core OT

Industrial Controls Security
- Chip Hardware Internals Security Architect
- Cybersecurity Hardware Engineer
- Distributed Controls Systems Analyst
- Distributed Controls Systems Engineer
- Industrial Controls Network Security Analyst
- Industrial Controls Network Security Architect
- Industrial Controls Network Security Engineer
- Industrial Controls Systems Analyst
- Supervisory Controls and Data Acquisition (SCADA) Engineer
- Supervisory Controls and Data Acquisition (SCADA) Security Analyst

Automation & Controls
- Autonomous Plant Remote Manager
- Autonomous Remote Plant Operator
- Cybersecurity Systems Operator
- Factory Automation Engineer
- Factory Automation Manager
- Hardware Engineer
- Industrial Control Engineer
- Industrial Controls System Specialist
- Industrial (Process) Automation Engineer
- Industrial Process Automation Support Specialist
- Industrial Process Management Manager
- Instrumentation/Sensor Engineer
- Manufacturing Execution System (MES) Engineer
- Manufacturing Execution System (MES) Support Specialist

Infrastructure Management
- Infrastructure Administrator
- Infrastructure Engineer
- Infrastructure Lead
- Infrastructure Security Architect
- Infrastructure Specialist Technician

Physical Systems & Facility Security
- Physical Security Administrator
- Site Emergency Services and Security Leader

Cyber-Physical Asset Management
- Cyber-Physical Asset Controller
- Cybersecurity Operations Specialist

Integration & Convergence
- Cybersecurity IT/OT Integration Engineer

Mechatronics
- Mechatronics Engineer

Operating Technologies & Integration

Business & Technical Alignment, Governance & Response

Secure Design & Secure Product Management
- Autonomous Device Security Engineer
- Chip Hardware Internals Security Engineer
- Embedded Code Developer – Security Focused
- IoT (Internet of Things) Security Specialist
- Mobile Security Engineer
- Mobile Security Technician
- Personally Identifiable Information (PII) Advisor
- Product Designer
- Product Security Engineer
- Product Specialist
- Quality Assurance Specialist
- Secure Design Product Life Cycle Manager

Enterprise Risk Management & Manufacturing Target Profile
- Business Continuity Consultant
- Business Impact Analyst
- Chief Risk Officer
- Cybersecurity Assessor/ Planner – Manufacturing Profile
- Cybersecurity Insurance Specialist
- Cybersecurity Risk Manager
- Governance, Compliance & Risk Manager
- Lead Internal Auditor
- Risk Advisor

User & Consumer Support
- Application Security Support Representative
- Citizen Security Smart Grid Sentinel
- End Consumer/Customer (Products)
- End User/Customer (Systems)
- Personally Identifiable Information (PII) Advocate
- Personally Identifiable Information (PII) Customer Support Representative
- Personal Privacy and Data Guardian

Financial Assurance
- Cryptocurrency Accountant
- Cybersecurity Accountant
- Cybersecurity Economist

Leadership, Governance & Policy Management
- AI Ethics Advisor
- Anti-Counterfeiting Advisor
- Chief Executive Officer (CEO)
- Chief Information Officer (CIO)
- Chief Information Security Convergence Officer (CISCO)
- Chief Security Officer (CSO)
- Company Owner (SMM)
- Cyber Policy Analyst
- Cybersecurity Ethicist
- Cybersecurity Governance Business Analyst
- Data Privacy Officer
- Information Systems Security Officer (ISSO)
- Internal Manufacturing Cybersecurity Standards Developer
- Manufacturing Operations Senior Leader
- Plant Manager/Site Manager
- Privacy Policy Analyst
- Program Manager
- Project Manager
- Security Director

Culture Change & Transformation
- All Employees
- All Managers
- Cybersecurity Awareness Communications Specialist
- Cybersecurity Knowledge Bank Manager
- DevSecOps Transformation Leader
- Digital Transformation Advisor
- Enterprise Cybersecurity Culture Change Management Specialist
- Security Evangelist
- Security Program Management Office (SPMO) Leader

Cybersecurity Emergency Response Management
- Agency Response Coordinator
- Breach Response Analyst
- Breach Response Manager
- Corporate Crisis Management Leader
- Disaster Recovery Coordinator
- Incident Analyst
- Incident Communication Facilitator
- Incident Containment Responder
- Incident Historian/Archivist
- Incident Responder
- Incident Response Manager
- Incident Specialist (Specific Actor/Vector/Target)
- Incident Task Force Leader

Security Operations
- Cybersecurity Analyst
- Cybersecurity Economist
- Security Auditor
- Security Operations Center (SOC) Analyst
- Security Operations Center (SOC) Engineer
- Security Operations Center (SOC) Manager
- SOC Operations Analyst
- SOC Operations Lead
- SOC Operations Specialist

Smart Factory - Smart Cities Strategy
- Autonomous Factory Engineer
- Secure Smart Factory-Smart Grid (Meta Systems) Engineer
- Smart Factory Architect
- Smart Factory Designer
- Smart Grid Security Engineer

Information Technologies & Integration

Data & Information Management & Security
- Client/Server Analyst
- Data Architect
- Data Loss Prevention (DLP) Analyst
- Data Loss Prevention (DLP) Auditor
- Data Loss Prevention (DLP) Engineer
- Data Owner
- Data Security Analyst
- Data Warehousing Archiving Specialist (Data Custodian)
- Database Administrator
- IoT (Internet of Things) Data Manager

Intrusion Detection
- Cryptanalyst
- Cybersecurity Intelligence Specialist
- Firewall (Network Access Control) Analyst
- Intrusion Detection Analyst
- Malware Analyst
- Virus and Malicious Code Technician
- Vulnerability Assessor
- Vulnerability Manager
- Vulnerability Specialist

Integration & Convergence
- Cybersecurity IT/OT Integration Engineer
- IoT (Internet of Things) Communications Architect

Cloud / Edge Computing & Security
- Cloud Security Architect
- Cloud Security Engineer
- Cloud Security Specialist
- Edge Device Engineer

Systems Management & Security (Secure Systems Development)
- Biometrics Engineer
- Blockchain Developer
- Blockchain Engineer
- Cryptography Analyst
- Cybersecurity AI Engineer
- Cybersecurity AI Specialist
- Cybersecurity AI Trainer
- Cybersecurity Scrum Master
- Cybersecurity Systems Testing and Evaluation Specialist
- Machine Learning Specialist
- Penetration Tester / Ethical Hacker (Operational)
- Public Key Infrastructure (PKI) Analyst
- Public Key Infrastructure (PKI) Engineer
- Secure Software Developer
- Secure Systems Developer
- Security Systems Architect
- Source Code Auditor
- System Administrator
- System Architect
- System Engineer
- Technical Support Specialist

Application Management & Security
- Application Security Administrator
- Application Security Architect
- Application Security Developer
- Application Security Engineer
- Application Security Specialist

Network Management & Security
- Enterprise Encryption Engineer
- Linux Administrator
- MS Exchange Administrator
- Network Administrator
- Network Redundancy Engineer
- Network Security Administrator
- Network Security Advisor
- Network Security Architect
- Network Security Engineer
- Network Security Operator
- Network Specialist
- Windows Administrator

Connecting Cyber[ME] Roles to Transitioning and Ready to Move Up Worker Roles

Other components of this project have emphasized the size of the cybersecurity skill gap. Citing the ISC2 data from 2019, the massive U.S. current cybersecurity workforce shortage is projected to be almost 500,000. An area of critical importance when planning for the Cyber[ME] workforce is to understand how much the talent strategies of in-place transitions and modernizing-in-place - also known as in-house employee development or “shopping from your own closet” - are to the future of cyber in manufacturing.

These in-house strategies are key to closing the gap and allowing for newer workers to enter the workforce, possibly in other areas with different entry profiles and begin their early career contributions and gain ongoing development. There also are inter-company, local/regional, large scale strategies that identify transitioning groups of workers and use larger scale group reskilling solutions to create more candidates in the cyber workforce, enabling the mobility of workers in manufacturing as the industry demographics shift and move across role stages (modernized, cyber native and emergent) and connects domains.

Recruiting Generation Z who aren’t even in college to consider manufacturing as a career that has tech roles as interesting and well-paying as other high-tech industries is essential. This is actually an opportunity for manufacturing as a whole to modernize its image. Sharing the many roles where cybersecurity skills and opportunities will be valued will help update and improve the public relations image of manufacturing as a destination workplace. Adding to high schools and middle school STEM programs is another high-value, early engagement strategy to build a pipeline for manufacturing cybersecurity future workers.

Changes to the number and range of roles on the shop floor – the manufacturing production space – are often seen as the only manufacturing roles that are changing. As the first Digital Manufacturing Taxonomy showed, and now this Cyber taxonomy as well, manufacturers need to understand the full range of roles necessary for a successful and cyber-resilient digital organization. From HR roles, to governance roles, to secure design roles, IT/OT convergence roles and supply network roles, there is a broad range of work, and therefore, workers to be developed and incorporated.

As manufacturing technologies and processes change, it is essential to mobilize and progress the well-matched team members from declining worker roles into needed cybersecurity manufacturing positions. This leverages the capabilities and manufacturing and company knowledge, and the investment made in those employees to date. We asked ourselves:

- What roles from the Cyber[ME] community map could be opportunities for the reskilling and development of experienced skilled workers?
- Which roles in the production area are going through a transition to “more digital,” gaining more digital base knowledge and experience?
- What target roles might be of interest to and can leverage workers from other areas of changing need in addition to production?
- What target roles are good step-up roles for existing in-demand workers and make room through backfilling to bring in new workers who can gain beginning cybersecurity awareness skills in those roles?

Two-Years or Less Progression

From the Shop Floor, Warehouse or Back Office to 50+ Transition Roles

The following graphic presents 10 Cyber^{ME} Roles that offer an entry or bridge for new-to-work or transitioning workers to build on existing skills and progress into Cyber^{ME} pathways with two years or less of required education, training and skills development. Depending on prior learning and experience, the credentials often required as qualifications for these roles can be attained in less than two years and may include an apprenticeship, industry certification, or completion of a technical or academic degree. See the Career Progressions section at the end of this report for more information on pathways, qualifications, and anticipated 2020 salary and labor market/job growth data.

Business Impact Analyst	Cybersecurity Analyst	Compliance Analyst	Compliance Auditor	Cybersecurity Recruiting Specialist
Penetration Tester/ Ethical Hacker (Operational)	System Administrator	Technical Support Specialist	Cybersecurity Operations Specialist	Industrial Control Systems Analyst

Where May Transition Roles Build Cyber^{ME}?

We have identified almost 50 roles that are seen as opportunistic for transitioning workers. These roles:

1. Leverage and enhance existing expertise, skills, and knowledge, including general or domain knowledge in manufacturing.
2. Require additional education and training potentially equivalent to a 2-year effort (Note: As stated elsewhere, project observations include many existing efforts for cybersecurity apprenticeships, certifications, fast-track recruiting and hiring programs that are already available to be scaled and or modeled; and other continued design work with educational and workforce development partners continues in this “transition and get to work in cyber” space).
3. Provide a path to other Cyber^{ME} roles not listed here but likely in terms of continued progression and need (see our Career Paths component). After performing “Transition” roles and with time and experience in various Analyst or Specialist roles, additional development and education will open candidates to other more advanced or specialized cybersecurity in manufacturing roles such as Engineer or Developer.

Following is a list view of the roles seen as "Transition" opportunities into the cybersecurity in manufacturing space.

Domain	Cyber Role
Business & Technical Alignment	Application Security Support Representative Business Impact Analyst Citizen Security Smart Grid Sentinel Cybersecurity Awareness Communications Specialist Cybersecurity Governance Business Analyst Cybersecurity Knowledge Bank Manager Incident Communication Facilitator Incident Historian/Archivist Incident Responder IoT (Internet of Things) Security Specialist Mobile Security Technician Personal Privacy and Data Guardian Personally Identifiable Information (PII) Advisor Personally Identifiable Information (PII) Advocate
Compliance, Legal & Forensics	Personally Identifiable Information (PII) Customer Support Representative Product Specialist Project Manager Quality Assurance Specialist Security Operations Center (SOC) Analyst SOC Operations Analyst (Cybersecurity Analyst) Compliance Administrator Compliance Analyst Endpoint Forensics Specialist
Information Technologies and Integration	Application Security Administrator Data Security Analyst Data Warehousing Archiving Specialist (Data Custodian) Database Administrator MS Exchange Administrator Network Security Operator Penetration Tester/Ethical Hacker (Operational) Public Key Infrastructure (PKI) Analyst System Administrator Technical Support Specialist Virus and Malicious Code Technician Windows Administrator
Operating Technologies and Integration	Autonomous Remote Plant Operator Cybersecurity Operations Specialist Cybersecurity Systems Operator Industrial Control Systems Analyst Industrial Process Automation Support Specialist Infrastructure Specialist Technician Manufacturing Execution System (MES) Support Specialist Physical Security Administrator Supervisory Controls and Data Acquisition (SCADA) Security Analyst
Readiness & Development	Cybersecurity Recruiting Specialist Cybersecurity User Trainer/Coach Wireless Tester
Supply Network and Partnering	Electronic Data Interchange (EDI) Analyst Logistics Compliance Analyst

Highlighted Roles

All 247 Cyber^{ME} Roles are important. From an introductory perspective and a where-to-start perspective, it's hard to start a review of a company's talent pool with all of those roles. From an awareness and early adoption point of view, a shorter initial list can begin or accelerate workforce planning and conversations about the broader Cyber^{ME} workforce needs.

Creating a few versions of these shorter and targeted lists was helpful with the first taxonomy for digital manufacturing and should be again for the cybersecurity roles.

The first additional view is Highlighted Roles. A Highlighted Role is a Role from Cyber^{ME} Role Community which we expect to contribute significantly to the cyber evolution for manufacturing, and to possibly attract major early interest for more definition and development focus. In identifying Highlighted Roles, we asked ourselves:

- Which Roles are possibly some of the best examples of the wider Cyber^{ME} community?
- Which Roles as an initial set can be better understood in terms of being important, innovative or differentiating across all sizes of manufacturers?
- Is there a list that highlights a good mix of domains, impacts, and types that would be a good initial audit to begin the assessment of Cyber^{ME} talent plans?
- Which 35-40 roles do the industry and academia partners see as appropriate for early messaging and introducing the taxonomy as whole?

Highlighted Roles won't be the only ones to be seen as important – that is certain – but we believe it is critical that they receive initial further study and consideration.

There may be some overlap with some of the Roles we have identified as having major impacts such as Pioneer or Keystone Roles. Highlighted Roles that are also Pioneer and Keystone deserve even more attention or further consideration as an early Role for focus.

Some of these Roles may be newer or future roles and so they are not necessarily the same as our Pioneer Roles. They may also be solo players of sorts and so may not be a key link across bands of other Roles as some of our Keystone Roles.

Highlighted Roles can be some of the most novel Roles that showcase how the broader set of Roles establishes differentiators for digital manufacturing and design. The Highlighted list is notable as specific roles and capabilities that showcase the transition of conventional manufacturing; some can qualify as game-changing roles for broader Cyber^{ME} development and use.

Domain	Highlighted Role
Business & Technical Alignment	Autonomous Factory Engineer Chief Information Security Convergence Officer (CISO/CISCO) Cybersecurity Accountant Cybersecurity Analyst Cybersecurity Assessor/Planner-Manufacturing Profile Cybersecurity Governance Business Analyst Enterprise Cybersecurity Culture Change Management Specialist Incident Response Manager Information Systems Security Officer (ISSO) Internal Manufacturing Cybersecurity Standards Developer Personally Identifiable Information (PII) Advisor Secure Design Product Life Cycle Manager Smart Factory Architect
Compliance, Legal & Forensics	Chief Legal Officer/Legal Advisor Cybercrimes Investigations Coordinator IT/OT Cybersecurity Compliance Auditor
Cyber R&D and Innovation	Manufacturing Cybersecurity R&D Specialist Manufacturing Industry Cybersecurity Standards Developer
Information Technologies and Integration	Application Security Administrator Data Security Analyst Data Warehousing Archiving Specialist (Data Custodian) Database Administrator MS Exchange Administrator Network Security Operator Penetration Tester/Ethical Hacker (Operational) Public Key Infrastructure (PKI) Analyst System Administrator Technical Support Specialist Virus and Malicious Code Technician Windows Administrator
Operating Technologies and Integration	Autonomous Remote Plant Operator Cybersecurity Operations Specialist Cybersecurity Systems Operator Industrial Control Systems Analyst Industrial Process Automation Support Specialist Infrastructure Specialist Technician Manufacturing Execution System (MES) Support Specialist Physical Security Administrator Supervisory Controls and Data Acquisition (SCADA) Security Analyst
Readiness & Development	Cybersecurity Recruiting Specialist Cybersecurity User Trainer/Coach Wireless Tester
Supply Network and Partnering	Electronic Data Interchange (EDI) Analyst Logistics Compliance Analyst

We also suggest the Highlighted Roles may or should get some early special attention of workforce development resources, digital manufacturing organizations, hiring managers, and potential or current candidates.

These groups should consider how Highlighted Roles would have significant importance for the associated organization or be attractors for workforce that want to make contributions, develop key skills, and have opportunities for progression.

Career Paths Overview

A tool for promoting industry's needs to fill essential positions while making potential candidates aware of opportunities is one of the most essential tools in talent management and workforce development: representative career paths.

Every good career counselor uses them with students; many recruiters add them to their "hiring tools" portfolio. Internal HR and Managers incorporate them into development conversations; workforce planners craft them as key pieces of solution plans for how to move and progress cohorts of candidates and individual employees.

One of the outputs of the project were 8 career paths that demonstrate sample Cyber[ME] career path possibilities for the three targeted talent pools. Themes for types of careers were selected to demonstrate to new to work, transitioning, and experienced workers how they might consider careers in cybersecurity in manufacturing.

Three levels of career paths were established as part of the Cyber[ME] taxonomy, each to appeal to potential candidates with different levels of work experience.

Newer to work: No substantial paid experience in cyber, technology or manufacturing; graduating students new to the workforce; returning to work after significant workplace absence.

Transitioning workers: Candidates with paid experience in manufacturing business or technical areas but not experienced in cyber who are needing to move to a new opportunity often because of downsizing and or skill shift or other changes to their prior positions; candidates with solid business experience outside manufacturing in shared business or business-technical areas.

Experienced Workers: Candidates with experience in cybersecurity, in manufacturing or other industries and/or public-sector roles.

Within those three levels we illustrate the needed diversity with 9 possible samples of the many possible and use those as examples when thinking of individuals that could make possible candidates for various roles in various career paths.

Each path is documented in summary chart form and can be used by candidate or recruiter/planner alike to have a specific or general career conversation.

The table below identifies the 8 themes, the three targeted roles in the possible path, and which employee group it is targeted towards.

	Path Theme and Targeted Audience	Role A	(Progressing to) Role B	(Progressing to) Role C
Path 1	Cyber[ME] Assessing & Advising (Starting Point – Entry for New(er) to Work Talent Pools) Business-Technical Path	Cybersecurity Technical Support Representative	Cybersecurity Analyst	Cybersecurity Advisor
Path 2	Cyber[ME] Risk Management & Governance (Experienced Talent Pools) Business Path	Cybersecurity Governance Business Analyst	Cybersecurity Risk Manager	Intellectual Property Manager (non-JD)
Path 3	Cyber[ME] Vulnerability Detection & Investigation (Starting Point – Entry for New(er) to Work Talent Pools) Business-Technical Path	Industrial Control Systems Analyst	Incident (Breach) Response Manager	White Hat/Ethical Hacker
Path 4	Cyber[ME] Secure Factory Automation (Starting Point - Transitional; moving from conventional manufacturing production areas) Technical Path	SCADA Security Analyst	IT/OT Integration Engineer	Cybersecurity AI Engineer
Path 5	Cyber[ME] Secure Design (Experienced Talent Pools) Business-Technical Path	Cybersecurity Testing & Evaluation Specialist	IoT Security Specialist	Secure Design Product Life Cycle Manager
Path 6	Cyber[ME] SecureDevOps (Starting Point – Entry for New(er) to Work Talent Pools) Technical Path	System Administrator	Secure Software Developer	Cybersecurity Systems Architect
Path 7	Resilient Cyber[ME] Transformation (Starting Point – Experienced Talent Pools) Business Path	Cybersecurity User Trainer/Coach	Cybersecurity Asset Manager	SecDevOps Transformation Leader
Path 8	Secure Cyber[ME] Supply Chain (Starting Point - Transitional; moving from conventional manufacturing warehousing and logistics areas) Business-Technical Path	Logistics Compliance Analyst	Vendor/Alliance Collaboration Coordinator	Supply Network Cybersecurity Compliance Manager

See page 56 for Career Paths references

Personas Overview

Personas are another key tool in the talent war for cybersecurity workers or in any other highly competitive talent pursuit. Personas are lightly fictionalized descriptions of targeted candidates. Persona development is a research driven, yet generalized, profile of workers or potential workers for needed roles and skill sets. From career interests to previous experiences; from types of work cultures to management styles used, personas can include a number of different elements. In most any format, they are useful for both the candidate who can ask:" Does that sound like me? Might I be a good match?" and for recruiters and hiring managers who ask: "Can I describe general candidates who might be a good fit or an adjacent candidate that I can invest in?".

Personas also can help:

- Understand and informally assess emerging talent targets.
- Design specific roles or pools of more general skilled workers.
- Align hiring and sourcing managers in their talent acquisition, development, and retention efforts.

See page 66 for the four Personas.

Success Profile Overview

Initial Roles Selected for Success Profiles

Of the 247 roles, a subset were identified as imperative to the work of manufacturers and designated as Critical Roles. These Critical Roles are positioned as early focus for employers, educators, government and the workforce. Seen as important to the ecosystem for a number of reasons, these roles are not the only critical roles, but a solid set of the "first critical" roles to consider. Through collaboration with our most senior representatives from business, education and government the targeted list below of Cyber[ME] roles is the First Critical List.

Readiness & Development	• IT/OT White Hat/Ethical Hacker (Exercise Role) • Cybersecurity Recruiting Specialist
Business & Technical Alignment, Governance & Response	• Autonomous Factory Engineer • Cybersecurity Analyst • Chief Information Security Convergence Office • (CISCO) • Cybersecurity Assessor/Planner- Manufacturing Profile • Cybersecurity Governance Business Analyst • Incident Response Manager
Information Technologies & Integrations	• Cybersecurity AI Engineer • Cybersecurity IT/OT Integration Engineer • Edge Device Engineer • Penetration Tester/Ethical Hacker (Operational) • Secure Software Developer • Security Systems Architect
Operating Technologies & Integration	• Cyber-Physical Asset Controller • Cybersecurity IT/OT Integration Engineer • Cybersecurity Operations Specialist • Cybersecurity Systems Operator • Hardware Engineer • Industrial Control Network Security Architect
Supply Network & Partnering	• Smart Contract Advisor • Supply Network Cybersecurity Compliance Manager
Compliance, Legal, & Forensics	• IT/OT Cybersecurity Compliance Auditor
Cybersecurity R&d & Innovation	• Manufacturing Cybersecurity R&D Specialist • Manufacturing Industry Cybersecurity Standards Developer

Success Profiles: Three Profiles Kickoff a Focus on Critical Cyber[ME] Role

These roles are representative of the kinds of cybersecurity role structures needed in manufacturing. These roles pave the way for deeper understanding of the needs for manufacturers and the opportunities for the workforce. The Critical Roles also represent possible targets for educators and workforce development programs.

Further decisions on ranking or quantifying more Cyber[ME] roles would be good topics for further institute efforts. Also, with the available full taxonomy, those decisions can be made by individual companies and within targeted ecosystem exchanges between academia, industry, government and workforce community resource representatives.

Success Profiles

Three of the first 30 important roles were selected for Success Profiling. Those nominated and then chosen for profiling were:

- Cybersecurity IT/OT Integration Engineer
- Secure Design Product Life Cycle Manager
- Supply Network Cybersecurity Compliance Manager

The purpose of Success Profiling is to do a deep detailing of the role; beyond a job description, there is information in the profile that not only describes the role but also builds the business case for the investment in the role.

Cybersecurity IT/OT Integration Engineer

Secure Design and Product Life Cycle Manager

Supply Network Cybersecurity Compliance Manager

These three success profiles are presented in greater detail at the end of this report.

The profiles have the following elements for each identified role:

Success Profile Content Preview

Job Role Identification

- Role Title • Impact • Summary Scope
- Outcomes • Work Domain Profile
- Business Case Contribution

Competencies

- Essential Technical Competencies
- Essential Business & Professional Competencies

Experience & Education

- Education Profile
- Experience Profile

Key Responsibilities

- Activities

Below is the key to the Success Profile template used for the three profiles.

