SANS | GIAC

DEEPER KNOWLEDGE.
ADVANCED SECURITY.

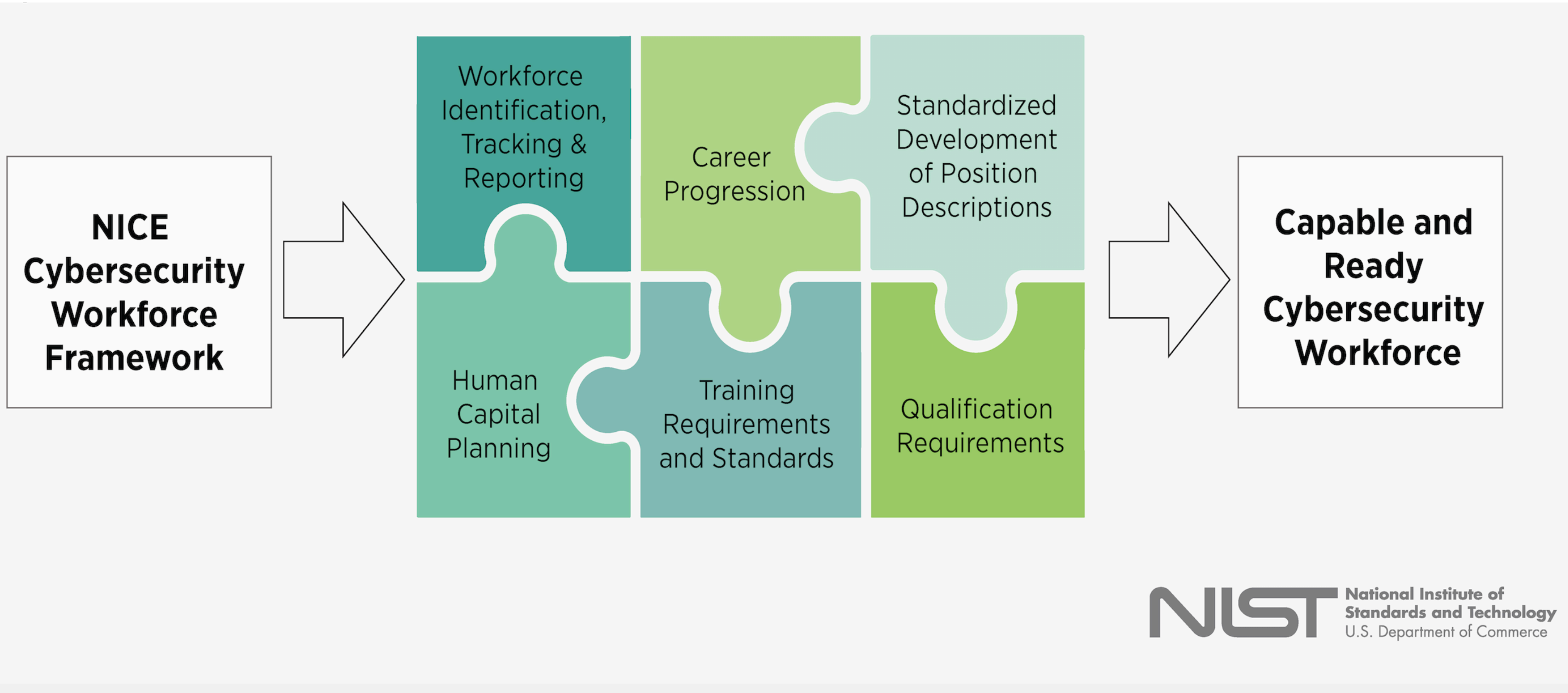
SANS and GIAC Certifications

in alignment with the
NICE Cyber Security
Workforce Framework

NIST Special Publication 800-181

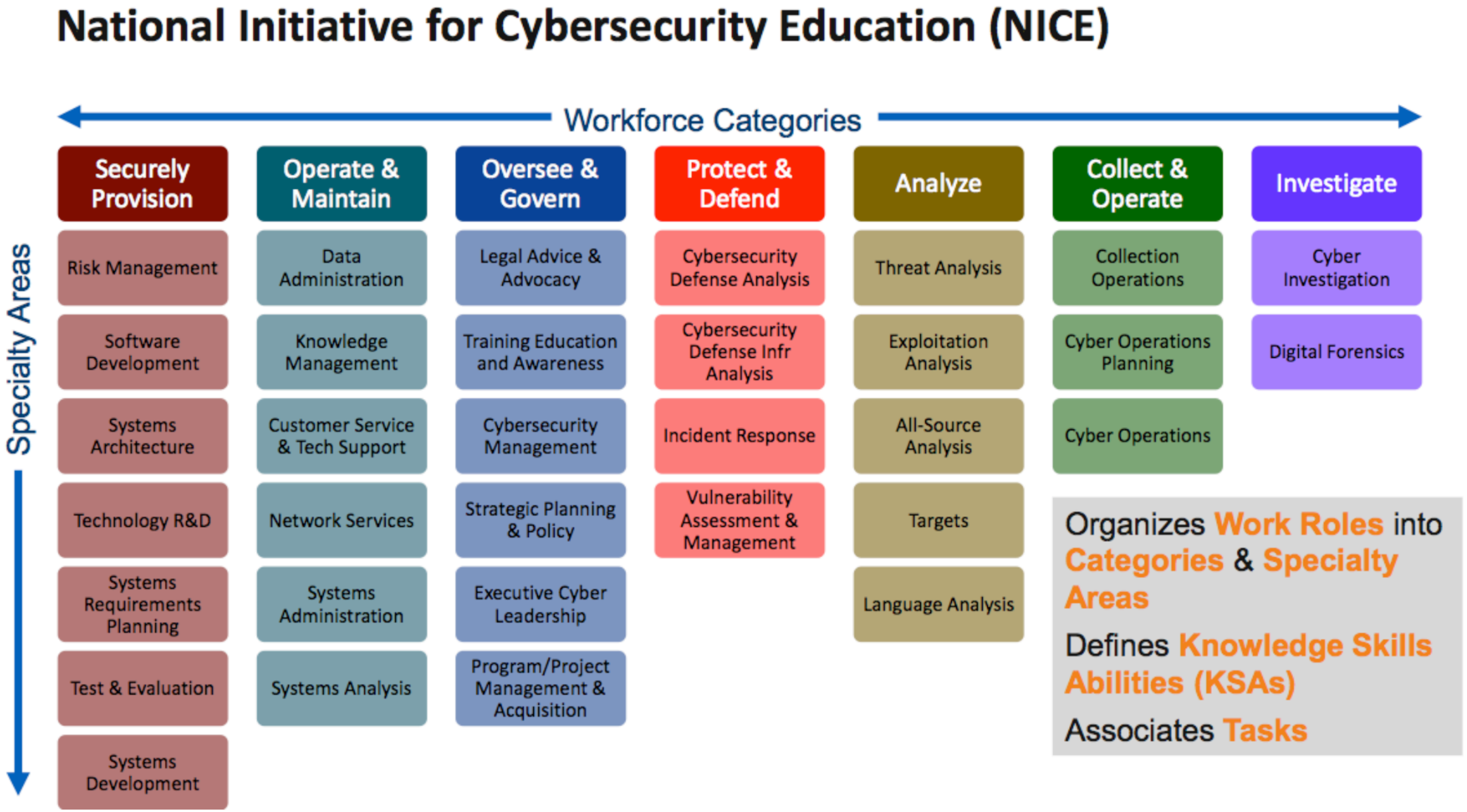
Ensuring a trained and certified cyber security workforce

Using the NICE Framework


NICE Cybersecurity Workforce Framework
Workforce Identification, Tracking & Reporting
Career Progression
Standardized Development of Position Descriptions
Human Capital Planning
Training Requirements and Standards
Qualification Requirements
Capable and Ready Cybersecurity Workforce
NIST National Institute of Standards and Technology U.S. Department of Commerce

Newhouse, William, Stephanie Keith, Benjamin Scribner, and Greg Witte. Building Blocks for a Capable and Ready Cybersecurity Workforce. Digital image. (NICE) Cybersecurity Workforce Framework. NIST, National Institute of Standards and Technology, Aug. 2017. Web. <https://doi.org/10.6028/NIST.SP.800-181>.

