CYBERSECURITY

ALL ABOUT SECURITY OPERATION CENTER (SOC)

INTRODUCTION

The SOC is responsible for monitoring, investigating, and remediating security events. Their scope of responsibility depends on who is staffing the SOC. As previously discussed, SOCs can be internal to the company or outsourced to an MSSP. Internal SOCs typically have higher privileges to take remedial actions during an incident, where Managed Security Services Providers (MSSPs) usually must report the incident to a customer's information technology (IT) team. The key benefit to an internal SOC vs. an MSSP is the ability of the internal SOC to learn the details of a single network. MSSPs have multiple customers and must monitor several enterprise networks at once. This leaves the SOC analysts at a disadvantage as they never truly learn the granular details of a customer's enterprise.

SOC JOB ROLES

Security Analyst

The security analyst role evaluates various types of data and plans and implements security measures to protect computer systems, networks, and data. Reviewing data can mean evaluating live network traffic or a copy of evidence such as event logs generated by security and network tools. Regarding a security operations center, SOC analyst can be responsible for reviewing security logs and responding to events based on the services offered by the SOC.

Responsibilities	Skills	Certifications
Evaluate security measures and controls for vulnerabilities	Penetration and vulnerability testing, information security knowledge	CEH: Certified Ethical Hacker OSCP and PEN-200 from offensive security CPT: Certified Penetration Tester CEPT: Certified Expert Penetration Tester GPEN: GIAC Certified Penetration Tester CISM: Certified Information Security Manager
Establish plans and protocols to protect digital files and information systems against unauthorized access, modification, or destruction	Host security tools (antivirus, anti-malware, VPN), data loss prevention technologies, encryption concepts, identity management, access control	ECSA: EC-Council Certified Security Analyst Vendor NAC certification Vendor Data Loss certification Identity Management certification (e.g., Microsoft Active Directory)
Maintain data and monitor security access	TCP/IP, computer networking, routing and switching	GSEC: GIAC Security Essentials GCIH: GIAC Certified Incident Handler GCIA: GIAC Certified Intrusion Analyst CISM: Certified Information Security Manager
Perform security assessments and recommend security controls	Firewall and intrusion detection/prevention protocols	CISSP: Certified Information Systems Security Professional Vendor product certifications
Anticipate security alerts,	Windows, UNIX, macOS, and	Operating system certifications

incidents, and disasters and reduce their likelihood	Linux operating systems	
Manage network and security systems	Network protocols and packet analysis tools. Windows, UNIX, macOS, and Linux operating systems	Vendor network certification (e.g., Cisco CCNA/CCNP/CCIE) Operating system certifications
Analyze security breaches to determine their root cause and impacted parties	Digital forensics and threat hunting	EC Council Computer Hacking Forensic Investigator certification
Recommend and install tools and countermeasures	Understand industry frameworks, security tools, and security process	ISC2 CISSP CompTIA CySA+
Provide training to employees in security awareness and procedures	Developing training programs	SANS Security Awareness Professional (SSAP)

Penetration Tester

The penetration tester role is focused on identifying vulnerabilities and testing those vulnerabilities in a similar manner to how an adversary would. Assessment officers and others that are responsible for identifying vulnerabilities tend to leverage automated tools and focus on identifying potential vulnerabilities but do not validate how realistic the vulnerability may or may not be. Penetration testers invest additional time validating that vulnerabilities exist using the same tools used by adversaries.

Responsibilities	**Skills**	**Certifications**
Perform penetration tests and assessments of web-based applications, networks, and computer systems	Exploitation, assessment, and audit skillsets; technical writing; legal and compliance understanding	CEH: Certified Ethical Hacker OSCP and PEN-200 from offensive security CPT: Certified Penetration Tester CEPT: Certified Expert Penetration Tester GPEN: GIAC Certified Penetration Tester
Conduct physical security assessments of servers, systems, and networks	Vulnerability and physical security assessment capabilities Lock picking	A+ and other hardware certifications
Design and create new tools and tests for penetration testing and assessments	Network servers, networking tools, security tools and products	OSCP and PEN-200 from offensive security CEPT: Certified Expert Penetration Tester
Probe targets and pinpoint methods that attackers could use to exploit weaknesses and logic flaws	Computer hardware and software systems; vulnerability management and exploitation tactics	GPEN: GIAC Certified Penetration Tester CEH: Certified Ethical Hacker OSCP and PEN-200 from offensive security CPT: Certified Penetration Tester CEPT: Certified Expert Penetration Tester

Employ social engineering to uncover security holes	Web-based applications and behavior science	OSCP: Offensive Security Certified Professional
Incorporate business goals into security strategies and policy development	Security frameworks (e.g., ISO 27001/27002, NIST cybersecurity framework, etc.)	CISSP: Certified Information Systems Security Professional CISM: Certified Information Security Manager
Research, document, and review security findings with management and IT teams	Vulnerability analysis and reverse engineering	CCFE: Certified Computer Forensics Examiner
Improve security services, including the continuous enhancement of existing methodology material and supporting assets	Security frameworks (e.g., ISO 27001/27002, NIST cybersecurity framework, etc.)	CISSP: Certified Information Systems Security Professional
Provide feedback, support, and verification as an organization fixes security issues.	Communication and writing	College degree

Assessment Officer

An assessment officer is responsible for identifying potential vulnerabilities or gaps in corporate policy, compliance requirements, or general security best practices as defined in popular frameworks. Unlike a penetration tester, an assessment officer works within specific scopes as defined by policies, compliance, or frameworks, meaning he or she must be aware of the latest requirements and continuously validate the organization is meeting those requirements. Any vulnerabilities out of scope of such.