Section 1: Job Role Identification Section

This section identifies the role and provides an overview as well as its impact, generation and business case. Sidebar roles – digital roles closely associated with the role being profiled – may be introduced

Summary Scope	The summary scope is used to capture the overall scope and contributions of a successful employee in this role. The summary captures the role's focus in work efforts, the environment of work, its importance, and the current/future influence the role will have on digital manufacturing enterprise.
Role Title	Title of job role
Role Impact	Indicates the impact of the role within an organization within our classification of Pioneer, Keystone, and Producer. Role impacts may progress over time such as a Pioneer becoming a Keystone or Producer; or a Producer becoming Keystone as more staff begin to work in various areas and the business environments mature. Producer – The majority of roles are known as producer roles. These essential functions occur at all levels and where some are more specialized and others more generalized, are responsible for much of the continuous work output within an organization. They convert key resources into outcomes for the business and produce the lion's share of the overall work effort. Pioneer – The early emerging roles that establish new primary digital capabilities and play a broader initial role are referred to as pioneer roles. These roles often lead to more specialized roles as an organization's capabilities grow. Approximately one quarter of the roles in the community map are pioneers. Keystone roles are less common than their pioneer and producer counterparts, yet they exert a high impact on the growth and performance of Cyber^{ME} technologies within an organization. They support the other types of roles and facilitate output often positioning themselves as a central hub of workflow and direction within an organization.
Business Case Contribution	The business case contribution captures the "elevator pitch" for the job role, an efficient pitch for the value of the job role within an organization. The business case contribution offers the job role value to the business including contributions towards company objectives, and how the role differentiates an organization.
Domain	The assigned domain for the role.
Outcomes	The outcomes list focuses on foundation items or tangible outputs and outcomes of a successful employee in this role; these are inputs to Key Performance Indicators (KPIs) and performance measures that serve as an indicator of the value an organization receives from the job role.

Section 2: Key Responsibilities

Key Responsibilities is the section that provides the behavioral and mental task profile that the role is accountable for achieving.

Activities	A list of the key duties of successful workers in this role. A focus is placed on behaviors/tasks/actions, and outputs from the role. The listing works to capture a relatively full range of representative work including the activities that set this role apart from others.

Section 3: Competencies

Lists of technical, business and professional competencies or skill areas seen as essential to strong performance in the role.

Section 4: Experience and Education

Education	Degrees, certifications and other formal education experiences preferred or required for the role.
Experience	Previous (entry) experiences preferred or required for the role.

See page 75 for the Success Profiles

This section answers the question **Where is the workforce of tomorrow, today?**

As we consider a landscape in which available cyber talent continues to fall dramatically short of what is required, we will need to be incredibly resourceful in our approach to talent. In addition to looking at the typical supply channels of available workforce and those in education, we need to consider adjacent pools of talent that, with some skilling-up, can be a fit for the needs of industry. There are two primary ways of viewing adjacency: a) consider pipelining talent from non-traditional pools and b) targeting talent in more conventional and immediate pools, but where there is declining demand.

Non-Traditional Pools

The following graphic illustrates where there could be opportunity for manufacturing to tap into non-traditional pools.

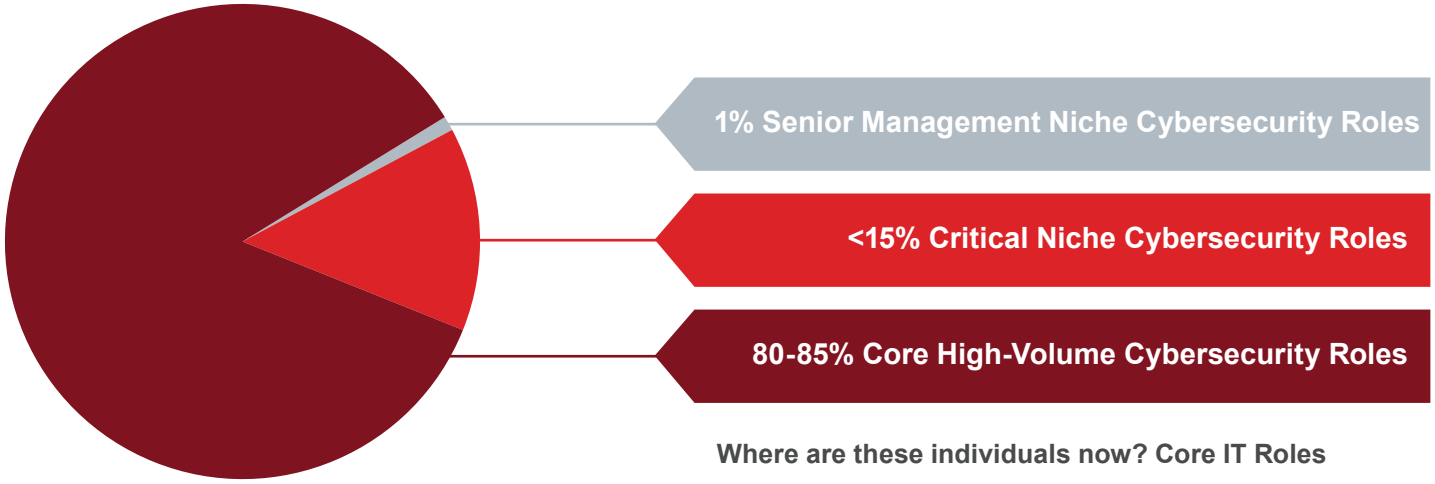
Targeting Talent Adjacencies for Cyber in Manufacturing Non-Traditional Pools

Some, like Retail, are in decline with an increasingly displaced workforce looking for new career opportunities. Others, like Hospitality and Food Service, offer limited career potential for employees. All generally require individuals to abide by a fixed and in-person schedule, making roles with more schedule and work mode flexibility more attractive. All have roles that leverage similar skills to certain cyber roles in Manufacturing. This is a longer-term play that requires greater investment than tapping into traditional pools with a skills match that is generally <80%; however, the pools are relatively deep. Appendix F provides an example of the alignment between an Inventory Manager (Retail and Food Service) and a Threat Analyst, as well as a General Manager (Hospitality) and the same role. We believe that creative interventions like this and a willingness to see talent based on full potential should be in the arsenal of strategies for the full Cyber^{ME} Workforce Development System.

Conventional and Immediate

We believe there is significant opportunity in conventional talent pools that may be available more immediately and require less significant skilling-up interventions due to their closer adjacency with Cyber^{ME} roles. Many of the core, high-volume cybersecurity roles are well suited for quick alignment with conventional, core IT roles.

Cyber Roles Mix



Where are these individuals now? Core IT Roles

- Systems Administrator
- Application Developer
- Analysts
- Systems Engineer
- Developers
- Information Security Analyst

In many cases, these roles are currently in declining demand as IT faces its own cycles of evolution. Appendix F focuses on this more immediate and quicker return set of adjacencies.

As you can see from the summary table on the following page, many conventional IT roles can be ‘feeder pools’ for multiple target Cyber[ME] roles, providing workforce planners and workforce developers ample opportunity for targeting and developing talent that can feed into multiple career pathways. illustrations to target for targeting of more conventional roles.

	Application Security Engineer	Cloud Security Engineer	Incident Response Manager	Manufacturing Industry Cyber-security Stan-dards Developer	Cyberse-curty IT/OT Integration Engineer	Threat Analyst	Cyber Policy Analyst	Distributed Controls Systems Engineer	Systems Adminis-trator	Autonomous Factory Engineer
Dev Ops Engineer		X								
Software Engineer		X								
Information Technology Security Analyst		X								
Systems Engineer	X	X								
Network Engineer		X	X							
Information Security Engineer	X									
Information Security Analyst	X		X			X	X	X		
Fullfillment Analyst	X									
Cybersecurity Engineer	X			X						X
Information Security Manager			X							
Security Analyst			X			X	X	X		
Cyber Intelligence Analyst			X							
Cyber Defense Engineer				X						X
Security Analyst				X						
Integration Team Developer				X						X
Application Developer				X						
Information Assurance Security Engineer					X					
Project Associate Technical Engineer					X					
Cybersecurity Professional					X					
Senior Systems Engineer					X					
ICS Cybersecurity Engineer					X					
Cybersecurity Analyst						X	X	X		
Principle Security Engineer							X			
Senior Cybersecurity Analyst							X			
Senior Information Security Analyst						X		X		
Senior Security Analyst						X		X		
Systems Administrator									X	
Senior Systems Administrator									X	
Linux System Administrator									X	
Network Administrator									X	
Window Systems Administrator									X	
Embedded Systems IOT Developer										X
Senior Manager Cybersecurity Risk Analysis										X

Appendix F provides two (2) illustrations of non-traditional talent pools to target for adjacency and thirty-three (33) illustrations to target for targeting of more conventional roles.

PARTNERS

Leveraging the Ecosystem towards Shared Resiliency

Many of the cybersecurity roles and skills demonstrate that convergence is a theme in cybersecurity for manufacturing. Cybersecurity in manufacturing has clearly been established as a team sport: from major alignment between business and technical roles and functions, shared governance, mutual accountability, a focus on IT and OT, cross-functional testing and response teams, and the connections to supply chains. Partnerships are the key to meeting the need for cyber resiliency across the internal and external workings of any one manufacturer and their platforms, supply chains or collaboratives and joint ventures. We also know that this connected world – whether local or global physically – is also where some of the risk emerged. It is also where the solution will continuously evolve.

Cybersecurity is as much a shared state of capability as a single company's status. It's the power of the group – whether manufacturers as a group, educators as a group, etc. - or the entire system of workforce partners, that together is needed to address the large gaps and serious risks in today's Cyber^{ME}. Cyber risks and impacts are a problem of the group in both individual and business behaviors and decisions, and it will require the personal and professional commitments of the group to meet the challenge.

As a result, when thinking of 'what's next', action planners and solution-minded organizations have a role to ensure the Manufacturing 4.0 workforce of our first taxonomy turns into the cyber-capable workforce of this second taxonomy. Heavy lifting from more than just one entity is required.

In this section, we provide a working tool for solution conversations: an ecosystem map of this team, the group, that can serve as a frame of reference for the needs, contributions and connections between stakeholders. We also position ten key connections and high-level calls to action that can serve as a starting point for further dialogue and tactical workforce solution design.

There are five primary entities in our view of the Cyber^{ME} as introduced below and as mapped on the following page. The ecosystem map defines the five core entities including the ring of outputs and contributions to the ecosystem that each entity produces. Each of those outputs is an input to one of more of the other entities in the system. In the end, it is the management, the flow and best consideration of each of the outputs that determines the health and performance of the entire system

Where to Begin

Employers, Government & Policy Advisors, Education, and Individuals must begin by asking some essential questions about their needs, contributions, and connections. These questions would serve as a useful start to any initial or ongoing dialogue about closing the gap and ensuring the sustainability of the cybersecurity workforce in manufacturing.

Employers

1. How do we build cybersecurity mindedness into the fabric of our culture and measure progress?
2. How are we approaching the convergence of IT/OT and related questions of accountability and governance?
3. How well have we mapped and timed our cybersecurity talent needs to our product life cycle? With shorter time to market and PLM cycles, how does this affect planning/re-skilling/re-deployment, etc. How well do we understand where the gaps are today and are likely to emerge over time?
4. Where do we stand on the digital transformation horizon and its related creation of increased cybersecurity needs? Are we delaying one or the other over the demands each places on us? What moves on the chessboard enable speed and continuity?
5. Have we linked our workforce plan with our business continuity plan?
   a. How routine is it for teams to do cross training as a workaround strategy?
   b. Have we identified and secured sources of contingent ST and LT alternative workforces?
   c. Have we done sufficient readiness and response training?
6. Have we looked at internal adjacent talent pools for prioritized training?
7. How well have we done our own cyber workforce scan and plan? What is the right mix of Build, Buy, Borrow & Bridge?

Individuals

1. What are the new career opportunities that are possible?
2. How high is my learnability to navigate and adapt?
3. What skills do I need to learn and evolve rapidly?
4. How much am I willing to invest in my own development? How can I make a business case to partner with my employer for development funding?
5. How does my behavior and skillset need to adapt to a more cyber-secure reality in my personal, professional and community life?

Government & Policy

1. How do we optimize the work channels for a comprehensive framework of federal, state, and local leadership to drive alignment on cybersecurity policies & practices?
2. How do we ensure that this framework not only protects us, but also supports local, regional, and national economic development and innovation?
3. How can we establish a national and dynamic view of available supply channels so that our investments and systems are coordinated to build a healthy ecosystem of talent?
4. How do we ensure that our framework has the right balance of fixed and flexible elements that enables compliance of small and mid-size employers, including provisions for WF development?
5. As a national defense imperative, how do we fund at appropriate levels and reduce unnecessary restrictions on funding?

Education

1. Given the wide range of skills and disciplines spanned by cyber, how do we introduce a basic framework that crosses all curricula at all levels?
2. How do we create the right mix of quick strike, middle effort and more traditional interventions (e.g. – 4-year degrees) to protect and defend what we have, but also have the ability to expand in the future?
3. Considering the expansive number of business-technical roles in Cyber^{ME}, how can we bridge more cross-disciplinary training into engineering (OT) and computer science (IT) curriculum to widen the pool of available and qualified cyber talent? How does converged business leadership (like IT/OT), cyber ethics, privacy and personal security ethics become a part of the development of both our technical and business leaders?

Workforce/Economic Community Development Support

1. How do we align players across the system to collaborate on key actions that will drive talent development in a focused and disciplined way?
2. How do we help stakeholders understand the connection between focused action on talent development policies and economic growth?
3. Where can we accelerate current efforts of disjointed or even overlapping or competing stakeholders to better effect?
4. How can we enhance our value as an ‘honest broker’ in the system?

From Questions to Specific Connections to Improve

From our research, we have identified several potential starting points for action for connections and partner stakeholders in Cyber^{ME}. These come first in the identification of 10 more specific connections we see as being important for ongoing dialogue, and then initial suggestions for starter calls to action.

Industry

Cybersecurity workforce strategies & specialists

Private sector employment / jobs

Resources & experiences for ongoing development & progression

Increasing needs for vendor / 3rd party partnership

Willingness for diverse candidacy, employment & experience proxies

Experienced workforce

Constantly changing cybersecurity systems, standards & capability

Data / tech / cybersecurity demand creation

Needs / requirements for workforce skills & knowledge

Connections: **1** **2** 4 8 **10**

Academia

Research, in Cyber[ME] domain knowledge & practice

Educational experiences (formal / informal /prof. Dev.)

Diplomas, degrees & formal credentials

Teachers, faculty & educational infrastructure & platforms

Relationships & programs for target industry needs

Education & Academia Jobs

Graduates, educated students-feeder stock of the workforce

Resources for educational experiences

Career exposure, readiness & support (curr.. & extra-curr..)

Connections: **2** **3** 9 **10**

Individuals

Tech-life consumers, data producers, data owners & privacy seekers

Candidacy / availability for employments

Time & $ as consumers of educ/development

Changing attitudes / investments in self-development

Employment, compensation & career expectations

Changing attitudes / investments in degrees & formal education

Citizenship & community membership

Applied ethical behavior

Connections: **1** **3** 5 7

Government & Policy Advisors

Domain / technology research & funding

National defense, state & local support & macro security

Public sector employment

Legal systems, structures, regulations

Cybersecurity standards & reference models

Workforce strategies & specialists

Government procurement programs & requirements

Workforce development, education & training funding

Data / tech / cybersecurity demand creation

Connections: 4 5 6 **10**

Workforce & Economic Community Development Support

Localized, perceived more credible development experiences

Access to & local workforce & communities; sanctioning & sponsorship

Proxy & correction for educ. & employment access from Govt., Industry, Academia

Recruitment channels to local employment

Connections to local employers

Convener opportunities & resources

Requests for funding more than availability of funding; yet some funding

Workforce strategies & specialists

Connections: 6 7 8 9

Cyber[ME] Workforce Development Ecosystem Map: Highlighted Connections

1 Industry to Individual: The Employment Value Exchange

2 Industry to Academia: The Entrusted Development Exchange

3 Academia to Individual: The Employment Capability Exchange

4 Government to Industry: The Standards/Compliant Expertise Exchange

5 Government to Individual: The Security-Citizenship Exchange

6 Government to WECDS: The Community Connection/Federal Resource Exchange

7 WECDS to Individual: The Employment Access and Trusted Guidance Exchange

8 WECDS to Industry: The Shared Local Development Exchange

9 WECDS to Academia: The Destination Quality Education Exchange

10 WECDS to Industry, Academia and Gov't: The Meta-Conveners Exchange

The Highlighted roles displayed in the graphic above are explained and explored in depth in the table below.

	Partnerships	Connection Brief	Impact	Call to Action
1	Industry & Individuals	The Employment Value Exchange: Business plans/ needs and workforce employment choices	Employers' business plans determine what kind of talent is needed and when; these translate into employment needs that are marketed to individuals, who can choose to whom they supply their talent	• Employers should link their long-term workforce plan with your Buy, Build, Borrow, and Bridge strategies, approaching talent with a 'renewable resource' mindset • Employers should create attraction strategies that are based on Knowledge, Skills, and Abilities vs. degrees and years of experience • Employers should work with individuals in their organization to craft a modern employer value proposition that explicitly links willingness to learn and grow with career opportunities • Individuals who are employees should assume shared accountability for both cyber readiness and security within their organization
2	Employers & Academia	The Entrusted Development Exchange: Business plans/ needs for skilled employees and academia's relationships & targeted programs	Employers are faced with rapidly evolving role & skill requirements. Educators are critical intermediaries in the supply channel, providing skills development to the individuals that employers employ.	• Employers should provide educators with a view to their short, mid and long-term demand for cyber roles and offer support in calibrating curricula to industry needs • Employers should consider educators as a critical part of their Build and Borrow strategies – a legitimate extension of their L&D teams • Educators should provide transparency to how student learning outcomes are linked to data-informed labor market trends • Educators and employers should partner to enable expanding career entry points that recognize the increase in cyber workforce diversity • Educators should demonstrate how academia is creating research that helps employers stay up to date not only on technology, but also on the ethical dimensions of cyber
3	Academia & Individuals	The Employment Capability exchange: Academia's Educational experiences and student's time and $	Educators market their ability to prepare individuals for employment – both now and in the future. Individuals must see educators as relevant to future-proof their skillset as the outcome of their tuition and time	• Educators need to demonstrate to individuals that their educational offerings provide a flexible way to develop their skills not only once, but on an ongoing basis and in a way that is aligned with employer needs • Educators need to demonstrate that they are a helpful 'broker' between what employers need (right skills/right time) and what the individual needs (flexibility, affordability, and future-proofed) • Educators should provide a balance of skills development sprints with longer term degree attainment • Individuals need to approach their educational experience holistically, understanding that their education is not a one-time experience, but rather an ongoing development process

	Partnerships	Connection Brief	Impact	Call to Action
4	Government & Industry	The Standards/ Compliant Expertise Exchange: Government Cybersecurity standards and Industry's (compliant) experienced workforce	Government relies on employers to safeguard our cybersecurity, and in large part that also assumes that employers are preparing talent for the future. In order to establish 'herd immunity' to cyber risk, government must help employers align on cyber standards and the talent that is required to support those standards.	• Government should recognize that frameworks and standards around cybersecurity have a clear impact on roles and skills; incentives need to be made available to develop talent across all categories of employers • Government should broaden its funding incentives to invite 'collectives' of employers to solve problems around skills development
5	Government & Individuals	The Security-Citizenship Exchange: Government's National defense, state & local support & macro security and Individual Citizenship and Community Membership	Government has the most holistic view of our cyber-preparedness and must engage the citizenry in a shared view of our biggest national security threat, engaging them to help keep us safe.	• Government should engage in a national campaign to market the shared national interest around collective cybersecurity – similar to Victory Gardens in World War II and Man on the Moon. This creates not only awareness, but also a sense of shared responsibility for the collective welfare and defense of the nation. • Government should consider the creation of a National Cyber^{ME} Corps that serves in the defense of the nation and from which employers can recruit talent. The National Cyber Corps would forgive student loans after three years of service, provide opportunities at every level of Cyber^{ME}, and ongoing development opportunity.
6	Government & Workforce/ Economic Community Development Support	The Community Connection/ Federal Resource Exchange: WECD access & sanctioning and Government workforce funding	Workforce/Economic & Community Development support organizations provide a critical link between our goals for GDP and investments for employment growth as a nation to where the action happens – on a state and local level.	• Government should recognize the unique role that Workforce/ Economic Community Development plays at the state and intra-state regional level in convening multiple stakeholders and providing a unifying direction as it relates to workforce and economic development. As the 'broker' across multiple stakeholders, this group of stakeholders provides a natural channel for communicating federal standards and making them relevant at the state and local level. Funding for these entities can help accelerate critical connections between economic and Cyber^{ME} workforce development • A framework for demonstrating progress to national standards should be provided to Workforce/Economic Community Development entities so that the federal government can appropriately monitor and fund progress • WIOA-funded workforce development entities should have particular incentives for workforce development that aligns with the national interest around Cyber^{ME} security.

	Partnerships	Connection Brief	Impact	Call to Action
7	Workforce/ Economic Community Development Support & Individual	The Exchange: Employment Access and Trusted Guidance Exchange WECDS 'Proxy .... & employment access ...' and Individual 'Employment... & career expectations"	Workforce Development entities provide skill-up opportunities for workers in transition and must help individuals make career choices that support long-term employment in high demand roles.	• Workforce Development entities should prioritize and communicate Cyber^{ME} career progressions and pathways to job seekers and provide appropriate training to develop them into in-demand roles.
8	Workforce/ Economic Community Development Support & Industry	The Shared Local Development Exchange: WECDS 'Recruitment channels to local employment' and Employers 'Business plans/needs for skilled employees'	Economic development organizations help attract and retain business to states and localities not only through tax incentives and shovel ready sites, but increasingly through available skilled workforce. More and more, economic and workforce development go hand in hand and are always enacted at the community level.	• Work with employers to create a neutral, fact-based view of how their growth plans will create Cyber^{ME} talent demand over specific time horizons. From this view, create a clear picture of where the shared gaps are in terms of talent supply and demand.
9	Workforce/ Economic Community Development Support & Academia	The Destination 'Quality Education' Exchange: WECDS 'access & sanctioning' and Academia's 'Graduates, educated ... workforce'	Educators are a vital link in the talent supply chain and are a key part of EDC's relocation and retention strategies for new and existing businesses.	• Convene educators in a neutral environment to align on how they can collectively help close the gap between Cyber^{ME} demand and supply in their geography. • Develop the 'asks' of employers into a business case that employers can understand and collectively co-fund with appropriate levels of government support.
10	Workforce/ Economic Community Development Support & Collective of Industry, Academia, and Government	The Meta-Conveners Exchange: WECDS 'Convener opportunities and resources' and many outputs from Industry, Academia and Government	Work across the Ecosystem is vital to success so that efforts are not diffused; WDC's and EDC's are credible brokers to ensure that business and workforce strategies are aligned.	• Economic Development organizations are well-positioned to act as the broker across workforce development, education, and employers to align on common interests, and to direct funding for shared risks and opportunities. There is tremendous opportunity to create a common blueprint for how stakeholders in the system can be aligned around common goals, language, and scorecards, and to create transparency to where incentives and financial awards are mis-aligned across the system. By helping stakeholders find common ground on Cyber^{ME} risk, these entities can be productive drivers on closing the Cyber^{ME} skills gap.

Conclusion

In 2017, we released the Digital Manufacturing & Design jobs taxonomy. This work was foundational and pointed toward both the risks and opportunities business, individuals, and government would face in a more digitally enabled future. The work in this study, just three years later, anticipates the rapid evolution of related roles as greater adoption opens a landscape of both opportunity and risk. This requires a broad-based and panoramic approach to ongoing, evolving, and escalating gap closure.

The starting point for manufacturing is in a shared and comprehensive view of where skills and roles are evolving so that stakeholders across the ecosystem can align and move together better and more quickly than before. If digital is defined by fast and transparent fluidity, so to must our response. The time is now for a shared charter and accountability.

In particular, we need to focus on conservation and renewability. In the US, our demographics and present supply/demand tightness leave no room for system leakage. A prioritization of training our current base of talent is critical and requires three things:

1. Understanding of not only future roles and skills, but where there are talent adjacencies.
2. Relaxation of 'exact fit' job requirements in favor of finding talent with high learnability that can be trained to evolve with us over time.
3. Alignment of both actions and incentives across the ecosystem so that prioritization of our current base of talent is rewarded.

Of course, we must balance this focus on conservation and renewability without neglecting our longer-term talent pipelines. The good news is that in having one foot in the world of longer-term talent pipelines and the other in conservation and renewability, we can bridge the two, ensuring that we will be better prepared to ensure that longer-term pipelines have a lifetime payoff as all talent will be treated as a renewable resource.

As a shared accountability across the ecosystem, the talent gap we face today, and in the future, can be closed. For our personal privacy, commercial viability, and national security, we need action across the ecosystem now because next is right around the corner.

CyberME Career Paths

Cyber Assessing & Advising Pathway Overview

	Role 1	Role 2	Role 3
Path A	Cybersecurity Tech Support	Cybersecurity Analyst	Cybersecurity Advisor
Path B	Cybersecurity Operations Specialist	Cybersecurity Solutions Planner	

Introduction to Career Pathway:

The Cyber Assessing and Advising pathway begins with the entry-level roles of Cybersecurity Tech Support and Cyber Operations Specialist. According to CyberSeek, about 21% of job openings for Cybersecurity Specialists or Technicians require less than a Bachelor's degree. These job roles are good entry-level targets for apprentices and community college students. Progression into the Analyst and Solutions Planner roles most often requires a 4-year degree and professional certification plus enough on-the-job exposure to various IT and/or OT settings to craft a manufacturing profile for risk and vulnerabilities. Cybersecurity Advisors and Consultants often have at least 5 years of experience, including management experience and/or an advanced degree, and with that, they bring even broader perspectives and more scenarios where they have assessed gaps and planned cybersecurity solutions.