Broad Organization of the NICE Framework



National Initiative for Cybersecurity Education (NICE)

Workforce Categories

Specialty Areas

Securely Provision	Operate & Maintain	Oversee & Govern	Protect & Defend	Analyze	Collect & Operate	Investigate
Risk Management	Data Administration	Legal Advice & Advocacy	Cybersecurity Defense Analysis	Threat Analysis	Collection Operations	Cyber Investigation
Software Development	Knowledge Management	Training Education and Awareness	Cybersecurity Defense Infr Analysis	Exploitation Analysis	Cyber Operations Planning	Digital Forensics
Systems Architecture	Customer Service & Tech Support	Cybersecurity Management	Incident Response	All-Source Analysis	Cyber Operations	
Technology R&D	Network Services	Strategic Planning & Policy	Vulnerability Assessment & Management	Targets		
Systems Requirements Planning	Systems Administration	Executive Cyber Leadership		Language Analysis		
Test & Evaluation	Systems Analysis	Program/Project Management & Acquisition				
Systems Development						

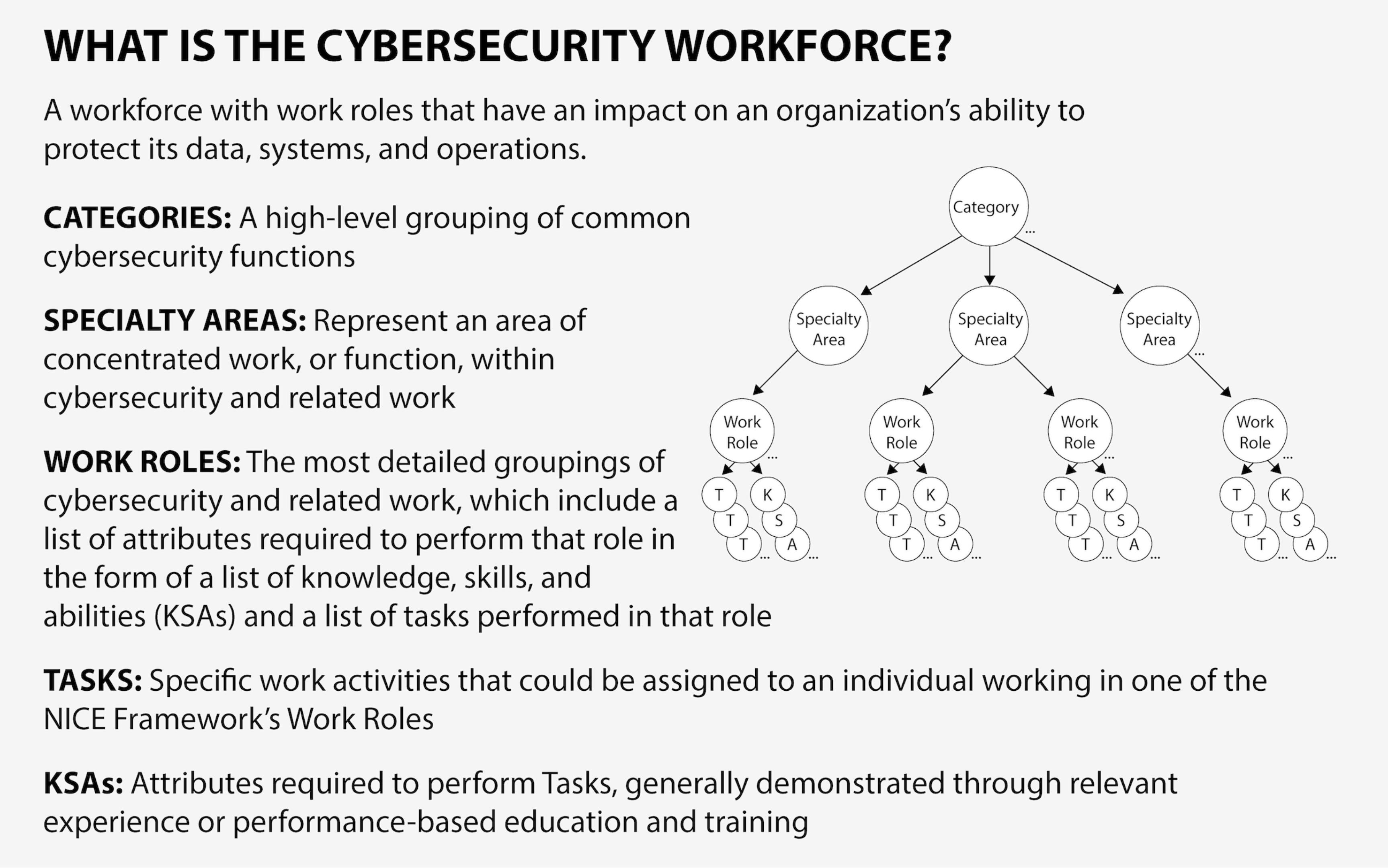
Organizes **Work Roles** into **Categories** & **Specialty Areas**

Defines **Knowledge Skills Abilities (KSAs)**

Associates **Tasks**

https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework

Broad Organization of the NICE Framework



WHAT IS THE CYBERSECURITY WORKFORCE?

A workforce with work roles that have an impact on an organization's ability to protect its data, systems, and operations.

CATEGORIES: A high-level grouping of common cybersecurity functions

SPECIALTY AREAS: Represent an area of concentrated work, or function, within cybersecurity and related work

WORK ROLES: The most detailed groupings of cybersecurity and related work, which include a list of attributes required to perform that role in the form of a list of knowledge, skills, and abilities (KSAs) and a list of tasks performed in that role

TASKS: Specific work activities that could be assigned to an individual working in one of the NICE Framework's Work Roles

KSAs: Attributes required to perform Tasks, generally demonstrated through relevant experience or performance-based education and training

https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework

NICE Category: Highest Level Grouping

Specialty Area: Distinct areas of cyber security work

Work Role: Grouping level that maps to specific KSAs (Knowledge, Skills, and Abilities) and tasks within a specific job role. Dependent on size and type of organization, these work roles may go by different names.

SANS Training Course	GIAC Certification	Work Role Proficiency
Recommended SANS Course	Associated Recommended GIAC Certification	Level of Proficiency 1, 2, 3, 4
Recommended SANS Course	Associated Recommended GIAC Certification	Level of Proficiency 1, 2, 3, 4
Recommended SANS Course	Associated Recommended GIAC Certification	Level of Proficiency 1, 2, 3, 4

Other Mapped SANS Training and GIAC Certifications:
These courses and certifications map to the Specialty Area and Work Role but are not the top recommended courses and certifications.

Specialty Area: Risk Management (RSK)

Oversees, evaluates, and supports the documentation, validation, assessment, and authorization processes necessary to assure that existing and new information technology (IT) systems meet the organization's cybersecurity and risk requirements. Ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives.

Work Role: Authorizing Official/Designating Representative (SP-RSK-001)

Senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation (CNSSI 4009).

SANS Training Course	GIAC Certification	Work Role Proficiency
SEC301: Introduction to Cyber Security	GISF: GIAC Information Security Fundamentals	2: Intermediate
MGT414: SANS Training Program for CISSP® Certification	GISP: GIAC Information Security Professional	2: Intermediate
MGT512: SANS Security Leadership Essentials For Managers	GSLC: GIAC Security Leadership Certification	3: Advanced

Other Mapped SANS Training and GIAC Certifications:

SEC401: Security Essentials Bootcamp Style / GSEC: GIAC Security Essentials

Securely Provision (SP)

Specialty Area: Risk Management (RSK)

Oversees, evaluates, and supports the documentation, validation, assessment, and authorization processes necessary to assure that existing and new information technology (IT) systems meet the organization's cybersecurity and risk requirements. Ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives.

Work Role: Security Control Assessor (SP-RSK-002)

Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (as defined in NIST SP 800-37).

SANS Training Course	GIAC Certification	Work Role Proficiency
SEC401: Security Essentials Bootcamp Style	GSEC: GIAC Security Essentials	2: Intermediate
SEC566: Implementing and Auditing the Critical Security Controls - In-Depth	GCCC: GIAC Critical Controls Certification	2: Intermediate
AUD507: Auditing & Monitoring Networks, Perimeters & Systems	GSNA: GIAC Systems and Network Auditor	3: Advanced

Other Mapped SANS Training and GIAC Certifications:

SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling / GCIH: GIAC Certified Incident Handler

SEC560: Network Penetration Testing and Ethical Hacking / GPEN: GIAC Certified Penetration Tester

Securely Provision (SP)

Specialty Area: Software Development (DEV)

Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.

Work Role: Secure Software Developer (SP-DEV-001)

Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.

SANS Training Course	GIAC Certification	Work Role Proficiency
DEV522: Defending Web Applications Security Essentials	GWEB: GIAC Certified Web Application Defender	3: Advanced
SEC540: Secure DevOps and Cloud Application Security	N/A	3: Advanced

Other Mapped SANS Training and GIAC Certifications:

DEV541: Secure Coding in Java/JEE: Developing Defensible Applications
DEV544: Secure Coding in .NET: Developing Defensible Applications
DEV534: Secure DevOps: A Practical Introduction

Securely Provision (SP)

Specialty Area: Software Development (DEV)

Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.

Work Role: Secure Software Assessor (SP-DEV-002)

Analyzes the security of new or existing computer applications, software, or specialized utility programs and provides actionable results.

SANS Training Course	GIAC Certification	Work Role Proficiency
DEV522: Defending Web Applications Security Essentials	GWEB: GIAC Certified Web Application Defender	3: Advanced
SEC542: Web App Penetration Testing and Ethical Hacking	GWAPT: GIAC Web Application Penetration Tester	3: Advanced
SEC642: Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques	N/A	4: Expert

Other Mapped SANS Training and GIAC Certifications:

DEV541: Secure Coding in Java/JEE: Developing Defensible Applications

DEV544: Secure Coding in .NET: Developing Defensible Applications

Securely Provision (SP)

Specialty Area: Systems Architecture (ARC)

Develops system concepts and works on the capabilities phases of the systems development life cycle; translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes.

Work Role: Enterprise Architect (SP-ARC-001)

Develops and maintains business, systems, and information processes to support enterprise mission needs; develops information technology (IT) rules and requirements that describe baseline and target architectures.

