Workforce Categories	Positions	Brief Position Description	Minimum Certification & Education Requirements	Level 1 Certifications	Level 2 Certifications	Level 3 Certifications	Recommended Training Sustainment Methods
Oversee & Govern	CISO	Establishes enterprise-wide security policies, develops data breach resiliency plans, oversees system update communications, and manages the information security financials.	Current standing in one of the following certifications: • (ISC)2 Information Security System Professional (CISSP) • ISACA Certified Information Security Manager (CISM) • EC Council Certified Chief Information Security Officer (CCISO) Preferred qualification: Bachelor's degree in information technology, cybersecurity, computer science or other related discipline.	Level 1 certifications would already be accomplished in order to meet the minimum certifications required for the position of CISO; those certifications are not documented here. See map of stackable certification credentials.	Level 2 certifications would already be accomplished in order to meet the minimum certifications required for the position of CISO; those certifications are not documented here. See map of stackable certification credentials.	An advanced certification (above Level 3) is recommended for this position: • (ISC)2 Information System Security Management Professional (CISSP-ISSMP) Level 3 certifications are listed below: • (ISC)2 Information Security System Professional (CISSP) • ISACA Certified Information Security Manager (CISM) • EC Council Certified Chief Information Security Officer (CCISO)	Individuals must meet certification maintenance requirements by attending relevant conferences, seminars, webinars, and industry conventions, and conducting self-study. Requirements vary. Minimum of 40 hours of continuing education per year is recommended. **RECOMMENDED TRAINING** • Attend annual threat intelligence training from SANS or other provider • Participate in annual incident response table-top scenario exercises • Complete (CFR) CyberSec First Responder: Threat Detection and Response (Exam CFR-210) • Attend training in cybersecurity governance, risk, and compliance • Maintain familiarity with cybersecurity operations, trends, and toolsets Advanced certification options include the following: • GIAC Security Expert (GSE) • (ISC)2 Information System Security Management Professional (CISSP-ISSMP) • Axelos ITIL Master
Oversee & Govern	Information Security Manager	Manages the agency cybersecurity program to include security awareness and training, maintains security strategies, incident response plans, and disaster recovery plans. This role is responsible for the cybersecurity of a program, organization, system, or enclave.	Current standing in one of the following certifications: • GIAC Security Leadership (GSLC) • (ISC)2 Certified Information Systems Security Professional (CISSP). • ISACA Certified Information Security Manager (CISM). Preferred qualification: Bachelor's degree in IT security management, information security, cybersecurity, or related discipline. Degree requirement may be waived based on professional experience.	Level 1 certifications would already be accomplished to meet the minimum certifications required for the position of an ISM; those certifications are not documented here. See map of stackable certification credentials.	Attain and maintain at least one of the following certifications: • GIAC Security Essentials Certification (GSEC) • EC Council Certified Ethical Hacker (CEH) • CompTIA Advanced Security Practitioner (CASP+)	• Mile2 Certified Information Systems Security Manager (CISSM) • IAPP Certified Information Privacy Manager (CIPM)	Individuals must meet certification maintenance requirements by attending relevant conferences, seminars, webinars, and industry conventions, and conducting self-study. Requirements vary. Minimum of 40 hours of continuing education per year is recommended. **RECOMMENDED CONTINUING EDUCATION** • Attend annual threat intelligence training from SANS (or other provider) • Participate in annual incident response table-top scenario exercises • Complete (CFR) CyberSec First Responder: Threat Detection and Response (Exam CFR-210) Recommend attaining specialty certifications relevant to the agency being supported. Examples include training/certifications in data privacy and regulatory controls, incident response, risk management, or infrastructure management.
Oversee & Govern	Risk/Compliance Manager	Performs risk assessments and establishes tolerance for risk based on mission, critical information systems infrastructure and efficacy of countermeasures / resilience. Quantifies residual risk.	Current standing in at least one of the following certifications based on certification levels noted to the right. Preferred qualification: Bachelor's degree in IT security management, information security, cybersecurity, or related discipline.	• CompTIA Security+ • (ISC)2 System Security Certified Practitioner (SSCP)	• GIAC Security Essentials Certification (GSEC) • ISACA Certified Information Security Auditor (CISA) • ISACA Certified in Risk & Information Systems Control (CRISC) • GRMI Certified Risk Management Professional (CRMP)	• PMI Project Management Professional-Risk Management Certification (PMP-RMC) • (ISC)2 Information System Security Professional (CISSP)	Individuals must meet certification maintenance requirements by attending relevant conferences, seminars, webinars, and industry conventions, and conducting self-study. Requirements vary. Minimum of 40 hours of continuing education per year is recommended. **RECOMMENDED CONTINUING EDUCATION** • Attend annual threat intelligence training from SANS (or other provider) • Participate in annual incident response table-top scenario exercises Recommend attaining one or more of the following specialty certifications such as: • GIAC Strategic Planning, Policy, and Leadership (GSTRT) • (ISC)2 Certified in Governance, Risk, and Compliance (CGRC) • PMI Project Management Professional (PMP) • (ISC)2 Information System Security Engineering Professional (CISSP-ISSEP)
Oversee & Govern	Cyber Policy Planner	Develops and maintains cybersecurity plans, policies, and strategy to support and align with enterprise cybersecurity initiatives and regulatory compliance.	Current standing in at least one of the following certifications based on certification levels noted to the right. Preferred qualification: Bachelor's degree in cybersecurity, IT security management, IT management, information security. Bachelor's degree in political science, business management, communications, or public administration may be acceptable WITH cybersecurity experience.	• CompTIA Security+ • (ISC)2 System Security Certified Practitioner (SSCP)	• GIAC Security Essentials Certification (GSEC) • CompTIA Advanced Security Practitioner (CASP+)	• GIAC Security Leadership (GSLC) • (ISC)2 Certified Information Systems Security Professional (CISSP). • ISACA Certified Information Security Manager (CISM)	Individuals must meet certification maintenance requirements by attending relevant conferences, seminars, webinars, and industry conventions, and conducting self-study. Requirements vary. Minimum of 40 hours of continuing education per year is recommended. **RECOMMENDED CONTINUING EDUCATION** • Attend annual threat intelligence training from SANS (or other provider) • Complete (CFR) CyberSec First Responder: Threat Detection and Response (Exam CFR-210) • Participate in annual incident response table-top scenario exercises Recommend attaining one or more of the following specialty certifications such as: • GIAC Strategic Planning, Policy, and Leadership (GSTRT) • (ISC)2 Certified in Governance, Risk, and Compliance (CGRC) • ISACA Certified in Risk and Information Systems Control (CRISC) • PMI Project Management Professional (PMP)