Cyber Assessing & Advising Pathway A

	Role 1	Role 2	Role 3
Path A	**Cybersecurity Tech Support** Average Salary: $65,000 Projected Growth Rate: 115%	**Cybersecurity Analyst** Average Salary: $95,000 Projected Growth Rate: 116%	**Cybersecurity Advisor** Average Salary: $148,000* Projected Growth Rate: 127%

	Cybersecurity Tech Support	Cybersecurity Analyst	Cybersecurity Advisor
Education (Certification & Certificates)	• Micro-Credential (Post-High School Coursework) • Apprenticeship • Associate's Degree with Certification	• Bachelor's degree in Computer Science or Information Technology. • Professional certifications: Certified Information Systems Security Professionals (CISSP), GIAC Security Essentials, Certified Ethical Hacker (CEH)	Master's Degree or higher in a relevant field (e.g. Cybersecurity, Computer Science, Manufacturing, Cyber-Physical Systems, Public Policy, JD)
Work Experience	1-4 years' Customer Support or Technical Support experience	Minimum 3 years information security experience or equivalent experience/ specialized	Minimum 6 years experience (4 years with Master's level or higher degree) in executive program analysis and direct support. Experience with policy development.
Considerations	• Knowledge in cybersecurity products and troubleshooting • Familiarity with monitoring and troubleshooting tools • Account provisioning and password, identity and access management domain knowledge	• Problem solving, multi-tasking & other soft skills • Broad knowledge and experience with the NIST security framework stages and controls • Increasing knowledge of Actors, Vectors, Targets and other threat and vulnerability profiles	• Ability to research, analyze, interpret, and resolve complex issues, policies, and operating procedures • Strong understanding of national cybersecurity guidelines and regulations

** Influenced by relatively high numbers of consultants/contractors filling these roles*

CyberME Career Paths

Cyber Risk Management & Governance Pathway Overview

	Role 1	Role 2	Role 3
Path A	Cybersecurity Governance Business Analyst	Cybersecurity Risk Manager	Intellectual Property Manager
Path B			AI Ethics Advisor
Path C			Legal Advisor

Introduction to Career Pathway:

The Cyber Risk Management and Governance career progression outlines opportunities for a fairly diverse set of workers with 3 or more years of experience in general business, engineering, management, risk mitigation and crisis management, and/or governance/policy positions to support Cybersecurity and start a progression to Cybersecurity leadership roles. The Cybersecurity Governance Business Analyst is a generalist position not necessarily requiring a 4-year degree to help communicate and enable the business to understand and implement business-technical strategies and align the organization to a culture of cybersecurity. The more they have a skillset with business and technical acumen, an analytical mindset, and a strong understanding of the generalized cyber-threat landscape, the more likely they can take on Risk Management roles. Promotion to the role of Cybersecurity Risk Manager may be attained with a Bachelor's degree and exposure to broad business risk issues and ongoing risk management practices, in addition to relevant certifications. Intellectual Property Managers, as well as Legal or Ethical Advisors, will have experience (5-10 years) in compliance/ licensing/contracts and an advanced degree; a law degree is required for advancement to a legal advisor.

Cyber Risk Management & Governance Pathway A

	Role 1	Role 2	Role 3
Path A	**Cybersecurity Governance** Average Salary: $95,000* Projected Growth Rate: 124%	**Cybersecurity Risk Manager** Average Salary: $108,000* Projected Growth Rate: 124%	**Intellectual Property Manager** Average Salary: $147, 700 Projected Growth Rate: 35%

	Cybersecurity Governance Business Analyst	Cybersecurity Risk Manager	Intellectual Property Manager
Education (Certification & Certificates)	Relevant business experience; Bachelor's Degree in Business, Risk Management, Computer Science, IT preferred	Business, Risk Management, Computer Science, IT or related area preferred. Security+ or equivalent certification preferred.	• Bachelor's degree in Computer Science, Information Technology or a related discipline preferred. • Security+ or equivalent professional certification required
Work Experience	1-4 years Business Support or Technical Support experience, especially with major program launches and implementation support	Minimum 3 years equivalent risk mitigation/management experience supporting major risk programs or equivalent experience	Minimum 6 years of experience (4 years with Master's level or higher degree) in executive program analysis and direct support. Experience with policy development
Considerations	• Generalist business experience from many areas can be effective if it comes with a program and policy implementation mindset • Interest in understanding enterprise-wide functions and how to implement cybersecurity governance practices	• Experience supporting major risk-related programs (IS, DR, BC CM, etc.) is highly valuable with increasing responsibilities for integration to cybersecurity and broad risk factors beyond technology • Ability to use standards and industry models to guide policies	As a non-attorney expert in IP management, works with counsel, internal product owners, licensing partners, etc. so varied IP strategy development experience is often preferred.

** Influenced by relatively high numbers of consultants/contractors filling these roles*

CyberME Career Paths

Vulnerability Detection & Investigation Pathway Overview

Introduction to Career Pathway:

The entry-level role on this sample Vulnerability Detection and Investigation progression is the Industrial Control Systems Analyst who meets entry-level, fundamental knowledge and skills requirements through completion of an apprenticeship or 2-year technical degree with relevant experience. Further experience and certifications, along with lead/coordination roles experience and/or completion of a Bachelor's degree will often meet minimum qualifications for the Vulnerability Analyst roles and opportunities to serve as Incident (Breach) Response Manager. Advancement through this progression, especially into the more experienced White Hat/SOC Analyst role, is supported through continuing education, especially the attainment of professional cybersecurity certifications. In government contract arenas or employment, it is essential to qualify for security clearances and passing background checks. Related experience in military, law enforcement, intelligence, government or complex IT and network management can also lead to additional opportunities in this pathway. A SOC Analyst, Pen Tester and White Hat/Ethical Hacker role are some of today's most cited cybersecurity roles.

Vulnerability Detection & Investigation Pathway A

Path A

Role 1

Industrial Control Systems Analyst

Average Salary: $113,600*

Projected Growth Rate: 69%

Role 2

Incident (Breach) Response Manager

Average Salary: $136,250*

Projected Growth Rate: 41%

Role 3

SOC Analyst; White Hat/ Ethical Hacker; Pen Tester

Average Salary: $143,000*

Projected Growth Rate: 48%

	Industrial Control Systems Analyst	Incident (Breach) Response Manager	White Hat/ Ethical Hacker
Education (Certification & Certificates)	• Technical degree or equivalent experience • Industry certification preferred (ITPM, GIAC, CISSP)	• Bachelor's degree in Computer Science or Information Technology. • Professional certifications: Certified Information Systems Security Professionals (CISSP), GIAC Security Essentials, Certified Ethical Hacker (CEH)	• Master's Degree or higher in a relevant field (e.g. Cybersecurity, Computer Science, Manufacturing, Cyber-Physical Systems, Public Policy, JD)
Work Experience	Experience in industrial manufacturing environment and background in electrical, instrumentation and process controls. 0-2 years working experience in process control technology/ manufacturing IT environment desired.	Minimum of 5 years of experience in digital forensics and incident response	Including 2+ years required experience in the design and conduct of penetration testing is required
Considerations	Also an excellent early career role for progression into various OT /infrastructure and facility security roles.	• Experience on response teams for major risk related programs (IS, DR, BC CM, etc.) is highly valuable with increasing responsibilities for integration to cybersecurity and broad risk factors beyond technology • Ability to use standards and industry models to guide policies	• Increasingly important for this role to have strong communication skills and the ability to tie vulnerabilities and breaches to business risks and be part of the broader business-technical cyber culture change • Important participant in exercising and other readiness activities

** Influenced by relatively high numbers of consultants/contractors filling these roles*

CyberME Career Paths

Secure DevOps in Manufacturing Pathway Overview

	Role 1	Role 2	Role 3
Path A	Cybersecurity Tester / Evaluation Specialist	Cybersecurity Standards Developer	Cybersecurity Systems Architect
Path B	Cybersecurity Operations Specialist	Cybersecurity Solutions Planner	SecDevOps Transformation Leader

Introduction to Career Pathway:

The Secure DevOps (SecDevOps) in Manufacturing progression outlines another opportunity in CyberME for the creation of another newer-to-work path. The initial roles - Cybersecurity Tester/Evaluation Specialist and Cybersecurity Operations Specialist at entry levels - are possible entry-points for robust apprentice program graduates and community college graduates. It would be important for new-to-work individuals to have gained high degrees of hands-on experience before taking on those specialist roles, i.e. through a structured work share program with the college or apprentice sponsor. These roles involve both internal and customer-, product-, system-, or supply chain-facing cybersecurity support, awareness, and evaluation. Additional experience, especially with a range of evaluation and testing targets or operations areas, and/or certification in cybersecurity standards and compliance, change management, and technical solutions, will support progression after several years experience, possibly into roles like a Standards Developer or Solutions Planner roles. A relevant Bachelor's degree is also highly preferred for these roles, and is required for advancement into the senior professional ranks such as Cyber Systems Architect and SecDevOps Transformation Leader roles.

Secure DevOps in Manufacturing Pathway A

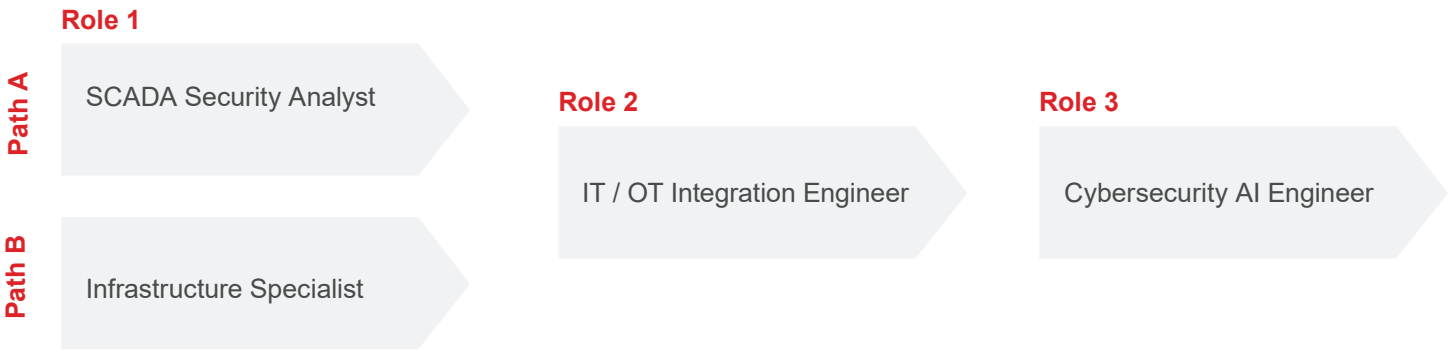
	Role 1	Role 2	Role 3
Path A	**System Administrator** Average Salary: $90,000* Projected Growth Rate: 18%	**Secure Software Developer** Average Salary: $141,800 Projected Growth Rate: 63%	**Cybersecurity Systems Architect** Average Salary: $159,800 Projected Growth Rate: 136%

	System Administrator	Secure Software Developer	Cybersecurity Systems Architect
Education (Certification & Certificates)	Associate's degree in IT, Computer Engineering or a related technical field preferred; BA or BS degree a plus	Bachelor's degree in Computer Science or related discipline	• Bachelor's degree in related discipline and equivalent experience • CISSP Certification
Work Experience	0-2 years of experience with working in a network operation environment, traditionally, help desk to specialty of Veritas, Windows, Sun, or UNIX	Standard 2-3 years prior experience for entry-level and 5-10 years for senior application development roles	3-5 years' professional experience in areas such as complex systems development and evaluation
Considerations	• Possible apprenticeship pathway • Excellent entry and early career role with system specializations and movement to other technical roles	• Strong programming skills, particularly in Java, Python, C/C++ or client favorite programming language • Experience with distributed systems • Strong commitment needed to Secure by Design approach	• Knowledge of cybersecurity open architecture principles across the full cybersecurity lifecycle • Important peer leadership role with major impact on technical direction, strategies and investments

** Influenced by relatively high numbers of consultants/contractors filling these roles*

Cyber[ME] Career Paths

Secure Factory Automation Pathway Overview



Introduction to Career Pathway:

The Secure Factory Automation Pathway is ideal for those with technical or engineering backgrounds, including military, administrative, or factory experience, to enter the Cyber[ME] workforce. The starting roles, SCADA Security Analyst and Infrastructure Specialist, often require at least 1 to 2 years of technical experience and at least a 2-year technical degree or equivalent military training and certification. Progression into the IT/OT Integration and Cybersecurity AI Engineer roles will require further education and experience, including a degree in Engineering, IT, or Computer Science at the baccalaureate level or beyond.

Secure DevOps in Manufacturing Pathway A

	SCADA Security Analyst	IT/OT Integration Engineer	Cybersecurity AI Engineer
Education (Certification & Certificates)	Certifications such as CISSP, CSSA, and Microsoft and Linux OS, Server, and Database certifications and/or relevant experience are highly desired	Bachelor's degree in Engineering, Computer Science, Information Systems, Cybersecurity, or related field, plus professional certifications	Bachelor's degree in Engineering, Computer Science, Information Systems, Cybersecurity, or related field, plus professional certifications
Work Experience	2 years experience with any industrial standard SCADA systems/ cybersecurity projects on SCADA	15-20 years of experience in OT or IT required with broad manufacturing experience	• 5+ years of relevant work experience in endpoint or network security space. • Training in ICS and SCADA is required. • Security and Facilities Operation Center experience is highly desired
Considerations	• Strong working database knowledge • Programming languages, security clearance	• Highly interactive role • Influencing skills critical to have • Knowledge of NIST SP 800-53, Revision 4 and NIST SP 800-82, Revision 2 are required • Systems Administration, Change Management, Engineering Best Practices	• Can work collaboratively with Engineering, Sales, Marketing and the Technical Assistance Center • Networking and IP Protocols, Network Security, Monitoring Systems

** Influenced by relatively high numbers of consultants/contractors filling these roles*

Cyber[ME] Career Paths

Secure Design Pathway Overview

Introduction to Career Pathway:

The Secure Design experienced progression is suitable for experienced workers with engineering and/or product management backgrounds. The initial role, Cybersecurity Tester/Evaluation Specialist is involved in delivering customer-facing cybersecurity assessment and professional services. While at least 3-5 years of experience is required, starting as a Tester/Evaluation Specialist may not always require a 4-year degree. Progression into the IoT Security Specialist or Product Security Engineer roles will require a Bachelor's degree and additional skills and experience in engineering skills and technical proficiency in addition to product management and development. At least one certification or working toward a credential/certification related to IT Risk Management, IT Systems Control, IT Audit or IT Governance is highly desired. Secure Design Product Life Cycle Manager roles will require at least 6-9 years of experience, including management experience.

Secure Design Pathway A

Path A

Role 1

Cybersecurity Tester / Eval Specialist

Average Salary: $80,000

Projected Growth Rate: 113%

Role 2

IoT Security Specialist

Average Salary: $133,800*

Projected Growth Rate:137%

Role 3

Secure Design Product Life Cycle Manager

Average Salary: $145,950

Projected Growth Rate: 61%

	Cybersecurity Tester/ Eval Specialist	IoT Security Specialist	Secure Design Product Life Cycle Manager
Education (Certification & Certificates)	At least one security certification is strongly preferred, such as CISM, CRISC, or CISSP	Bachelor's degree in Computer Science or related field, or equivalent work experience	Bachelor's degree in Computer Science, Engineering, IT or equivalent experience, plus CSPO or PMI-ACP
Work Experience	Prior experience of management of technology infrastructure is preferred Experience with AWS, Azure and/or cloud solutions in general	Minimum of 1-2 years of cybersecurity experience in addition to prior professional/ business experience, including an understanding of web services and cloud architecture and infrastructures	• 3+ years experience in hands-on technical role writing production code, solution engineering, or technical architecture • 5+ years of relevant Product Management experience in an agile software product development environment
Considerations	Knowledge of risk management policies, current industry trends, methods, standards, processes, governance models, and industry-standard risk analysis	• Experience with programming languages (such as C/C++, Ruby, Python, etc.) a plus • Possess self-drive to keep moving things forward even in the face of ambiguity and imperfect knowledge	• Relies heavily on cross-functional interactions and workshare, and the ideal candidate will be equally comfortable interacting with both technical and business-oriented workstreams • Leadership via influence of distributed teams • Practiced in increasingly larger or more complex cross-functional project management

** Influenced by relatively high numbers of consultants/contractors filling these roles*

Cyber[ME] Career Paths

Resilient Cyber Transformation Pathway Overview

Introduction to Career Pathway:

The Resilient Cyber Transformation progression presents opportunities for experienced professionals with backgrounds in business management and leadership, human resource development, education, and other fields. Professionals with degrees in non-STEM disciplines may enter the pathway as a Cybersecurity User Trainer/Coach. Deeper knowledge and experience, including professional certification in addition to relevant undergraduate or higher coursework will prepare workers for opportunities in the Cyber Asset Manager, Enterprise Change Management Specialist, and Cyber Standards Developer roles. The third level on this progression includes senior leadership roles that will require at least 6 years of cyber-related experience, professional certification, and often, though not always, an advanced degree.

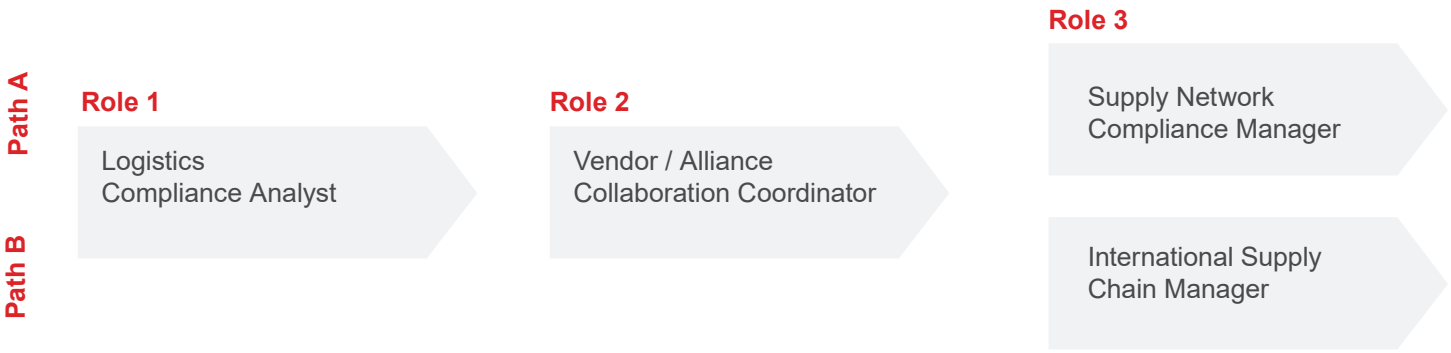
Secure Design Pathway A

	Cybersecurity User Trainer/Coach	Cybersecurity Asset Manager	SecDevOps Transformation Leader
Education (Certification & Certificates)	Bachelor's degree or equivalent 4 to 6 years experience	• Bachelor's degree in Business, Computer Science, Engineering or other relevant field • One or more professional certifications are preferred, such as ITIL Foundations certification, International Association of Information Technology Asset Managers (IAITAM) certification, or ISO Auditor	• Bachelor's degree in Business, Computer Science, Engineering or other relevant field • One or more professional certifications are preferred, such as ITIL Foundations certification, International Association of Information Technology Asset Managers (IAITAM) certification, or ISO Auditor
Work Experience	2+ years experience in managing/ overseeing complex training programs	5 years experience, including 2 years supervisory experience	• 6-9 years experience, including 5 years of project or change management. Agile experience preferred.
Considerations	• Customer service, organizational skills, strong written and oral communication skills • Strong time-management and prioritization skills	• Experience with and understanding of RFID technology to help manage assets • "Expert-level" skills in Microsoft Excel	• Agile, Scrum, Project Management, DevOps

** Influenced by relatively high numbers of consultants/contractors filling these roles*

Cyber[ME] Career Paths

Secure Cyber Supply Chain Pathway Overview



Introduction to Career Pathway:

The Secure Cyber Supply Chain progression outlines opportunities for workers transitioning into Cyber[ME] roles without high levels of technical or engineering experience and expertise. The Logistics Compliance Analyst role offers a transition opportunity for workers with at least 1 to 2 years of office administration experience and completion of at least some post-HS college coursework, although a Bachelor's degree will often be highly preferred. Progression in the Vendor/Alliance Collaboration Coordinator position can be achieved primarily through further professional experience and development. The Supply Network Compliance Manager and International Supply Chain Manager roles will require further professional and/or management experience, and are highly likely to require a Bachelor's degree and professional certification.

Secure Design Pathway A

	Logistics Compliance Analyst	Vendor/Alliance Collaboration Coordinator	Supply Network Compliance Manager
Education (Certification & Certificates)	Bachelor's degree required in supply chain management, logistics or other business related disciplines	Bachelor's degree required in supply chain management, business admin or other related business field	• Bachelor's degree in a relevant field • One or more professional certifications are preferred
Work Experience	Experience in Human Resources, Education, Corporate Development, Safety Compliance or Coaching roles.	Varied from minimal experience in customer management and office management to 2-3 years of vendor relations or procurement experience	Security Protocols, Firewall Management, Cybersecurity Systems Architecture
Considerations	• Logistics management, inventory or transportation experience, business analysis • Human Resources is an adjacency and this candidate pool brings highly-transferable and shared compliance skillsets	• Document control, procurement technologies, contractual review	• Experience in security management is highly preferred

** Influenced by relatively high numbers of consultants/contractors filling these roles*

CyberME Career Paths

Cybersecurity Systems Operations & Development Pathway Overview

Path A / Path B / Path C

Role 1

Manufacturing Cybersecurity Systems Operator

Role 2

Cybersecurity Operations Specialist

Role 3

- Industrial Controls Network Security Specialist
- Embedded Code Developer-Secure Systems (> SW Developer/Engineer)
- IT/OT Integration Engineer (see Hiring Guide for this path)

Introduction to Career Pathway:

The Cybersecurity Systems Operator is an example of one of the cybersecurity operations roles supporting IT/OT convergence and likely one of those roles that CyberSeek.org indicates are part of the 21% of cyber job openings that require less than a bachelor's degree. These job roles require technical cybersecurity learning and development and experience that can be gained via micro credentials, initial skills courses, bootcamps, apprenticeships and certifications. These apprenticeships and the follow-on actual job experience should also provide professional and early leadership skills. Progression into a more advanced and independent operations specialist would further enable experience in more complex integration, automation and security scenarios; and that additional time and widened experience as a Specialist along with additional certification and experience can open up several higher-level routes. Branching into deeper and more complex Network Security specialization, or into engineering arenas such as Software/Hardware code development, or broader IT/OT integration engineering are all possible when starting as a generalist cybersecurity Systems Operator. Also possible are technical and people leadership routes.