SANS Training Course	GIAC Certification	Work Role Proficiency
SEC530: Defensible Security Architecture and Engineering	GDSA: GIAC Defensible Security Architecture	3: Advanced
SEC540: Secure DevOps and Cloud Application Security	N/A	3: Advanced
SEC545: Cloud Security Architecture and Operations	N/A	3: Advanced

Other Mapped SANS Training and GIAC Certifications:

SEC401: Security Essentials Bootcamp Style / GSEC: GIAC Security Essentials

DEV534: Secure DevOps: A Practical Introduction

Specialty Area: Systems Architecture (ARC)

Develops system concepts and works on the capabilities phases of the systems development life cycle; translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes.

Work Role: Security Architect (SP-ARC-002)

Ensures that the stakeholder security requirements necessary to protect the organization's mission and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting systems supporting those missions and business processes.

SANS Training Course	GIAC Certification	Work Role Proficiency
SEC511: Continuous Monitoring and Security Operations	GMON: GIAC Continuous Monitoring Certification	3: Advanced
SEC530: Defensible Security Architecture and Engineering	GDSA: GIAC Defensible Security Architecture	3: Advanced

Other Mapped SANS Training and GIAC Certifications:

SEC401: Security Essentials Bootcamp Style / GSEC: GIAC Security Essentials
SEC501: Advanced Security Essentials - Enterprise Defender/ GCED: GIAC Certified Enterprise Defender
SEC555: SIEM with Tactical Analytics / GCDA: GIAC Certified Detection Analyst

Specialty Area: Technology R&D (TRD)

Conducts technology assessment and integration processes; provides and supports a prototype capability and/or evaluates its utility.

Work Role: Research & Development Specialist (SP-TRD-001)

Conducts software and systems engineering and software systems research to develop new capabilities, ensuring cybersecurity is fully integrated. Conducts comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems.

SANS Training Course	GIAC Certification	Work Role Proficiency
SEC540: Secure DevOps and Cloud Application Security	N/A	3: Advanced
DEV522: Defending Web Applications Security Essentials	GWEB: GIAC Certified Web Application Defender	3: Advanced

Other Mapped SANS Training and GIAC Certifications:

SEC401: Security Essentials Bootcamp Style / GSEC: GIAC Security Essentials
SEC573: Automating Information Security with Python / GPYC: GIAC Python Coder
DEV534: Secure DevOps: A Practical Introduction
SEC545: Cloud Security Architecture and Operations

Specialty Area: Systems Requirements Planning (SRP)

Consults with customers to gather and evaluate functional requirements and translates these requirements into technical solutions. Provides guidance to customers about applicability of information systems to meet business needs.

Work Role: Systems Requirements Planner (SP-SRP-001)

Consults with customers to evaluate functional requirements and translate functional requirements into technical solutions.

SANS Training Course	GIAC Certification	Work Role Proficiency
MGT525: IT Project Management, Effective Communication, and PMP® Exam Prep	GCPM: GIAC Certified Project Manager	2: Intermediate

Other Mapped SANS Training and GIAC Certifications:

SEC401: Security Essentials Bootcamp Style / GSEC: GIAC Security Essentials

MGT414: SANS Training Program for CISSP® Certification / GISP: GIAC Information Security Professional

MGT512: SANS Security Leadership Essentials For Managers / GSLC: GIAC Security Leadership Certification

Securely Provision (SP)

Specialty Area: Test and Evaluation (TST)

Develops and conducts tests of systems to evaluate compliance with specifications and requirements by applying principles and methods for cost-effective planning, evaluating, verifying, and validating of technical, functional, and performance characteristics (including interoperability) of systems or elements of systems incorporating IT.

Work Role: System Testing and Evaluation Specialist (SP-TST-001)

Plans, prepares, and executes tests of systems to evaluate results against specifications and requirements as well as analyze/report test results.

SANS Training Course	GIAC Certification	Work Role Proficiency
SEC401: Security Essentials Bootcamp Style	GSEC: GIAC Security Essentials	2: Intermediate
SEC573: Automating Information Security with Python	GPYC: GIAC Python Coder	3: Advanced

Other Mapped SANS Training and GIAC Certifications:

SEC301: Introduction to Cyber Security / GISF: GIAC Information Security Fundamentals
MGT414: SANS Training Program for CISSP® Certification / GISP: GIAC Information Security Professional

Specialty Area: Systems Development (SYS)

Works on the development phases of the systems development life cycle.

Work Role: Information Systems Security Developer (SP-SYS-001)

Designs, develops, tests, and evaluates information system security throughout the systems development life cycle.

SANS Training Course	GIAC Certification	Work Role Proficiency
DEV522: Defending Web Applications Security Essentials	GWEB: GIAC Certified Web Application Defender	3: Advanced
SEC542: Web App Penetration Testing and Ethical Hacking	GWAPT: GIAC Web Application Penetration Tester	3: Advanced
SEC540: Secure DevOps and Cloud Application Security	N/A	3: Advanced

Other Mapped SANS Training and GIAC Certifications:

DEV541: Secure Coding in Java/JEE: Developing Defensible Applications
DEV544: Secure Coding in .NET: Developing Defensible Applications
DEV534: Secure DevOps: A Practical Introduction
SEC642: Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques

Securely Provision (SP)

Specialty Area: Systems Development (SYS)

Works on the development phases of the systems development life cycle.

Work Role: Systems Developer (SP-SYS-002)

Designs, develops, tests, and evaluates information systems throughout the systems development life cycle.

SANS Training Course	GIAC Certification	Work Role Proficiency
DEV522: Defending Web Applications Security Essentials	GWEB: GIAC Certified Web Application Defender	3: Advanced
SEC540: Secure DevOps and Cloud Application Security	N/A	3: Advanced

Other Mapped SANS Training and GIAC Certifications:

SEC401: Security Essentials Bootcamp Style / GSEC: GIAC Security Essentials
DEV541: Secure Coding in Java/JEE: Developing Defensible Applications
DEV544: Secure Coding in .NET: Developing Defensible Applications
DEV534: Secure DevOps: A Practical Introduction

Operate and Maintain (OM)

Specialty Area: Data Administration (DTA)

Develops and administers databases and/or data management systems that allow for the storage, query, protection, and utilization of data.

Work Role: Database Administrator (OM-DTA-001)

Administers databases and/or data management systems that allow for the secure storage, query, protection, and utilization of data.

SANS Training Course	GIAC Certification	Work Role Proficiency
SEC401: Security Essentials Bootcamp Style	GSEC: GIAC Security Essentials	2: Intermediate
DEV522: Defending Web Applications Security Essentials	GWEB: GIAC Certified Web Application Defender	3: Advanced

Operate and Maintain (OM)

Specialty Area: Data Administration (DTA)

Develops and administers databases and/or data management systems that allow for the storage, query, protection, and utilization of data.

Work Role: Data Analyst (OM-DTA-002)

Administers databases and/or data management systems that allow for the secure storage, query, protection, and utilization of data.

SANS Training Course	GIAC Certification	Work Role Proficiency
SEC401: Security Essentials Bootcamp Style	GSEC: GIAC Security Essentials	2: Intermediate
DEV522: Defending Web Applications Security Essentials	GWEB: GIAC Certified Web Application Defender	3: Advanced

Specialty Area: Knowledge Management (KMG)

Manages and administers processes and tools that enable the organization to identify, document, and access intellectual capital and information content.

Work Role: Knowledge Manager (OM-KMG-001)

Responsible for the management and administration of processes and tools that enable the organization to identify, document, and access intellectual capital and information content.

SANS Training Course	GIAC Certification	Work Role Proficiency
SEC301: Introduction to Cyber Security	GISF: GIAC Information Security Fundamentals	2: Intermediate

Other Mapped SANS Training and GIAC Certifications:

SEC401: Security Essentials Bootcamp Style / GSEC: GIAC Security Essentials

MGT414: SANS Training Program for CISSP® Certification / GISP: GIAC Information Security Professional

Operate and Maintain (OM)

Specialty Area: Customer Service and Technical Support (STS)

Addresses problems; installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries (e.g., tiered-level customer support). Typically provides initial incident information to the Incident Response (IR) Specialty.

Work Role: Technical Support Specialist (OM-STS-001)

Provides technical support to customers who need assistance utilizing client-level hardware and software in accordance with established or approved organizational process components (i.e., Master Incident Management Plan, when applicable).

SANS Training Course	GIAC Certification	Work Role Proficiency
SEC401: Security Essentials Bootcamp Style	GSEC: GIAC Security Essentials	2: Intermediate
SEC505: Securing Windows and PowerShell Automation	GCWN: GIAC Certified Windows Security Administrator	3: Advanced
SEC506: Securing Linux/Unix	GCUX: GIAC Certified UNIX Security Administrator	3: Advanced

Other Mapped SANS Training and GIAC Certifications:

SEC301: Introduction to Cyber Security / GISF: GIAC Information Security Fundamentals

Operate and Maintain (OM)

Specialty Area: Network Services (NET)

Installs, configures, tests, operates, maintains, and manages networks and their firewalls, including hardware (e.g., hubs, bridges, switches, multiplexers, routers, cables, proxy servers, and protective distributor systems) and software that permit the sharing and transmission of all spectrum transmissions of information to support the security of information and information systems.

Work Role: Network Operations Specialist (OM-NET-001)

Plans, implements, and operates network services/systems, to include hardware and virtual environments.