Oversee & Govern	Cybersecurity Training Coordinator	Manages the cybersecurity training, education, and awareness program for the enterprise. Coordinates individual and group training opportunities; organizes cybersecurity color teams practices and captures effectivity metrics.	Current standing in at least one of the following certifications based on certification levels noted to the right. Preferred qualification: Bachelor's degree in cybersecurity, IT security management, IT management, information security. Bachelor's degree in education, communications, or public administration may be acceptable WITH cybersecurity experience.	• CompTIA Security+ • (ISC)2 System Security Certified Practitioner (SSCP) • EC Council Certified Network Defender (CND)	• GIAC Security Essentials Certification (GSEC)	• GIAC Security Leadership (GSLC) • (ISC)2 Certified Information Systems Security Professional (CISSP). • ISACA Certified Information Security Manager (CISM)	Individuals must meet certification maintenance requirements by attending relevant conferences, seminars, webinars, and industry conventions, and conducting self-study. Requirements vary. Minimum of 40 hours of continuing education per year is recommended. **RECOMMENDED CONTINUING EDUCATION** • Attend annual threat intelligence training from SANS (or other provider) • Attend instructional design/workforce training seminars • Attend MITRE ATT&CK training • Observe annual incident response table-top scenario exercises

Investigate	Host Forensics Analyst	Analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/operating system vulnerability mitigation.	Current standing in at least one of the following certifications based on certification levels noted to the right. Preferred qualification: Bachelor's degree in computer science, computer engineering, information systems, computer forensics, or related discipline.	Level 1 certifications would already be accomplished in order to meet the minimum certifications required for the position of Host Forensics Analyst; those certifications are not documented here. See map of stackable certification credentials.	• GIAC Security Essentials (GSEC) • CompTIA Cybersecurity Analyst (CySA+) • CompTIA Advanced Security Practitioner (CASP+) • GIAC Certified Intrusion Analyst Certification (GCIA) • GIAC Certified Incident Handler (GCIH) • DFCB Digital Forensics Certified Associate (DCFA) • ISFCE Certified Computer Examiner (CCE)	• IACIS Certified Forensic Computer Examiner (CFCE) • GIAC Certified Forensic Analyst (GCFA) • GIAC Certified Forensic Examiner (GCFE)	Individuals must meet certification maintenance requirements by attending relevant conferences, seminars, webinars, and industry conventions, and conducting self-study. Requirements vary. Minimum of 40 hours of continuing education per year is recommended. **RECOMMENDED CONTINUING EDUCATION** • Participate in hands-on labs to maintain proficiency with Linux forensics, mobile forensics, iOS forensics • Participate in hands-on labs to learn techniques for forensic analysis within Industrial Control Systems (ICS) • Work toward Cloud certifications relevant to the enterprise environment The following are advanced specialty certifications which may interest an Expert Host Forensic Analyst: • GIAC Battlefield Forensics and Acquisition • GIAC Reverse Engineering Malware (GREM)
Investigate	Cloud Forensics Analyst	Uses forensic techniques to investigate cyber incidents in cloud environments.	Current standing in at least one of the following certifications based on certification levels noted to the right. Preferred qualification: Bachelor's degree in computer science, computer engineering, information systems, computer forensics, or related discipline.	Level 1 certifications would already be accomplished to meet the minimum certifications required for the position of Cloud Forensics Analyst; those certifications are not documented here. See map of stackable certification credentials.	• (ISC)2 Certified Cloud Security (CCSP) • AWS Certified Security • Microsoft Certified: Azure Fundamentals • Google Professional Cloud Security Engineer • GIAC Cloud Threat Detection (GCTD)	• (ISC)2 Certified Cloud Forensics Professional (CCFP) • GIAC Cloud Forensics Responder (GCFR) • GIAC Certified Forensic Examiner (GCFE) • Microsoft Certified: Azure Security Engineer Associate	Individuals must meet certification maintenance requirements by attending relevant conferences, seminars, webinars, and industry conventions, and conducting self-study. Requirements vary. Minimum of 40 hours of continuing education per year is recommended. **RECOMMENDED CONTINUING EDUCATION** • Attend courses such as SANS SEC541: Cloud Security, Attacker Techniquest, Monitoring, and Threat Detection The following are advanced specialty certifications which may interest an Expert Cloud Forensic Analyst: • GIAC Battlefield Forensics and Acquisition • GIAC Reverse Engineering Malware (GREM)
Analyze	Penetration Tester	Performs penetration testing on web applications, networks, and infrastructure along with physical security reviews and social engineering tests to identify an organization's vulnerabilities and security weaknesses.	Current standing in at least one of the following certifications based on certification levels noted to the right. Preferred qualification: Associate's degree in computer science, computer engineering, software development, information systems, cybersecurity, or related discipline.	Level 1 certifications would already be accomplished to meet the minimum certifications required for the Penetration Tester; those certifications are not documented here. See map of stackable certification credentials.	• CompTIA PenTest+ • GIAC Certified Penetration Tester (GPEN) • EC Council Certified Ethical Hacker (CEH) • GIAC Certified Intrusion Analyst Certification (GCIA)	• EC Council Licensed Penetration Tester - Master (LPT) • GIAC Web Application Penetration Tester (GWAPT) • Offensive Security Certified Professional (OSCP)	Individuals must meet certification maintenance requirements by attending relevant conferences, seminars, webinars and industry conventions, and conducting self-study. Requirements vary. Minimum of 40 hours of continuing education per year is recommended. **RECOMMENDED CONTINUING EDUCATION** • Attend OWASP training • Attend MITRE ATT&CK training • Attend annual threat intelligence training from SANS or other provider • Attend scripting or programming language training needed for environment