Cyber Risk Management & Governance Pathway A

Path B

Role 1

Manufacturing Cybersecurity Systems Operator

Role 2

Cybersecurity Operations Specialist

Role 3

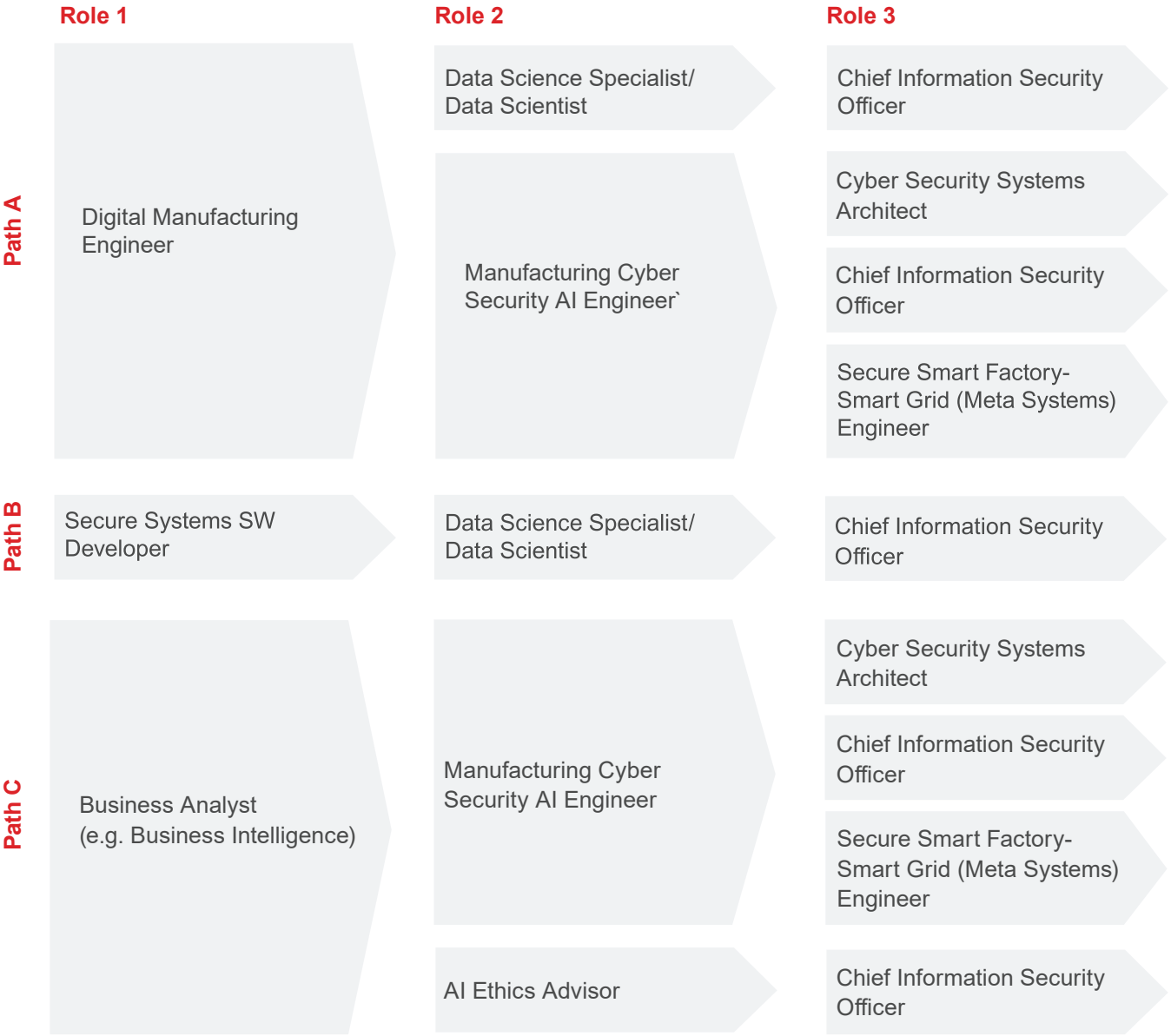
Embedded Code Developer-Secure Systems

	Manufacturing Cybersecurity Systems Operator	Cybersecurity Operations Specialist	Embedded Code Developer-Secure Systems
Education (Credentials, Certification & Certificates)	• High school/GED required; some additional related coursework highly preferred (towards associate degree or evidence based micro credentials) • Technical training and development • Certifications such as CCT, CCNA, CompTIA Sec+ or NW+ • CCA, CCST; GICSO, GRID, GCIP or other industrial controls related • Specific systems training as required by local operations • Relevant Military Training	• Associates Degree and progress towards Bachelor's degree in Cybersecurity, Computer Science, Information Technology or related area. • Continued or completed professional certification as previous plus additional such as SSCP or movement from Associate certifications into fully granted certifications	• Bachelor's Degree in a relevant field. Cybersecurity, Computer Science, Information Technology or related area. • Additional secure software development certifications from MTA to Azure • CCDH; • CISSP and other Info Security and Cyber certifications; • PSD1 (Srum) and PMP-ACD (Agile Certified) professional certifications • Associate to full certification as experience enables
Experience	• Previous production, technical support or general business experience preferred • Apprenticeships and other applied/hands-on experiences and development required	• Minimum 3-5 years' Systems Operator experience, with progression to Level II and III and related increased independence, complexity and responsibility • Other equivalent experience/ specialized IT and OT Operations experience • Other professional and early leadership skills	• Minimum 6 years' experience (4 years with Master's level or higher degree) in executive program analysis and direct support. • Experience with policy development
Considerations	• Interest in continued development of IT and OT integration and modernized operations • Fundamental knowledge of production/processing activities and industrial controls and communications. • Foundational knowledge of cybersecurity principles, processes, and practices. • Familiarity with related cybersecurity regulations, compliance and standards (industry, company, supplier, customers). • Increasing hands-on experience with applicable systems	• Problem solving, multi tasking & other soft skills • Cross function initiatives and practices • Broad knowledge and increasing experience with various DoD and or other security compliance and standards experience	• Ability to work with other computer and information science roles, hardware engineers and automation experts to secure data and ensure performance. • Increasing ability to support entire Secure Software Development Life Cycle • Strong understanding of industry and product cybersecurity guidelines and regulations

Development of this Career Path was made possible by a grant from the Siemens Foundation

CyberME Career Paths

AI Enabled Manufacturing Cybersecurity Systems Engineering Pathway Overview



Introduction to Career Pathway:

With its rocket-propelled speed of increasing demand, the trifecta role of an AI engineer focused on cyber in the top ranked target industry for hackers (Manufacturing!) couldn't be more pivotal to many strong career paths. While the Cybersecurity AI Engineer does require education and specific skills, it is also a strong destination for experienced technical and business types looking for a transition, change of arena, or likely longer career path. Manufacturing centric engineers can add cyber experience/certificates and AI experience/certificates; Software Developers already designing for secure systems can add AI experience/certificates; and business-oriented roles also can invest in engineering programs, experiential projects, and certificates to gain entry level Cyber AI Engineering roles. As an AI focused role in cyber, there are adjacent areas like Data Science and AI Ethics that can feed the AI Engineer role or be a lateral move for AI engineers looking to specialize or round out engineer job scopes. And when it comes to progression, here are senior technical and leadership paths as well. Typically the highest-ranking cyber position in a company (larger or smaller), the CISO role is both strategic and lucrative. It can be a career goal for the leadership and business minded experienced Cybersecurity AI Engineer who has worked through business cases and programs to implement cyber solutions using these advanced technologies. Other AI engineers can move into Architect or large scale, connected meta engineer roles where AI will be the everyday mode of cyber and systems management.

Development of this Career Path was made possible by a grant from the Siemens Foundation

AI Enabled Manufacturing Cybersecurity Systems Engineering Pathway Overview Continued

For the two roles in the AI Enabled Manufacturing Cybersecurity Systems Engineering path that are not highlighted in the corresponding success profile, general role descriptions can be found below:

Digital Manufacturing Engineer	Manufacturing Cybersecurity AI Engineer	Chief Information Security Officer
A general Digital Manufacturing Engineer determines, establishes, and maintains digital processes, equipment, tools, and procedures to ensure continuous production flow, quality, and performance within the manufacturing industry. • Develops, maintains, and designs new automation equipment and automation lines to support product production, improve efficiencies, and eliminate waste within manufacturing processes. • Troubleshoots and resolves technical problems with equipment, product, and systems. Responds to any manufacturing problems by investigating and resolving to assure a continuing flow of production. • Collaborates across organizational lines to establish and maintain effective work relationships to achieve individual and team goals.	SEE CORRESPONDING SUCCESS PROFILE	A Chief Information Security Officer executes decision-making authorities and establishes vision and direction for an organization's information security strategy and roadmap, taking overall business strategy and threat landscape into account. • Participates as a member of the senior management team in governance processes of the organization's security strategies. • Leads strategic security planning to achieve business goals by prioritizing defense initiatives and coordinating the evaluation, deployment, and management of current and future security technologies. • Develops, implements, maintains, and oversees enforcement of policies, procedures, and associated plans for system security administration and user system access based on industry-standard best practices. • Communicates security strategies and plans to executive team, staff, partners, customers, and stakeholders.

AI Enabled Manufacturing Cybersecurity Systems Engineering Pathway

Path A

Role 1

Manufacturing Engineer
Average Salary: $76,000
(Range $54k - $100k)
Projected Growth Rate: 10%

Role 2

Manuf. Cybersecurity AI Engineer
Average Salary: $146,000
(Range $99k - $220k)
Projected Growth Rate: 74% - 116%

Role 3

Chief Information Security Officer
Average Salary: $172,000
(Range $100k - $310k)
Projected Growth Rate: 11% - 32%

Development of this Career Path was made possible by a grant from the Siemens Foundation

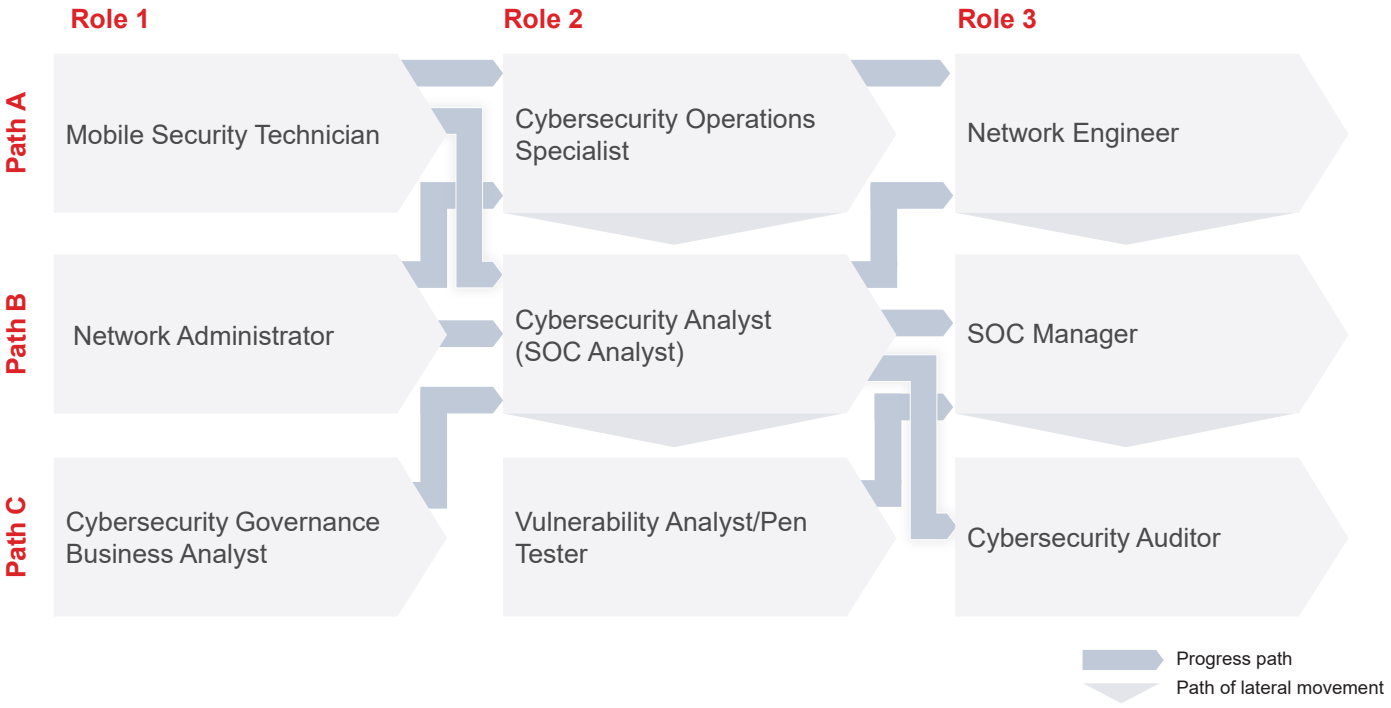
AI Enabled Manufacturing Cybersecurity Systems Engineering Pathway Overview Continued

	Manufacturing Engineer	Manufacturing Cybersecurity AI Engineer	Chief Information Security Officer
Education (Credentials, Certification & Certificates)	Bachelor's degree in manufacturing engineering domain (e.g. mechanical engineering, industrial engineering, or process engineering) is required; mathematics, physics, chemistry degrees with strong industrial exposure and engineering foundations may be accepted; some associate degreed candidates with strong engineering support role experience and additional engineering coursework are eligible; MS in related engineering or other technical areas, especially new technologies, are highly valued. Institute of Electrical and Electronics Engineers (IEEE) certifications or equivalent often desired in addition to a degree. Licensure not usually required for this domain; professional engineer (PE) designation still highly valued.	Bachelor's degree or higher usually required in Computer Science with AI, Machine Learning, or related specialization plus Cybersecurity course/skill focus and ideally embedded professional certifications. Other strong degrees are Computer and Information Sciences focused on Cyber-Physical Systems, Networking or Systems Engineering; Information Security and Cybersecurity. Related degrees with appropriate AI enabling coursework supplemented with recent AI and Cyber certifications increasingly considered: AiE (ARTiBA)); ML-AI (Stanford via Coursera); IBM AI Engineering (IBM via Coursera); CompTIA Security+; CISSP; CISM (for a business and leadership focus); NIST Cybersecurity Framework; CCSP; CCNA Security. Many other universities (eCornell, Northwestern, etc.) offering non-degreed continuing education programs in AI/ML and related areas.	Bachelor's degree or higher usually required in related technical area, including Computer Science, Information Sciences and Security; a wider variety of technical master's degrees with a security focus increasingly valued. CISSP and CISM in particular are professional and management certifications valued here. Increasingly, CISOs augment their degrees and/or certifications with a Masters in Business Administration or equivalent hybrid business-technical or non-technical management degree
Experience	1- 2 years of applied engineering work via apprenticeships and degree program portfolios are entry requirements; 4-7 years for mid level and 7-10 years as senior with increasing experience in these areas: • General engineering practices from requirements through testing and implementation support. • General production and processing methods and standards; automation, instrumentation, control systems. • Design engineering tools. • Company or sector specific hardware, materials, assets. • Quality improvement practices and standards. • Product development exposure. • Ability and passion for handling complexity and ambiguity. • Communications – verbal and written for business and technical stakeholders at all levels. • Leadership and supervision of junior team members.	1-3 years engineering experience and 2-3 years of experience in cyber threat detection and analysis or equivalent applied education experience for entry requirements are preferred; 4-7 years for mid level and 7-10 years as senior with increasing experience in these areas: • General production and processing methods and standards; automation, instrumentation, control systems. • Data science foundations. • Security practices and standards. • Ability and passion for dealing with complexity and ambiguity. • Ethical issues in AI, Cyber and Data Privacy. • Analytical thinking and attention to detail. • Deductive and inductive reasoning. • Creative problem solving. • Communications – verbal and written for business and technical stakeholders at all levels. • For managed or advisory service roles, strong client management skills.	Requires a wide range of IT experience, education, strong leadership and communication skills. • 7-15 years of increasingly responsible and varied Information Security, OT/ICS Security or Cybersecurity experience; 5+ years in leadership and management roles. An increasing option are CISOs with strong business and transformation capabilities with less deep technical knowledge. • Demonstrated experience in implementing and managing security systems and controls technology. • Significant IT/OT integration experience. • A consultative mindset applied to business challenges. • Business and technical process improvement. • Governance, alignment, and policy development. • Enterprise risk management assessment. • Improving organizational resiliency for the business.
Considerations	Experienced industrial engineers without recent training or exposure to advanced technologies and modernized digital or cyber practices are highly encouraged to update their broader skill set to maintain employment value and impact. Extensive options at all program lengths and investment levels exists.	• A major variant is how much AI systems programming and development is in scope. True to engineer focus, less versus more is assumed. • This role isn't assumed to perform operational and ongoing use of the systems; that would be in Cyber Analysts, Cyber System Operators and other operations roles.	Range, depth of CISO role – and also requirements and pay - may vary depending on the sector of manufacturing, the company cyber/AI maturity, the types of technology as assets, and the regulatory or standards environment.

Development of this Career Path was made possible by a grant from the Siemens Foundation

CyberME Career Paths

Manufacturing Cybersecurity Analyst Pathway Overview



Introduction to Career Pathway:

These general Cybersecurity Analysis Pathways center around the highly-scalable and wide-ranging scope of the Cybersecurity Analyst. This role is a highly valuable destination role important to inhouse capabilities and at third-party employers and it is a gateway role to many cyber roles well beyond those shown since it offers diverse exposure to many cyber domains. Hardware, software, and business operations entry level roles can all feed into an Analyst opportunity; the Analyst opportunity itself can laterally specialize in industrial and systems operations or vulnerability and pen testing as examples, each of which are often adjacent roles within the generalist Cybersecurity Analyst role scope. A key enabler for these diverse options are the many available training and certifications in broad or special cyber analysis areas. This supports the possibility that employers may be increasingly accepting of Associates versus Bachelor degrees for this role. Further progression, with experience, additional coursework, or degrees and responsibility offers advancement into technical tracks, management opportunities and consultant/advisor/auditor roles, some of which are shown here (Network Engineering, SOC Management and Cybersecurity Auditing). It is essential to support - and create a great benefit from a wider career opportunity perspective –more specific and varied competency mapping for entering and progressing through any Cybersecurity Analyst pathway. A small price to pay for the great versatility of this role.

For the two roles in the AI Enabled Manufacturing Cybersecurity Systems Engineering path that are not highlighted in the corresponding success profile, general role descriptions can be found below:

Mobile Security Technician	Cybersecurity Analyst	Cybersecurity Auditor
A mobile security technician uses advanced skills to perform functions associated with the secure installation, integration and/or maintenance of wireless equipment to protect portable devices such as smartphones, smartwatches, and tablets from threats and vulnerabilities. • Uses sophisticated electronic test equipment and measuring devices in analyzing, adjusting, installing, wiring, repairing, maintaining, and testing wireless, transmission, and associated equipment. • Carries out proper fault diagnosis to improve the quality of mobile devices and repair them including both the network connections systems and end devices/IoT devices themselves. • Performs required incidental and preventative maintenance on cell sites, power equipment, transmission, and associated equipment, and completes necessary logs, reports and postings.	SEE CORRESPONDING SUCCESS PROFILE	A cybersecurity auditor conducts evaluations of cybersecurity and general IT processes and operations to determine compliance and recommend improvements. • Assists with the plan, design, and execution of audit procedures necessary to comply with cybersecurity requirements and identify any risks, working closely with IT, compliance management, and external auditors to do so. • Conducts IT governance audits and operational risk assessments across functional areas, processes, and applications. • Provides strategic insight, advice, and guidance with respect to cybersecurity risk management, governance, policy, and operations.

Development of this Career Path was made possible by a grant from the Siemens Foundation

Manufacturing Cybersecurity Analyst Pathway Overview Continued

Path A

Role 1

Mobile Security Technician
Avg. Salary: $50,000
(Range $34K - $72K)
Projected Growth Rate: 32%

Role 2

Cybersecurity Analyst
Average Salary: $95,000
(Range $60k - $156k)
Projected Growth Rate: 116%

Role 3

Cybersecurity Auditor
Average Salary: $105,000
(Range $58k - $208k)
Projected Growth Rate: 32%

	Manufacturing Engineer	Manufacturing Cybersecurity AI Engineer	Chief Information Security Officer
Education (Credentials, Certification & Certificates)	• High School, GED required. • Some technical school training a plus. • Completion of certificates (vendor or school) highly preferred in areas like Electronic Security/Mobile Security/Wearable Computing/Specific Systems (e.g. physical security, alarm, low voltage field devices, augmented reality). • Some specialized areas may prefer Cisco Certified Network Associate Wireless (CCNA Wireless), Cisco Certified Network Professional Wireless (CCNP Wireless), CompTIA Network+, Certified Wireless Network Administrator (CWNA), Certified Wireless Security Professional (CWSP) or similar for higher level positions. • Apprenticeships highly preferred.	• Increasingly accepting of Associates Degree and Certification with apprenticeship, portfolio or related experience in lieu of 4-year degree. • Bachelor's degree in Computer Science, Information Technology or related discipline preferred. • Professional certifications: (CompTIA Security+501; Certified Information Systems Security Professionals (CISSP), GIAC Security Essentials, Certified Ethical Hacker (CEH); Certified Information Systems Management (CISM) and related. • Apprenticeships or certificate of completion of internal training programs highly preferred.	• Bachelor's degree in Computer Science, Information Technology or related discipline, including Business, Accounting, Finance, or Risk Management. • Master's degree valuable or preferred, especially for third party provider and consultancy employers. • Professional certifications: Certified Information Systems Security Professionals (CISSP), Certified Information Systems Auditor (CISA); Certified Information Systems Manager (CISM), Certificate in Risk Management Assurance (CRMA), GIAC Security Essentials, Certified Information Systems Management (CISM) and related. • Apprenticeships or certificate of completion of internal training programs highly preferred.
Experience	• 0-3 years Field Support/Implementation and Maintenance of systems, equipment and technologies. • Experience in corporate security, managed security services, field technical support service delivery or similar preferred • Experience in building and maintaining relationships with internal and external customers.	• 0-3 years' information security experience or equivalent experience/specialization in priority tasks or tools for specific environment; 2-3 years other/general technical experience highly desired. • Multiple levels often available leading up to Senior Analyst or equivalent with additional 2-3 years experience per level. • Increasing industry knowledge and specialization often desired but can maintain a generalist job scope as well.	• 4-7 years' related experience in IT, security or audit operations or equivalent experience/specialization required including: - Informational and Industrial Systems Audits and Evaluation - Governance, Policy and Standards - System Evaluation, Implementation - Risk Mitigation • Multiple levels often available leading up to Senior Auditor or equivalent with additional 2-3 years experience per level.
Considerations	• Associates degree highly valued for future progressions and additional certificate eligibility. • Interest in increasingly sophisticated system applications. • Increasingly able to complete designs and solutioning beyond installation and maintenance.	• Role frequently seen in both manufacturing organizations and in third party service provider settings (partial influence on wide salary and skill range). • Problem solving, multi tasking & other soft skills • Broad knowledge and experience with the various NIST, DoD or other relevant frameworks and toolsets. • Increasing knowledge of Manufacturing and Industrial context for Actors, Vectors, Targets and other threat and vulnerability profiles. • Employers benefit from using and accepting flexible "in kind" assessment methods and skill demonstrations.	• Role frequently seen in both manufacturing organizations and in third party service provider settings (partial influence on wide salary and skill range); insurance and investigative areas have some overlap with this role. • Supervisory opportunities and ability to manage others on audit projects comes with increased responsibility. • Increasingly context-specific knowledge and experience with the various NIST, DoD or other relevant frameworks and standards is required for increasingly complex or custom audits. • Various international standards audit practices are increasingly being implemented.

Development of this Career Path was made possible by a grant from the Siemens Foundation

PERSONAS

Where's My Next? Four Personas to Kickstart Cyber[ME] Recruiting

Joaquin: Experienced, the link to IT/OT integration

I'm a Hardware Engineer at an industrial manufacturer where I've been growing for the past 25 years, designing the manufacturing production systems that are propelling us into the future. I've been leading our automation efforts for part of one of the main product platforms over the last decade. It's been a great ride and I have seen firsthand how new manufacturing systems have changed our factory footprint and positively impacted the speed, efficiency, safety and data analytics of our operations.

Now that I'm in my early 50's, I'm ready for a new challenge and know I can get more current. My degree was in manufacturing engineering, but I've been working alongside our IT department long enough to have a solid understanding of how the line between IT and OT is merging more by the day. Our digital factories bring more and more opportunity, and I recognize how this means that we need to secure our systems tighter than ever before. To me, cybersecurity is the great unknown, and it's the direction I want my career to go next. I've learned quite a bit about cyber on the job, but also invested in some classes on nights and weekends to possibly pick up some additional IT certificates.

I'm getting ready for the next horizon and I know it's where the physical factory and the information systems connect. Keeping those connected systems safe and productive is where my next is.

Joaquin: Experienced, the link to IT/OT integration

Why employers should want to talk to Joaquin and others like him:

Manufacturing expertise and industry perspective: Joaquin brings a tremendous amount of experience and deep knowledge of his company's process and product. With that also comes years of following the vendors and other manufacturers as competition. He also has awareness of the broader changes in manufacturing physical systems, including physical and data security. This knowledge and attitude is something to value and protect whether internally or at another manufacturer.

Change and skills evolution: Adding to a complete understanding of operating technologies, and the added benefit of experiencing past successes and failures of technology implementation and emerging cybersecurity issues, his experience with automation and now with some additional IT certifications makes him a prime candidate to help converge IT and OT or specialize in OT cybersecurity, although there could be other domains like compliance that could also use Joaquin's experience.

Individual maturity and responsibility and a cross-team mentality: Even with a very viable current role, he is also dedicated to upskilling himself and understands that as an individual, he plays a large part of being responsible for his own development. He appreciates growth and change in himself and others to bring new solutions to operational areas.

Roles focus

Where you will find me

Manufacturing Engineer, Industrial Process Automation Engineer, Hardware Engineer, Distributed Controls Systems Engineer and other Operational Technology related roles

Target roles

IT/OT Convergence Engineer, Smart Factory Engineer; Lead Engineer in any of the above Engineering areas involved in IT/OT Convergence; in time through to (Senior) Program Manager, Industrial Systems/ Operational Technology Security Advisor and/or ISSO

Mutual work domain interests

Capabilities to consider

- Business
- Cross-functional program design and deployment
- Program and system implementation
- Change management
- Quality and process management
- Critical thinking
- Problem solving
- Innovation and ideation
- Prototyping and field testing

Technical

- Engineering design (strategic and tactical), development and deployment
- Mechanical design, engineering and tooling
- Systems and process optimization
- DfX (Design for Excellence)
- Board design

Soft Skills

- Leadership, formal and through influence
- Transformation skills

"Give me a role that takes on cross-functional engineering, technical and operations issues and challenges me to lead in solving those problems. The closer I can get to influencing the business of manufacturing operations, the better. Most of the success I've seen, and have had personally, is when any set of business groups move to a very pragmatic but shared focus and we each break from our siloed thinking. Let's keep learning, respect each other's evolving knowledge and quickly make room for new solutions."

Paige: Transitioning, from many hats to cyber business-tech pro

I've been working at my uncle's small, local service-oriented company for the past 7 years – since I received my associate's degree. I really enjoy working for a small company and value the experience that I've been able to gain by wearing multiple hats.

Running customer relations and account management for the sales team is my day job, but I've also had a knack for and a draw to tech. I've been able to improve our sales efficiency and customer experience by implementing a more updated website and some CRM software.

Lately, I've been branching out into more functional areas of the company, like HR and community relations and outreach. I can see that a company connected online and internally is what will keep us smart, right-sized, and competitive. And I understand that as a business, the more we become connected, the more we're responsible for protecting ourselves and our customers' info. If I can make the case for my own personal learning and for bringing in more cyber expertise - a cyber vendor partner or even a team member - I think I could step up into a new role, allowing me to manage that relationship or individual. I want to learn more about cybersecurity and how even a small manufacturer needs to be thinking about this. Our IT team and their vendors are probably looking at this but I would want to be involved, especially for customer and employee info issues. I will be the one to get the call if something goes wrong.