Responsibilities	**Skills**	**Certifications**
Incorporate business goals into security strategies and policy development	Security frameworks (e.g., ISO 27001/27002, NIST cybersecurity framework, etc.)	CISSP: Certified Information Systems Security Professional CISM: Certified Information Security Manager
Conduct physical security assessments of servers, systems, and networks	Vulnerability and physical security assessment capabilities; lock picking	GPEN: GIAC Certified Penetration Tester CEH: Certified Ethical Hacker OSCP and PEN-200 from offensive security CPT: Certified Penetration Tester CEPT: Certified Expert Penetration Tester
Interview employees, obtain technical information, and assess audit results	Management and strong communication skills	College degree or special communication skills training CISM: Certified Information Security Manager
Understand industry data security regulations	Understand HIPAA, PCI DSS, etc.	Specific industry data security certification and experience
Develop and execute tests based on regulations being audited	Critical-thinking skills	College degree and/or programming certification

Research, document, and review security findings with management and IT teams	Critical-thinking skills	College degree and/or programming certification
Understand organization policies and procedures	Critical-thinking skills and experience with SOC policies and procedures	College degree
Provide feedback, support, and verification as an organization fixes security issues	Critical-thinking, project management, and communication skills	College degree

Incident Responder

An incident responder is a cyber first-responder or a higher-tier resource responsible for responding to a security incident. This role involves providing rapid initial response to IT security threats, incidents, and cyberattacks on the organization. The role can also include some penetration and vulnerability testing, network management, intrusion detection, security audits, network forensics, and maintenance of IT security systems. The primary responsibility may be monitoring traffic for any unusual activity or unauthorized access attempts and initiating the appropriate response when a potential event is identified. The response can include patching systems, initiating segmentation, isolating systems, alerting all associated parties, and assisting with returning impacted systems back to an operational state.

Responsibilities	**Skills**	**Certifications**
Actively monitor systems and networks for intrusions	Windows, UNIX, macOS, and Linux operating systems	Operating system certifications CompTIA CySA+
Identify security flaws and vulnerabilities	Computer hardware and software systems; vulnerability management and exploitation tactics	GPEN: GIAC Certified Penetration Tester CEH: Certified Ethical Hacker OSCP and PEN-200 from offensive security CPT: Certified Penetration Tester CEPT: Certified Expert Penetration Tester
Perform security audits, risk analysis, network forensics, and penetration testing	Exploitation, assessment and audit skillsets; technical writing; legal and compliance understanding; TCP/IP-based network communication	GCFE: GIAC Certified Forensic Examiner GPEN: GIAC Certified Penetration Tester CEH: Certified Ethical Hacker OSCP and PEN-200 from offensive security CPT: Certified Penetration Tester CEPT: Certified Expert Penetration Tester
Perform desktop security assessments and update/patch potential vulnerabilities	Computer hardware and software systems; vulnerability assessments	CISSP: Certified Information Systems Security Professional CISM: Certified Information Security Manager
Develop a procedural set of	Operating system installation,	Operating system certifications

responses to security problems	patching, and configuration	
Establish protocols for communication within an organization and dealing with law enforcement during security incidents	Critical-thinking, project management, and communication skills	College degree
Create a program development plan that includes security gap assessments, policies, procedures, playbooks, training, and tabletop testing	Security frameworks (e.g., ISO 27001/27002, NIST cybersecurity framework, etc.); Critical thinking, project management, and communication skills	CISSP: Certified Information Systems Security Professional College degree
Produce detailed incident reports and technical briefs for management, administrators, and end users	Critical-thinking, project management, and communication skills	College degree
Liaison with other cyberthreat analysis entities	Critical-thinking, project management, and communication skills	College degree
Handle case management duties of an incident and be involved with lessons-learned post incident meetings	Case management experience and tools	CompTIA CySA+ CISM: Certified Information Security Manager College degree

Systems Analyst

A systems analyst is responsible for monitoring and interpreting different forms of data. Data can include logs from security tools, alerts from networking equipment, or other event data. A systems analyst might also be responsible for analyzing various types of artifacts, including files and programs, the goal being to determine whether there is any potential risk to the organization and discover the purpose of the artifact (meaning why it was created). For example, a word document might have a rootkit included, so the purpose of the document is to trick a user into running it and installing the rootkit.

Responsibilities	**Skills**	**Certifications**
Actively monitor systems and networks for intrusions	Windows, UNIX, macOS, and Linux operating systems	CCE: Certified Computer Examiner
Identify security flaws and vulnerabilities	Computer hardware and software systems; vulnerability management and exploitation tactics	GPEN: GIAC Certified Penetration Tester CEH: Certified Ethical Hacker OSCP and PEN-200 from offensive security CPT: Certified Penetration Tester CEPT: Certified Expert Penetration Tester
Perform security audits, risk analysis, network forensics, and penetration testing	Computer hardware and software systems; vulnerability management and exploitation tactics TCP/IP-based network	GPEN: GIAC Certified Penetration Tester CEH: Certified Ethical Hacker OSCP and PEN-200 from offensive security