SANS Training Course	GIAC Certification	Work Role Proficiency
SEC401: Security Essentials Bootcamp Style	GSEC: GIAC Security Essentials	2: Intermediate
SEC501: Advanced Security Essentials - Enterprise Defender	GCED: GIAC Certified Enterprise Defender	3: Advanced
SEC555: SIEM with Tactical Analytics	GCDA: GIAC Certified Detection Analyst	4: Expert

Other Mapped SANS Training and GIAC Certifications:

SEC301: Introduction to Cyber Security / GISF: GIAC Information Security Fundamentals

ICS410: ICS/SCADA Security Essentials / GICSP: Global Industrial Cyber Security Professional

SEC511: Continuous Monitoring and Security Operations / GMON: GIAC Continuous Monitoring Certification

SEC546: IPv6 Essentials

Specialty Area: Systems Administration (ADM)

Installs, configures, troubleshoots, and maintains server configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Manages accounts, firewalls, and patches. Responsible for access control, passwords, and account creation and administration.

Work Role: System Administrator (OM-ADM-001)

Responsible for setting up and maintaining a system or specific components of a system (e.g. for example, installing, configuring, and updating hardware and software; establishing and managing user accounts; overseeing or conducting backup and recovery tasks; implementing operational and technical security controls; and adhering to organizational security policies and procedures).

SANS Training Course	GIAC Certification	Work Role Proficiency
SEC401: Security Essentials Bootcamp Style	GSEC: GIAC Security Essentials	2: Intermediate
SEC505: Securing Windows and PowerShell Automation	GCWN: GIAC Certified Windows Security Administrator	3: Advanced
SEC506: Securing Linux/Unix	GCUX: GIAC Certified UNIX Security Administrator	3: Advanced

Other Mapped SANS Training and GIAC Certifications:

SEC501: Advanced Security Essentials - Enterprise Defender / GCED: GIAC Certified Enterprise Defender

Specialty Area: Systems Analysis (ANA)

Studies an organization's current computer systems and procedures, and designs information systems solutions to help the organization operate more securely, efficiently, and effectively. Brings business and information technology (IT) together by understanding the needs and limitations of both.

Work Role: Systems Security Analyst (OM-ANA-001)

Responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security.

SANS Training Course	GIAC Certification	Work Role Proficiency
SEC501: Advanced Security Essentials - Enterprise Defender	GCED: GIAC Certified Enterprise Defender	3: Advanced
AUD507: Auditing & Monitoring Networks, Perimeters & Systems	GSNA: GIAC Systems and Network Auditor	3: Advanced

Other Mapped SANS Training and GIAC Certifications:

SEC401: Security Essentials Bootcamp Style / GSEC: GIAC Security Essentials

ICS410: ICS/SCADA Security Essentials / GICSP: Global Industrial Cyber Security Professional

SEC511: Continuous Monitoring and Security Operations / GMON: GIAC Continuous Monitoring Certification

SEC545: Cloud Security Architecture and Operations

SEC555: SIEM with Tactical Analytics / GCDA: GIAC Certified Detection Analyst

Specialty Area: Legal Advice and Advocacy (LGA)

Provides legally sound advice and recommendations to leadership and staff on a variety of relevant topics within the pertinent subject domain. Advocates legal and policy changes, and makes a case on behalf of client via a wide range of written and oral work products, including legal briefs and proceedings.

Work Role: Cyber Legal Advisor (OV-LGA-001)

Provides legal advice and recommendations on relevant topics related to cyber law.

SANS Training Course	GIAC Certification	Work Role Proficiency
LEG523: Law of Data Security and Investigations	GLEG: GIAC Law of Data Security & Investigations	3: Advanced

Other Mapped SANS Training and GIAC Certifications:

SEC301: Introduction to Cyber Security / GISF: GIAC Information Security Fundamentals

MGT414: SANS Training Program for CISSP® Certification / GISP: GIAC Information Security Professional

Specialty Area: Systems Administration (ADM)

Installs, configures, troubleshoots, and maintains server configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Manages accounts, firewalls, and patches. Responsible for access control, passwords, and account creation and administration.

Work Role: Privacy Officer/Privacy Compliance Manager (OV-LGA-002)

Develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance, governance/policy, and incident response needs of privacy and security executives and their teams.

SANS Training Course	GIAC Certification	Work Role Proficiency
SEC301: Introduction to Cyber Security	GISF: GIAC Information Security Fundamentals	2: Intermediate
MGT414: SANS Training Program for CISSP® Certification	GISP: GIAC Information Security Professional	2: Intermediate
MGT512: SANS Security Leadership Essentials For Managers	GSLC: GIAC Security Leadership Certification	3: Advanced

Other Mapped SANS Training and GIAC Certifications:

ICS456: Essentials for NERC Critical Infrastructure Protection / GCIP: GIAC Critical Infrastructure Protection

Specialty Area: Training, Education, and Awareness (TEA)

Conducts training of personnel within pertinent subject domain. Develops, plans, coordinates, delivers and/or evaluates training courses, methods, and techniques as appropriate.

Work Role: Cyber Instructional Curriculum Developer (OV-TEA-001)

Develops, plans, coordinates, and evaluates cyber training/education courses, methods, and techniques based on instructional needs.

SANS Training Course	GIAC Certification	Work Role Proficiency
SEC401: Security Essentials Bootcamp Style	GSEC: GIAC Security Essentials	2: Intermediate
MGT433: Securing The Human: How to Build, Maintain, and Measure a Mature Awareness Program	N/A	3: Advanced

Other Mapped SANS Training and GIAC Certifications:

SEC301: Introduction to Cyber Security / GISF: GIAC Information Security Fundamentals

Oversee and Govern (OV)

Specialty Area: Training, Education, and Awareness (TEA)

Conducts training of personnel within pertinent subject domain. Develops, plans, coordinates, delivers and/or evaluates training courses, methods, and techniques as appropriate.

Work Role: Cyber Instructor (OV-TEA-002)

Develops and conducts training or education of personnel within cyber domain.

SANS Training Course	GIAC Certification	Work Role Proficiency
SEC401: Security Essentials Bootcamp Style	GSEC: GIAC Security Essentials	2: Intermediate
SEC501: Advanced Security Essentials - Enterprise Defender	GCED: GIAC Certified Enterprise Defender	3: Advanced

Other Mapped SANS Training and GIAC Certifications:

SEC301: Introduction to Cyber Security / GISF: GIAC Information Security Fundamentals

MGT433: Securing The Human: How to Build, Maintain and Measure a Mature Awareness Program

Oversee and Govern (OV)

Specialty Area: Cybersecurity Management (MGT)

Oversees the cybersecurity program of an information system or network, including managing information security implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, requirements, policy enforcement, emergency planning, security awareness, and other resources.

Work Role: Information Systems Security Manager (OV-MGT-001)

Responsible for the cybersecurity of a program, organization, system, or enclave.

SANS Training Course	GIAC Certification	Work Role Proficiency
MGT512: SANS Security Leadership Essentials For Managers	GSLC: GIAC Security Leadership Certification	3: Advanced

Other Mapped SANS Training and GIAC Certifications:

SEC301: Introduction to Cyber Security / GISF: GIAC Information Security Fundamentals
SEC401: Security Essentials Bootcamp Style / GSEC: GIAC Security Essentials
MGT414: SANS Training Program for CISSP® Certification / GISP: GIAC Information Security Professional

Specialty Area: Cybersecurity Management (MGT)

Oversees the cybersecurity program of an information system or network, including managing information security implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, requirements, policy enforcement, emergency planning, security awareness, and other resources.

Work Role: Communications Security (COMSEC) Manager (OV-MGT-002)

Individual who manages the Communications Security (COMSEC) resources of an organization (CNSSI 4009) or key custodian for a Crypto Key Management System (CKMS).

SANS Training Course	GIAC Certification	Work Role Proficiency
SEC301: Introduction to Cyber Security	GISF: GIAC Information Security Fundamentals	2: Intermediate
MGT414: SANS Training Program for CISSP® Certification	GISP: GIAC Information Security Professional	2: Intermediate
MGT512: SANS Security Leadership Essentials For Managers	GSLC: GIAC Security Leadership Certification	3: Advanced

Oversee and Govern (OV)

Specialty Area: Strategic Planning and Policy (SPP)

Develops policies and plans and/or advocates for changes in policy that support organizational cyberspace initiatives or required changes/enhancements.

Work Role: Cyber Workforce Developer and Manager (OV-SPP-001)

Develops cyberspace workforce plans, strategies, and guidance to support cyberspace workforce manpower, personnel, training and education requirements and to address changes to cyberspace policy, doctrine, materiel, force structure, and education and training requirements.

SANS Training Course	GIAC Certification	Work Role Proficiency
MGT512: SANS Security Leadership Essentials For Managers	GSLC: GIAC Security Leadership Certification	3: Advanced
MGT514: Security Strategic Planning, Policy, and Leadership	GSTRT: GIAC Strategic Planning, Policy, and Leadership	3: Advanced

Other Mapped SANS Training and GIAC Certifications:

SEC301: Introduction to Cyber Security / GISF: GIAC Information Security Fundamentals

MGT414: SANS Training Program for CISSP® Certification / GISP: GIAC Information Security Professional

Specialty Area: Strategic Planning and Policy (SPP)

Develops policies and plans and/or advocates for changes in policy that support organizational cyberspace initiatives or required changes/enhancements.