Analyze	Malware Analyst	Collaborates with network and host forensics analysts to collect malware and analyze the behavior and techniques used in the code to exploit systems.	Current standing in at least one of the following certifications based on certification levels noted to the right. Preferred qualification: Bachelor's degree in computer engineering, computer science, cybersecurity, programming, mathematics, or related field.	Level 1 certifications would already be accomplished to meet the minimum certifications required for the Malware Analyst; those certifications are not documented here. See map of stackable certification credentials.	• GIAC Certified Intrusion Analyst Certification (GCIA)	• Offensive Security Certified Professional (OSCP) • Offensive Security Exploitation Expert (OSEE) • Offensive Security Advanced Evasion Techniques and Breaching Defenses (OSEP) • GIAC Exploit Researcher & Advanced Penetration Tester (GXPN) • GIAC Reverse Engineering Malware Certification (GREM)	Individuals must meet certification maintenance requirements by attending relevant conferences, seminars, webinars, and industry conventions, and conducting self-study. Requirements vary. Minimum of 40 hours of continuing education per year is recommended. **RECOMMENDED CONTINUING EDUCATION** • Attend assembly language training to expanding knowledge of computer architecture and low-level programming Recommend attaining one or more of the following specialty certifications such as • C++ Certified Associate Programmer Certificate (CPA) • Python Institute Certified Associate in Python Programming (PCAP) • Oracle Certified Associate Java Programmer (OCAJP)
Oversee & Govern	Business Process Analyst	Works within the organization and stakeholder entities to improve performance and processes using technology.	Current standing in at least one of the following certifications based on certification levels noted to the right. Preferred qualification: Bachelor's degree in business, economics, information systems, computer science, or related discipline.	• ABPMP Certified Business Process Associate (CBPA) • IIBA Certified Business Analysis Professional (CBAP) • Axelos IT Infrastructure Library (ITIL) Foundations	• Six Sigma Green Belt • ABPMP Certified Business Process Professional (CBPP)	• (ISC)2 Certified Information Security Professional (CISSP) • PMI Project Management Professional (PMP) • Six Sigma Black Belt • AICPA Certified Information Technology Professional (CITP)	Individuals must meet certification maintenance requirements by attending relevant conferences, seminars, webinars, and industry conventions, and conducting self-study. Requirements vary. Minimum of 40 hours of continuing education per year is recommended. **RECOMMENDED CONTINUING EDUCATION** • Attend training on conducting information security risk assessments • Attend training on data security and regulation Recommend attaining one or more of the following certifications: • CompTIA Security+ • (ISC)2 System Security Certified Practitioner (SSCP) • EC Council Certified Network Defender (CND) • GIAC Security Essentials Certification (GSEC)
Investigate	Network Forensics Analyst	Analyzes network traffic and investigates computer security incidents to derive useful information in support of network vulnerability mitigation.	Current standing in at least one of the following certifications based on certification levels noted to the right. Preferred qualification: Bachelor's degree in computer science, computer engineering, information systems, computer forensics, or related discipline.	Level 1 certifications would already be accomplished to meet the minimum certifications required for the position of a Network Forensic Analyst; those certifications are not documented here. See map of stackable certification credentials.	• GIAC Security Essentials (GSEC) • CompTIA Cybersecurity Analyst (CySA+) • CompTIA Advanced Security Practitioner (CASP+) • GIAC Certified Intrusion Analyst Certification (GCIA) • GIAC Certified Incident Handler (GCIH) • GIAC Global Industrial Cyber Security Professional (GICSP)	• GIAC Network Forensic Analyst (GNFA) • (ISC)2 Certified Cyber Forensics Professional (CCFP) • GIAC Certified Intrusion Analyst (GCIA)	Individuals must meet certification maintenance requirements by attending relevant conferences, seminars, webinars, and industry conventions, and conducting self-study. Requirements vary. Minimum of 40 hours of continuing education per year is recommended. **RECOMMENDED CONTINUING EDUCATION** • Participate in hands-on lab training for simulated attacks • Participate in capture-the-flag events • Attend MITRE ATT&CK training Recommend attaining one or more of the following specialty certifications such as • IACRB Certified Cyber Threat Hunting Professional (CCTHP) • GIAC Reverse Engineering Malware (GREM)

Collect & Operate	Systems Analyst	Responsible for analyzing, modifying, designing, and managing IT systems and networks for the organization or its affiliated agencies / clients.	Current standing in at least one of the following certifications based on certification levels noted to the right. Preferred qualification: Bachelor's degree in computer science, computer engineering, information systems, cybersecurity or related discipline.	• CompTIA A+ • CompTIA Network+ • CompTIA Security+ • EC Council Certified Network Defender (CND) • (ISC)2 System Security Certified Professional (SSCP) • Axelos IT Information Library Foundations (ITIL)	• GIAC Security Essentials (GSEC) • CompTIA Cybersecurity Analyst (CySA+) • CompTIA Advanced Security Practitioner (CASP+) • ISACA Certified Information Systems Auditor (CISA) • GIAC Certified Enterprise Defender (GCED)	• (ISC)2 Certified Information Security Professional (CISSP) • ISACA Certified Information Security Manager (CISM) • PMI Project Management Professional (PMP)	Individuals must meet certification maintenance requirements by attending relevant conferences, seminars, webinars and industry conventions, and conducting self-study. Requirements vary. Minimum of 40 hours of continuing education per year is recommended. RECOMMENDED CONTINUING EDUCATION • Attend annual threat intelligence training from SANS (or other provider) • Attend Systems Development Lifecycle (SDLC) training Recommend attaining one or more of the following specialty certifications such as • PMI Agile Certified Practitioner (ACP) • PMI Certified Scrum Master (CSM) • GIAC Certified Incident Handler (GCIH) • GIAC Certified Intrusion Analyst Certification (GCIA)
Collect & Operate	SIEM Engineer	Configure and customize Security Information and Event Management (SIEM), Data Loss Prevention (DLP), and Intrusion Detection/Prevention System (IDS/IPS) tools. Review suspicious patterns and signatures and write custom scripts to detect malware and eliminate network noise.	Recommend vendor-specific certifications focused on technology in use the environment such as Splunk, QRadar, or other SIEM toolset. Preferred qualification: Bachelor's degree in computer science, computer engineering, information systems, cybersecurity, or related discipline.	Level 1 certifications would already be accomplished to meet the minimum certifications required for the SIEM Engineer; those certifications are not documented here. See map of stackable certification credentials.	• CompTIA Cybersecurity Analyst (CySa+) • CompTIA Advanced Security Practioner (CASP+) • GIAC Defensible Security Architect (GDSA) • GIAC Certified Enterprise Defender (GCED) • EC Council Certified SOC Analyst (CSA) • SBT Blue Team Level 2 (BTL2) • GIAC Certified Intrusion Analyst Certification (GCIA)	• SBT Certified Security Operations Manager (CSOM) • (ISC)2 Certified Information Security Professional (CISSP) • ISACA Certified Information Security Manager (CISM)	Individuals must meet certification maintenance requirements by attending relevant conferences, seminars, webinars and industry conventions, and conducting self-study. Requirements vary. Minimum of 40 hours of continuing education per year is recommended. **RECOMMENDED CONTINUING EDUCATION** • Attend annual threat intelligence training from SANS (or other provider) • Maintain vendor-specific training depending on environment such as Splunk or QRadar. • Attend training on MITRE ATT&CK Framework • Attend SANS SEC555: SIEM with Tactical Analytics or similar course Recommend attaining one or more of the following specialty certifications such as • GIAC Certified Incident Handler (GCIH) • EC Council Certified Incident Handler (ECIH) • IACRB Certified Cyber Threat Hunting Professional (CCTHP)