	communications	CPT: Certified Penetration Tester CEPT: Certified Expert Penetration Tester
Perform malware analysis and reverse engineering	Computer hardware and software systems	GCFA: GIAC Certified Forensic Analyst
Experience working with SIEM and SOAR orchestration and automation	DevOps and playbooks skills	Certification in DevOps
Reverse engineer/ disassemble malware and other artifacts	Disassemblers, debuggers, and other static-analysis tools	GIAC Reverse Engineering Malware (GREM)
Develop sandboxes and analyze software behavior	Sandboxes and other dynamic analysis tools	GIAC Reverse Engineering Malware (GREM)
Analyze logs and other data sources	Security tool logs (firewall, IDS/IPS, etc.), SIEMs, and SOAR	CCNA Cyber Ops, CompTIA Cybersecurity Analyst (CySA+)
Liaison with other cyberthreat analysis entities	Forensic software applications (e.g., EnCase, FTK, Helix, Cellebrite, XRY, etc.)	CREA: Certified Reverse Engineering Analyst
Understand assembly language and how computer systems operate (RAM, ROM, storage, etc.)	IDA Pro, Ghidra, RAM/ROM dumps	GIAC Reverse Engineering Malware (GREM)

Security Administrator

A security administrator is responsible for managing IT-related security and safety issues within a company. Tasks can include developing policies and procedures as well as overseeing that policies are followed by employees. Security administrators also oversee the implementation of solutions that prevent cyberthreats and protect data's confidentiality, integrity, and availability. Tasks include administering security controls to reduce the risk associated with potential vulnerabilities.

Responsibilities	**Skills**	**Certifications**
Protect systems against unauthorized access, modification, and/or destruction	Windows, UNIX, and Linux operating systems; system security capabilities	CompTIA Security+ (popular base-level security certification)
Perform vulnerability and networking scanning	Computer hardware and software systems; vulnerability management and exploitation tactics TCP/IP-based network communications	CCNA: Cisco Certified Network Associate CEH: Certified Ethical Hacker
Monitor network traffic for unusual or malicious activity	Strong understanding of firewall technologies	ECSA: EC-Council Certified Security Analyst CompTIA CySA+
Configure and support security tools such as firewalls, antivirus software, and patch management system	TCP/IP, computer networking, routing and switching	CISSP: Certified Information Systems Security Professional
Implement network security policies, application security,	Network protocols and packet analysis tools	CISM: Certified Information Security Manager CISSP: Certified Information

access control, and corporate data safeguards		Systems Security Professional
Train employees in security awareness and procedures	Critical-thinking, project management, and communication skills	College degree
Perform security audits and make policy recommendations determine their root cause and impacted parties	Intermediate to expert IDS/IPS knowledge; vulnerability evaluation; security frameworks (e.g., ISO 27001/27002, NIST cybersecurity framework, etc.).	CISSP: Certified Information Systems Security Professional College degree
Develop and update business continuity and disaster recovery protocols	Security frameworks (e.g., ISO 27001/27002, NIST cybersecurity framework, etc.); critical-thinking, project management, and communication skills	College degree

Security Engineer

This role is similar to a security analyst, with responsibilities of performing security monitoring, security and data/log analysis, and forensic analysis. The goal of this role is to detect security incidents and launch a response. A security engineer can also have responsibilities for identifying which security technologies are used by an organization, maintenance of existing security technologies, development and maintenance of security policy, and developing methods to improve policies.

Responsibilities	**Skills**	**Certifications**
Configure and install firewalls and intrusion detection/ prevention systems	IDS/IPS, penetration testing, and vulnerability testing	CISM: Certified Information Security Manager CISSP: Certified Information Systems Security Professional CEH: Certified Ethical Hacker
Perform vulnerability testing, risk analyses, and security assessments	Firewall and intrusion detection/prevention protocols	CCNP Security: Cisco Certified Network Professional Security CEH: Certified Ethical Hacker
Develop or work with automation scripts to handle and track incidents	Secure coding practices, ethical hacking, and threat modeling	GSEC: Security Essentials GCIH: GIAC Certified Incident Handler GCIA: GIAC Certified Intrusion Analyst
Investigate intrusion incidents, conduct forensic investigations, and launch incident responses	Windows, UNIX, macOS, and Linux operating systems	CISSP: Certified Information Systems Security Professional CompTIA CySA+ CCFE: Certified Computer Forensics Examiner
Collaborate with colleagues on authentication, authorization, and encryption solutions	Critical-thinking, project management, and communication skills; encryption technology concept	Systems Security Professional College degree

Evaluate new technologies and processes that enhance security capabilities	Critical-thinking, project management, and communication skills	College degree
Deliver technical reports and formal papers on test findings	Communication and technical writing skills	College degree
Supervise changes in software, hardware, facilities, telecommunications, and user needs	Critical-thinking, project management, and communication skills	College degree
Define, implement, and maintain corporate security policies	Security frameworks (e.g., ISO 27001/27002, NIST cybersecurity framework, etc.); critical thinking, project management, and communication skills	CISSP: Certified Information College degree
Analyze and advise on new security technologies and program conformance	Critical-thinking, project management, and communication skills	College degree
Recommend modifications in legal, technical, and regulatory areas that affect IT security	Security frameworks (e.g., ISO 27001/27002, NIST cybersecurity framework, etc.); critical thinking, project management, and communication skills	CISSP: Certified Information CISM: Certified Information Security Manager Systems Security Professional College degree

Security Trainer

A security trainer is responsible for implementing standardized training programs based on the organization's policies and the current threat landscape. Security trainers develop and schedule training needs based on feedback from interviewing leadership and employees. Responsibilities include developing the training material, coordinating and monitoring enrollment, schedules, costs, and equipment, and delivering training metrics to leadership. Other duties include researching industry training concepts, training people to deliver training content, and updating content as needed.