Work Role: Cyber Policy and Strategy Planner (OV-SPP-002)

Develops cyberspace workforce plans, strategies, and guidance to support cyberspace workforce manpower, personnel, training and education requirements and to address changes to cyberspace policy, doctrine, materiel, force structure, and education and training requirements.

SANS Training Course	GIAC Certification	Work Role Proficiency
MGT512: SANS Security Leadership Essentials For Managers	GSLC: GIAC Security Leadership Certification	3: Advanced
MGT514: Security Strategic Planning, Policy, and Leadership	GSTRT: GIAC Strategic Planning, Policy, and Leadership	3: Advanced

Other Mapped SANS Training and GIAC Certifications:

SEC301: Introduction to Cyber Security / GISF: GIAC Information Security Fundamentals

MGT414: SANS Training Program for CISSP® Certification / GISP: GIAC Information Security Professional

Oversee and Govern (OV)

Specialty Area: Executive Cyber Leadership (EXL)

Supervises, manages, and/or leads work and workers performing cyber and cyber-related and/or cyber operations work.

Work Role: Executive Cyber Leadership (OV-EXL-001)

Executes decision-making authorities and establishes vision and direction for an organization's cyber and cyber-related resources and/or operations.

SANS Training Course	GIAC Certification	Work Role Proficiency
MGT512: SANS Security Leadership Essentials For Managers	GSLC: GIAC Security Leadership Certification	3: Advanced
MGT514: Security Strategic Planning, Policy, and Leadership	GSTRT: GIAC Strategic Planning, Policy, and Leadership	3: Advanced

Other Mapped SANS Training and GIAC Certifications:

SEC301: Introduction to Cyber Security / GISF: GIAC Information Security Fundamentals

MGT414: SANS Training Program for CISSP® Certification / GISP: GIAC Information Security Professional

Specialty Area: Program/Project Management (PMA) and Acquisition

Applies knowledge of data, information, processes, organizational interactions, skills, and analytical expertise, as well as systems, networks, and information exchange capabilities to manage acquisition programs. Executes duties governing hardware, software, and information system acquisition programs and other program management policies. Provides direct support for acquisitions that use information technology (IT) (including National Security Systems), applying IT-related laws and policies, and provides IT-related guidance throughout the total acquisition life cycle.

Work Role: Program Manager (OV-PMA-001)

Leads, coordinates, communicates, integrates, and is accountable for the overall success of the program, ensuring alignment with agency or enterprise priorities.

SANS Training Course	GIAC Certification	Work Role Proficiency
MGT512: SANS Security Leadership Essentials For Managers	GSLC: GIAC Security Leadership Certification	3: Advanced
MGT514: Security Strategic Planning, Policy, and Leadership	GSTRT: GIAC Strategic Planning, Policy, and Leadership	3: Advanced

Other Mapped SANS Training and GIAC Certifications:

SEC301: Introduction to Cyber Security / GISF: GIAC Information Security Fundamentals

MGT414: SANS Training Program for CISSP® Certification/ GISP: GIAC Information Security Professional

MGT525: IT Project Management, Effective Communication, and PMP® Exam Prep/ GCPM: GIAC Certified Project Manager

Specialty Area: Program/Project Management (PMA) and Acquisition

Applies knowledge of data, information, processes, organizational interactions, skills, and analytical expertise, as well as systems, networks, and information exchange capabilities to manage acquisition programs. Executes duties governing hardware, software, and information system acquisition programs and other program management policies. Provides direct support for acquisitions that use information technology (IT) (including National Security Systems), applying IT-related laws and policies, and provides IT-related guidance throughout the total acquisition life cycle.

Work Role: IT Project Manager (OV-PMA-002)

Directly manages information technology projects.

SANS Training Course	GIAC Certification	Work Role Proficiency
MGT512: SANS Security Leadership Essentials For Managers	GSLC: GIAC Security Leadership Certification	3: Advanced
MGT525: IT Project Management, Effective Communication, and PMP® Exam Prep	GCPM: GIAC Certified Project Manager	3: Advanced

Other Mapped SANS Training and GIAC Certifications:

SEC301: Introduction to Cyber Security / GISF: GIAC Information Security Fundamentals

MGT414: SANS Training Program for CISSP® Certification/ GISP: GIAC Information Security Professional

Specialty Area: Program/Project Management (PMA) and Acquisition

Applies knowledge of data, information, processes, organizational interactions, skills, and analytical expertise, as well as systems, networks, and information exchange capabilities to manage acquisition programs. Executes duties governing hardware, software, and information system acquisition programs and other program management policies. Provides direct support for acquisitions that use information technology (IT) (including National Security Systems), applying IT-related laws and policies, and provides IT-related guidance throughout the total acquisition life cycle.

Work Role: Product Support Manager (OV-PMA-003)

Manages the package of support functions required to field and maintain the readiness and operational capability of systems and components.

SANS Training Course	GIAC Certification	Work Role Proficiency
MGT512: SANS Security Leadership Essentials For Managers	GSLC: GIAC Security Leadership Certification	3: Advanced
MGT525: IT Project Management, Effective Communication, and PMP® Exam Prep	GCPM: GIAC Certified Project Manager	3: Advanced

Other Mapped SANS Training and GIAC Certifications:

SEC301: Introduction to Cyber Security / GISF: GIAC Information Security Fundamentals

MGT414: SANS Training Program for CISSP® Certification/ GISP: GIAC Information Security Professional

Specialty Area: Program/Project Management (PMA) and Acquisition

Applies knowledge of data, information, processes, organizational interactions, skills, and analytical expertise, as well as systems, networks, and information exchange capabilities to manage acquisition programs. Executes duties governing hardware, software, and information system acquisition programs and other program management policies. Provides direct support for acquisitions that use information technology (IT) (including National Security Systems), applying IT-related laws and policies, and provides IT-related guidance throughout the total acquisition life cycle.

Work Role: IT Program Auditor (OV-PMA-005)

Conducts evaluations of an IT program or its individual components to determine compliance with published standards.

SANS Training Course	GIAC Certification	Work Role Proficiency
AUD507: Auditing & Monitoring Networks, Perimeters & Systems	GSNA: GIAC Systems and Network Auditor	3: Advanced

Other Mapped SANS Training and GIAC Certifications:

SEC301: Introduction to Cyber Security / GISF: GIAC Information Security Fundamentals

MGT414: SANS Training Program for CISSP® Certification / GISP: GIAC Information Security Professional

MGT512: SANS Security Leadership Essentials For Managers / GSLC: GIAC Security Leadership Certification

Protect and Defend (PR)

Specialty Area: Cybersecurity Defense Analysis (CDA)

Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network to protect information, information systems, and networks from threats.

Work Role: Cyber Defense Analyst (PR-CDA-001)

Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.

SANS Training Course	GIAC Certification	Work Role Proficiency
SEC401: Security Essentials Bootcamp Style	GSEC: GIAC Security Essentials	2: Intermediate
SEC501: Advanced Security Essentials - Enterprise Defender	GCED: GIAC Certified Enterprise Defender	3: Advanced
SEC503: Intrusion Detection In-Depth	GCIA: GIAC Certified Intrusion Analyst	3: Advanced
SEC511: Continuous Monitoring and Security Operations	GMON: GIAC Continuous Monitoring Certification	4: Expert

Cyber Defense Analyst Continued Next Page

Protect and Defend (PR)

Cyber Defense Analyst Continued

Specialty Area: Cybersecurity Defense Analysis (CDA)

Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network to protect information, information systems, and networks from threats.

Work Role: Cyber Defense Analyst (PR-CDA-001)

Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.

Other Mapped SANS Training and GIAC Certifications:

SEC301: Introduction to Cyber Security / GISF: GIAC Information Security Fundamentals

ICS410: ICS/SCADA Security Essentials / GICSP: Global Industrial Cyber Security Professional

SEC460: Enterprise Threat and Vulnerability Assessment

ICS515: ICS Active Defense and Incident Response / GRID: GIAC Response and Industrial Defense

SEC555: SIEM with Tactical Analytics / GCDA: GIAC Certified Detection Analyst

FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response / GNFA: GIAC Network Forensic Analyst

SEC599: Defeating Advanced Adversaries – Purple Team Tactics & Kill Chain Defenses / GDAT: GIAC Defending Advanced Threats

Specialty Area: Cybersecurity Defense Infrastructure Support (INF)

Tests, implements, deploys, maintains, reviews, and administers the infrastructure hardware and software that are required to effectively manage the computer network defense service provider network and resources. Monitors network to actively remediate unauthorized activities.

Work Role: Cyber Defense Infrastructure Support Specialist (PR-INF-001)

Tests, implements, deploys, maintains, and administers the infrastructure hardware and software.