I'm getting ready for the next horizon of our smaller business – or maybe another small business in this community I care about. I want to keep advancing my career and stay connected, so a more modern business role with some more technical content is where my next is.

Paige: Transitioning, from many hats to cyber business-tech pro

Why employers should want to talk to Paige and others like her:

She's tech literate: though Paige doesn't know cyber, we know that she led her company's tech adoption to date even though it's basic by some standards, and that she understands how pieces fit together – from sales to production to finance. She's done some software evaluation and purchasing, systems configuration, systems administration, and user training, enough to know how to spell IT and to get their in-house engineers and production teams onboard with new technology.

She's off to a good start on being well rounded in basic information and cybersecurity needs: leading customer relations and account management, she's responsible for client information, order management and emails and recognizes that she also has a responsibility to protect this information. She's active online in her personal life, active in her community and has likely learned about the importance of cybersecurity (especially at small companies like hers) from local business association meetings. She's the person in her company who could have been overseeing securing their general business office automation systems and training the staff.

She brings business-technical connections: Paige will be key to a successful implementation of cybersecurity measures at her smaller company. The leaders have an opportunity to promote her, allow her to keep growing, and keep this valuable talent. With her base knowledge and the addition of a few company-sponsored business-it certifications, Paige could thrive in a business-technical hybrid role. She has deep understanding of her company's supply network and partnering space, and has internal credibility and personal relationships. She'd be well matched with IT to co-hire a cybersecurity partner and create a concrete, actionable plan to secure their information including recruiting and co-managing another business-technical team member that she and her IT or plant systems team could both use for cyber business and tech tasks.

Roles focus

Where you will find me

Many multi-skilled office management roles; sales and marketing and related support roles; systems support specialists; trainers and implementation support; finance and administration roles

Target roles

Vendor/alliance collaboration coordinator; cybersecurity awareness communications specialist, incident communication facilitator, business impact analyst; asset manager and many more business-technical areas.

Mutual work domain interests

Capabilities to consider

- Strong business acumen
- Cross-functional processes
- Compliance and/or process management mindset
- Connected processes: sales, vendors, customers; supply chain, purchasing management

Technical

- Basic technical and systems management, including system access and license management
- Most any area of technical or systems support: configuration, user coaching, troubleshooting, reporting
- Social media and online presence – site management, cloud services, search optimization

Soft Skills

- Ability to engage multiple levels of employees and leadership
- Ability to work across functions and geographies

"I am a fast learner and have been willing to take on many roles for our small company. It seems like tech people today need both people and computer or online skills; I know I can do both and I'd like to apply that capability I have to a more modern business role with better options if someday I want to move to a larger city or company."

Darius: New to work, eager to learn

I'm a rising senior in high school, thinking about what I want to do "when I grow up." I'm not sure yet. I spend a lot of my time gaming, and I know I want to go into tech in some way. I've been tinkering with building an app, and one of my friends has already made some money through e-gaming.

I'm getting pretty good grades in school, but I don't feel like a 4-year college is right for me. I've aced my programming classes, my robotics and other STEM classes. Even was in a couple of local hackathons. I don't know exactly which direction to go but I do know there are options for me. I've even been approached at some of the events by companies that want to keep talking to me, especially later on when I'm in college.

But I just don't want the debt of college or the time lag before I can bank some money. At least not now. Maybe I can work and go to school? My counselor said that I could start out with some community college or maybe even earn some tech certifications online. Then, especially if I can somehow break in to any job experience while I am going to class or getting certs, maybe I could land a good entry-level job actually in a tech career path.

Honestly? I'm really wanting to get into tech as a career. I know I am pretty smart. I keep hearing there's good money and a lot of opportunities in cybersecurity and I can move most anywhere for those jobs or work from my own place. I'm not sure of my options or specific steps, but I am pretty sure tech and cyber overall is where my next is.

Darius: New to work, eager to learn

Why employers should want to talk to Darius and others like him:

He's a globally aware, digital native with some realistic preview of cyber work: Darius is a young, digital-native with a natural understanding of tech. After school, he spends the majority of his time in a virtual environment, connecting with global group of friends through online gaming. In school, he's choosing all the tech electives and learning enough about programming and coding to play around with some light system development or hacking for fun.

He's in the stage of active exploration: He's likely being advised by his teachers and counselors on different ways of breaking into tech, and they may be recommending that he take supplemental classes online to earn badges and certifications, or guided to take for-credit classes at the local community college. While he's been exposed to the growing value of developing skills in cybersecurity, he may not have considered a career in manufacturing and would need to be coached on why that's the right move as a place to apply his cybersecurity skills. He could be a candidate for apprenticeships, work-study and early non-degree required positions such as tech support or business back office roles. With the many options in several domains to be 'online' and monitoring and assessing, he's a good early candidate for potential investment and development.

He's easily reachable: How do you tap into this necessary talent pool? He'll be online – Information sharing on cyber degrees in manufacturing on gaming and social media platforms will draw his attention. Partnerships with high schools and community colleges will also be invaluable to reaching Darius. Meeting him through his community connections is another opportunity. He'll be quick to learn, but companies need to understand that he'll need some on-the-job training or access to quick training programs or certifications that won't add too much delay to his first paycheck. With early interest and connections, a good employer-employee relationship can get started.

Roles focus

Where you will find me

School channels; community groups, hacker conferences and student tech events, gaming competitions, robotics and other high school STEM channels; more custom outreach to local community contacts; and online gaming communities

Target roles

Apprenticeships, Student Work Study (Internship)
Sponsorships to provide even entry level work experience as needed towards Certification exam sitting

Mutual work domain interests

Capabilities to consider

- Problem solving
- Critical thinking
- Regulations and compliance
- Business priorities
- Communicating and documenting events and actions/resolutions

Technical

- Aptitude for STEM content
- Programming fundamentals
- Networking fundamentals
- Security fundamentals
- Quality fundamental
- Process flow fundamentals

Soft Skills

- Teamwork AND independence
- Follow through
- Adaptability
- Learnability

"I'd like to get some guidance on careers, and some real-life work experience somehow. If someone can show me some personal attention to my school and work choices that let me earn money in some area of tech sooner than later, that would go a long way to signing me up. I'm game!"

Max: Experienced, growing in IT

I'm Max, an experienced cybersecurity professional who's had many different related roles over the years. I've got a BA in Computer Science and went right into a general systems administrator role, then specialized. About 6 years ago, I started on general cyber analyst roles. I've been in IT ever since and now I have a CISSP. I've been a Threat Analyst, a Pen Tester, have done some tech auditing and DR planning, and have been on incident response and investigation teams.

I spend at least half of my PTO at hacker conferences across the US – I'm lucky that I've been able to turn my passion into a career! I'm always looking to grow, and I'm ready for that next step. I know that cybersecurity is where I want to stay, and I've got enough depth and breadth of knowledge to step into a new role - maybe something more in architecture or leadership focused, or something with broader business exposure yet still security focused, wherever it might be.

I am flexible about industries: I've worked for a federal agency, then a large utility and then a SaaS platform provider. I'm pretty mobile right now and would move just about anywhere for the right job. Or not. I've been picking up more required prep courses for some additional certifications here and there as I have time, and I'd be open to picking up another degree. If it will help me reach my next goal and be something I could leverage for the next decade or two, I might do it. With as fast moving as the technologies are and how fast the bad actors are coming after business, I know a position where I can focus on managing vulnerabilities, cyber risk management, or even larger scale security architecture with more broad impact in cybersecurity is where my next is.

Max: Experienced, growing in IT

Why employers should want to talk to Max and others like him:

Cybersecurity expertise and cross-industry perspective: With experience in general secure software development and vulnerability testing, both on the preparation/product development side and on the detection/response side, Max is well-positioned for a number of IT roles with a mid-size to large corporation. Max enjoys the creativity, skill, and precision required for vulnerability/penetration testing, and he's able to get into the mind of black hats from all angles. And he's had to act on vulnerabilities through his incident team experiences. With some additional certifications alongside on-the-job training, he could move into an Cyber Assessor/Planner role or if he's willing to invest time and potentially money, an AI Cybersecurity role. His willingness to relocate makes him an extra attractive candidate.

Adaptable, yet looking to focus: Max seems to like or do well with business change but he may also be looking for more focus as he heads towards mid-career years. His willingness to put in some more investment at this point of his career and his openness to move or not offers many options to him and to a prospective employer.

Possible candidate for formal tech or team leadership roles: Cybersecurity in manufacturing will also need many leaders at various levels, both informal and formal. Many roles require credible business-technical leaders, and Max might be a solid candidate for some of those essential roles where he can advance his technical, business and people leadership skills and leverage his experience and varied exposure.

Roles focus

Where you will find me

SOC Analyst, Cybersecurity Analyst, White Hat/Ethical Hacker, Pen Tester, Incident Team Member (various roles), Secure Software Developer, (Senior) Testing and Evaluation Specialist

Target roles

Cybersecurity Assessor/Planner, Incident Task Force Leader, Lead Internal Auditor, Supply Network Cybersecurity Compliance Manager, Engineer or Architect role in various IT subdomains

Mutual work domain interests

Capabilities to consider

- Governance and alignment on business-technical cybersecurity commitments
- Cross-functional crisis management and incident response
- Incident management and team collaboration
- Forensics guidelines

Technical

- Operating system expertise
- Networking security expertise
- Penetration and vulnerability testing and assessments
- Some programming and scripting to augment analysis
- Expanded actor, vector, target knowledge: methods, motivations, behaviors, toolsets

Soft Skills

- Curiosity
- Learnability
- Tolerance for high stakes, fast pace, natural stressors in frontline cyber roles
- Adaptability

"I don't think I will ever have to leave cybersecurity as my primary career area. Sure the field will change, but so will I. I like the team aspect, the pace, the chase and the importance of my work. It can be stressful at times but it's a tradeoff for the good pay, the co-workers (some are 'crazy' brilliant) and the portable skillset."

SUCCESS PROFILES

Cybersecurity IT/OT Integration Engineer

Role Title: Cybersecurity IT/OT Integration Engineer

Role Impact: Keystone

Summary Scope

Moving from closed, in-house, industrial control systems in manufacturing facilities to more open systems in the increasingly automated and connected manufacturing world has created both promise and pain. More equipment, devices and sensors connect to networks, more IT solutions are being integrated with OT systems with more data moving to the cloud; standards-based hardware and systems are replacing internal proprietary controls systems. All of these create opportunities for connections and business and customer improvements. At the same time, these connections create increased risks and vulnerabilities for attacker-led penetrations of the manufacturing enterprise. Both IT and OT technologies bring unique security knowledge to the informational and industrial controls and access involved. Convergence is increasing, and minimal collaboration isn't an option. Who will carry out much of the policy and direction for convergence, detail what it means, and lead in its application? Who will insure the convergence of IT and OT happens at the applied level and becomes part of the business and operating culture? The role of the Cybersecurity IT/OT Integration Engineer is key to convergence and industrial controls and production security.

This convergence covers a complex set of processes and systems that needs guidance from a holistic point of view, especially the dual perspectives of IT and OT engineers who are dedicated to the secure integration and performance of industrial controls and communications and the related networks, access, and data life cycles. Engineers with this integration role are the bigger-picture, yet applied, security-focused engineers, members of the mutual appreciation society of both IT and OT, regardless of whether they come from an IT, OT or cybersecurity background. They advance, design and implement secure systems policies and practices that prevent incidents and breaches, maintain production capacity and capability, protect assets while in production and in use, and contribute to brand value as a secure manufacturer.

This role works under the direction of Security, IT and Operational leaders who are sponsoring, directing and resourcing the IT/OT convergence. Taking direction from collaborating leaders - CISO/CISCO and IT Security Leadership as well as Manufacturing Operations and Process Control leadership – will be essential to balance security and OT business requirements (latency, bandwidth, availability, etc.). The Cybersecurity IT/OT Integration Engineer works closely with other cybersecurity program professionals, production and delivery leads, other OT engineers and IT engineers, and development/production teams. Together they identify, build and execute the shared and respective roadmaps that recognize both areas' expertise and responsibilities and move forward with shared and connected methods and tools. In this role, the Cybersecurity IT/OT Integration Engineer is a key professional to further develop, socialize, implement and evaluate the frameworks, guidelines, and technical standards that ensure that security solutions are deployed in ways that decrease threat landscapes and maintain safe and competitive production environments. A Cybersecurity IT/OT Integration engineer is an action-oriented, dual-focused, hybrid business and technically adept engineering transformation practitioner.

Cybersecurity IT/OT Integration Engineer

Outcomes

- Mutually developed and operationalized security policies, designs, frameworks, systems, processes, roles and accountabilities.
- More effective and more shared investment in the buildout and implementation of a holistic and shared IT/OT cybersecurity strategy, alignment of resources, responsibilities and accountabilities.
- Connection of business information technologies (IT) and manufacturing operation technologies (OT) through coordinated construction, maintenance, and expansion of an organization's security-enabled systems and production approach.
- Elimination of security gaps and reduction in cyber risks including:
    - Comprehensive and accurate inventories and control for hardware and software assets in the industrial, production and processing sites.
    - Enhanced continuous vulnerability analysis and management.
    - Controlled administration privileges that reinforce dual/shared IT/OT management.
- Expertly evaluated solutions for IT/OT monitoring, provisioning, threat response and continuous improvement.
- Change past fundamental disconnects between IT and OT; remove security silos between business and manufacturing environments; decrease resistance and conflicts that impede security practices.
- Role modeling for ongoing culture change, establishment of common ground, and integrated work methods and information sharing.
- Increased brand equity and social impact as a secure manufacturer and trusted business partner, information steward, and process/asset guardian.

Domain Profile

This role will reside in or come from either (and both!) Informational (IT) Technologies and Integration AND Operational (OT) Technologies and Integration. The role focus is on actionable convergence and leveraging the shared capabilities of the two domains towards cybersecurity goals.

Business Case Contribution

The primary business case contribution of this role is to make cybersecurity policies real; to enable their buildout and implementation; to serve as the lead operational integration resource; to demonstrate dual area representation and consideration; and coach at the team levels what the necessary business and technical culture change looks like. The Cybersecurity IT/OT Integration Engineer is a primary designer and implementer of cross-functional engineering, technical and operations security programs and systems that converge IT and OT while decreasing risk, managing the dynamic threat landscape and maintaining production. An important role in moving to a shared focus on security and protection, the Cybersecurity IT/OT Integration Engineer is key to breaking from the false security of past separate plant/facility operations from "high-tech", and key to removing work culture differences between "corporate IT" and "production".

Every organization needs the right level of technically oriented convergence practitioners who can speak the language and enable the work of these dual areas. They make numerous cybersecurity and operational benefits including:

- Better investments via aligned and mutually supportive strategies, budget and roadmaps.
- Cost avoidance of dual resources, duplicative projects or cross-purposes in either work area.
- Reduced cyber compliance risk.
- Reduced cyber threat risks.
- Improved prevention, detection and recovery capabilities.
- Faster incident response.
- Lower production impacts.
- Maintained brand value; less potential reputational or liability access from cybersecurity incidents and breaches.

Section 2: *Key Responsibilities*

Activities

1. Works under overall strategic guidance of CISO/ISSO/Security Program Office(r) and Manufacturing Operations / Process Control to counsel and guide on implementing key cybersecurity approaches and initiatives

   a. Promotes and aligns a unified and cohesive view of the enterprise's IT and OT security approach.

   b. Balances cybersecurity and OT business imperatives (latency, bandwidth, availability, etc.) to keep process automation and control systems running and productive to support manufacturing production activities.

   c. Helps advance alignment and cybersecurity policies.

   d. Ensures secure practices and ongoing security operations are implemented and used to upgrade or integrate legacy operations; produces and implements security specifications and design documents.

2. Optimizes secure manufacturing facilities and communications through the engineering design, development and deployment of IT and OT security and data governance systems using a holistic and agreed-upon approach.

3. Deploys an integrated security framework and infrastructure and works towards an integrated centralized set of security systems and capabilities.

   a. Designs and implements security and data assurance systems, protecting connected assets in business and manufacturing environments.

   b. Provides dual IT/OT cybersecurity expertise and seeks to achieve shared interests during the adoption, execution, and integration of legacy and new systems and production platforms.

   c. Develops and configures applications to interconnect disparate systems (software, data, control, etc.).

   d. Participates in and/or leads pilot programs and/or solution evaluations.

4. Creates security solutions for real time business-level systems and communication networks and performance-sensitive systems:

   a. Applies the aligned policies, procedures, and standards for IT and OT that protect assets and data to specific needs.

   b. Guides/leads the development of applications, systems, and network and physical systems and platforms.

   c. Enables full visibility across both IT and OT networks and inventories.

   d. Creates functional design specs, detailed design specs, process specs and reference frameworks.

   e. Leads/completes: asset inventories; network and endpoint protection efforts; security monitoring and reporting; secure remote and site access management; maintenance and continuous improvement and other security efforts converging IT and OT.

   f. Develops IT/OT project roadmaps and workflows.

   g. Integrates secure approaches connecting equipment, assets, processes, and other sources onto and across networks.

   h. Ensures network and data security, integrity, and access across both IT & OT networks, and between systems by implementing unified policies and security measures.

   i. Identifies new and ongoing opportunities for convergence and integration including evaluation of cybersecurity policies and initiatives and makes recommendations to leadership, governance and compliance sources.

5. Promotes awareness and action while serving as trusted advisor for secure IT/OT convergence both at local/facility level and across functions:

   a. Advocates across IT/OT team members for their shared mission.

   b. Provides coaching and training to IT groups, OT groups, Security Operations Centers, site management teams, engineers, operators, technicians, specialists, analysts and others involved in IT/OT convergence.

   c. Coordinates with third parties and suppliers and is part of any broader IT/OT cybersecurity network for the company.

Section 3: *Competencies*

Risk Analysis and Manufacturing Threat Landscapes	Application Management and Security	Product Security
Security Operations	Cloud/Edge Computing and Security	Personal/Product Edge (Proximity) Computing
Secure Design and Secure Product Management	Automation and Controls	Supply Network Cyber Compliance
Smart Factory Management	Infrastructure Management	Vendor/Partner Integration
Network Management and Security, including Firewall and Network Segmentation	Telemetry and Mechatronics	Regulatory and Compliance requirements: NIST frameworks, standards and guidelines; Manufacturing Profile- NIST 8183; ISA99/ IEC 6244; ISO 27001; DFARS and other contracting/supplier cyber guidelines, etc.
Intrusion Detection	Industrial Controls Security	Risk Mitigation (Business Continuity, Disaster Recovery, Information Security, etc.) Program Management
Systems Management and Security	Cyber-Physical Asset Management	Basic Legal, Compliance and Privacy knowledge
Data and Information Management and Security	Physical Systems and Facility Security	Public Key Infrastructure

This role requires solid to expert knowledge in their representative home arenas of OT and/or IT and high interest in excelling on knowledge and practices for the convergence of IT and OT. Depending on their originating “home domain” or if they are an experienced cross-discipline professional, there are many primarily technical competencies that will contribute to the success of this role. Along with increasing business competencies across the modernized and native cybersecurity, IT and/or OT subdomains listed below should be brought to the role and developed further:

Other general, business and personal competencies include:

- Knowledge of the evolution of IT/OT and ICT in modern manufacturing.
- Demonstrated mutual appreciation for the specific and unique requirements of both informational technologies and environments and operational technologies and environments. Increasing shared knowledge of the dual technologies and operating environments.
- Analytical and problem-solving skills.
- Leadership via influence of distributed teams.
- Ability to clearly communicate technical ideas in business language to varied stakeholders.
- Fundamentals of Technology Transformation and Culture Change.

Cybersecurity IT/OT Integration Engineer

Section 4: *Experience And Education*

Education

Bachelor's Degree or advanced studies preferred in related fields, including industrial engineering, manufacturing engineering, computer science, information technology, cybersecurity, electrical engineering or a related discipline.

Certifications:

- GICSP
- CISSP
- ISA
- CCNA
- CCNA-Security

Experience Profile

- 5-8 years of related professional experience depending on the cyber-manufacturing profile and existing IT and OT maturity.
- Ideally 2 years or more of directly related environment experience: supporting OT/ICS; supporting IT in manufacturing; working and leading cybersecurity related projects.
- Experience with broad issues of increasing digital use and threats in the manufacturing setting (from physical safety to data and asset security; from to automation to AI/ML, IIOT, etc.).
- Commitment to essential IT/OT convergence mindsets: 'Security First, 'Safety = Security and Security = Safety', 'Stronger Together', 'Secure Design and Smart, Secure Manufacturing' and other beneficial core beliefs.
- Experience that crosses a) technical architecture interpretation and use with b) engineering specific solutions and c) promoting local change.
- Experience with cybersecurity policies, processes, tools and methods.
- Experience securing cross-domain IT/OT communications and pathways to/from business networks, suppliers and other third parties, and wide area networks internal and external.
- Demonstrated business acumen connecting IT/OT/Cybersecurity to core business value.
- Ability to engage all levels of employees, leadership, and board members; and ability to work across functions and geographies.
- Experience in applying both structured and discretionary judgment.
- Personal reputation for maturity, objectivity, and high standards.

Secure Design Product Life Cycle Manager

Role Title: Secure Design Product Life Cycle Manager

Role Impact: Keystone

Summary Scope

Refrigerators serve to upload Instagram photos when a teenager's phone dies; toilets perform in-home medical lab tests; car seats detect a baby's weight and adjust seat height and straps; autonomous geo-spatial military weaponry run by remote AI shifts geo-political seas in an instant. Our future is full of those smart devices connecting along with billions of other 'products' to networks while we and future generations of customers entrust manufacturers with their access, data protection, privacy and performance. Manufacturers and their supply chains invest billions of dollars in the research, design, and production of those same products in the first place. They need to protect their intellectual property, their physical and digital assets, and their employees before and after those refrigerators get into a home and those defense systems activate in the military theatre.

Who will manufacturers and customers rely on to be the working 'human drive gear'– with a bit of the long view and the end in mind - to shine the light on security along the way for both the manufacturing process and the performance of the product? The Secure Design Product Life Cycle Manager is a product-value-driven working visionary, orchestrator, advocate, and point of assurance for the secure design and development of a manufactured product. No longer is it enough to use a bench test checklist or wait until the end to run the gauntlet of a reliability certification lab like decades past. Gone is the assumption that IT or some other technical team will take care of "all that cyber stuff" – thinking by putting it the project plan it will be enough for the product manager or the customer, now or in the future. If it's not secure, it won't endure is a new reality product adage. Gone is cybersecurity as an after-thought or something to catch in production if not in testing. The Secure Design Product Life Cycle Manager and related secure design programs are all about avoiding security issues in the first place.

Today's modernized Product Manager rises up to serve a significant fuller-cycle role with a cross-domain view when it comes to securing digital product design and IoT product development. Product teams and managers can't dismissively pawn security off; they can't make it only an engineering or compliance or user's post-purchase problem. And who is better positioned literally to establish and monitor a hybrid business and technical security commitment across the cycles? Who is already a grand master of managing multiple stakeholder needs? Importantly, this Secure Design Product Life Cycle Manager is one of the few roles in the increasingly hybrid business-technical manufacturing environment that can take the long view of both the human and commercial value users get from products. These managers understand that product management's value to the business is to bring product value to the buyer: value in that the product does what it was promised to do – and maintains privacy and performs as reliably as intended, and does that at the user/customer's intent, and only their intent.

The Secure Design Product Life Cycle Manager will work closely across the business and supply chain to bring the right experts and practices to designing secure performance into products and doing it in secure ways.

Secure Design Product Life Cycle Manager

Outcomes

1. Higher value product strategies and designs.
2. Broader organizational adoption of “secure from the start” and other cybercritical business orientations.
3. Longer-term views of the product value and the role that security plays in product integrity and product performance.
4. Increased trust in the product.
5. Increased security of the process.
6. Improved brand and product integrity and reliability.
7. Better oversight into security related build steps and their impact on roadmaps and timelines.
8. Enable company to mitigate risks and address evolving threat landscapes by using the appropriate and most advanced technologies and security practices while considering product and market factors.
9. Improved communications between product design and technical team members.

Domain Profile

Business Alignment and Governance

Business Case Contribution

The Secure Design Product Life Cycle Manager is chief visionary, orchestrator, advocate, and assurance point of coordination for the secure design and development of a manufactured product. This key cyber role brings business impact by contributing to:

- Long term sustainable product value strategies where security is a demonstration of brand value and commercial worth.
- Establishing a unique cross-functional commercial view; the role lives in the intersection of Business, User Design, Security and Technology.
- Continuity across program efforts; minimized cost and rework,
- Minimizing impact by anticipation and address of security vulnerabilities.

Section 2: *Key Responsibilities*

Activities

Overall Cross-Functional Product Strategy and Management

1. Serves a chief product design and development advocate for secure product design across every stage of the product lifecycle and maintains company product design commitments to implementing 'Secure from the Start' and 'Secure Design' principles and practices.

   a) Primary lead practitioner from the business side who operationally raises the profile of secure product life cycle management.

   b) Accountable for the cybersecurity aspects of Product Strategy and the ongoing success of the products from launch through the end-of-life, contributing to meeting overall product strategy, relevance, profitability, and quality measures.

2. Co-owns, designs and drives product or portfolio level Internet of Things (IoT) cybersecurity solutions at the product or product portfolio level.