Responsibilities	**Skills**	**Certifications**
Develop a schedule to assess training needs	Experience with technologies and best practices for instructional manuals and teaching platforms	Certification from talent and training associations
Ensure strict adherence to company philosophy/mission statement/sales goals	Understanding policies, procedures, and industry guidelines, standards, and frameworks	CISSP: Certified Information Systems Security Professional
Deliver training to customers or other trainers	Excellent verbal and written communication skills	College degree
Manage security awareness program based on threat research	Strong project management skills with the ability to supervise multiple projects	College degree
Deliver technical reports and formal papers on test findings	Identity and access management principles	College degree

Test and review created materials	Critical-thinking, project management, and communication skills	College degree
Maintain a database of all training materials	Basic database and program management skills	College degree

Security Architect

A security architect oversees the implementation of network and computer security for an organization. This role is typically a senior-level employee responsible for creating security structures, defenses, and responses to security incidents. Additional responsibilities may include providing technical guidance, assessing costs and risks, and establishing security policies and procedures for the organization.

Responsibilities	**Skills**	**Certifications**
Plan, research, and design robust security architectures for any IT project	Risk assessment procedures, policy formation, role-based authorization methodologies, authentication technologies, and security attack concepts	CISSP: Certified Information Systems Security Professional
Perform vulnerability testing, risk analyses, and security assessments	Computer hardware and software systems; vulnerability management and exploitation tactics	GPEN: GIAC Certified Penetration Tester CEH: Certified Ethical Hacker OSCP and PEN-200 from offensive security CPT: Certified Penetration Tester CEPT: Certified Expert Penetration Tester
Research security standards, security systems, and authentication protocols	Security frameworks (e.g., ISO 27001/27002, NIST cybersecurity framework, etc.); critical-thinking, project management, and communication skills	CISM: Certified Information Security Manager CISSP: Certified Information Systems Security Professional
Develop requirements for LANs, WANs, VPNs, routers, firewalls, and related network devices	Security controls such as firewall, IDS/IPS, network access control, and network segmentation	CISM: Certified Information Security Manager
Design public key infrastructures (PKIs), including use of certification authorities (CAs) and digital signatures	Security and encryption technologies	CISM: Certified Information Security Manager EC-Council Certified Encryption Specialist (ECES)
Review and approve installation of firewall, VPN, routers, IDS/IPS scanning technologies, and servers	Security concepts related to DNS, routing, authentication, VPN, proxy services, and DDOS mitigation technologies	GSEC: GIAC Security Essentials GCIH: GIAC Certified Incident Handler GCIA: GIAC Certified Intrusion Analyst
Provide technical supervision for security team(s)	Critical-thinking and communication skills	College degree

Define, implement, and maintain corporate security policies and procedures	Critical-thinking and communication skills	CISSP: Certified Information Systems Security Professional College degree
Oversee security awareness programs and educational efforts	Developing training programs	College degree
Update and upgrade security systems as needed	Windows, UNIX, macOS, and Linux operating systems	A+ Security CISSP: Certified Information Systems Security Professional

Cryptographer/Cryptologist

A SOC that uses encryption to secure information or to build a system will assign these requirements to a cryptologist. A cryptologist researches and develops stronger encryption algorithms. A cryptologist may also be responsible for analyzing encrypted information from malicious software to determine the purpose and functions of the software.

Responsibilities	**Skills**	**Certifications**
Protect information from interception, copying, modification and/or deletion	Computer architecture, data structures, and algorithms	The cryptologist field is new and only has programs in universities and special learning programs. Certification programs include cryptology aspects, but dedicated certifications are not available now.
Evaluate, analyze, and target weaknesses in cryptographic security systems and algorithms	Linear/matrix algebra and/or discrete mathematics	EC-Council Certified Encryption Specialist (ECES)
Develop statistical and mathematical models to analyze data and solve security problems	Probability theory, information theory, complexity theory, and number theory	EC-Council Certified Encryption Specialist (ECES) College degree in math and cryptologist certification
Investigate, research, and test new cryptology theories and applications	Principles of symmetric cryptography and asymmetric cryptography	EC-Council Certified Encryption Specialist (ECES) College degree in math and cryptologist certification
Probe for weaknesses in communication lines	Principles of symmetric cryptography and asymmetric cryptography	EC-Council Certified Encryption Specialist (ECES) College degree in math and cryptologist certification
Ensure financial data is securely encrypted and accessible only to authorized users	Network Access Control Concepts Data loss prevention technologies, encryption concepts, identity management, access control	Operating system certifications Vendor security certifications Authentication vendor certifications
Ensure message transmission data is not illegally accessed or altered in transit	Principles of symmetric cryptography and asymmetric cryptography	EC-Council Certified Encryption Specialist (ECES) College degree in math and

		cryptologist certification
Decode cryptic messages and coding systems for military, political, and/or law enforcement agencies	Principles of symmetric cryptography and asymmetric cryptography	EC Council Computer Hacking Forensic Investigator Certification College degree in math and cryptologist certification
Advise colleagues and research staff on cryptical/mathematical methods and applications	Principles of symmetric cryptography and asymmetric cryptography	College degree in math and cryptologist certification

Forensic Engineer

Digital forensics is the art of collecting evidence regarding a security incident. Evidence can be used for legal actions, to remediate the vulnerability used to cause the breach, or as part of a lessons-learned exercise. Forensic engineers require specific skillsets focused on collecting data without creating changes to what they are collecting. These engineers may also have legal knowledge to assist with investigations that lead to legal actions.