Collect & Operate	DevSecOps Engineer	Creates and maintains secure systems with a focus on integrating security throughout the development lifecycle. Works with stakeholders to ensure systems are protected from potential threats and vulnerabilities.	Recommend vendor-specific certifications focused on technology in use the environment (such as AWS, Azure, or RedHat), Recommend certifications in deployment tools such as Puppet, Terraform, and Chef. Preferred qualification: Bachelor's degree in computer science, computer engineering, information technology, cybersecurity or related discipline.	Level 1 certifications would already be accomplished in order to meet the minimum certifications required for the SIEM Engineer; those certifications are not documented here. See map of stackable certification credentials.	• GIAC Defensible Security Architect (GDSA) • GIAC Certified Enterprise Defender (GCED) • Puppet Certified Professional • Certified Kubernetes Administrator (CKA) • Docker Certified Associate (DCA) • Jenkins Certified Engineer	• AWS Certified DevOps Engineer • Azure DevOps Engineer • RedHat Certified Engineer in DevOps Automation	Individuals must meet certification maintenance requirements by attending relevant conferences, seminars, webinars and industry conventions, and conducting self-study. Requirements vary. Minimum of 40 hours of continuing education per year is recommended. RECOMMENDED CONTINUING EDUCATION • Attend security training for development within the Software/Systems Development Lifecycle (SDLC) • Attend training on security development for Cloud infrastructures (i.e. Kubernetes Security Specialist) Recommend attaining one or more of the following specialty certifications such as • PMI Agile Certified Practitioner (ACP) • PMI Certified Scrum Master (CSM) • (ISC)2 Certified Cloud Security Professional (CCSP) • GIAC Certified Incident Handler (GCIH)
Collect & Operate	Application Developer	Creates, tests, programs, and maintains cybersecurity software, utilities, and tools for a specific device, operating system, or client/purpose.	Recommend vendor-specific certifications focused on technology in use the environment (such as Python, C/C++, Java). Should be familiar with Git, API development, data structures and algorithms, and cloud infrastructures. Recommended cybersecurity certifications are listed by level on the right. Preferred qualification: Bachelor's degree in software engineering, computer science, cybersecurity, information technology, or a related discipline.	• CompTIA Security+ • EC Council Certified Network Defender (CND) • (ISC)2 System Security Certified Professional (SSCP)	• EC Council Certified Secure Programmer (ECSP) • EC Council Certified Secure Application Developer (CSAD) • (ISC)2 Certified Secure Software Lifecycle Professional (CSSLP)	• IEEE Certified Software Development Professional (CSDP) • IEEE Software Engineering Master Certification (SEMC).	Individuals must meet certification maintenance requirements by attending relevant conferences, seminars, webinars and industry conventions, and conducting self-study. Requirements vary. Minimum of 40 hours of continuing education per year is recommended. **RECOMMENDED CONTINUING EDUCATION** • Attend training for Software Development Lifecycle (SDLC) Recommend attaining one or more of the following specialty certifications such as • PMI Agile Certified Practitioner (ACP)

Analyze	Threat Intelligence Analyst	Analyzes cyber threat intelligence and indicators of compromise to communicate awareness of cyber threats throughout the business environment.	Current standing in at least one of the following certifications based on certification levels noted to the right. Preferred qualification: Bachelor's degree in cybersecurity, information technology, or a related discipline.	• CompTIA Security+ • (ISC)2 System Security Certified Practitioner (SSCP) • EC Council Certified Network Defender (CND)	• GIAC Security Essentials Certification (GSEC) • GIAC Cyber Threat Intelligence (GCTI) • EC Council Threat Intelligence Analyst (CTIA)	• (ISC)2 Certified Information Security Professional (CISSP) • ISACA Certified Information Security Manager (CISM)	Individuals must meet certification maintenance requirements by attending relevant conferences, seminars, webinars and industry conventions, and conducting self-study. Requirements vary. Minimum of 40 hours of continuing education per year is recommended. **RECOMMENDED CONTINUING EDUCATION** • Attend annual threat intelligence training from SANS or other provider • Attend MITRE ATT&CK training • Participate in annual incident response table-top scenario exercises Recommend attaining one or more of the following specialty certifications such as: • GIAC Certified Incident Handler (GCIH) • IACRB Certified Cyber Threat Hunting Professional (CCTHP) • GIAC Certified Intrusion Analyst Certification (GCIA)
Collect & Operate	Cybersecurity Analyst	Analyzes cybersecurity policies and protocols, conducts audits and risk assessments. Assesses security technology, monitors networks for security breaches and investigates when breaches occur. Researches latest cybersecurity trends and prepares reports of metrics for cyber incidents and attacks.	Current standing in at least one of the following certifications based on certification levels noted to the right. Preferred qualification: Associate's degree in cybersecurity, information technology, networking, or a related discipline.	• CompTIA Network+ • CompTIA Security+ • EC Council Cyber Network Defender (CND) • (ISC)2 System Security Certified Professional (SSCP)	• GIAC Security Essentials (GSEC) • CompTIA Cybersecurity Analyst (CySA+) • CompTIA Advanced Security Practitioner (CASP+) • ISACA Certified Information Systems Auditor (CISA) • GIAC Certified Enterprise Defender (GCED) • GIAC Certified Intrusion Analyst Certification (GCIA) • GIAC Certified Incident Handler (GCIH)	Level 3 certifications for a Cybersecurity Analyst depend on the career focus. See Level 3 certification in any of the Govern, Investigate, Analyze, or Protect & Defend workforce categories.	Individuals must meet certification maintenance requirements by attending relevant conferences, seminars, webinars and industry conventions, and conducting self-study. Requirements vary. Minimum of 40 hours of continuing education per year is recommended. **RECOMMENDED CONTINUING EDUCATION** • Attend training on SIEM tools in use to gain advanced skills in creating dashboards and filtering data • Attend training on MITRE ATT&CK Framework • Attend training for NIST policies • Attend training for privacy regulation and identity access management (IAM) best practices Recommend attaining one or more of the following specialty certifications such as • (ISC)2 Information Systems Security Engineer (CISSP-ISSEP)