3. Works closely with other product or portfolio technical and business leaders and the many teams involved in product design and development: user product design, user experience design, engineering teams, industrial (hardware/device) design, SecDevOps, embedded developers, IT/OT, developers, front-end developers, QA, integration team, and security testing and others.

4. Works with a cybersecurity economist to be able to make a financial case for the security process and product investments.

   a) Develops a cybersecurity focused roadmap.

   b) Manages the product roadmap and an adjunct product security roadmap for its entire life-cycle from concept, proposal, planning, development, launch, release and post-sale operations.

   c) Earns buy-in from company stakeholders for the trade-offs and requirements of a secure product from customer experience teams, operations, production, cybersecurity, compliance, field support, supply chain, and others.

Product Security

1. Performs various activities across risk and threat analysis, security architecture, security evaluation and testing, vulnerability management and other primary product security focused areas.

2. Proactively positions product/customer focused approaches to firmware updates and security patches.

   a) Manages triage and prioritization of tasks/issues as required by the DevOps and testing teams.

   b) Keep process and product security as a visible workstream with related roadmap and workplan.

3. May also work with Secure Configuration teams to secure purchased applications and solutions.

4. Projects end-of-life cyber vulnerabilities and addresses through risk mitigation strategies, technology designs and product improvement or management life cycle decisions.

5. Works with the various field teams to appropriately map out customer use cases and requirements.

6. Creates and maintains an updated understanding of IoT threat landscape and building product collateral to communicate how to deliver solutions.

7. Functional requirement gathering, development and maintenance of security-oriented PLM functional specifications in synergy with the program or project team.

8. Defines product features, functions and data flows that represent security vulnerabilities across the IoT Technology Stack.

9. Performs, facilitates, and oversees IoT security testing.

Product Design and Development Compliance and Transformation

1. Effectively communicates progress on compliance related activities and/or transformation of broader product management towards Secure by Design goals, demonstrating accountability for functional and business objectives.

   a) Interacts with, influences and negotiates IoT security requirements with internal and external parties.

   b) Reviews and approves cybersecurity activity to ensure compliance with information and cybersecurity policy and best practices.

   c) Provides input and recommendations on cybersecurity policy, risk, and overall security best practices concerning IoT.

2. Participates in and co-assures ability to be able to pass internal and external security audits.
3. Practices and coaches others on design thinking and agile techniques to assure security in the development and operational lifecycle.
4. Serves as primary champion and agent of Secure Design in practice and as part of the culture.

   a) Breaks down silos between business and technical teams.

   b) Maintains status and communication with internal and external stakeholders; routinely presents with other program and portfolio leaders to executives, sales teams, technical conferences.

   c) Provides thought leadership on innovation, customer experience, product strategy and future direction of the market.

   d) Balances pressures from the many involved teams and maintains long-term product security value positions in both decision making and everyday actions.

Section 3: *Competencies*

Representative Capabilities

This role requires solid to increasingly expert knowledge in both business and technical areas. It is a hybrid role and relies on strong cross-functional interactions and workshare with others to deliver on secure modernized Product Management capabilities.

The core responsibilities of a 'generic' Product Manager still apply and are not addressed here. This role profile and the competency areas listed below are those in addition to the primary Product Manager role competencies; these highlight competency areas more specific to Cyber[ME].

Design Thinking	IoT Product Strategy
Risk Analysis and Supply Network/Procurement Threat Landscapes	Product Security and related general and industry privacy and protection requirements and expectations
Security Operations	Supply Chain and Procurement Legal, Compliance and Privacy Knowledge
Secure Sourcing for Secure Design and Secure Product Management	Supply Network Cyber Compliance
Smart Contracts	Smart Contracts
Risk Mitigation (Business Continuity, Disaster Recovery, Information Security, etc.) Program Management	Regulatory and Compliance requirements: NIST frameworks, standards and guidelines; Manufacturing Profile- NIST 8183; ISA99/IEC 6244; ISO 27001; DFARS and other contracting/supplier cyber guidelines, etc.

Other general, business and personal competencies include:

- Thorough knowledge of product management (see note above).
- Equally comfortable with addressing or interacting with both technical and business-oriented workstreams.
- Increasingly expert understanding of related industry or sector cybersecurity related regulations.
- Curiosity about and appreciation of the consumer/customer value to build in security at all technology stack levels.
- If more business and/or pure product oriented, able to be conversant in the technical solution stack the product uses, can hold their own in discussions with technical areas while enabling mutual accountability.
- If more technically oriented, increasingly able to broaden strategic product management capabilities, particularly multi-stakeholder and cross-functional value-focused designs and management.
- Demonstrated ability to develop and manage broader market focused business case positions.
- Analytical and problem-solving skills.
- Leadership via influence of distributed teams.
- Ability to clearly communicate technical ideas in business language to varied stakeholders, and vice versa.
- Practiced in increasingly larger or more complex cross-functional project management.

Secure Design Product Life Cycle Manager

Section 4: *Experience And Education*

Education

Degrees
BS or MS in Computer Science, Computer Engineering, Product Design/ Development, Business Management or related business or technical area

Certifications:

- Certified Scrum Product Owner (CSPO)
- PMI-Agile Certified Practitioner (PMI-ACP)
- Certified Product Manager Credential – AIPMM
- Certified Innovation Leader Credential (CIL)

Experience Profile

- 5+ years of product management or equivalent experience with a complex technical product with deep security requirements.
- Experience designing and building IoT/connected software and or device products.
- Demonstrated success as a product manager, technical product manager or design or development lead on a fast-paced, growing team.
- Demonstrated stage presence and comfort delivering large group talks.
- IoT thought and technology leader with a passion for delivering world class customer experience.
- Respect for Manufacturing commitment to delivering the best products yielding highest value without compromising personal or product security.
- Experience in the security testing of new systems or the vulnerability assessment of existing systems to meet business requirements, changing needs, or newer technology.
- Ability to work with multiple levels of management across Technology and the supported Business Units.
- Excellent written, verbal communication and presentation skills.
- Demonstrates a craving for continuous improvement, thorough understanding of new technology innovation and its application.
- Strong technical competence up and down the technology stack - user interface, applications, communications, infrastructure, database, storage, etc.
- Experience in Agile methodology and leadership for cross skilled teams.
- Strong desire and aptitude for continuous learning and keeping abreast of new and emerging technology and cyber threats/vulnerabilities.
- Ability to write, promote, and execute business cases.
- Passion for keeping the organization, its products, processes and people safe, secure, and reliable.

Supply Network Cybersecurity Compliance Manager

Role Title: Supply Network Cybersecurity Compliance Manager

Role Impact: Keystone

Summary Scope

Manufacturers face supply chain cybersecurity compliance concerns from two dimensions at the same time: as suppliers or contractors to others, and as customers themselves relying on vendors to enable their operations. Supply networks broadly present manufacturers with many security vulnerabilities: they have no direct control of the security measures of their supply chain partners; they can face increasing regulations and standards both for internal controls as well as controls in their customers' environments; and the nature of manufacturing and procurement processes are becoming more automated and distributed, requiring equally automated and decentralized yet well-managed and legally binding controls. Who will be most aware of these risks and call to action solutions to address gaps and protect the various stakeholders in today's dynamic supply networks? Who can increase visibility into the network's required internal and external security practices, assess overall cyber risks and capabilities, require improved cyber hygiene, and partner with others to close gaps and mitigate risks? Who will ensure compliance of the supply network with company policies, laws, government regulations, government contracting programs, and overall supplier-industry-geo complexity?

The Supply Network Cybersecurity Compliance Manager brings experience in several areas to this often sub-optimized role: risk management, procurement management, supply chain management, cyber governance and security technology. While responsible for compliance, this role also must deliver on improving the honest collaboration between supplier and contractor communities and the manufacturer. The Supply Network Cybersecurity Compliance Manager role is established to focus on security compliance and the performance improvements that can come from secure practices. This role will lead a team of cyber analysts/auditors and work with individuals from a variety of technical and functional disciplines to guide cyber compliance across business areas and supplier domains. They may also be highly involved in BC/DR/IS related tabletop exercises and facilitate or practice with designated suppliers.

This role may also be a related contract risk and procurement specialist on the team as a contracted expert but at some scale, this role would likely be internal. Whether internal or external, under the general direction of the Chief Information Security Officer, Chief Purchasing Officer, and Supply Chain executives, the Supply Network Cybersecurity Compliance Manager performs as a modernized, higher-value compliance leader whose impact goes beyond "captain of the box-checking, form-filling, audit-happy team". This role is also a proactive implementer of cybersecurity programs that improve operational and business performance and maintain competitiveness while being conscientiously compliant.

Outcomes

- Improved contracting compliance performance.
- Competitive advantages from secure supplier designations or certifications.
- Mitigation of vulnerabilities and risks that could lead to cyber incidents and breaches, fraud, and other damages from uncontrolled network or data access.
- Achievement of supply chain transformation goals relating to innovations in secure practices and increasing supply network compliance.
- Preventative practices to lower the damages associated with loss of intellectual property or client sensitive data.
- Lower unnecessary costs.
- Increased schedule efficiencies.
- Increased resilience (as measured by response and/or recovery metrics).

Supply Network Cybersecurity Compliance Manager

Domain Profile

This role aligns with the Supply Networking and Partnering domain. It maintains a close alliance with the Compliance, Forensics and Legal domain, and works under overall direction from the leadership and governance roles in that domain.

Business Case Contribution

The primary business case contribution of this role is to maintain a robust supplier network while identifying cyber risks needing mitigation. This role improves awareness of the cyberhealth of suppliers and partners, ensures their awareness of company cybersecurity policies and requirements, and, with improved visibility into the supply network, clarifies blind spots and assesses vulnerabilities from a security perspective. It also escalates trends and issues to cross-functional leaders and together, mitigates the risks and threat landscape through increasingly innovative co-developed supply network standards and enablement solutions.

This role ensures applicable regulations are met, including internal and external auditing in related compliance areas inclusive of: DFARS, NIST and other cybersecurity focused guidelines, ISO, General Data Protection Regulations (GDPR), payment card industry (PCI) requirements and other financial compliances if applicable (e.g. Sarbanes-Oxley), quality controls and other compliance areas as required per industry, segment and defense acquisition participation status.

Section 2: *Key Responsibilities*

Activities

1. Drives contractor/supplier/company performance by leading the development and implementation of supply chain cybersecurity governance, policies, and procedures.
   - Leads the development and ongoing maintenance of standards for both internal procurement related cybersecurity and third-party and supply chain cybersecurity and health.
   - Constructs compliance and eligibility frameworks to identify covered vendors and business teams to meet compliance standards, regulations, and practices. Continuously manages, maintains, and updates supply network Policies and Standards, and ensures procedures include information and cybersecurity.
   - Manages oversight of end-to-end supply chain compliance processes and relationships. Works to gain alignment and maintain agreed upon principles/standards that optimize the network cybersecurity resilience.
   - Contributes to the remediation and repair of non-compliant systems, software, and technologies across functions and regions.
   - Acts as primary compliance liaison between the business and network of suppliers, vendors, and partners to ensure alignment with business objectives, compliance needs, company-specific Supply Network Strategy and business-technical transformation programs.
   - Participates in benchmarks with like companies and other entities to test the cyber compliance program.
2. Maintains risk and compliance performance for strategic and/or required contractor or acquisition programs. (e.g., Cyber DFARS, SOX, Fedramp, CMMC, etc.).
   - Implements proactive, ongoing and post-performance cybersecurity certification and audit programs. Oversees application of risk assessment programs, monitors appropriate strategy development, maintains metrics and reporting.
   - Supports internal and external audits of contracts for inclusion and enforcement of contractual cybersecurity controls and requirements. Prepares, responds and remediates action plans for audit non-conformance when on the part of the company, contracting business group, or company purchasing/ procurement.
3. Provides feedback to those managing the company's overall risk model, and in coordination with other functional teams (e.g. HR, Finance, IT, Engineering), establishes plans to securely manage the cyber risks associated with business activities and technical systems.
   - Communicates risks, vulnerabilities, and compliance levels to leadership, enabling balanced risk decisions. Ensures all critical procurement and supply network management applications have Business Continuity/Disaster Recovery plans as part of compliance requirements or mitigation approaches.
   - Resolves issues arising from non-compliance by developing solutions that are acceptable to regulators, that account for budget constraints, and that are technically feasible. Participates as needed in all response, recovery and investigations.
   - Provides adequate security on their internal networks to protect Covered Defense Information (CDI) and those that are required to flow DFARS safeguarding and key reporting clauses to subcontractors.
   - Participates in any other related company cyber compliance and risk management efforts: Global Cybersecurity Risk Management including Global Threat & Vulnerability Management, Global Insider Threat Management, Data Governance, Cloud Security, Supplier Risk Management, Global Cybersecurity Policies, and InfoSec Governance & Compliance.
   - Directs data and documentation management initiatives to collect and maintain supplier information that could assist in future forensic analysis and cyber event response.

4. Manages the compliance function as a continuous improvement and enablement function for the company and its suppliers. Establishes a culture of enablement that can be observed in the interactions between internal staff and with customers when balancing the protection of the corporation with business needs. Shifts from compliance to benefits/ incentive mindset.
    - Serves as a key cybersecurity change advisor for the supply network: continuously advances subject matter expertise in supply network and cybersecurity, as well as in specific product/process areas.
    - Manages increased use and sharing of integrated business continuity or resiliency approaches and tools, including increased shared data, forecasts, and other digital decision support systems.
    - Sponsors supply network/procurement cybersecurity training and awareness across the enterprise and into supply networks.
    - Encourages and supports providers/vendors/suppliers to collaborate and improve collective performance and to support their connections through available digital platforms, shared data, and community connections
    - Supports and manages knowledge bases, libraries, and other collective resources on and across the supply network and leads the drive for increased knowledge and capability across the supply network.
5. Discovers and builds relationships with new and/or innovative sources of potential resource supplies or services
    - Assesses emerging technologies and their impact to supply chain compliance, security guidelines and security innovations. Stays up on emerging industry security trends and threats to help proactively improve the security posture. Identifies and brings forward innovations in secure supply chain evolution.
    - Works with other legal, business and technical roles to determine the potential use/expansion of Smart Contracts as both an operational improvement and a secure mode of managing contractual transactions, steps, and milestones.
    - Understands applications of blockchain and other distributed ledger technologies for identify management, secure logistics management, material/product tracking, billing and payment and other supply network transactions.
    - Explores the security pros and cons of 3D printing at locations that expand the “build” footprint and impact supply chain logistics as a supplier or contractor.

Section 3: *Competencies*

Risk Analysis and Supply Network/Procurement Threat Landscapes	Product Security
Security Operations	Supply Chain and Procurement Legal, Compliance and Privacy Knowledge
Secure Sourcing for Secure Design and Secure Product Management	Supply Network Cyber Compliance
Smart Contracts	Vendor/Partner Integration
Risk Mitigation (Business Continuity, Disaster Recovery, Information Security, etc.) Program Management	Regulatory and Compliance requirements: NIST frameworks, standards and guidelines; Manufacturing Profile- NIST 8183; ISA99/IEC 6244; ISO 27001; DFARS and other contracting/supplier cyber guidelines, etc.

Representative Capabilities

This role requires solid to increasingly expert knowledge in business and technical areas. It is a hybrid business and increasingly business-technical role, and relies on strong cross-functional interactions and access to more specialized:

Other general, business and personal competencies include:

1. Thorough knowledge of purchasing and procurement management.
2. Increasingly expert understanding of related industry or sector regulations.
3. Demonstrated experience of viewing compliance as an enablement strategy versus viewing compliance as a low-value, routine, and obligatory function.
4. Curiosity and ability to build an innovation culture while establishing and requiring structure and compliance.
5. Analytical and problem-solving skills.
6. Leadership via influence of distributed teams.
7. Ability to clearly communicate technical ideas in business language to varied stakeholders, and vice versa.
8. Practiced in business process and/or technical transformation program management.

Supply Network Cybersecurity Compliance Manager

Section 4: *Experience And Education*

Education

Bachelor's degree in Cybersecurity, Supply Chain Management, Computer Science, Computer Engineering, Legal Studies or a related business or technical field (Master's / graduate degree preferred)

Certifications:

- CISSP
- CISM
- CEH
- CSSP
- CCSP
- AWS CSA
- CompTIA Cloud
- CCSK

Experience Profile

1. Five (5) + years of professional experience in a technical and/or supply chain role required; 3+ years of professional experience in a Cybersecurity or security-related role preferred.
2. Commitment to essential mindsets: 'supply chain resiliency versus management', 'security first', 'regulatory/ compliance as a capability', 'stronger together', 'secure design and smart, secure manufacturing' and other beneficial core beliefs.
3. Experience with cybersecurity policies, processes, tools and methods.
4. Demonstrated business acumen connecting Supply Chain Cybersecurity to core business value.
5. Ability to engage all levels of employees, leadership, and board members; and ability to work across functions and geographies.
6. Experience in applying both structured and discretionary judgment.
7. Personal reputation for maturity, objectivity, and high standards.
8. A passion for supply chain technology, risk management and strategic enablement.
9. Ability to obtain and maintain a DoD clearance as required.

Manufacturing Cybersecurity Systems Operator

Section 1: *Job Role Identifier Section*

Role Title: Manufacturing Cybersecurity Systems Operator

Role Impact: Pioneer

Summary Scope

Transforming to a smart manufacturing factory means integrating security practices and technology into plant processes via interconnected machinery, automation, data driven operations, communications, and software. The systems and roles that protect these increasingly digital operations and resources are essential. Of these roles, who can assist determining what and if something changed from a cybersecurity perspective – a configuration setting, firmware version, new port opened, new device connected to the network, etc.? Who is a junior part of the prevention, detection, and resolution capability when there is a production outage that is impacting the plant's ability to make product? Keeping the human, physical, and digital assets secure is the responsibility of both the operating technology and information technology areas and many job roles at all levels that ensure secure operations.

So, which of these roles is the entry-level operations role who is the "on the ground eyes, ears and voice" for IT (Information Technology) and OT's (Operational Technology) shared interests, closest to the operating environment and its security protections? The Manufacturing Cybersecurity Systems Operator has a primary focus to monitor, record, detect, and report security system performance and functions. Who is the role that may overlap into other adjacent cyber roles as experience and skill increases, but usually does not take on tasks associated with production or assembly operations? The Manufacturing Cybersecurity Systems Operator is not a conventional equipment operator but a systems operator who uses security software and processes for protecting factory floor automation and control technology assets, information, processes, and employees. On a daily basis, these systems operators watch and report the security status in diverse industrial and product settings: they monitor and escalate OT and IT concerns crossing plant automation and control platforms, components, IoT devices, access points, network connections, and more.

Who can be a bridge with IT and help advance old paradigms of plant isolation, creating better practices and improved performance? As an entry level cybersecurity "utility player", these System Operators can more broadly support plant engineering, production management, quality and ICS by leveraging varying worker backgrounds and experiences. And who then can help to revert that change back so that the process is back to operating at a functional, productive state?

This Manufacturing Cybersecurity Systems Operator role may be an internal role of a manufacturer and may have other IT and/or OT responsibilities; it also may be a role employed at a manufacturer, through a third-party vendor, systems integrator, or factory automation technology provider. The scope of systems that an operator works with can be proprietary or third-party, including across multiple manufacturers, software packages, network architectures, and/or industrial components. Systems and technologies under the umbrella of OT that relate to this role are Industrial Control Systems (ICS), SCADA, DCS, PLC, etc.

As experience increases, this role - which can start as a Level I and progress to a Level II or III operator - may add analysis and detection tasks, engage more deeply with related functions, and participate in cyber testing and exercising. Also, this role may serve as an incident SME if a specific threat, incident or breach occurs and the operator is needed for further response, recovery, and restoration.

With numerous available certifications and training programs available to learn and practice, and then supported on-the-job by technology and further training, this role is a solid opportunity to bring or transition diverse backgrounds into both the manufacturing and cybersecurity environment, a win-win for the workforce and manufacturers.

Development of this Success Profile was made possible by a grant from the Siemens Foundation

Manufacturing Cybersecurity Systems Operator

Outcomes

From a core business perspective, this role produces or supports the production of these valued outputs:

- Reduction of cyber threat risks and improved defenses for Industrial Control zones and production and product assets.
- Increased cyber compliance.
- Realization of the same security benefits for OT that are enabled for other business and administrative IT systems.
- Ensured confidentiality.
- Protection of the control logic; first line monitoring to avoid changes or improper communications with OT systems without proper procedures or authority.
- Improved prevention, detection, and recovery efforts.
- Safeguarded device, component, process, and control logic and configuration data.
- Lowered production time stoppage due to improved incident response and recovery.
- Increased timeliness and accuracy of version control.
- Maintained safety.

Some technology or production stakeholders may connect this role to the notion of 'Shadow IT' - the classic term for where a line of business (not central IT) purchases, implements, and uses new tech for its own processes. Shadow IT presents issues when it's a symptom of disconnected tech strategy and operations. Here it is 'shadow IT' in the best of both worlds as this role is one that formalizes the system operations essential to manufacturers converging OT and IT. It is core to success that this role is both IT-oriented (systems use, monitoring information and reporting) and OT-oriented (direct and deep interaction with the cybersecurity systems operations on the plant floor).

Compliance Requirements and Employer Profile

Federal agencies including the Department of Defense (DoD) have put implementing strong cybersecurity practices into every aspect of production and procurement as a top priority on their list of critical activities. In this effort, the Office of the Under Secretary of Defense for Acquisition and Sustainment has created the Cybersecurity Maturity Model Certification (CMMC) which will require a Third-Party Assessment Organization (C3PAO) to certify applicable defense contractors participating in the DoD supply chain. CMMC accreditation builds upon existing regulation (DFARS 252.204-7012) by adding a cybersecurity verification component. Businesses providing products and/or services to the DoD must prepare for compliance with CMMC guidelines in anticipation of the requirements being included on future RFPs, anticipated beginning in early 2021. For additional detail on CMMC requirements, visit https://www.acq.osd.mil/cmmc/.

Domain Profile

This role aligns with Operating Technologies & Convergence domain and the Automation & Controls subdomain.

Development of this Success Profile was made possible by a grant from the Siemens Foundation

Manufacturing Cybersecurity Systems Operator

Business Case Contribution

The true value of this role is in the routine completion of convergence and shared cyber solutions practices most closely associated with plant and physical production and processing equipment. These operators will make their everyday work the integrated security operations and systems use. This role helps ensure accurate information is delivered to people, machines, switches, sensors and devices at the right time and in the best format; and helps to minimize complexity and lower the operating costs of siloed IT and OT.

From a talent perspective, this role provides human capital value in meeting workforce objectives such as:

- Providing an opportunity to place IT candidates/professionals in the core business and production environment of manufacturing.
- Offering an opportunity to diversify the cyber workforce with candidates from varied incoming experiences.
- Serving as an example of modern manufacturing and factory of the future opportunities and messaging.
- Lowering academic degree requirement enhances community and technical college connections with manufacturing employers for a steadier influx of new workers with new skills.
    - Note: This role may be a suitable consideration for an Industry-Recognized Apprenticeship Program (IRAP), designed to enhance the workforce in rapidly-expanding sectors of the economy, such as cybersecurity, by providing individuals with opportunities to obtain relevant workplace knowledge and progressively advanced skills.
- Creating a potential career pathway opportunity through reskilling for military veterans and professionals with IT and cybersecurity training and experience, as well as relevant security clearances, into the manufacturing workforce.
- Serving as an excellent feeder role into other areas of cybersecurity, based on its generalist exposure to, informational technologies, operational technologies and the convergence between them for improved cybersecurity performance,

Development of this Success Profile was made possible by a grant from the Siemens Foundation

Section 2: *Key Responsibilities*

Activities

Summary Activities:

This role contributes to the achievement and maintenance of confidentiality, integrity, and availability of production/processing controls and communications that guard physical, financial, human, and customer assets.
A Manufacturing Cybersecurity Systems Operator routinely:

1. Performs security systems operations tasks on the plant/factory floor as this role's primary day-to-day work environment and also works at SOC or ICS command center systems monitoring stations and/or a remote operations console.
2. Interprets and translates system operations requests into operational duties and tasks.
3. Operates and maintains diverse facility and process specific systems and platforms working between hardware controllers, sensors, and related communication protocols connecting to business and enterprise software across internal and external networks.
4. Interacts with many other OT roles and IT roles as convergence efforts and solutions increase; supports plant engineering, quality, production management and other key manufacturing functions.

Additional detailed tasks aligned to the NIST Cybersecurity Framework stages include:

Identify

1. Applies and improves asset inventory tracking and knowledge of the asset/device/equipment/system layout
2. Assists with creating and managing any exceptions to cyber security standards or system usage/configurations as required.
3. Ensures all work fits within the broad cyber systems architecture while meeting local facility operational functions and goals.
4. Understands that any local variances would impact the ability to scale the system or extend it to other facilities.

Protect

1. Understands, applies, and improves assessments of vulnerability and risks; updates the risk profile from networks and or IT devices to the controls level.
2. Maintains, tunes, and upgrades related systems and software.
3. Monitors preventative controls in place to enforce communication patterns; observes data on the industrial processes and protocols to ensure and enforce authorized communication between devices and/or networks
4. Assists in establishing and defending ICS security zones with appropriate countermeasures.
5. Supports and implements coordinated efforts with supply chain on remote access, data sharing and security process calibration.