Responsibilities	**Skills**	**Certifications**
Conduct data breach and security incident investigations	Network skills, including TCP/IP-based network communications	CCE: Certified Computer Examiner
Recover and examine data from computers and electronic storage devices	Windows, UNIX, and Linux operating systems	CEH: Certified Ethical Hacker
Dismantle and rebuild damaged systems to retrieve lost data	Windows, UNIX, macOS, and Linux operating systems; digital forensics concepts	EnCE: EnCase Certified Examiner
Identify systems/networks compromised by cyberattacks	Computer hardware and software systems	GCFE: GIAC Certified Forensic Examiner
Compile evidence for legal cases	Operating system installation, patching, and configuration	GCFA: GIAC Certified Forensic Analyst
Draft technical reports, write declarations, and prepare evidence for trial	Backup and archiving technologies; technical writing	GCIH: GIAC Certified Incident Handler
Give expert counsel to attorneys about electronic evidence in a case	Cryptography principles; legal experience; digital forensics experience; strong communication skills	CCFE: Certified Computer Forensics Examiner
Advise law enforcement on the credibility of acquired data	eDiscovery tools; strong communication skills	CPT: Certified Penetration Tester
Stay proficient in forensic, response, and reverse engineering	Data processing skills in electronic disclosure environments	CCFE: Certified Computer Forensics Examiner College degree

Chief Information Security Officer

Part of high-level management and is positioned as the person responsible for the entire information security division of an organization. A CISO is responsible for all assurance activities related to the availability, integrity, and confidentiality of customers, business partner, employee, and business information in compliance with the organization's information security policies. A CISO works with executive management to determine acceptable levels of risk for the organization.

Responsibilities	Skills	Certifications
Appoint and guide a team of IT security experts	Practices and methods of IT strategy, enterprise architecture, and security architecture	CISA: Certified Information Systems Auditor
Create strategic plan for the deployment of information security technologies and program enhancements	Security concepts; critical-thinking and communication skills	CISM: Certified Information Security Manager
Supervise development of corporate security policies, standards, and procedures	ISO 27002, ITIL, and COBIT frameworks	GSLC: GIAC Security Leadership College degree
Integrate IT systems development with security policies and information protection strategies	PCI DSS, HIPAA, NIST, GLBA, and SOX compliance assessments	CCISO: Certified Chief Information Security Officer
Collaborate with key stakeholders to establish an IT security risk management program	Network security architecture development and definition	CGEIT: Certified in the Governance of Enterprise IT
Anticipate new security threat sand stay up to date with evolving infrastructures	Knowledge of third-party auditing and cloud risk assessment methodologies	CISSP: Certified Information Systems Security Professional
Develop strategies to handle security incidents and coordinate investigative activities	Critical-thinking and communication skills	CISSP-ISSMP: CISSP Information Systems Security Management Professional
Act as a focal point for IT security investigations	Critical-thinking and communication skills	CISSP: Certified Information Systems Security Professional College degree
Prioritize and allocate security resources correctly and efficiently	Critical-thinking and communication skills	College degree
Prepare financial forecasts for security operations and proper maintenance coverage for security assets	Critical-thinking and communication skills; contract experience	College degree
Work with senior management to ensure IT security protection policies are being implemented, reviewed, maintained, and governed effectively	Security frameworks (e.g., ISO 27001/27002, NIST cybersecurity framework, etc.); critical-thinking, project management, and communication skills	College degree

SOC SERVICES AND ASSOCIATED JOB ROLES

The roles and job skill requirements for your SOC will depend on the different services the SOC is responsible for delivering to its customers.

Risk Management Service

The risk management service is responsible for managing all aspects of risk to the organization. This includes analyzing risk, calculating the potential impact of risk, and making decisions based on the organization's risk appetite. Employees responsible for risk management must have great communication skills, enabling them not only to ensure that everybody in the organization understands any significant risk but also to explain the organization's risk management strategy. Working for the risk management service also requires a solid understanding of business, because decisions of the service will impact various internal and external elements of the organization. Successful employees responsible for risk management are skilled at negotiation and diplomacy. They can work under pressure and are able to modify strategies as various factors change the current state of the organization's risk status.

Possible job titles include chief information manager, chief information security officer, security officer, risk management analyst, and analyst.

Vulnerability Management Service

Successful employees responsible for vulnerability management have experience in and understanding of network and computer security. They can analyze hardware, software, networks, and communication to discover and address vulnerabilities. SOC members involved with vulnerability management have solid communication skills so they can explain identified vulnerabilities as well as work with various parties to validate findings, including third-party vendors and other external experts. Employees responsible for vulnerability management are detail-oriented, have strong problem-solving skills, and can adapt methods used to manage vulnerabilities based on the ever-changing threat landscape.

Possible job titles include penetration tester, vulnerability engineer, ethical hacker, red team tester, security analyst, and security engineer.

Incident Management Service

SOC employees responsible for incident management actively monitor systems and networks for intrusions. The incident management team develops a procedural set of responses to security problems and oversees their execution. This team is also responsible for restoring services back to a normal state following an incident as quickly as possible while minimizing the impact to business operations. Communication and diplomacy skills are required to produce incident reports and provide technical briefings to various parties about incidents in a diplomatic fashion. Employees are required to be able to work under pressure while coordinating all activities required to perform, monitor, and report on the incident management process.

Possible job titles include incident responder, security analyst, computer network defense, IT network defense, incident analyst, intrusion detection specialist, and network intrusion analyst.