Operate & Maintain	Helpdesk	Serves as the first point of contact for customers seeking technical assistance via phone or email, performs remote troubleshooting through diagnostic techniques and asking pertinent questions. Determines the best solution to resolve the issue or escalates the issue to more experienced resources.	Current standing in at least one of the following certifications based on certification levels noted to the right. Preferred qualification: Associate's degree in cybersecurity, information technology, or a related discipline.	• CompTIA A+ • CompTIA Network+ • CompTIA Security+ • ITIL Foundations • Microsoft 365: Certified Endpoint Administrator Associate			Individuals must meet certification maintenance requirements by attending relevant conferences, seminars, webinars and industry conventions, and conducting self-study. Requirements vary. Minimum of 40 hours of continuing education per year is recommended. **RECOMMENDED CONTINUING EDUCATION** • Attend training on specific tools and applications used within the environment such as specialty printers, virtual machines, or operating systems other than Windows. Recommend attaining one or more of the following specialty certifications such as • CompTIA Linux+ • CompTIA Server+ • CompTIA Cloud+
Operate & Maintain	Network Technician	Monitors and analyzes network traffic to identify and resolve cyber threats. Configures, maintains, and troubleshoots routers, switches, firewalls, and other network and security devices.	Current standing in at least TWO of the following certifications based on certification levels noted to the right. Preferred qualification: Associate's degree in cybersecurity, information technology, network technology, or a related discipline.	• CompTIA A+ • CompTIA Network+ • Cisco Certified Technician (CCT) • CompTIA Security+ • CompTIA Linux+ • CompTIA Cloud+ • EC-Council Certified Network Defender (CND) • (ISC)2 System Security Certified Practitioner (SSCP)	• Cisco Certified Network Associate (CCNA) • Cisco Certified CyberOps Associate (CCNA-CyberOps) • EC Council Network Security Administrator (ENSA)	• Cisco Certified Network Professional - Enterprise (CCNP)	Individuals must meet certification maintenance requirements by attending relevant conferences, seminars, webinars and industry conventions, and conducting self-study. Requirements vary. Minimum of 40 hours of continuing education per year is recommended. **RECOMMENDED CONTINUING EDUCATION** • Attend training on how to secure specific tools and applications used within the environment such as vendor-specific firewalls, Juniper networks, or cloud configurations. Recommend attaining one or more of the following specialty certifications such as • AWS Cloud Practitioner • Azure Cloud Fundamentals • Google Cloud Digital Leader
Protect & Defend	Cyber Operations Coordinator	Direct CSOC operations, responsible for syncing between analysts and engineers; hiring; training; and creating and executing on cybersecurity strategy. Direct and orchestrate the responses to cybersecurity threats.	Current standing in at least TWO of the following certifications based on certification levels noted to the right. Preferred qualification: Bachelor's degree in cybersecurity, information technology, networking, or a related discipline.	• CompTIA Network+ • CompTIA Security+ • EC Council Cyber Network Defender (CND) • (ISC)2 System Security Certified Professional (SSCP) • CompTIA Cloud+	• EC Council Certified Ethical Hacker (CEH) • CompTIA Cybersecurity Analyst (CySA+) • CompTIA Advanced Security Practitioner (CASP+) • EC Council Certified Incident Handler (ECIH) • GIAC Certified Incident Handler (GCIH) • GIAC Certified Detection Analyst (GCDA) • SBT Blue Team Level 1 (BTL1)	• SBT Blue Team Level 2 (BTL2) • SBT Certified Security Operations Manager (CSOM) • Mile2 Certified Incident Handling Engineer (CIHE) • GIAC Security Leadership (GSLC) • (ISC)2 Information Security System Professional (CISSP) • ISACA Certified Information Security Manager (CISM)	Individuals must meet certification maintenance requirements by attending relevant conferences, seminars, webinars, and industry conventions, and conducting self-study. Requirements vary. Minimum of 40 hours of continuing education per year is recommended. **RECOMMENDED CONTINUING EDUCATION** • Attend USG CISA Incident Response Training (IRT) • Attend annual threat intelligence training from SANS or other provider • Participate in annual incident response table-top scenario exercises • Complete (CFR) CyberSec First Responder: Threat Detection and Response (Exam CFR-210) • Attend Public Relations/Communications training for Incident Response Recommend attaining one or more of the following specialty certifications such as • Mile2 Certified Disaster Recovery Specialist (CDRE) • GIAC Battlefield Forensics & Acquisition (GBFA)
Protect & Defend	SIEM Analyst	Monitors and analyzes network security sensors to identify, triage, remediate, or escalate cyber incidents. Maintains and tunes security rule, queries, and filters for collection within the Security Information and Even Management (SIEM) toolset.	Current standing in at least one of the following certifications based on certification levels noted to the right. Preferred qualification: Associate's degree in cybersecurity, information technology, networking, or a related discipline.	• CompTIA Network+ • CompTIA Security+ • EC Council Cyber Network Defender (CND) • (ISC)2 System Security Certified Professional (SSCP)	• EC Council Certified Ethical Hacker (CEH) • CompTIA Cybersecurity Analyst (CySa+) • CompTIA Advanced Security Practioner (CASP+) • GIAC Certified Enterprise Defender (GCED) • EC Council Certified SOC Analyst (CSA) • SBT Blue Team Level 1 (BTL1) • EC Council Certified Incident Handler (ECIH) • GIAC Certified Intrusion Analyst Certification (GCIA)	• SBT Blue Team Level 2 (BTL2) • SBT Certified Security Operations Manager (CSOM) • (ISC)2 Certified Information Security Professional (CISSP) • ISACA Certified Information Security Manager (CISM)	Individuals must meet certification maintenance requirements by attending relevant conferences, seminars, webinars, and industry conventions, and conducting self-study. Requirements vary. Minimum of 40 hours of continuing education per year is recommended. **RECOMMENDED CONTINUING EDUCATION** • Attend digital or network forensics training • Attend incident response training • Attend vendor-specific training on security infrastructure toolsets for IDS/IPSs and SIEMs, and vulnerability scanning tools in use in the environment. • Participate in Capture-the-Flag events Recommend attaining one or more of the following specialty certifications such as • GIAC Network Forensic Analyst (GNFA) • DFCB Digital Forensics Certified Associate (DCFA) • IACRB Certified Cyber Threat Hunting Professional (CCTHP)

Protect & Defend	Senior Incident Responder	Supports end-to-end incident response process for the enterprise including analysis, containment, eradication, recovery, and stakeholder communications. Develops and oversees cybersecurity metrics to measure operational effectiveness to drive improvement.	Current standing in at least one of the following certifications based on certification levels noted to the right. Preferred qualification: Bachelor's degree in cybersecurity, information security, or a related discipline. Bachelor's degree in political science, business management, communications, or public administration may be acceptable WITH cybersecurity experience.	Level 1 certifications would already be accomplished to meet the minimum certifications required for the Senior Incident Responder; those certifications are not documented here. See map of stackable certification credentials.	• CompTIA Cybersecurity Analyst (CySa+) • CompTIA Advanced Security Practioner (CASP+) • GIAC Certified Enterprise Defender (GCED) • EC Council Certified Incident Handler (ECIH) • GIAC Certified Incident Handler (GCIH) • GIAC Certified Intrusion Analyst Certification (GCIA) • CertNexus CyberSec First Responder: Threat Detection and Response (CFR) • SBT Blue Team Level 2 (BTL2)	• Mile2 Certified Incident Handling Engineer (CIHE) • (ISC)2 Certified Information Security Professional (CISSP) • ISACA Certified Information Security Manager (CISM)	Individuals must meet certification maintenance requirements by attending relevant conferences, seminars, webinars and industry conventions, and conducting self-study. Requirements vary. Minimum of 40 hours of continuing education per year is recommended. **RECOMMENDED CONTINUING EDUCATION** • Attend USG CISA Incident Response Training (IRT) • Attend annual threat intelligence training from SANS or other provider • Complete (CFR) CyberSec First Responder: Threat Detection and Response (Exam CFR-210) • Participate in annual incident response table-top scenario exercises • Attend Public Relations/Communications training for Incident Response Recommend attaining one or more of the following specialty certifications such as • Mile2 Certified Disaster Recovery Specialist (CDRE) • GIAC Battlefield Forensics & Acquisition (GBFA)