Development of this Success Profile was made possible by a grant from the Siemens Foundation

1. Supports the enforcement of expected communication patterns or data flows with network segmentation.
2. Supports acceptable changes to varied devices such as controllers, HMI's, RTU's, engineering workstations, operator workstations, routers, switches, databases, and firewalls.
3. Uses or maintains older and/or proprietary software with heightened awareness of existing and previous changes, workarounds, or undocumented patches.
4. Schedules and completes maintenance and patch activities in a way that minimizes production impacts.
5. Monitors data transfer performance between automation, production, and administrative systems with business systems (MES, ERP, etc.).
6. Maintains system reference information and documentation.
7. Maintain system logs and other reports and records.

Detect

1. Applies a standardized set of security product and system requirements and produces metrics to report performance against those requirements.
2. Detects security risks, responds to product security incidents and works with customers, plant engineers, and other related functions regarding security issues.
3. Monitors system operations and reacts to events in response to triggers and/or observations of trends or unusual activity.
4. Monitors device data flows, what is expected and what is abnormal.
5. Monitors and address real time variances and alarms.

Respond

1. Responds to alarms and complete initial analysis, response, and notification; coordinate and escalate as needed and per cyber and plant management guidelines.
2. Reviews and processes appropriate incident tickets.

Recover

1. Contributes to roadmaps for cybersecurity actions and improvements.
2. Assists with security code reviews.
3. Assists and supports Engineering, ICS, IT, IS, ESH, etc. and fuller life cycle activities related to planning, improvements, and communications of recovery activities.

Development of this Success Profile was made possible by a grant from the Siemens Foundation

Section 3: *Competencies*

Representative Capabilities

This role is often a generalist role, encompassing a range of tasks, responsibilities, and competencies of a cybersecurity systems operator. As a transitional role requiring 2 years or less of additional training in related IT/OT and cyber areas, this is an excellent entry point into cybersecurity for individuals who may not possess a four-year degree but have sufficient and appropriate experience, training, and/or education to begin an operator progression.

(See also the Experience and Education Section 4 and the connections to progression levels of the Cybersecurity Operator Role (Level I, II, and III).

At a minimum, this role at entry levels requires:

1. Fundamental knowledge of production and processing activities and industrial controls and communications.
2. Foundational knowledge of cybersecurity principles, processes, and practices.
3. Familiarity with related cybersecurity regulations, compliance and standards (industry, company, supplier, customers).
4. Increasing hands-on experience with applicable systems and interfaces.

The role also requires increasing levels of knowledge and skill in the application of these competencies:

Systems and Equipment Monitoring, Troubleshooting and Reporting	Cyber-Physical Asset Management
Routine Systems Testing and Maintenance	Industrial Controls Security
Facility and Process Security and Operations	Supply Network Cyber Compliance
Network Security and Operations	Knowledge Management and Analysis
Wireless Network Testing	Incident Handling & Analysis
Intrusion Detection and Prevention	Regulatory Compliance & Audit
Automation and Controls	Basic programming proficiency of PLCs, HMIs, and SCADA systems

Development of this Success Profile was made possible by a grant from the Siemens Foundation

Other general, business and personal competencies include:

1. Drive and eagerness to learn with a strong interest in expanding personal cybersecurity skillsets.
2. Increasing knowledge of plant production/processing information, automation and controls environments, and impacts of related physical and digital security concerns.
3. Appropriate and necessary human and environmental safety knowledge and training for particular plant/operational environments.
4. Customer experience mindset for representing both IT and OT concerns; curiosity and ability to bridge production and security concerns and opportunities.
5. Increasing capability in clearly communicating related technical issues and operations in business language to various stakeholders, and vice versa.
6. Ability to work independently and collaboratively.
7. Strong verbal communication skills.
8. Attention to detail and troubleshooting.

Section 4: *Experience And Education*

The Cybersecurity Systems Operator role is structured as a skilled technical worker role also referred to as a "new-collar job," or "middle-skill job." It requires certain technical skills, knowledge and experience but does not necessarily require a four-year college degree (or an extensive cyber or industrial work history) to enter. Over time and with expansion, the role can work into both higher-level operator roles and other professional roles, some of which will require a four-year degree. At the onset of entering the Operator progression, apprenticeships and other high-simulation education and development experiences will be essential to early success for this role due to its overall high degree of applied, hands on responsibilities.

Depending on the cybersecurity and plant automation profile of the IT/OT environment where the role would be employed, multiple position levels of the operator role exist for advancement. This overall profile is directed initially at the Operator I level as a transition role for production or industrial controls workers interested in more technical careers or other new(er) to cyber work candidates with diverse backgrounds supplemented with appropriate education and/or certification.

Most duties, outputs, and value in the profile would also hold for an Operator II and III level. Increasing independent responsibility and broadened proficiency in areas of security operations and team coaching and/or customer responsibility, support to other IT, OT and plant operations or network security could come with progression. As a result, the education and experience needs will vary for the Level I, II and III Cybersecurity Systems Operator role.

Development of this Success Profile was made possible by a grant from the Siemens Foundation

Manufacturing Cybersecurity Systems Operator

Education

Level I:

Entry-level to Intermediate-level education and or demonstrated training or work experience program completion:

- Minimum high school diploma or GED required.
- Completion of Cyber Systems Operations Initial Skills course, background investigation and Basic Military Training if military transitioning to civilian roles.
- Cybersecurity Operations Apprenticeship or equivalent hands on experience and development.

Level II:

Intermediate-level community college or equivalent education and or demonstrated training or work experience program completion.

As above with Associates Degree and hands on experience and development required;

Bachelor's degree preferred (Cybersecurity, Manufacturing Automation Engineering, Computer or Information Science, Computer Engineering, or a related technical field).

Level III:

Continuing education and/or demonstrated training or work experience program completion.

As above, with Bachelor's degree highly preferred and often required, continuing hands-on experience. (Cybersecurity, Manufacturing Automation Engineering, Computer or Information Science, Computer Engineering, or a related technical field).

Certifications

These are representative certifications that may be desirable or required for particular employers. Some certifications are vendor-specific, and some are vendor-neutral; some may have specific experience requirements and others do not require specific experience requirements. All of them with as much hands-on or applied practice will be important.

	Level I	Level II	Level III
Micro-credentials in related areas (see competencies for topic areas)	●	●	●
Formal Certifications such as:			
CISSP			●
CISM			
CCT, CCNA	●	●	●
CSSP			●
CCSK			●
SSCP		●	●
CompTIA Sec+, NW+	●	●	●
CCA, CCST or related general industrial controls certifications	●	●	●
GICSP, GRID, GCIP or other Industrial controls security certifications	●	●	●

Development of this Success Profile was made possible by a grant from the Siemens Foundation

Manufacturing Cybersecurity AI Engineer

Section 1: *Job Role Identifier Section*

Role Title: Manufacturing Cybersecurity AI Engineer

Role Impact: Producer

Summary Scope

Technology is reshaping manufacturing – and specifically artificial intelligence (AI) is improving many manufacturing life cycle points: speeding up parts inspection, enabling predictive diagnostics, optimizing staffing and supply chains, and more. Advanced technologies - especially those like AI - are both progress and pain. They enable the manufacturing ecosystem to achieve value not seen before but also give bad actors more tools to attack a wider range of manufacturing assets from trade secrets to customer devices and after-market services. New combinations of human, technical, and business capabilities are needed to put up the good fight. If employers, cyber tool developers, and service providers combine the capabilities of AI and human cyber guardians with specific knowledge and needs focused on manufacturing vulnerabilities, manufacturers may stay ahead or come out on top instead of increasingly being a top target for cyber disruption and damage.

- So, which role can bring to manufacturers an engineer's rigor, a technologist's passion and portfolio of emerging AI/ML tech, and an evangelist's dedication to security solutions, including natural language processing, human language technologies, multimodal sense-making, and other AI/ML based approaches?
- Who can help build security systems, applications, and other tools harnessing massive signal and event triage to help security operations analysts and other target users with instant insights that avoid alert fatigue and disconnected data? Who can help significantly reduce breach impacts and response times?
- Who can help envision and design applications and systems that go beyond defining the conventional and explicit agents/vectors/targets that we know to detect and accelerate awareness of unknown or implicit threats?
- And which role may have a significant influence on other future cyber role redesigns as AI shifts or expands the current set of human-performed cyber tasks?

For all of those opportunities, it is the role of a Manufacturing Cybersecurity AI Engineer.

An image to consider when thinking of this essential role is a three-part picture that should have a cobot (a human working hand in hand collaboratively with robotics), a cloud and a funnel. Think of the cobot standing in for the production and processing environment and all its direct and indirect assets for manufacturers including employees, facilities, processes, and finished products; think of the cloud symbolizing all of the data and digital assets for manufacturers and consumers for those processes and products; and think of the funnel encircling the other two as the pathways and pipeline where resides the safe and securely managed flow of billions of pieces of data and task performance between the cobot landscape and the cloud (and all of the stakeholders and users involved).

Who can access and manage all three in staggering efficiencies to manage and then key in on and respond to threats and vulnerabilities, familiar and novel?

Capturing all of that data across the business and product life cycle, channeling it, and siphoning off the data and decisions that shows deviations and risks is the Manufacturing AI Cybersecurity Engineer role. Every manufacturer needs to know about this role, whether to be on staff inhouse or on the teams of key vendors and service providers or virtually built into the systems and tools. Why? Because more and more AI capabilities must be and are being built into cyber solutions combining security expert insights and massive data processing capabilities that can look at billions if not trillions of data points. Every year and every new application can bring AI, cyber, and manufacturing specifics at incremental scale to

Development of this Success Profile was made possible by a grant from the Siemens Foundation

these capabilities taking on the often-heavy human lift now with smarter automation of conventional “watch and respond” tasks, especially those happening across multi-point networks and landscapes of diverse assets. The resulting triage and attention focus is then on even more of the novel or important incidents for security professionals to focus on as a result of a highly refined, high-confidence set of vulnerabilities or incidents.

This AI-leading, cyber-focused, manufacturing-immersed role is positioned to solve the hardest and biggest problems at the intersection of engineering, design, production, IT/OT, and specific risk profiles/threat landscapes in manufacturing, IoT, and general networking situations. Whether across cloud platforms, within a defined industrial control setting, or behind an end product function, a Manufacturing Cybersecurity AI Engineer can model, design and oversee the build of security systems, tools, and approaches, especially security information and event management (SIEM) technologies, that generate visibility across assets and landscapes impossible to come from humans and conventional cyber solutions alone.

These engineers bring core capabilities in engineering, cyber, and industrial areas, again the tribrid picture. They collaborate and communicate with diverse business, operations, and technical teams, all while bringing energy of a startup visionary, the rigor of an engineer who introduces next generation technology, and super sleuth focused impacts. These engineers must focus on delivering results and prioritizing cyber vulnerabilities and business needs while dealing with ambiguity that is often the front end of AI solutions and the unknowns of diverse, large data sets. In partnership with data and process owners, product and system developers, engineering teams and production and supply networks, they assess, design, and support development of AI systems from specs to prototypes to production training pipeline and inference workflows.

Broad educational backgrounds (computer science, manufacturing, product design, etc.) can be appropriate for this role and energize the diversity. This role is closely adjacent to numerous subdomains and roles: IT/OT Integration; Security Operations roles; Automation and Robotics roles; Product Embedded Specialists; Systems Architects, Engineers and Developers; Cognitive Systems Engineers; etc.).

Together, often with the Manufacturing Cybersecurity AI Engineer as a workhorse, they protect manufacturers and their stakeholders from harmful attacks, unauthorized access, and anything else that could interfere with the process, product use, safety and value of data, employees, consumers, and other assets. The AI Engineer will need to be skilled at integrating disparate tools and domains.

While not all size manufacturers will need or be able to employ one of these engineers, they should know and trust these capabilities are available to them directly at the right time should maturing or growth demand, and indirectly through partners and tools now and along the way. For midsize manufacturers and larger enterprises as well as the advisor space and system/service providers, this role is a critical one that increasingly has to be a more common tribrid combination of skill and capability. The impact of a Manufacturing Cybersecurity AI Engineer is immeasurable at this time of cat and mouse races between manufacturers and the bad guys and gals.

Note: The Manufacturing Cybersecurity AI Engineer is a broader engineering role and focused on cyber applications but continues the more specialized and highly related Machine Learning Specialist already profiled. (See Success Profile #9 from original Digital Manufacturing Taxonomy effort).

Outcomes

Business Needs Addressed:

- Solution strategies for optimizing the management and analysis of cybersecurity related data coming from diverse sources across the broad range of manufacturing assets.

Development of this Success Profile was made possible by a grant from the Siemens Foundation

- Needs and requirements for service, system, and product architectures enabled by AI enabled security models and solutions.
- Engineered designs, early models, training pipelines, and continuous improvement of proof of concept and production AI enabled security systems and tools.
- Business cases and evaluations for investments in deploying emerging technologies.
- Natural progression of a high value talent pool to advanced technology and business leadership roles reflecting an optimization of the tribrid nature of this role.

Domain Profile

This role aligns with the Information Technologies & Integrations domain and the Systems Management & Security (Secure Systems Development) subdomain.

Business Case Contribution

From a core business perspective, this role brings business value through these representative contributions:

1. Lowers the cost to detect and respond to breaches and threats and increases the higher value focus of AI enabled security solutions.
2. Delivers scalable solutions to ensure the security of the organization as it:
   - Magnifies human efforts, filtering out most of the noise and ensuring that the attention of analysts and operations is focused where it's most needed.
   - Reduces response time through massive filtering of routine alerts converting them to high-quality/high-impact investigation targets.
   - Relieves alert fatigue for human analysts and responders.
3. Improves data quality for broad business benefits even beyond cybersecurity; proof point for investing in digital talent who have the opportunity to shape next generation technology use.
4. Avoids or minimizes business losses through resulting impacts of lost customer confidence, damages, fines, and other tangible costs from breaches and loss of assets.
5. Increases customer or company brand value through creation of thought leadership in areas of AI, cybersecurity and manufacturing.

In the cases where this role would not be an internal hire for any reason, it should be noted that relying on external consultant and third party does add a supply-chain risk for services and products/tools that also constrains the organization's degree of control but in many cases will still be the appropriate staffing option based on the calculated risk and consideration of many factors.

Development of this Success Profile was made possible by a grant from the Siemens Foundation

Section 2: *Key Responsibilities*

Activities

Overall, this role front ends the creation of scalable, secure and robust, and human-centered cybersecurity focused Artificial Intelligence (AI) and Machine Learning (ML) powered systems. This role is a practicing systems engineer who collaborates as part of a core team assessing and applying latest AI and ML tools and technologies. This role identifies, designs, and supports AI systems development, management and integration of cybersecurity solutions that improve various manufacturing and industrial process, product and physical/digital outcomes.

This role is established with the following assumptions:

- Practices as a tribrid role; it is first and foremost a systems ENGINEER role (needs analysis through design and development planning, architectures and systems management) with a specialization in the use of AI/ML and related technologies and methods (including data exploration, predictive models, machine learning, and other AI technologies) in the functional area of CYBERSECURITY and applied in the MANUFACTURING ecosystem.
- This role profile targets responsibilities as a junior to mid-level Manufacturing Cybersecurity AI engineer. Senior engineers would and do exist in this area.
- While experienced roles transitioning into this area are probable so are a “new to work” candidate path with recent target academic achievement and some portfolio demonstration. In manufacturing and processing environments, at least some experience and context will be highly desired.
- A major variant for this role is how much AI systems programming and development is in scope. Some is likely but could vary greatly, and some knowledge of programming and tools is assumed to be required to facilitate the “systems engineering” aspect of the role. The orientation of the role is more towards staying true to an “engineer” focus (versus developer or programmer role).
- The aspect of engineering, particularly systems engineering anchors this role:
  - Systems engineering is an interdisciplinary field of engineering and engineering management that focuses on how to design, integrate, and manage complex systems over their life cycles. At its core, systems engineering utilizes systems thinking principles to organize this body of knowledge. The individual outcome of such efforts, an engineered system, can be defined as a combination of components that work in synergy to collectively perform a useful function.
- This role is not assumed to perform operational and ongoing use of the systems; that would be in the scope of Cyber Analysts, Cyber System Operators and other SecOp (Security Operations) roles.

1. Requirements Analysis and Needs Identification

a. Assess and define the security problem that the AI system is designed to solve; in the cyber arena, be prepared to continuously update and predict what is a dynamic threat landscape and business environment and as a result, update a changing problem set.

b. Complete systems view evaluation of problem and complete any root cause analysis as required.

c. Identify and propose prioritized use cases for the security solutions, e.g., Threat Intelligence, Incident Response and Vulnerability Management

Development of this Success Profile was made possible by a grant from the Siemens Foundation

d. Translate and connect requirements explanations across the design, development, integration, management, and user teams. For example, if the solution is a product security focus, this role would work closely with internal product and engineering teams (Software and Hardware) to formulate security strategies that are compatible with the product development roadmap and feature rollout schedule.

e. Adopt a consultative technical advisor mindset whether internal or external and provide clients/stakeholders with innovative yet feasible requirements to potential solution ideas.

f. Serve as a key advocate for Security by Design/Secure from the Start generally.

g. Introduce and create increasing awareness for ethical and high-return AI advances; provide thought leadership beginning in the needs and requirements phase.

h. Build business cases as needed.

2. Design

a. Break use cases into discrete minimal viable products (MVPs)

b. Inventory, analyze, and determine how various data sources connect and contribute to the problem solution; serve as key navigator of the data potential, use and AI enabled structure.

c. Develop possible solutions, complete feasibility analysis, and promote the most promising solution(s).

d. Assess, understand, and select for use various AI/ML technology approaches (for example, data set analysis and improvement approaches, e.g., Feature Engineering, Regression, Clustering, Classification, etc.).

e. Develop functional system specifications that enable other senior technical specialists and development teams to best recommend and implement architectures and other key technical directions.

f. Advise, consult, mentor, and support stakeholders (e.g., business or data owners, data scientists/data consumers / users on model standards, scalability, management, and deployment).

3. (Specify and Maintain Design Integrity in) Development and Testing

a. Manage traceability between requirements, test cases, and different data hierarchies and AI system functions.

b. Recommend and oversee the use and share of code repositories; Analyze tools for and results of secure code analyzers and work with Security leadership and software leads on secure development practices.

c. (Oversee and consult on) Build and validation of core models/AI platform pipelines/machine learning pipelines to model AI and ML processes: oversee or advise on writing code, constructing a prototype; performing data extractions, creating training models, and tuning the algorithm(s). (Depends on degree of active programming this role may perform).

d. Monitor and retrain models; apply testing and validation of the security of high-performance complex systems that include safety critical hardware, software, sensing, and actuation components.

e. Establish scalable and efficient automated processes for large scale data analyses, model development, validation, and implementation.

f. Develop and establish model management technology and processes to enable AI/ML/SecDevOps such as: measure on-going accuracy, tooling for data / model drift, etc.

g. Develop and report KPIs for test data.

h. Work with security requirement owners to ensure that all requirements are verifiable and are linked to test cases with well-defined pass/fail criteria.

i. Interface with business owners to ensure that the security verification plan meets product, regulatory, and business needs.

Development of this Success Profile was made possible by a grant from the Siemens Foundation

j. Work with engineering leadership to ensure that security verification plans are coherent and in sync.

k. Refine system and software level test cases to ensure compliance with system and software level security requirements.

l. Use and manage security test suite execution and reporting automation; use modern test planning and reporting tools such as Jira or Polarion.

4. Deployment

a. Lead integrated deployment and adoption planning and ensure successful integration and management activities of models and solutions (e.g., models via APIs into applications or workflows).

b. Release to production; continue data ingestion/extractions and tuning of the algorithms.

c. Visualize the output of the data insights and stories in ways that is meaningful and consumable by all stakeholders.

d. Support incident response process as necessary and participate in after-action activities as appropriate.

5. Continuous Improvement

a. Apply and use CI/CD oriented tools and approaches, making the platforms and pipelines a continuous cycle and effort.

b. Establish best practices to publish status and progress towards verification and validation of requirements throughout the product development lifecycle.

c. Serve as a primary technical and business communicator on the design, redesign, and continuous improvement, regeneration, or replacement.

d. Participate in internal technical communities and in the broader industry through events, blogs, whitepapers, training, and articles for related AI, cyber, and manufacturing domains.

Development of this Success Profile was made possible by a grant from the Siemens Foundation

Section 3: *Competencies*

Representative Capabilities

The role of a Manufacturing Cybersecurity AI Engineer is a true tribrid: primarily an AI Engineer expert, secondarily a Cybersecurity focused practitioner, and third, an increasingly knowledgeable Manufacturing security problem solver. The competency profile obviously becomes broad and extensive with that triple focus.

There will be weighting across the three major domains for a particular position, and a successful candidate will likely bring primary expertise in either AI or Cybersecurity initially based on employer hiring needs and then add to their secondary core capabilities and manufacturing specifics. While we position that this role positions the AI capability first, below are representative core competencies that provide a mix across the three major domains.

That said, a specific ration of Cyber versus AI versus Manufacturing is not proposed nor should it be expected. Variations of the ratio that suit employer needs and candidate profiles is a positive trait of this role as long as the tribrid skill set and application on the job is utilized.

Also, note that with the high interdependency of technology and tools for this role, both generally and per employer, and given the ever-changing threat landscape, there will be frequent need to reassess this role and its skill/knowledge needs.

AI/ML Foundations and Applied Skills:
Expertise and hands-on experience in various AI and ML approaches, and the background knowledge areas such as: math: statistics, probability, predictions, Bayesian algorithms and logic; physics, mechanics; cognitive learning theory, language processing; Natural Language Processing, Computer Vision, Speech Recognition, Reinforcement Learning, Ranking and Recommendation, or Time Series Analysis. Deep Learning architectures and ML learning frameworks such as PyTorch and TensorFlow.

Proficiency in machine learning practices and algorithms such as user behavioral modeling, multi-class classifications, decision trees, support vector machines, deep learning and familiarity with NLP/ML tools and packages like PyTorch, TensorFlow, Weka, scikit-learn, XGBoost, Onnx, TensorFlow serving, etc.

Security and Compliance Systems Engineering:
Experience and ability to design key solutions and architectures for confidentiality and access, integrity, and availability across multiple cybersecurity and compliance needs including access management solutions, threat hunting and forensics, information protection, application management, security management and/or auditing and governance endpoint detection and response, anti-malware, persistent threats, email security, user behavior and analytics, threat intelligence, and cloud-based identity required.
Able to design cloud-based identity and access management solutions as well as hybrid architectures and integration of cloud-based apps (SaaS) required.

Experience with modern cloud systems and app platforms, e.g., AWS and AWS Sagemaker. Cloud Trust. Practical expertise in sophisticated identity, authentication, security, privacy, and compliance requirements, and experience integrating them into cloud and hybrid solutions required. Experience with cloud and hybrid infrastructures, architecture designs, migrations, and technology management, e.g., Microsoft 365 Security, Azure Security and Enterprise Mobility + Security.

Development of this Success Profile was made possible by a grant from the Siemens Foundation

Manufacturing Cybersecurity AI Engineer

Standards and Regulations:
Expertise in applying, adhering to and tailoring existing security practices such as the NIST Framework, Cyber Security Standards (ISO 21434, SAE J3061), federal contracting and standards, vulnerability management standards, and other applicable standards.

Computer Science and Systems Engineering:
Information ordering, critical thinking, complex problem solving, systems engineering and management, systems analysis, data management and excellence (see below also), programming (see below also), logic and efficiency, including experience and skills with tools of agile development methodology environments like Gitlab, JIRA, Confluence, Bitbucket and CI/CD.

Big Data and AI Data Optimization and Excellence:
General data analysis skills, analytics, data mining, data cleaning, and data management techniques. Experience in data science application to complex problems and data sets/ warehouses/ hybrid sources.

Experience in:

Data Modelling and Evaluation data ingestion, feature engineering, modeling including ensemble methods, predicting, explaining, deploying, and diagnosing ML models.

Training, integrating, and curating big data sets, cloud AI and big data systems, ETL pipelines, both batch and real-time data processing. Skills and tools such as: Hadoop, Hive, Spark, Amazon Kinesis, Azure Stream Analytics, Spark, Storm, Kafka, S3 / Azure Data Lake (Data Lake), Azure ML Studio, Sagemaker, etc.

Visualization tools and techniques (e.g., Periscope, Business Objects, D3, ggplot, Tableau, SAS Visual Analytics, PowerBI).

More strategically, experience with AI Ethics decision making and influences on cyber and systems development.

Data privacy policies and regulations.

Data ownership, governance, and commercialization considerations.

Functional Programming: (depending on degree of actual systems development as part of this engineering role) growing expertise in one or more languages, such as Python, C++, JavaScript, Java, C#, Julia, Shell, R, TypeScript, Scala, Rust, ML, Racket, Common Lisp, Haskell.

Some AI modes can include human-machine interface development programming tools (to include augmented and virtual reality (AR/VR)) e.g., Ignition, FactoryTalk View, Wonderware, iFIX, etc.).

Software development experience developing API's, DevOps Pipelines, and/or frontend applications and experience with core software and experience with data engineering tools: Spark/PySpark, SparkML, Auto-ML, Containers, GitHub for version control.

Development of this Success Profile was made possible by a grant from the Siemens Foundation

Manufacturing Cybersecurity AI Engineer

Manufacturer Operating Environment and Industrial Security Context: Understanding of general and specific manufacturing assets, production, and processing environments; industrial networking and control systems; robotics, advanced automation, instrumentation, control systems, and other in scope manufacturing technologies. Awareness of specific and general threat landscape, actors, vectors, and targets for manufacturing.