Analysis Service

A security analyst is responsible for detecting and preventing cyberthreats to an organization. Members of the analysis team review security logs from various types of devices and work with the team responsible for incident management when a threat is confirmed. In addition to dealing with real-time threats, the analysis team analyzes and responds to undisclosed hardware and software vulnerabilities when a dedicated vulnerability management team isn't present. The analysis team can also take on responsibilities as a security advisor and develop security strategy based on data captured and analyzed. Members of the analysis team must be analytical and detail-oriented with specific skills

in understanding how devices generate logs and how to work with network and security tools that generate logs. Analysis engineers can also be responsible for analyzing and reverse engineering various types of artifacts, requiring a different set of analytical and technical skills than an analyst that works with security logs. Analysis engineers are technical, detail-oriented, and specialized in the types of data they are responsible for analyzing.

Possible job titles include security analyst, security engineer, security administrator, security specialist, security consultant, network engineer, operations analyst, business intelligence analyst, and data analyst.

Compliance Service

The most fundamental skill for employees responsible for compliance is the ability to deal with risk and conflict management. A compliance officer uses specific factors for scoring risk, which will be based on the requirements for the type of compliance being enforced. A compliance officer will encounter situations requiring explaining and defending their point of view to internal employees as well as external agencies such as regulators. Communication and analytical thinking are critical for this role as well as a willingness to learn, as the world of compliance is continuously changing. Other skills associated with successful members of the compliance team are being detailed-oriented, being capable of interpreting data, and having strong problem-solving skills.

Possible job titles include compliance officer, assessment officer, policy officer, and infosec officer.

Digital Forensics Service

Roles in digital forensics are technology-focused, requiring a desire to learn, deep analytical skills, and the ability to work with various technologies ranging from desktop computers to mobile devices. Digital forensics requires acute attention to details and a comprehension of cybersecurity fundamentals. Communication skills and an understanding of law and criminal investigation are important because the results from a forensic investigation might be used in court, in which case the investigator will be required to defend his or her work. Digital forensics requires working with different groups, from legal to technical, as well as tolerance for disturbing material that might be discovered during an investigation. Successful digital forensic engineers have experience in both legal and technical matters related to cybersecurity.

Possible job titles include forensic engineer, forensic scientist, forensic consultant, and digital forensic engineer.

Situational and Security Awareness Service

The key purpose of this service is to address the human element of security. The goal of the work performed by the situational and security awareness team is to change the behavior of employees so that they operate with security in mind, reducing their risk to the organization. Duties include everything regarding security awareness and developing an education program. Roles responsible for situational and security awareness require strong written and verbal communication skills. Members in this role must be able to interpret all industry regulations, standards, and compliance requirements as well as ensure that everybody understands the organization's risk management strategy. Successful situational and security awareness officers can accomplish these goals using a positive and engaging approach, which includes creating a metrics framework that can effectively measure results of the program.

Possible job titles include security trainer, training instructor, information assurance analyst, training analyst, security service training manager, and development manager.

Research and Development Service

SOC members of the research and development service are responsible for researching, planning, and implementing new programs and protocols for the organization. Duties include market research, tracking costs related to the creation of new programs and protocols, and making decisions on which projects are worth investing in. This group also validates if current programs, procedures, and technology being used are up to date with current and advanced industry standards. Members in this role have project management experience, are able to manage a budget, and are detail-oriented and creative.

Possible job titles include researcher, threat researcher, threat analyst, analyst, security analyst, programmer, software developer, and DevOps engineer.

NICE CYBERSECURITY WORKFORCE FRAMEWORK

Nice Framework Components

- Seven categories representing a high-level grouping of common cybersecurity functions
- Thirty-three Specialty Areas representing distinct areas of cybersecurity work
- Fifty-two Work Roles representing the most detailed groupings of cybersecurity work and composed of specific knowledge, skills, and abilities (KSAs) required to perform tasks in a Work Role

Categories

For better understanding, I shared about Protect and Defend category (Cyber Defense Analysis & Incident Response) below:

Cyber Defense Analysis

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.

Abilities

A0010: Ability to analyze malware.
A0015: Ability to conduct vulnerability scans and recognize vulnerabilities in security systems.
A0066: Ability to accurately and completely source all data used in intelligence, assessment and/or planning products.
A0123: Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
A0128: Ability to apply techniques for detecting host and network-based intrusions using intrusion detection technologies.
A0159: Ability to interpret the information collected by network tools (e.g. Nslookup, Ping, and Traceroute).

Knowledge

K0001: Knowledge of computer networking concepts and protocols, and network security methodologies.
K0002: Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
K0003: Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
K0004: Knowledge of cybersecurity and privacy principles.
K0005: Knowledge of cyber threats and vulnerabilities.
K0006: Knowledge of specific operational impacts of cybersecurity lapses.
K0007: Knowledge of authentication, authorization, and access control methods.
K0013: Knowledge of cyber defense and vulnerability assessment tools and their capabilities.
K0015: Knowledge of computer algorithms.