Protect & Defend	Incident Responder	Responsible for monitoring and analyzing an organization's network and systems for security threats and vulnerabilities. Detects and responds to cybersecurity incidents covering all phases of attack to include containment and eradication. Analyzes cybersecurity incidents and escalates responses to the CSIRT as needed.	Current standing in at least one of the following certifications based on certification levels noted to the right. Preferred qualification: Associate's degree in cybersecurity, information security, or a related discipline. A degree in political science, business management, communications, or public administration may be acceptable WITH cybersecurity experience.	• CompTIA Security+ • EC-Council Certified Network Defender (CND)	• EC Council Certified Ethical Hacker (CEH) • SBT Blue Team Level 1 (BTL1) • CompTIA Cybersecurity Analyst (CySa+) • CompTIA Advanced Security Practioner CE (CASP) • GIAC Certified Enterprise Defender (GCED) • EC Council Certified Incident Handler (ECIH) • GIAC Certified Incident Handler (GCIH) • SBT Blue Team Level 1 (BTL1)	• SBT Blue Team Level 2 (BTL2) • Mile2 Certified Incident Handling Engineer (CIHE)	Individuals must meet certification maintenance requirements by attending relevant conferences, seminars, webinars and industry conventions, and conducting self-study. Requirements vary. Minimum of 40 hours of continuing education per year is recommended. **RECOMMENDED CONTINUING EDUCATION** • Attend training on SIEM tools in use, traffic analysis, • Attend training on MITRE ATT&CK Framework • Complete (CFR) CyberSec First Responder: Threat Detection and Response (Exam CFR-210) Recommend attaining one or more of the following specialty certifications such as • GIAC Network Forensic Analyst (GNFA) • (ISC)2 Certified Cyber Forensics Professional (CCFP) • GIAC Certified Intrusion Analyst (GCIA) • GIAC Global Industrial Cyber Security Professional (GICSP)

Operate & Maintain	Helpdesk	Serves as the first point of contact for customers seeking technical assistance via phone or email, performs remote troubleshooting through diagnostic techniques and asking pertinent questions. Determines the best solution to resolve the issue or escalates the issue to more experienced resources.	Current standing in at least one of the following certifications based on certification levels noted to the right. Preferred qualification: Associate's degree in cybersecurity, information technology, or a related discipline.	• CompTIA A+ • CompTIA Network+ • CompTIA Security+ • ITIL Foundations • Microsoft 365: Certified Endpoint Administrator Associate			Individuals must meet certification maintenance requirements by attending relevant conferences, seminars, webinars and industry conventions, and conducting self-study. Requirements vary. Minimum of 40 hours of continuing education per year is recommended. **RECOMMENDED CONTINUING EDUCATION** • Attend training on specific tools and applications used within the environment such as specialty printers, virtual machines, or operating systems other than Windows. Recommend attaining one or more of the following specialty certifications such as • CompTIA Linux+ • CompTIA Server+ • CompTIA Cloud+
Operate & Maintain	Network Technician	Monitors and analyzes network traffic to identify and resolve cyber threats. Configures, maintains, and troubleshoots routers, switches, firewalls, and other network and security devices.	Current standing in at least TWO of the following certifications based on certification levels noted to the right. Preferred qualification: Associate's degree in cybersecurity, information technology, network technology, or a related discipline.	• CompTIA A+ • CompTIA Network+ • Cisco Certified Technician (CCT) • CompTIA Security+ • CompTIA Linux+ • CompTIA Cloud+ • EC-Council Certified Network Defender (CND) • (ISC)2 System Security Certified Practitioner (SSCP)	• Cisco Certified Network Associate (CCNA) • Cisco Certified CyberOps Associate (CCNA-CyberOps) • EC Council Network Security Administrator (ENSA)	• Cisco Certified Network Professional - Enterprise (CCNP)	Individuals must meet certification maintenance requirements by attending relevant conferences, seminars, webinars and industry conventions, and conducting self-study. Requirements vary. Minimum of 40 hours of continuing education per year is recommended. **RECOMMENDED CONTINUING EDUCATION** • Attend training on how to secure specific tools and applications used within the environment such as vendor-specific firewalls, Juniper networks, or cloud configurations. Recommend attaining one or more of the following specialty certifications such as • AWS Cloud Practitioner • Azure Cloud Fundamentals • Google Cloud Digital Leader

Operate & Maintain	Systems Analyst	Deploy, maintain, and troubleshoot core business applications, including application servers, associated hardware, endpoints, and databases. Develop, analyze, and prioritize requirements specifications for developers and testers.	Current standing in at least one of the following certifications based on certification levels noted to the right. Preferred qualification: Bachelor's Degree in computer science, information science, technical writing, or a related analytics field.	• Axelos IT Infrastructure Library (ITIL) Foundations • CompTIA Security+ • (ISC)2 System Security Certified Practitioner (SSCP)	• GIAC Security Essentials Certification (GSEC) • EC Council Certified Security Analyst (ECSA) • CompTIA Cybersecurity Analyst (CySA+) • CompTIA Advanced Security Practitioner (CASP+)	• (ISC)2 Certified Information Security Professional (CISSP) • ISACA Certified Information Security Manager (CISM)	Individuals must meet certification maintenance requirements by attending relevant conferences, seminars, webinars and industry conventions, and conducting self-study. Requirements vary. Minimum of 40 hours of continuing education per year is recommended. **RECOMMENDED CONTINUING EDUCATION** • Attend compliance training for data and access management • Maintain familiarity with NIST and CIS Critical Security Controls • Attend annual threat intelligence training from SANS (or other provider) • Participate in annual incident response table-top scenario exercises Recommend attaining one or more of the following specialty certifications such as • EC Council Certified Ethical Hacker (CEH) • DAMA Certified Data Management Professional (CDMP) • PMI Project Management Professional (PMP)