SANS Training Course	GIAC Certification	Work Role Proficiency
SEC401: Security Essentials Bootcamp Style	GSEC: GIAC Security Essentials	2: Intermediate
SEC501: Advanced Security Essentials - Enterprise Defender	GCED: GIAC Certified Enterprise Defender	3: Advanced

Other Mapped SANS Training and GIAC Certifications:

SEC301: Introduction to Cyber Security / GISF: GIAC Information Security Fundamentals
ICS410: ICS/SCADA Security Essentials / GICSP: Global Industrial Cyber Security Professional
SEC503: Intrusion Detection In-Depth/ GCIA: GIAC Certified Intrusion Analyst
SEC511: Continuous Monitoring and Security Operations / GMON: GIAC Continuous Monitoring Certification
ICS515: ICS Active Defense and Incident Response / GRID: GIAC Response and Industrial Defense
SEC555: SIEM with Tactical Analytics / GCDA: GIAC Certified Detection Analyst
SEC599: Defeating Advanced Adversaries – Purple Team Tactics & Kill Chain Defenses / GDAT: GIAC Defending Advanced Threats

Specialty Area: Incident Response (CIR)

Responds to crises or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.

Work Role: Cyber Defense Incident Responder (PR-CIR-001)

Investigates, analyzes, and responds to cyber incidents within the network environment or enclave.

SANS Training Course	GIAC Certification	Work Role Proficiency
SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling	GCIH: GIAC Certified Incident Handler	2: Intermediate
FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics	GCFA: GIAC Certified Forensic Analyst	3: Advanced
FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response	GNFA: GIAC Network Forensic Analyst	3: Advanced

Other Mapped SANS Training and GIAC Certifications:

SEC401: Security Essentials Bootcamp Style / GSEC: GIAC Security Essentials
SEC501: Advanced Security Essentials - Enterprise Defender / GCED: GIAC Certified Enterprise Defender
ICS515: ICS Active Defense and Incident Response / GRID: GIAC Response and Industrial Defense
FOR518: Mac and iOS Forensic Analysis and Incident Response
FOR526: Advanced Memory Forensics & Threat Detection
SEC550: Active Defense, Offensive Countermeasures and Cyber Deception
SEC555: SIEM with Tactical Analytics / GCDA: GIAC Certified Detection Analyst
SEC599: Defeating Advanced Adversaries, Purple Team Tactics & Kill Chain Defenses / GDAT: GIAC Defending Advanced Threats

Specialty Area: Vulnerability Assessment and Management (VAM)

Conducts assessments of threats and vulnerabilities; determines deviations from acceptable configurations, enterprise or local policy; assesses the level of risk; and develops and/or recommends appropriate mitigation countermeasures in operational and nonoperational situations.

Work Role: Vulnerability Assessment Analyst (PR-VAM-001)

Performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities.

SANS Training Course	GIAC Certification	Work Role Proficiency
SEC460: Enterprise Threat and Vulnerability Assessment	N/A	2: Intermediate
SEC542: Web App Penetration Testing and Ethical Hacking	GWAPT: GIAC Web Application Penetration Tester	3: Advanced
SEC560: Network Penetration Testing and Ethical Hacking	GPEN: GIAC Certified Penetration Tester	3: Advanced
SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking	GXPN: GIAC Exploit Researcher and Advanced Penetration Tester	4: Expert

Vulnerability Assessment Analyst Continued Next Page

Protect and Defend (PR)

Vulnerability Assessment Analyst Continued

Specialty Area: Vulnerability Assessment and Management (VAM)

Conducts assessments of threats and vulnerabilities; determines deviations from acceptable configurations, enterprise or local policy; assesses the level of risk; and develops and/or recommends appropriate mitigation countermeasures in operational and nonoperational situations.

Work Role: Vulnerability Assessment Analyst (PR-VAM-001)

Performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities.

SEC642: Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques	N/A	4: Expert

<u>Other Mapped SANS Training and GIAC Certifications</u>:

SEC401: Security Essentials Bootcamp Style / GSEC: GIAC Security Essentials
SEC501: Advanced Security Essentials - Enterprise Defender / GCED: GIAC Certified Enterprise Defender
SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling / GCIH: GIAC Certified Incident Handler
AUD507: Auditing & Monitoring Networks, Perimeters & Systems / GSNA: GIAC Systems and Network Auditor
ICS410: ICS/SCADA Security Essentials / GICSP: Global Industrial Cyber Security Professional
ICS515: ICS Active Defense and Incident Response / GRID: GIAC Response and Industrial Defense
SEC617: Wireless Penetration Testing and Ethical Hacking / GAWN: GIAC Assessing Wireless Networks
SEC562: CyberCity Hands-on Kinetic Cyber Range Exercise
SEC760: Advanced Exploit Development for Penetration Testers

Specialty Area: Threat Analysis (TWA)

Identifies and assesses the capabilities and activities of cybersecurity criminals or foreign intelligence entities; produces findings to help initialize or support law enforcement and counterintelligence investigations or activities.

Work Role: Threat/Warning Analyst (AN-TWA-001)

Develops cyber indicators to maintain awareness of the status of the highly dynamic operating environment. Collects, processes, analyzes, and disseminates cyber threat/warning assessments.

SANS Training Course	GIAC Certification	Work Role Proficiency
FOR578: Cyber Threat Intelligence	GCTI: GIAC Cyber Threat Intelligence	3: Advanced

<u>Other Mapped SANS Training and GIAC Certifications</u>:

SEC401: Security Essentials Bootcamp Style / GSEC: GIAC Security Essentials

ICS410: ICS/SCADA Security Essentials / GICSP: Global Industrial Cyber Security Professional

FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics/ GCFA: GIAC Certified Forensic Analyst

Specialty Area: Exploitation Analysis (EXP)

Analyzes collected information to identify vulnerabilities and potential for exploitation.

Work Role: Exploitation Analyst (AN-EXP-001)

Collaborates to identify access and collection gaps that can be satisfied through cyber collection and/or preparation activities. Leverages all authorized resources and analytic techniques to penetrate targeted networks.

SANS Training Course	GIAC Certification	Work Role Proficiency
SEC542: Web App Penetration Testing and Ethical Hacking	GWAPT: GIAC Web Application Penetration Tester	3: Advanced
SEC560: Network Penetration Testing and Ethical Hacking	GPEN: GIAC Certified Penetration Tester	3: Advanced
SEC562: CyberCity Hands-on Kinetic Cyber Range Exercise	N/A	3: Advanced

Exploitation Analyst Continued Next Page

Analyze (AN)

Specialty Area: All-Source Analysis (ASA)

Analyzes threat information from multiple sources, disciplines, and agencies across the Intelligence Community. Synthesizes and places intelligence information in context; draws insights about the possible implications.

Work Role: Exploitation Analyst (AN-EXP-001)

Collaborates to identify access and collection gaps that can be satisfied through cyber collection and/or preparation activities. Leverages all authorized resources and analytic techniques to penetrate targeted networks.

Other Mapped SANS Training and GIAC Certifications:

SEC401: Security Essentials Bootcamp Style / GSEC: GIAC Security Essentials
SEC501: Advanced Security Essentials - Enterprise Defender / GCED: GIAC Certified Enterprise Defender
SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling / GCIH: GIAC Certified Incident Handler
AUD507: Auditing & Monitoring Networks, Perimeters & Systems/
GSNA: GIAC Systems and Network Auditor
ICS410: ICS/SCADA Security Essentials / GICSP: Global Industrial Cyber Security Professional
ICS515: ICS Active Defense and Incident Response / GRID: GIAC Response and Industrial Defense
SEC575: Mobile Device Security and Ethical Hacking / GMOB: GIAC Mobile Device Security Analyst
SEC617: Wireless Penetration Testing and Ethical Hacking/ GAWN: GIAC Assessing Wireless Networks
SEC642: Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques
SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking/
GXPN: GIAC Exploit Researcher and Advanced Penetration Tester
SEC760: Advanced Exploit Development for Penetration Testers

Specialty Area: All-Source Analysis (ASA)

Analyzes threat information from multiple sources, disciplines, and agencies across the Intelligence Community. Synthesizes and places intelligence information in context; draws insights about the possible implications.

Work Role: All Source Analyst (AN-ASA-001)

Analyzes data/information from one or multiple sources to conduct preparation of the environment, respond to requests for information, and submit intelligence collection and production requirements in support of planning and operations.

SANS Training Course	GIAC Certification	Work Role Proficiency
FOR578: Cyber Threat Intelligence	GCTI: GIAC Cyber Threat Intelligence	3: Advanced
SEC487: Open-Source Intelligence (OSINT) Gathering and Analysis	N/A	3: Advanced

Other Mapped SANS Training and GIAC Certifications:

SEC401: Security Essentials Bootcamp Style / GSEC: GIAC Security Essentials
ICS410: ICS/SCADA Security Essentials / GICSP: Global Industrial Cyber Security Professional
FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics / GCFA: GIAC Certified Forensic Analyst

Analyze (AN)

Specialty Area: All-Source Analysis (ASA)

Analyzes threat information from multiple sources, disciplines, and agencies across the Intelligence Community. Synthesizes and places intelligence information in context; draws insights about the possible implications.

Work Role: Mission Assessment Specialist (AN-ASA-002)

Develops assessment plans and measures of performance/effectiveness. Conducts strategic and operational effectiveness assessments as required for cyber events. Determines whether systems performed as expected and provides input to the determination of operational effectiveness.

Other Mapped SANS Training and GIAC Certifications:

SEC401: Security Essentials Bootcamp Style / GSEC: GIAC Security Essentials

ICS410: ICS/SCADA Security Essentials / GICSP: Global Industrial Cyber Security Professional

FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics / GCFA: GIAC Certified Forensic Analyst

FOR578: Cyber Threat Intelligence / GCTI: GIAC Cyber Threat Intelligence

Specialty Area: Targets (TGT)

Applies current knowledge of one or more regions, countries, non-state entities, and/or technologies.