K0001: Knowledge of computer networking concepts and protocols, and network security methodologies.
K0002: Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
K0003: Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
K0004: Knowledge of cybersecurity and privacy principles.
K0005: Knowledge of cyber threats and vulnerabilities.
K0006: Knowledge of specific operational impacts of cybersecurity lapses.
K0007: Knowledge of authentication, authorization, and access control methods.
K0013: Knowledge of cyber defense and vulnerability assessment tools and their capabilities.
K0015: Knowledge of computer algorithms.
K0018: Knowledge of encryption algorithms
K0019: Knowledge of cryptography and cryptographic key management concepts
K0024: Knowledge of database systems.
K0033: Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists).
K0040: Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).
K0042: Knowledge of incident response and handling methodologies.
K0044: Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
K0046: Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.
K0049: Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).
K0056: Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML).
K0058: Knowledge of network traffic analysis methods.
K0059: Knowledge of new and emerging information technology (IT) and cybersecurity technologies.
K0060: Knowledge of operating systems.
K0061: Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).
K0065: Knowledge of policy-based and risk adaptive access controls.
K0070: Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).
K0074: Knowledge of key concepts in security management (e.g., Release Management, Patch Management).

K0075: Knowledge of security system design tools, methods, and techniques.
K0093: Knowledge of telecommunications concepts (e.g., Communications channel, Systems Link Budgeting, Spectral efficiency, Multiplexing).
K0098: Knowledge of the cyber defense Service Provider reporting structure and processes within one's own organization.
K0104: Knowledge of Virtual Private Network (VPN) security.
K0106: Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.
K0107: Knowledge of Insider Threat investigations, reporting, investigative tools and laws/regulations.
K0110: Knowledge of adversarial tactics, techniques, and procedures.
K0111: Knowledge of network tools (e.g., ping, traceroute, nslookup)
K0112: Knowledge of defense-in-depth principles and network security architecture.
K0113: Knowledge of different types of network communication (e.g., LAN, WAN, MAN, WLAN, WWAN).
K0116: Knowledge of file extensions (e.g., .dll, .bat, .zip, .pcap, .gzip).
K0139: Knowledge of interpreted and compiled computer languages.
K0142: Knowledge of collection management processes, capabilities, and limitations.
K0143: Knowledge of front-end collection systems, including traffic collection, filtering, and selection.
K0157: Knowledge of cyber defense and information security policies, procedures, and regulations.
K0160: Knowledge of the common attack vectors on the network layer.
K0161: Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks).
K0162: Knowledge of cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored).
K0167: Knowledge of system administration, network, and operating system hardening techniques.
K0168: Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.
K0177: Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).
K0179: Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).
K0180: Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.
K0190: Knowledge of encryption methodologies.
K0191: Signature implementation impact for viruses, malware, and attacks.
K0192: Knowledge of Windows/Unix ports and services.
K0203: Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).

K0221: Knowledge of OSI model and underlying network protocols (e.g., TCP/IP).
K0222: Knowledge of relevant laws, legal authorities, restrictions, and regulations pertaining to cyber defense activities.
K0260: Knowledge of Personally Identifiable Information (PII) data security standards.
K0261: Knowledge of Payment Card Industry (PCI) data security standards.
K0262: Knowledge of Personal Health Information (PHI) data security standards.
K0290: Knowledge of systems security testing and evaluation methods.
K0297: Knowledge of countermeasure design for identified security risks.
K0300: Knowledge of network mapping and recreating network topologies.
K0301: Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).
K0303: Knowledge of the use of sub-netting tools.
K0318: Knowledge of operating system command-line tools.
K0322: Knowledge of embedded systems.
K0324: Knowledge of Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications.
K0332: Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.
K0339: Knowledge of how to use network analysis tools to identify vulnerabilities.
K0342: Knowledge of penetration testing principles, tools, and techniques.
K0624: Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)

Skills

S0020: Skill in developing and deploying signatures.
S0025: Skill in detecting host and network based intrusions via intrusion detection technologies (e.g., Snort).
S0027: Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.
S0036: Skill in evaluating the adequacy of security designs.
S0054: Skill in using incident handling methodologies.
S0057: Skill in using protocol analyzers.
S0063: Skill in collecting data from a variety of cyber defense resources.
S0078: Skill in recognizing and categorizing types of vulnerabilities and associated attacks.
S0096: Skill in reading and interpreting signatures (e.g., snort).
S0147: Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.).
S0156: Skill in performing packet-level analysis.
S0167: Skill in recognizing vulnerabilities in security systems. (e.g., vulnerability and compliance scanning).
S0169: Skill in conducting trend analysis.
S0367: Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
S0370: Skill to use cyber defense Service Provider reporting structure and processes within one's own organization.

Tasks

T0020: Develop content for cyber defense tools.
T0023: Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources.
T0043: Coordinate with enterprise-wide cyber defense staff to validate network alerts.
T0088: Ensure that cybersecurity-enabled products or other compensating security control technologies reduce identified risk to an acceptable level.
T0155: Document and escalate incidents (including event's history, status, and potential impact for further action) that may cause ongoing and immediate impact to the environment.
T0164: Perform cyber defense trend analysis and reporting.
T0166: Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack.
T0178: Perform security reviews and identify security gaps in security architecture resulting in recommendations for inclusion in the risk mitigation strategy.
T0187: Plan and recommend modifications or adjustments based on exercise results or system environment.
T0198: Provide daily summary reports of network events and activity relevant to cyber defense practices.
T0214: Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts.
T0258: Provide timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities and distinguish these incidents and events from benign activities.
T0259: Use cyber defense tools for continual monitoring and analysis of system activity to identify malicious activity.
T0260: Analyze identified malicious activity to determine weaknesses exploited, exploitation methods, effects on system and information.
T0290: Determine tactics, techniques, and procedures (TTPs) for intrusion sets.
T0291: Examine network topologies to understand data flows through the network.
T0292: Recommend computing environment vulnerability corrections.
T0293: Identify and analyze anomalies in network traffic using metadata (e.g., CENTAUR).
T0294: Conduct research, analysis, and correlation across a wide variety of all source data sets (indications and warnings).
T0295: Validate intrusion detection system (IDS) alerts against network traffic using packet analysis tools..
T0296: Isolate and remove malware.
T0297: Identify applications and operating systems of a network device based on network traffic.
T0298: Reconstruct a malicious attack or activity based off network traffic.
T0299: Identify network mapping and operating system (OS) fingerprinting activities.
T0310: Assist in the construction of signatures which can be implemented on cyber defense network tools in response to new or observed threats within the network environment or enclave.