Operate & Maintain	Compliance Analyst	Ensures enterprise operations and procedures meet appropriate local, federal, and state laws and regulation. Examines and develops policies and procedures, identifies areas out of compliance, and advises on methods for necessary modifications.	Current standing in at least one of the following certifications based on certification levels noted to the right. Preferred qualification: Bachelor's degree in IT security management, information security, cybersecurity, or related discipline.	• CompTIA Security+ • (ISC)2 System Security Certified Practitioner (SSCP)	• GIAC Security Essentials Certification (GSEC) • ISACA Certified Information Security Auditor (CISA) • ISACA Certified in Risk & Information Systems Control (CRISC) • GRMI Certified Risk Management Professional (CRMP)	• PMI Project Management Professional-Risk Management Certification (PMP-RMC) • (ISC)2 Information System Security Professional (CISSP) • (ISC)2 Information System Security Engineering Professional (CISSP-ISSEP)	Individuals must meet certification maintenance requirements by attending relevant conferences, seminars, webinars and industry conventions, and conducting self-study. Requirements vary. Minimum of 40 hours of continuing education per year is recommended. **RECOMMENDED CONTINUING EDUCATION** • Attend compliance training for data and access management • Maintain familiarity with NIST controls Recommend attaining one or more of the following specialty certifications such as: • GIAC Strategic Planning, Policy, and Leadership (GSTRT) • (ISC)2 Certified in Governance, Risk, and Compliance (CGRC) • PMI Project Management Professional (PMP)
Operate & Maintain	Network Administrator	Develops, manages, and maintains network infrastructure to include documentation of policies, procedures, inventory, and performance metrics.	Current standing in at least TWO of the following certifications based on certification levels noted to the right. Preferred qualification: Bachelor's degree in cybersecurity, information technology, network technology, or a related discipline.	• CompTIA A+ • CompTIA Network+ • Cisco Certified Technician (CCT) • CompTIA Security+ • CompTIA Linux+ • CompTIA Cloud+ • EC-Council Certified Network Defender (CND) • (ISC)2 System Security Certified Practitioner (SSCP)	• Cisco Certified Network Associate (CCNA) • Cisco Certified CyberOps Associate (CCNA-CyberOps) (CCNA-CyberOps) • EC Council Network Security Administrator (ENSA)	• Cisco Certified Network Professional - Enterprise (CCNP)	Individuals must meet certification maintenance requirements by attending relevant conferences, seminars, webinars and industry conventions, and conducting self-study. Requirements vary. Minimum of 40 hours of continuing education per year is recommended. **RECOMMENDED CONTINUING EDUCATION** • Attend Security Essentials for IT Administrators (offered by SANS, but similar content is available from other vendors) • Attend cloud security training in relevant enterprise cloud infrastructure Recommend attaining one or more of the following specialty certifications such as • VMware Certified Professional (VCP) • (ISC)2 Certified Cloud Security Professional (CCSP)
Operate & Maintain	System Admin	Installs, configures, manages, and monitors systems, networks, applications, and devices for the enterprise. Identifies vulnerabilities and maintains the patch management program. This position includes maintaining system firewalls, anti-virus programs, and managing user access. Troubleshoots servers and client systems and provides technical support to users.	Recommend vendor-specific certifications focused on technology in use the environment (such as Windows, Linux, iOS, VMware, Cisco, Palo Alto, etc. - as well as any cloud infrastructure in use). Recommended cybersecurity certifications are listed by level on the right. Preferred qualification: Bachelor's degree in computer science, cybersecurity, information technology, or a related discipline.	• CompTIA Network+ • CompTIA Server+ • CompTIA Security+ • CompTIA Linux+ • CompTIA Cloud+ • EC-Council Certified Network Defender (CND) • (ISC)2 System Security Certified Practitioner (SSCP)	• Microsoft Certified: Azure Administrator Associate • Microsoft 365 Certified: Security Administrator Associate • Cisco Certified Network Associate (CCNA)	• CompTIA Advanced Security Practitioner (CASP CE) • (ISC)2 Certified Information Security Professional (CISSP) • ISACA Certified Information Security Manager (CISM)	Individuals must meet certification maintenance requirements by attending relevant conferences, seminars, webinars and industry conventions, and conducting self-study. Requirements vary. Minimum of 40 hours of continuing education per year is recommended. **RECOMMENDED CONTINUING EDUCATION** • Attend training on Business Continuity and Disaster Recovery • Complete specialization training within the Microsoft Certified tracks such as Security, Compliance, & Identity Fundamentals; Endpoint Administrator; or Identity & Services. Recommend attaining one or more of the following specialty certifications if relevant to the enterprise environment: • Microsoft Cybersecurity Architect • Microsoft Identity and Access Administrator • Red Hat Certified Systems Administrator (RHCSA) • VMware Certified Professional - Data Center Virtualization

Securely Provision	Application Developer	Creates, tests, programs, and maintains cybersecurity software, utilities, and tools for a specific device, operating system, or client/purpose.	Recommend vendor-specific certifications focused on technology in use the environment (such as Python, C/C++, Java). Should be familiar with Git, API development, data structures and algorithms, and cloud infrastructures. Recommended cybersecurity certifications are listed by level on the right. Preferred qualification: Bachelor's degree in software engineering, computer science, cybersecurity, information technology, or a related discipline.	• CompTIA Security+ • EC Council Certified Network Defender (CND) • (ISC)2 System Security Certified Professional (SSCP)	• EC Council Certified Secure Programmer (ECSP) • EC Council Certified Secure Application Developer (CSAD) • (ISC)2 Certified Secure Software Lifecycle Professional (CSSLP)	• IEEE Certified Software Development Professional (CSDP) • IEEE Software Engineering Master Certification (SEMC).	Individuals must meet certification maintenance requirements by attending relevant conferences, seminars, webinars and industry conventions, and conducting self-study. Requirements vary. Minimum of 40 hours of continuing education per year is recommended. **RECOMMENDED CONTINUING EDUCATION** • Attend Software Development Lifecycle (SDLC) training • Attend training in secure coding principles, techniques, and best practices • Attend training in Agile/Scrum/DevOps Recommend attaining one or more of the following specialty certifications such as • PMI Agile Certified Practitioner (ACP)