Work Role: Target Developer (AN-TGT-001)

Performs target system analysis, builds and/or maintains electronic target folders to include inputs from environment preparation, and/or internal or external intelligence sources. Coordinates with partner target activities and intelligence organizations, and presents candidate targets for vetting and validation.

SANS Training Course	GIAC Certification	Work Role Proficiency
SEC542: Web App Penetration Testing and Ethical Hacking	GWAPT: GIAC Web Application Penetration Tester	3: Advanced
SEC560: Network Penetration Testing and Ethical Hacking	GPEN: GIAC Certified Penetration Tester	3: Advanced
SEC562: CyberCity Hands-on Kinetic Cyber Range Exercise	N/A	3: Advanced

Target Developer Continued Next Page

Analyze (AN)

Target Developer Continued

Specialty Area: Targets (TGT)

Applies current knowledge of one or more regions, countries, non-state entities, and/or technologies.

Work Role: Target Developer (AN-TGT-001)

Performs target system analysis, builds and/or maintains electronic target folders to include inputs from environment preparation, and/or internal or external intelligence sources. Coordinates with partner target activities and intelligence organizations, and presents candidate targets for vetting and validation.

Other Mapped SANS Training and GIAC Certifications:

SEC401: Security Essentials Bootcamp Style / GSEC: GIAC Security Essentials
SEC501: Advanced Security Essentials - Enterprise Defender / GCED: GIAC Certified Enterprise Defender
SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling / GCIH: GIAC Certified Incident Handler
AUD507: Auditing & Monitoring Networks, Perimeters & Systems/
GSNA: GIAC Systems and Network Auditor
ICS410: ICS/SCADA Security Essentials / GICSP: Global Industrial Cyber Security Professional
ICS515: ICS Active Defense and Incident Response / GRID: GIAC Response and Industrial Defense
SEC575: Mobile Device Security and Ethical Hacking / GMOB: GIAC Mobile Device Security Analyst
FOR578: Cyber Threat Intelligence / GCTI: GIAC Cyber Threat Intelligence
SEC617: Wireless Penetration Testing and Ethical Hacking / GAWN: GIAC Assessing Wireless Networks
SEC642: Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques
SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking/
GXPN: GIAC Exploit Researcher and Advanced Penetration Tester

Specialty Area: Targets (TGT)

Applies current knowledge of one or more regions, countries, non-state entities, and/or technologies.

Work Role: Target Network Analyst (AN-TGT-002)

Conducts advanced analysis of collection and open-source data to ensure target continuity; to profile targets and their activities; and develop techniques to gain more target information. Determines how targets communicate, move, operate and live based on knowledge of target technologies, digital networks, and the applications on them.

SANS Training Course	GIAC Certification	Work Role Proficiency
SEC542: Web App Penetration Testing and Ethical Hacking	GWAPT: GIAC Web Application Penetration Tester	3: Advanced
SEC560: Network Penetration Testing and Ethical Hacking	GPEN: GIAC Certified Penetration Tester	3: Advanced
SEC562: CyberCity Hands-on Kinetic Cyber Range Exercise	N/A	3: Advanced

Target Network Analyst Continued Next Page

Analyze (AN)

Target Network Analyst Continued

Specialty Area: Targets (TGT)

Applies current knowledge of one or more regions, countries, non-state entities, and/or technologies.

Work Role: Target Network Analyst (AN-TGT-002)

Conducts advanced analysis of collection and open-source data to ensure target continuity; to profile targets and their activities; and develop techniques to gain more target information. Determines how targets communicate, move, operate and live based on knowledge of target technologies, digital networks, and the applications on them.

SEC487: Open-Source Intelligence (OSINT) Gathering and Analysis	N/A	3: Advanced

<u>Other Mapped SANS Training and GIAC Certifications</u>:

SEC401: Security Essentials Bootcamp Style / GSEC: GIAC Security Essentials
SEC501: Advanced Security Essentials - Enterprise Defender / GCED: GIAC Certified Enterprise Defender
SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling / GCIH: GIAC Certified Incident Handler
AUD507: Auditing & Monitoring Networks, Perimeters & Systems / GSNA: GIAC Systems and Network Auditor
ICS410: ICS/SCADA Security Essentials / GICSP: Global Industrial Cyber Security Professional
ICS515: ICS Active Defense and Incident Response / GRID: GIAC Response and Industrial Defense
SEC575: Mobile Device Security and Ethical Hacking / GMOB: GIAC Mobile Device Security Analyst
FOR578: Cyber Threat Intelligence / GCTI: GIAC Cyber Threat Intelligence
SEC617: Wireless Penetration Testing and Ethical Hacking / GAWN: GIAC Assessing Wireless Networks
SEC642: Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques
SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking/
GXPN: GIAC Exploit Researcher and Advanced Penetration Tester

Analyze (AN)

Specialty Area: Language Analysis (LNG)

Applies language, cultural, and technical expertise to support information collection, analysis, and other cybersecurity activities.

Work Role: Multi–Disciplined Language Analyst **(**AN–LNG–001**)**

Applies language and culture expertise with target/threat and technical knowledge to process, analyze, and/or disseminate intelligence information derived from language, voice and/or graphic material. Creates and maintains language-specific databases and working aids to support cyber action execution and ensure critical knowledge sharing. Provides subject matter expertise in foreign language-intensive or interdisciplinary projects.

Mapped SANS Training and GIAC Certifications:

SEC401: Security Essentials Bootcamp Style / GSEC: GIAC Security Essentials

SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling / GCIH: GIAC Certified Incident Handler

SEC560: Network Penetration Testing and Ethical Hacking / GPEN: GIAC Certified Penetration Tester

FOR578: Cyber Threat Intelligence / GCTI: GIAC Cyber Threat Intelligence

Collect and Operate (CO)

Specialty Area: Collection Operations (CLO)

Executes collection using appropriate strategies and within the priorities established through the collection management process.

Work Role: All Source-Collection Manager (CO-CLO-001)

Identifies collection authorities and environment; incorporates priority information requirements into collection management; develops concepts to meet leadership's intent. Determines capabilities of available collection assets, identifies new collection capabilities; and constructs and disseminates collection plans. Monitors execution of tasked collection to ensure effective execution of the collection plan.

SANS Training Course	GIAC Certification	Work Role Proficiency
FOR578: Cyber Threat Intelligence	GCTI: GIAC Cyber Threat Intelligence	3: Advanced
SEC487: Open-Source Intelligence (OSINT) Gathering and Analysis	N/A	3: Advanced

<u>Other Mapped SANS Training and GIAC Certifications</u>:

SEC401: Security Essentials Bootcamp Style / GSEC: GIAC Security Essentials

FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics / GCFA: GIAC Certified Forensic Analyst

ICS410: ICS/SCADA Security Essentials / GICSP: Global Industrial Cyber Security Professional

Collect and Operate (CO)

Specialty Area: Collection Operations (CLO)

Executes collection using appropriate strategies and within the priorities established through the collection management process.

Work Role: All Source-Collection Requirements Manager (CO-CLO-002)

Evaluates collection operations and develops effects-based collection requirements strategies using available sources and methods to improve collection. Develops, processes, validates, and coordinates submission of collection requirements. Evaluates performance of collection assets and collection operations.

SANS Training Course	GIAC Certification	Work Role Proficiency
FOR578: Cyber Threat Intelligence	GCTI: GIAC Cyber Threat Intelligence	3: Advanced
SEC487: Open-Source Intelligence (OSINT) Gathering and Analysis	N/A	3: Advanced

Other Mapped SANS Training and GIAC Certifications:

SEC401: Security Essentials Bootcamp Style / GSEC: GIAC Security Essentials

FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics / GCFA: GIAC Certified Forensic Analyst

ICS410: ICS/SCADA Security Essentials / GICSP: Global Industrial Cyber Security Professional

Collect and Operate (CO)

Specialty Area: Cyber Operational Planning (OPL)

Performs in-depth joint targeting and cybersecurity planning process. Gathers information and develops detailed Operational Plans and Orders supporting requirements. Conducts strategic and operational-level planning across the full range of operations for integrated information and cyberspace operations.

Work Role: Cyber Intel Planner (CO-OPL-001)

Develops detailed intelligence plans to satisfy cyber operations requirements. Collaborates with cyber operations planners to identify, validate, and levy requirements for collection and analysis. Participates in targeting selection, validation, synchronization, and execution of cyber actions. Synchronizes intelligence activities to support organization objectives in cyberspace.

SANS Training Course	GIAC Certification	Work Role Proficiency
FOR578: Cyber Threat Intelligence	GCTI: GIAC Cyber Threat Intelligence	3: Advanced
SEC487: Open-Source Intelligence (OSINT) Gathering and Analysis	N/A	3: Advanced

Other Mapped SANS Training and GIAC Certifications:

SEC401: Security Essentials Bootcamp Style / GSEC: GIAC Security Essentials

FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics / GCFA: GIAC Certified Forensic Analyst

ICS410: ICS/SCADA Security Essentials / GICSP: Global Industrial Cyber Security Professional

Specialty Area: Cyber Operational Planning (OPL)

Performs in-depth joint targeting and cybersecurity planning process. Gathers information and develops detailed Operational Plans and Orders supporting requirements. Conducts strategic and operational-level planning across the full range of operations for integrated information and cyberspace operations.