Stakeholder Communications: Stakeholder engagement and communication skills for working with product teams, process owners, production teams, system, and asset owners as well as business leaders. Adept in sharing technical/ data science/machine learning outcomes with both technical and business-oriented stakeholders.

Other general, business, and personal competencies include:

1. Innovative mindset and an ability to take calculated risks balanced with contingency plans; demonstrate experience of making trade-offs between schedule, resources, model performance etc.
2. Strong analytical and critical thinking skills.
3. Self-motivation, great communication skills, and team player.
4. Ability and passion for dealing with complexity and ambiguity.
5. Analytical thinking and attention to detail.
6. Deductive and inductive reasoning.
7. Creative problem solving.
8. Communication, both verbal and written, for business and technical stakeholders at all levels.
9. For managed or advisory service roles, strong client solutioning, challenger mindset, client management skills including ability to gain approval for solution green lights.

Development of this Success Profile was made possible by a grant from the Siemens Foundation

Section 4: *Experience And Education*

Education

(Assuming primary focus of AI)

Bachelor's degree or higher usually required in Computer Science, Machine Learning, Electrical Engineering, Data Science, Cognitive Science, Computational Linguistics, Software Engineering, Applied Physics, Applied Mathematics, or related discipline, plus Cybersecurity course/skill focus and ideally embedded professional certifications certifying cyber capabilities.

For secondary cybersecurity focus:

Other degrees if coming in as a cyber expert who will gain AI credentials, are Computer and Information Sciences focused on Cyber-Physical Systems, Network Engineering or Systems Engineering, Information Security, and Cybersecurity; plus AI/ML course/skill focus and ideally embedded professional certifications certifying AI/ML capabilities.

Certifications

- AiE (ARTiBA)
- Microsoft Certified: Azure AI Engineer Associate
- CompTIA Security+
- NIST Cybersecurity Framework
- CEH
- LPT
- ML-AI Certificate (Stanford via Coursera)
- See other Azure Certifications, e.g. Azure Security Engineer Associate, etc.
- CISSP
- CCSP
- GPEN
- GSEC
- IBM AI Engineering (IBM via Coursera)
- CISM (for a business and leadership focus)
- OSCP
- CCNA Security
- GSED
- CCIA

Experience Profile

1. 1-3 years AI engineering experience and 1-3 years of experience in cyber threat detection and analysis or equivalent; applied education experience/portfolio/internship as demonstration of experience.
2. 4-7 years for mid-level roles and 7-10 years for senior roles, with increasing experience in core areas as previously described and summarized:
   - Full cycle (through deployment) of AI, Machine Learning based cyber applications and increasing data science capabilities.
   - Industrial and operational systems, networking, and core production and processing for manufacturing specific context.
   - Data privacy, AI and data ethics, and information management policy and governance.
3. Strong alignment to maintaining secure assets - people, data, product, etc. – via innovative AI enabled cybersecurity solutions.
4. Project Management best practices for scheduling, budgeting, and risk management.
5. Ability and passion for dealing with complexity and ambiguity.
6. Analytical thinking and attention to detail.
7. Creative problem-solving, innovation, and entrepreneurial mindset.
8. Communications excellence – verbal and written for business and technical stakeholders at all levels.
9. For managed or advisory service roles, strong client management skills and ability to quickly adapt to client environment and resource networks is necessary.

Development of this Success Profile was made possible by a grant from the Siemens Foundation

Manufacturing Cybersecurity Analyst

Section 1: *Job Role Identifier Section*

Role Title: Manufacturing Cybersecurity Analyst

Role Impact: Producer (for Large Employers and Service Providers); Pioneer for Small and Midsize Employers

Summary Scope

No one - in any public or private sector, let alone in the highly targeted manufacturing arena - can hide from the increasing cybersecurity threats to core operations, customer data, supply chains, and other data/product/human assets. Even updating this introduction to mention the December, 2020 SolarWinds breach to government and business provides global reality that vigilance, detection, and mitigation will be unceasing. It also serves as an object lesson that technology alone will not be the single answer. In fact, at times the technology - as with SolarWinds - meant to help security operations can be another source of vulnerability driving constant change to the tools, the security tasks, and needed skills and approaches. Another ever-present need that no manufacturer can hide from is that tools and threats change at the same time the cyber workforce gaps continue and the workforce morphs with role designs and skill priorities. Helping with both the changing needs and addressing the talent gap is the workforce opportunity to position, recruit, and reframe a longer standing role into a highly valuable and versatile baseline cyber role - the modernized Manufacturing Cybersecurity Analyst.

Positioning or performing as a Manufacturing Cybersecurity Analyst answers these capability needs:

- What role, even with great tools, does the heavy lifting to monitor/assess, detect, and mitigate – the functions that are still a mainstay of cyber activity?
- What role will very directly work with constantly evolving and advancing technologies to watch and manage security of digital and physical assets, systems, networks, and data?
- Who will monitor process, product, and physical and human safety by protecting virtual, network, and on-premises data, access points, and infrastructures?
- Who understands manufacturers' changing vulnerabilities to plan, monitor, and use security measures to identify suspicious activity and mitigate risks before there is a breach or as soon as one is identified? And work initially as a generalist incident responder to counter breaches or threats; and downstream assist in investigations as needed?
- Who will manage new versions of distributed workplaces as mobile and independent work environments continue to morph due to Covid and other major disruptions and IoT and smart endpoint devices widen and complicate the threat landscape?
- Who will need to increasingly understand how to monitor and manage not just the technical connections but the human behavior and vulnerabilities and the ethical and social implications that come with it?
- What role can be leveled to suit employer and employee needs as a transition role (in training and upskilling) or associate (junior) level or experienced (more senior level) position?

The answer to all these business needs is the Manufacturing Cybersecurity Analyst. This is a cross industry and well-established role, frequently seen as both internal to organizations and in third party service provider settings. Yet, for this role to be successful and to realize its true impact to manufacturers – as well as set the stage for expansive careers for workers who choose the path – the role will bring the most value when it is set up as a Versatilist role, focusing on monitoring, detection, and response, yet continuously adding additional layers of expertise, broader functions, more complex threat landscapes, and use of more modern tools across those primary functions.

Development of this Success Story was made possible by a grant from the Siemens Foundation

Manufacturing Cybersecurity Analyst

Of the many roles identified in the MxD Cybersecurity Hiring Guide, this role is hands on in the most direct security operations sense and is also by design one of the most adaptive roles. This role brings at least three overarching cyber workforce success strategies all that leverage adaptability:

- The Manufacturing Cybersecurity Analyst is a utility player by design in terms of functions and their core duties to monitor, assess, and mitigate in the world of cyber where there are dozens of identifiable, more narrowly focused adjacent roles.
- From a cyber security operations perspective, they are one of ***THE essential cybersecurity workers, a true front line cyber worker*** who is at the intersection of assets and vulnerabilities, data, networks, systems, users, and the threats landscape.
- The Manufacturing Cybersecurity Analyst – and its many other titles (see below) – brings great staffing and career flexibility if it is by design a Versatilist role (see Gartner perspectives on Versatilists) as opposed to being too shallow of a generalist or a sole focused deep specialist. The role can be developed and used to bridge enough areas to be a deeply skilled, multi domain analyst - a Versatilist who has wider and deeper skills than the “jack of all trades, master of none” Generalist. As a result of approaching this role as a Versatalist, workers here can pivot and focus as needed. This is a business and security advantage and a personal career advantage.

The versatility can position it in many subdomains, from manufacturing IT/OT/Product, supply chain, and connections to the data flow and the digital thread; to security Operations; to IT/OT convergence, user and consumer support, and product.

- As with other roles, but less so with this one because of standout Versatilist status, not all size manufacturers will need or be able to employ one of these engineers, but they should understand that:
- this role can be an excellent pioneer role early on as organizations start implementation of their cybersecurity strategies and operations because of the three major benefits described above;
- it is a role that can scale cybersecurity faster because of that versatility and can go from generalist to specialist with less effort than many other roles;
- this role, when a Cybersecurity Analyst at a service provider performing essential services for clients, is almost is like a “back office” role and sometimes less seen, but this profile describes the essential work it does and where it would connect to the client internally.

As a high value 3-for-the-price-of-1 role, it is one of the best examples of a Versatilist role available to employers, whether directly employing a Cybersecurity Analyst for inhouse focus or as an employer of these analysts for service delivery to clients or public infrastructure and broad network and usage needs. Analyst roles can be leveled from Transition/Upskilling to Associate/Junior or Experienced/Senior positions to add even more flexibility. Especially as some aspects of a Cybersecurity Analyst’s role are automated through advancing tools, taking on and progressing with adjunct skills and a multiple domain focus will leverage and customize the role and make it a key feeder role to upcycling cyber talent for future roles as SecOps becomes increasingly automated itself.

Modernizing this role to a purposeful Versatilist, one whose progression over time can pivot to address new tech, a role that can fill in various talent gaps immediately and downstream, and one that bridges key manufacturing areas, makes it a win-win role for workers and employers alike.

Outcomes

Business needs addressed are a wide potential range for this role. This role also answers a question that is getting an increasing amount of airtime in the broader IT/OT and cyber arenas: what is the tradeoff and future likelihood of specialists versus generalists in the world of infrastructure and operating technologies? This role brings to the conversation the opportunity for hiring and developing Cybersecurity Analysts as a continuously growing Versatilist to maintain the value (3 for the price of 1; buy one, get two free) regardless of the task focus, and the tool and tech

Development of this Success Story was made possible by a grant from the Siemens Foundation

journey. While it starts with a basic focus, it merits investment as the outcomes can evolve over time and a stretch of career.

- Provides a highly valuable Versatilist cybersecurity role; a truly adaptive role that can meet many needs for the business and provide excellent career growth for workers. To generalize, specialize, and bring high value versatility as a gateway role to many cyber roles well beyond those duties highlighted here.
- Both a contributor and revenue generating role; frequently seen in both manufacturing organizations and in third party service provider settings (partially influences a wide salary and skill range).
- Provides core work outputs (monitoring increasing attack surface; developing specific exposure and vulnerability profiles for manufacturers, strengthen overall data and asset security and privacy, corral and better manage IoT assets/devices; address the production and non-production arenas, varied storage and connection setups and the physical infrastructure and support the convergence of IT/OT and IoT environments; manage accelerated automation and remote work as driven by Covid, increasing AI and robotic production and processing, supply chain) as from its flexible nature.

When thinking of outcomes, it is important to recognize that the Cybersecurity Analyst is a very widely used title and position and can be the same general work and business needs being addressed as a Security Operations Center (SOC) Analyst; Information Security Analyst; Security Analyst; Cybersecurity Risk Analyst, and more. Depending on scope of role and employer, it can also merge or include more functions and values than those here and can include those we have identified elsewhere in the hiring guide as other (additional) roles, for example, specific adjacent roles can range from Distributed Control Systems Analyst; Threat Analyst; Vulnerability Analyst; White Hat/Ethical Hacker; and many other analyst and engineering, IT and OT supporting roles.

Domain Profile

This role aligns with Business & Technical Alignment domain overall, and the subdomain of Security Operations.

With its cross-role diversity as mentioned above, it can be closely adjacent to numerous other domains and subdomains: IT and Integration; OT and Integration; Integration and Convergence; Readiness and Development; Industrial Controls Security; Infrastructure Management; Automation and Controls; Product Design, and more.

Business Case Contribution

Business Value

From a core business perspective:

- Reduced cyber risk exposure across the digital manufacturing ecosystem.
- Better managed monitoring, detection, and containment volumes: Total Number of Security Incidents; Decreases in Reported Breaches; Increases in Mitigated Threats.
- Through improved threat landscape understanding, improved efficiencies and effectiveness: Mean Time to Identify (MTTI) and Mean Time to Contain (MTTC).
- Improvements or maintenance in targeted uptime.
- Maintained or improved regulatory, contractual, or internal compliance.
- Minimized/decreased costs of incidents: direct costs; indirect costs; opportunity cost.
- Maintained or improved data privacy, managed IP, safety, and other extended values.

Development of this Success Story was made possible by a grant from the Siemens Foundation

- Maintained or improved customer confidence and brand value.

From a core talent perspective:

- Because of their utility and versatility as a more flexible resource, better and more cost-effective handling of short-term cyber workforce spikes or changing operational needs.
- Major versatile feeder pool of talent for other cyber role demands.
- Highly leverageable talent investment for future progression.

Section 2: *Key Responsibilities*

Activities

Working as a cyber foot soldier and essential cyber worker, this role delivers on front-line cyber responsibilities. While also a robust role with wide-ranging options, there are core responsibilities for Manufacturing Cybersecurity Analysts that are central and form an organization's first line of defense. Entry-level analysts will perform fewer of these activities/stages for less complex situations; more experienced and senior roles will include leadership, more complex environments, broader scopes, and a fuller cycle of the NIST stages.

More specifically aligned to the NIST stages – although there can be overlaps and multiple stage use of some tasks - Manufacturing Cybersecurity Analysts would do:

1. Support business alignment and security services governance efforts to follow standards and guidelines, complete risk analyses, vulnerability assessments, and security prioritization.
2. Support security audits, internal and external.
3. Investigate and document emerging security trends and report potential security implications.
4. Make policy and guidance procedures specific for operating environment and provide feedback to leaders and governance teams for improvements.
5. Coordinate security plans with relevant users, functions, and vendors.
6. Optimize and maintain security information and event management (SIEM); network intrusion detection systems and other related tools.
7. Configure and script third party tools for the operating environment.
8. Recommend, implement new technologies.
9. Maintain data and monitor security access networks and systems including patching emerging vulnerabilities and completing ongoing security system updates.
10. Lead/assist with mitigations for existing weaknesses proactively.
11. Apply processes, tools, threat intelligence, and analytical approaches to complete risk assessments meeting industry, customer, or internal requirements that occur within a manufacturer's business and production environments (e.g. identify suspicious network traffic, abnormal user behaviors, monitoring of malware and virus signatures, heuristics, and other identifying vulnerability and threat characteristics).
    - Monitor and discern priorities of signal alerts.
    - Anticipate threats, incidents, and alerts to help prevent the likelihood of them occurring.
    - Maintain threat analysis and security logs for security processes and devices.
12. Connect with asset management, audit, and network administration.
13. Co-analyze threats and breaches to find the sources and root cause:
    - Use hashing algorithms for file integrity checking.
    - Complete log reviews of users, applications, cloud services, network devices, production platforms, equipment, and facility assets; operating systems, end user devices, etc.

Development of this Success Story was made possible by a grant from the Siemens Foundation

14. Analyze and address hardware and software weaknesses and vulnerabilities and increasingly interact with product and consumer teams, service providers and supply network partners, vendors, and regulatory agencies.
15. Increasingly be able to do advanced analysis based on AI/ML system outputs for deep fake threats.
16. Contribute and manage attack tree analysis and open-source reporting for product vulnerabilities.
17. Integrate and consolidate data from various cyber defense tools (e.g., alerts, firewalls, network traffic logs, etc.).
18. Analyze and respond to undisclosed hardware and software vulnerabilities.
19. Analyze any number of potential vectors such as Insider threat APT detection, social engineering schemes, phishing schemes, malware detections, system software glitches, nation state attacks, and other vectors of cyber threats.
20. Contain the event including disconnections, denial of access and privileges, guaranteeing, system back up patch installation etc.
21. Determine severity and impact.
22. Escalate and activate other response capabilities as needed.
23. Coordinate with other analysts, IT, OT, and functions regarding recovery activities.
24. Support recovery activities when needed such as system, network, operating system, user testing, and validation.
25. Recertify compromised components, processes, user, hosts, etc.
26. Make recommendations of future security operations improvements including countermeasures and adjusted use of approved tools.
27. Support evaluation, testing, and recommendation of related security policies, procedures, and systems, including hardware, firmware, and software.
28. Deliver user awareness, coaching, and support as needed.

With this role being a generalist/Versatilist role and often expanded or limited based on a variety of other cyber roles in place, there often can be particular areas of focus, whether for everyday work or development and progression. Within this range of duties or in addition to the these could be other tasks not included here but included in fuller analysis of other adjacent roles in the MxD Hiring Guide. Some of the most likely focus areas for a Manufacturing Cybersecurity Analyst could be:

- Asset Management (Auditing, Security Operations (e.g. Network Access and Management, Inventory and Portfolio Audits, Systems Management, Advanced persistent threat (APT) etc.)
- Risk Management and Manufacturing Impact Assessments (Audits)
- IoT/End User Product Design and Security (e.g. Application Security, Product Design/Secure by Design, etc.)
- IT/OT Operational Integration and Security Operations (Chemical & Mechanical Process Safety, Industrial Controls, Automation and Physical Asset Protection, etc.)
- Software Development (e.g. Extended security tool optimization, configuration, customization)
- Supply Network Management (e.g. Vendor Management, Supply Chain Cybersecurity Integration and Compliance)
- Business Continuity (e.g. communications, readiness and training; incident response; disaster recovery, etc.)
- Forensic Investigations

Other influences on the size and scope of this role will also be determined by the employment context of the particular role and cybersecurity requirements for primes and subcontractors (subject to DFARS Clause 252.204-7012 and NIST 800-171) and/or Cybersecurity Maturity Model Certification (CMMC).

As a result, there may also be duties for the Analyst for audit readiness and third party certification; understanding and application of how to leverage NIST 800-171 for CMMC certification; System Security Plan (SSP) creation and documentation; and addressing Plans of Action & Milestones (POAM).

Development of this Success Story was made possible by a grant from the Siemens Foundation

Section 3: *Competencies*

Representative Capabilities

Competencies will flex as the focus of the cybersecurity analyst role flexes with need, interest, change in approaches and technologies, etc. As part of the Versatilist framework of this role, some of these competencies will be basic, and for others it's likely that with time and still within the basic responsibilities of an analyst, an incumbent would need a broader set of some of the additional capabilities.

Also impacting a common set of capabilities is the versatility of this role and there are many entry points in manufacturing. As a "boots on the ground" role, there should also be many on the job opportunities to gain skills. From the wider set of capabilities below, we have asterisked (*) those that may be a common baseline for entry level experience or knowledge.

***Network Monitoring and Vulnerabilities and Security Information and Event Management / Security Operations:**
Knowledge of network basics such as access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML). Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]). Knowledge of network security and network defense basics relating to firewall management, intrusion detection, and intrusion prevention.

Network security and network defense tool use and related analytical and response actions relating to Firewall management, Intrusion Detection Systems, and Intrusion Prevention Systems. A wide variety of tools including Wireshark, KaliLinux, tcpdump, and Identity Access Management tools SEIM tools such as Splunk, IBM, ATT Security, Dell Security, Fortinet, etc.

Threat Intelligence:
Knowledge of attack methodologies and tools and increasing awareness of actor/vector/target profiles and patterns to enable predictions on future threat sources and activities. Requires increasing research, statistical, and analytical skills to work with data and identify significant patterns related to cyber threats; Written and verbal communication skills, analytics interpretation, reporting and visualization to create intelligence reports communicating the results to stakeholders (e.g., internal partners, business leaders, customer (e.g. federal or private) decision-makers and security officials or practitioners).

Development of this Success Story was made possible by a grant from the Siemens Foundation

Manufacturing Cybersecurity Analyst

***Web Security Risks and Vulnerability Scanning:**
Web security tool use and related analytical and response actions procedures and skills for scanning web applications and site scanning for security vulnerabilities such as cross-site scripting, SQL Injection, Command Injection, Path Traversal, and insecure server configuration. Ability to certify sites and applications including blacklisting and whitelisting. Knowledge and use of related open source and commercial tools (e.g. Nmap, Nikto, Nexpose, Nessus Professional, etc.).

***Information and Cybersecurity Basics:**
Ability to identify and resolve configuration of security settings, detect incomplete or missing patches, and apply security patches, manage software bugs, and general security misconfigurations in operating systems, software applications, and IT devices. NIST frameworks, industry standards, DoD, and other supply chain and contracting compliance requirements.

Security operations procedures, roles, and responsibilities, including shared use of third-party resources and tools and specific features and functions used by each role/procedure.
Vendor partnerships and management.

Ethical Hacking and Penetration Testing:
Tools, practices, and analysis skills for testing a computer system, network, or web application to find security vulnerabilities. Practices range from fuzz testing or fuzzing (discover security loopholes in software, operating systems, or networks by massive inputting of random data to the system in an attempt to make it crash) or honeypots of a network-attached system decoy to lure, detect, deflect or study hacking attempts.

Includes Tools like Metasploit, Acunetix, SQLMap, Veracode, etc.

Risk Management:
Knowledge and use of practices, standards, and tools to support security and risk governance and business alignment issues, and application of portfolio audits with threat and vulnerability landscapes to determine security priorities.

Ability to measure and communicate to multiple stakeholders the likelihood of attacks and the consequences of those attacks.
Abilities to support the increasing use of simulations, modeling, and game theory to model risks.

Incident Response and Forensics Compliance:
Generic and specific cyber event response team members, roles and responsibilities, processes, escalation decision points, etc.
General and specific knowledge of procedures and tools for:

- Source Determination
- Event Containment
- Recovery
- Severity and Impact Determination
- Recovery Testing and Validation
- Communications Notification
- Reverse engineering
- Computer forensics basics

Development of this Success Story was made possible by a grant from the Siemens Foundation

Manufacturing Cybersecurity Analyst

***Manufacturer Operating Environment, Industrial Security Context, and General Data Management:** Understanding of the dynamic, fuller landscape as well as specific manufacturing vulnerabilities and risks. Understanding of general and specific manufacturing data, assets, production, and processing environments; industrial networking and control systems; robotics, advanced automation, instrumentation, control systems, and other in scope manufacturing technologies. Awareness of specific and general threat landscape, actors, vectors, and targets for manufacturing and ability to prioritize and contextualize for the manufacturing setting.

Stakeholder and Partner Relationships and Communications: Inclusive relationship building, recognizing partnerships and connections are key to the ability to perform and protect. Regularly invest, engage, and communicate with a wide network of relationships at multiple levels in the company and with service providers. Understand needs and concerns with product teams, process owners, production teams, and system and asset owners as well as business leaders. Adept in sharing technical/- outcomes with both technical and business-oriented stakeholders.

Other general, business, and personal competencies include:

- Increasing experience and knowledge of the entire NIST cybersecurity cycle to support or perform related tasks.
- Multi-tasker with ability to balance routine/operational work and high-pressure, incident/issue driven work.
- Highly organized, procedurally focused, and detail-oriented, yet adaptive and quick shifting when needed.
- Investigative muscle; persistence and diligence.
- Objectivity with curiosity and willingness to question evidence and information.
- Quality orientation.

Development of this Success Story was made possible by a grant from the Siemens Foundation

Section 4: *Experience And Education*

Education

- Bachelor's degree in Computer Science, Information Technology, or related discipline desired.
- Increasingly accepting of Associates Degree and Certification with 1-5 years' experience (apprenticeship, portfolio or related experience in lieu of 4-year degree) including completion of internal training programs highly preferred

Certifications

- Security+ - CompTIA
- GPEN - GIAC Penetration Tester
- GSEC – GIAC Security Essentials
- CEH – EC Council Certified Ethical Hacker
- Certified Information Systems Security Professionals (CISSP) or CompTIA Advanced Security Professional (CASP) for more senior Analyst positions.

Experience Profile

1. At the entry/junior and mid-level analyst level, 55% of researched postings ask for 0-2 and 3-7 years of experience, including 0-3 years' information security experience or equivalent experience/specialization in priority tasks or tools for specific environment; 2-3 years other/general technical experience highly desired.
2. Hands on experience and apprenticeship required (or equivalent structured training experience completion).
3. Multiple levels of positions often available leading up to Senior Analyst or equivalent requiring an additional 2-3 years' experience per level with adjacent roles flex experience and/or experience with more complex threat landscapes, responses, investigations, etc. (and often with a further qualified title, e.g. Senior, or Advisor or incorporating other major functions in addition to Analyst functions).
4. Increasing industry knowledge and specialization in a set of subspecialties often desired to increase value as Versatilist but can maintain a generalist job scope as well. For example, strive for work experience in two or more of the eight domains of the (ISC)² CISSP certified book of knowledge (CBOK):
   - Domain 1. Security and Risk Management
   - Domain 2. Asset Security
   - Domain 3. Security Architecture and Engineering
   - Domain 4. Communication and Network Security
   - Domain 5. Identity and Access Management (IAM)
   - Domain 6. Security Assessment and Testing
   - Domain 7. Security Operations
   - Domain 8. Software Development Security
5. Broad knowledge and experience with the various NIST, DoD, or other relevant frameworks and toolsets.
6. Increasing knowledge of Manufacturing and Industrial context for Actors, Vectors, Targets and other threat and vulnerability profiles.

Note: Role frequently seen in both manufacturing organizations and in third party service provider settings (partial influence on wide salary and skill range) so specific experience requirements may vary highly depending on internal versus external duties.

Development of this Success Story was made possible by a grant from the Siemens Foundation

Interested in partnering with MxD to add to future editions of this Hiring Guide?

Contact Lizabeth Stuck, Senior Director of Workforce Development at MxD, at lizabeth.stuck@mxdusa.org.

We invite you to share this report with others in the industry. Visit the Hiring Guide Page on the MxD website at mxdusa.org/hiringguide.

ManpowerGroup

M D