Securely Provision	Security Architect	Plans and designs resilient security architectures for various IT projects based on stakeholder needs. Develops prerequisites for networks, firewalls, routers, and other network devices, then implements solutions with updated security standards, systems, and best practices.	Current standing in at least one of the following certifications based on certification levels noted to the right. Preferred qualification: Bachelor's degree in computer science, computer engineering, information technology, cybersecurity, or related discipline.	• CompTIA A+ • CompTIA Network+ • Cisco Certified Technician (CCT) • CompTIA Security+ • CompTIA Cloud+ • EC-Council Certified Network Defender (CND) • (ISC)2 System Security Certified Practitioner (SSCP)E	• GIAC Security Essentials Certification (GSEC) • Cisco Certified Network Associate (CCNA) • Cisco Certified Network Professional (CCNP) • CompTIA Cybersecurity Analyst (CySA+) • CompTIA Advanced Security Practitioner (CASP+) • ISACA Certified Information Systems Auditor (CISA)	• CREST Registered Technical Security Architect (CRTSA) • The Open Group Architecture Framework (TOGAF) certification • (ISC)2 Information System Security Architect Professional (CISSP-ISSAP)	Individuals must meet certification maintenance requirements by attending relevant conferences, seminars, webinars and industry conventions, and conducting self-study. Requirements vary. Minimum of 40 hours of continuing education per year is recommended. **RECOMMENDED CONTINUING EDUCATION** • Attend training on Business Continuity and Disaster Recovery • Complete specialization training within the Microsoft Certified tracks such as Security, Compliance, & Identity Fundamentals; Endpoint Administrator; or Identity & Services. Recommend attaining one or more of the following specialty certifications such as • GIAC Certified Enterprise Defender (GCED) • GIAC Certified Incident Handler (GCIH) • GIAC Enterprise Vulnerability Assessor • NICCS Certified Vulnerability Assessor (CVA) • (ISC)2 Information System Security Architect Professional (CISSP-ISSAP)
Securely Provision	System Admin	Installs, configures, manages, and monitors systems, networks, applications, and devices for the enterprise. Identifies vulnerabilities and maintains the patch management program. This position includes maintaining system firewalls, anti-virus programs, and managing user access. Troubleshoots servers and client systems, and provides technical support to users.	Recommend vendor-specific certifications focused on technology in use the environment (such as Windows, Linux, iOS, VMware, Cisco, Palo Alto, etc. - as well as any cloud infrastructure in use). Recommended cybersecurity certifications are listed by level on the right. Preferred qualification: Bachelor's degree in computer science, cybersecurity, information technology, or a related discipline.	• CompTIA Network+ • CompTIA Server+ • CompTIA Security+ • CompTIA Linux+ • CompTIA Cloud+ • EC-Council Certified Network Defender (CND) • (ISC)2 System Security Certified Practitioner (SSCP)	• Microsoft Certified: Azure Administrator Associate • Microsoft 365 Certified: Security Administrator Associate • Cisco Certified Network Associate (CCNA) • CompTIA Advanced Security Practitioner (CASP+)	• (ISC)2 Certified Information Security Professional (CISSP) • ISACA Certified Information Security Manager (CISM)	Individuals must meet certification maintenance requirements by attending relevant conferences, seminars, webinars and industry conventions, and conducting self-study. Requirements vary. Minimum of 40 hours of continuing education per year is recommended. **RECOMMENDED CONTINUING EDUCATION** • Attend training on Business Continuity and Disaster Recovery • Complete specialization training within the Microsoft Certified tracks such as Security, Compliance, & Identity Fundamentals; Endpoint Administrator; or Identity & Services. Recommend attaining one or more of the following specialty certifications if relevant to the enterprise environment: • Microsoft Cybersecurity Architect • Microsoft Identity and Access Administrator • Red Hat Certified Systems Administrator (RHCSA) • VMware Certified Professional - Data Center Virtualization
Securely Provision	Application Architect	Designs major aspects of an application including components such as user interface, middleware, and infrastructure. Provides technical leadership to the application development team; performs code review and ensures enterprise-wide application design standards are maintained.	Recommend vendor-specific certifications focused on technology in use the environment (such as Python, C/C++, Java, .NET, PHP). Should be familiar with Git, API development, data structures and algorithms, and cloud infrastructures, and SDLC. Recommended cybersecurity certifications are listed by level on the right. Preferred qualification: Bachelor's degree in software engineering, computer science, cybersecurity, information technology, or a related discipline.	Level 1 certifications would already be accomplished in order to meet the minimum certifications required for the Application Architect; those certifications are not documented here. See map of stackable certification credentials.	• EC Council Certified Secure Programmer (ECSP) • EC Council Certified Secure Application Developer (CSAD) • (ISC)2 Certified Secure Software Lifecycle Professional (CSSLP)	• IEEE Certified Software Development Professional (CSDP) • IEEE Software Engineering Master Certification (SEMC).	Individuals must meet certification maintenance requirements by attending relevant conferences, seminars, webinars and industry conventions, and conducting self-study. Requirements vary. Minimum of 40 hours of continuing education per year is recommended. **RECOMMENDED CONTINUING EDUCATION** • Attend OWASP training • Attend MITRE ATT&CK training • Attend training in secure coding principles, techniques, and best practices Recommend attaining one or more of the following specialty certifications such as • PMI Agile Certified Practitioner (ACP)
Securely Provision	Security Engineer	Works closely with cross-functional teams, including IT, network engineering, and cybersecurity, to ensure that systems and networks are secure, compliant with applicable regulations, and protected against unauthorized access and other security risks.	Current standing in at least one of the following certifications based on certification levels noted to the right. Preferred qualification: Bachelor's degree in computer science, computer engineering, information technology, cybersecurity or related discipline.	Level 1 certifications would already be accomplished to meet the minimum certifications required for the Security Engineer; those certifications are not documented here. See map of stackable certification credentials.	• GIAC Security Essentials Certification (GSEC) • CompTIA Cybersecurity Analyst (CySA+) • CompTIA Advanced Security Practitioner (CASP+) • ISACA Certified Information Systems Auditor (CISA) • (ISC)2 Certified Cloud Security Professional (CCSP)	• Cisco Certified Network Professional (CCNP) • Cisco Certified Network Professional - DevNet Professional (CCNP-DevNet)	Individuals must meet certification maintenance requirements by attending relevant conferences, seminars, webinars and industry conventions, and conducting self-study. Requirements vary. Minimum of 40 hours of continuing education per year is recommended. **RECOMMENDED CONTINUING EDUCATION** • Maintain awareness of NIST, ISO 27001, and CIS Critical Security Controls documentation and guidance • Attend vendor-specific training on security infrastructure toolsets for IDS/IPSs, SIEMs, and vulnerability scanning tools in use in the environment. Recommend attaining one or more of the following specialty certifications such as • PMI Project Management Professional (PMP) • EC Council Certified Ethical Hacker (CEH) • GIAC Certified Enterprise Defender (GCED) • GIAC Certified Incident Handler (GCIH) • GIAC Global Industrial Cyber Security Professional (GICSP)