Work Role: Cyber Ops Planner (CO-OPL-002)

Develops detailed plans for the conduct or support of the applicable range of cyber operations through collaboration with other planners, operators and/or analysts. Participates in targeting selection, validation, synchronization, and enables integration during the execution of cyber actions.

SANS Training Course	GIAC Certification	Work Role Proficiency
SEC542: Web App Penetration Testing and Ethical Hacking	GWAPT: GIAC Web Application Penetration Tester	3: Advanced
SEC560: Network Penetration Testing and Ethical Hacking	GPEN: GIAC Certified Penetration Tester	3: Advanced
SEC562: CyberCity Hands-on Kinetic Cyber Range Exercise	N/A	3: Advanced

Cyber Ops Planner Continued Next Page

Collect and Operate (CO)

Cyber Ops Planner Continued

Specialty Area: Cyber Operational Planning (OPL)

Performs in-depth joint targeting and cybersecurity planning process. Gathers information and develops detailed Operational Plans and Orders supporting requirements. Conducts strategic and operational-level planning across the full range of operations for integrated information and cyberspace operations.

Work Role: Cyber Ops Planner (CO-OPL-002)

Develops detailed plans for the conduct or support of the applicable range of cyber operations through collaboration with other planners, operators and/or analysts. Participates in targeting selection, validation, synchronization, and enables integration during the execution of cyber actions.

SEC487: Open-Source Intelligence (OSINT) Gathering and Analysis	N/A	3: Advanced

<u>Other Mapped SANS Training and GIAC Certifications</u>:

SEC401: Security Essentials Bootcamp Style / GSEC: GIAC Security Essentials
SEC501: Advanced Security Essentials - Enterprise Defender / GCED: GIAC Certified Enterprise Defender
SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling / GCIH: GIAC Certified Incident Handler
AUD507: Auditing & Monitoring Networks, Perimeters & Systems / GSNA: GIAC Systems and Network Auditor
ICS410: ICS/SCADA Security Essentials / GICSP: Global Industrial Cyber Security Professional
ICS515: ICS Active Defense and Incident Response / GRID: GIAC Response and Industrial Defense
SEC575: Mobile Device Security and Ethical Hacking / GMOB: GIAC Mobile Device Security Analyst
FOR578: Cyber Threat Intelligence / GCTI: GIAC Cyber Threat Intelligence
SEC617: Wireless Penetration Testing and Ethical Hacking / GAWN: GIAC Assessing Wireless Networks
SEC642: Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques
SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking/
GXPN: GIAC Exploit Researcher and Advanced Penetration Tester

Collect and Operate (CO)

Specialty Area: Cyber Operational Planning (OPL)

Performs in-depth joint targeting and cybersecurity planning process. Gathers information and develops detailed Operational Plans and Orders supporting requirements. Conducts strategic and operational-level planning across the full range of operations for integrated information and cyberspace operations.

Work Role: Partner Integration Planner (CO-OPL-003)

Works to advance cooperation across organizational or national borders between cyber operations partners. Aids the integration of partner cyber teams by providing guidance, resources, and collaboration to develop best practices and facilitate organizational support for achieving objectives in integrated cyber actions.

SANS Training Course	GIAC Certification	Work Role Proficiency
FOR578: Cyber Threat Intelligence	GCTI: GIAC Cyber Threat Intelligence	3: Advanced

Other Mapped SANS Training and GIAC Certifications:

SEC401: Security Essentials Bootcamp Style / GSEC: GIAC Security Essentials

FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics / GCFA: GIAC Certified Forensic Analyst

ICS410: ICS/SCADA Security Essentials / GICSP: Global Industrial Cyber Security Professional

Specialty Area: Cyber Operations (OPS)

Performs activities to gather evidence on criminal or foreign intelligence entities to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or to support other intelligence activities.

Work Role: Cyber Operator (CO-OPS-001)

Conducts collection, processing, and/or geolocation of systems to exploit, locate, and/or track targets of interest. Performs network navigation, tactical forensic analysis, and, when directed, executes on-net operations.

SANS Training Course	GIAC Certification	Work Role Proficiency
SEC542: Web App Penetration Testing and Ethical Hacking	GWAPT: GIAC Web Application Penetration Tester	3: Advanced
SEC560: Network Penetration Testing and Ethical Hacking	GPEN: GIAC Certified Penetration Tester	3: Advanced
SEC562: CyberCity Hands-on Kinetic Cyber Range Exercise	N/A	3: Advanced

Cyber Operator Continued Next Page

Collect and Operate (CO)

Cyber Operator Continued

Specialty Area: Cyber Operations (OPS)

Performs activities to gather evidence on criminal or foreign intelligence entities to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or to support other intelligence activities.

Work Role: Cyber Operator (CO-OPS-001)

Conducts collection, processing, and/or geolocation of systems to exploit, locate, and/or track targets of interest. Performs network navigation, tactical forensic analysis, and, when directed, executes on-net operations.

Other Mapped SANS Training and GIAC Certifications:

SEC401: Security Essentials Bootcamp Style / GSEC: GIAC Security Essentials

SEC501: Advanced Security Essentials - Enterprise Defender / GCED: GIAC Certified Enterprise Defender

SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling / GCIH: GIAC Certified Incident Handler

AUD507: Auditing & Monitoring Networks, Perimeters & Systems/ GSNA: GIAC Systems and Network Auditor

ICS410: ICS/SCADA Security Essentials / GICSP: Global Industrial Cyber Security Professional

ICS515: ICS Active Defense and Incident Response / GRID: GIAC Response and Industrial Defense

SEC575: Mobile Device Security and Ethical Hacking / GMOB: GIAC Mobile Device Security Analyst

FOR578: Cyber Threat Intelligence / GCTI: GIAC Cyber Threat Intelligence

SEC617: Wireless Penetration Testing and Ethical Hacking / GAWN: GIAC Assessing Wireless Networks

SEC642: Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques

SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking/ GXPN: GIAC Exploit Researcher and Advanced Penetration Tester

Investigate (IN)

Specialty Area: Cyber Investigation (INV)

Applies tactics, techniques, and procedures for a full range of investigative tools and processes to include, but not limited to, interview and interrogation techniques, surveillance, counter surveillance, and surveillance detection, and appropriately balances the benefits of prosecution versus intelligence gathering.

Work Role: Cyber Crime Investigator (IN-INV-001)

Identifies, collects, examines, and preserves evidence using controlled and documented analytical and investigative techniques.

SANS Training Course	GIAC Certification	Work Role Proficiency
FOR500: Windows Forensics Analysis	GCFE: GIAC Certified Forensic Examiner	3: Advanced
FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics	GCFA: GIAC Certified Forensic Analyst	3: Advanced

Other Mapped SANS Training and GIAC Certifications:

SEC401: Security Essentials Bootcamp Style / GSEC: GIAC Security Essentials
SEC301: Introduction to Cyber Security / GISF: GIAC Information Security Fundamentals
FOR518: Mac and iOS Forensic Analysis and Incident Response
FOR526: Advanced Memory Forensics & Threat Detection
FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response

Investigate (IN)

Specialty Area: Digital Forensics (FOR)

Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations.

Work Role: Law Enforcement /Counterintelligence Forensics Analyst (IN-FOR-001)

Conducts detailed investigations on computer-based crimes establishing documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents.

SANS Training Course	GIAC Certification	Work Role Proficiency
FOR500: Windows Forensics Analysis	GCFE: GIAC Certified Forensic Examiner	3: Advanced
FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics	GCFA: GIAC Certified Forensic Analyst	3: Advanced
FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response	GNFA: GIAC Network Forensic Analyst	3: Advanced

Other Mapped SANS Training and GIAC Certifications:

SEC401: Security Essentials Bootcamp Style / GSEC: GIAC Security Essentials

FOR585: Smartphone Forensic Analysis In-Depth / GASF: GIAC Advanced Smartphone Forensics

FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques/ GREM: GIAC Reverse Engineering Malware

FOR518: Mac and iOS Forensic Analysis and Incident Response

FOR526: Advanced Memory Forensics & Threat Detection

Investigate (IN)

Specialty Area: Digital Forensics (FOR)

Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations.

Work Role: Cyber Defense Forensics Analyst (IN-FOR-002)

Analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/ network vulnerability mitigation.

SANS Training Course	GIAC Certification	Work Role Proficiency
FOR500: Windows Forensics Analysis	GCFE: GIAC Certified Forensic Examiner	3: Advanced
FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics	GCFA: GIAC Certified Forensic Analyst	3: Advanced
FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response	GNFA: GIAC Network Forensic Analyst	3: Advanced

Other Mapped SANS Training and GIAC Certifications:

SEC401: Security Essentials Bootcamp Style / GSEC: GIAC Security Essentials
FOR585: Smartphone Forensic Analysis In-Depth / GASF: GIAC Advanced Smartphone Forensics
FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques/
GREM: GIAC Reverse Engineering Malware
FOR518: Mac and iOS Forensic Analysis and Incident Response
FOR526: Advanced Memory Forensics & Threat Detection

Last Page