T0332: Notify designated managers, cyber incident responders, and cybersecurity service provider team members of suspected cyber incidents and articulate the event's history, status, and potential impact for further action in accordance with the organization's cyber incident response plan.
T0469: Analyze and report organizational security posture trends.
T0470: Analyze and report system security posture trends.
T0475: Assess adequate access controls based on principles of least privilege and need-to-know.
T0503: Monitor external data sources (e.g., cyber defense vendor sites, Computer Emergency Response Teams, Security Focus) to maintain currency of cyber defense threat condition and determine which security issues may have an impact on the enterprise.
T0504: Assess and monitor cybersecurity related to system implementation and testing practices.
T0526: Provides cybersecurity recommendations to leadership based on significant threats and vulnerabilities.
T0545: Work with stakeholders to resolve computer security incidents and vulnerability compliance.
T0548: Provide advice and input for Disaster Recovery, Contingency, and Continuity of Operations Plans.

Incident Response

Cyber Defense Incident Responder

(PR-CIR-001)

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

Abilities

A0121: Ability to design incident response for cloud service models.
A0128: Ability to apply techniques for detecting host and network-based intrusions using intrusion detection technologies.

Knowledge

K0001: Knowledge of computer networking concepts and protocols, and network security methodologies.
K0002: Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
K0003: Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
K0004: Knowledge of cybersecurity and privacy principles.
K0005: Knowledge of cyber threats and vulnerabilities.
K0006: Knowledge of specific operational impacts of cybersecurity lapses.
K0021: Knowledge of data backup and recovery.
K0026: Knowledge of business continuity and disaster recovery continuity of operations plans.
K0033: Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists).
K0034: Knowledge of network services and protocols interactions that provide network communications.
K0041: Knowledge of incident categories, incident responses, and timelines for responses.
K0042: Knowledge of incident response and handling methodologies.
K0046: Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.
K0058: Knowledge of network traffic analysis methods.
K0062: Knowledge of packet-level analysis.
K0070: Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).

K0106: Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.
K0157: Knowledge of cyber defense and information security policies, procedures, and regulations.
K0161: Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks).
K0162: Knowledge of cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored).
K0167: Knowledge of system administration, network, and operating system hardening techniques.
K0177: Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).
K0179: Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).
K0221: Knowledge of OSI model and underlying network protocols (e.g., TCP/IP).
K0230: Knowledge of cloud service models and how those models can limit incident response.
K0259: Knowledge of malware analysis concepts and methodologies.
K0287: Knowledge of an organization's information classification program and procedures for information compromise.
K0332: Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.
K0565: Knowledge of the common networking and routing protocols (e.g. TCP/IP), services (e.g., web, mail, DNS), and how they interact to provide network communications.
K0624: Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)

Skills

S0003: Skill of identifying, capturing, containing, and reporting malware.
S0047: Skill in preserving evidence integrity according to standard operating procedures or national standards.
S0077: Skill in securing network communications.
S0078: Skill in recognizing and categorizing types of vulnerabilities and associated attacks.
S0079: Skill in protecting a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters).
S0080: Skill in performing damage assessments.
S0173: Skill in using security event correlation tools.
S0365: Skill to design incident response for cloud service models.

Tasks

T0041: Coordinate and provide expert technical support to enterprise-wide cyber defense technicians to resolve cyber defense incidents.
T0047: Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation.
T0161: Perform analysis of log files from a variety of sources (e.g., individual host logs, network traffic logs, firewall logs, and intrusion detection system [IDS] logs) to identify possible threats to network security.
T0163: Perform cyber defense incident triage, to include determining scope, urgency, and potential impact, identifying the specific vulnerability, and making recommendations that enable expeditious remediation.
T0164: Perform cyber defense trend analysis and reporting.
T0170: Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on enterprise systems.
T0175: Perform real-time cyber defense incident handling (e.g., forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRTs).
T0214: Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts.
T0233: Track and document cyber defense incidents from initial detection through final resolution.
T0246: Write and publish cyber defense techniques, guidance, and reports on incident findings to appropriate constituencies.
T0262: Employ approved defense-in-depth principles and practices (e.g., defense-in-multiple places, layered defenses, security robustness).
T0278: Collect intrusion artifacts (e.g., source code, malware, Trojans) and use discovered data to enable mitigation of potential cyber defense incidents within the enterprise.
T0279: Serve as technical expert and liaison to law enforcement personnel and explain incident details as required.
T0312: Coordinate with intelligence analysts to correlate threat assessment data.
T0395: Write and publish after action reviews.
T0503: Monitor external data sources (e.g., cyber defense vendor sites, Computer Emergency Response Teams, Security Focus) to maintain currency of cyber defense threat condition and determine which security issues may have an impact on the enterprise.
T0510: Coordinate incident response functions.

ROLE TIERS

Tier/Level 1 (L1)

First-tier SOC analyst may be responsible for detecting, identifying, and troubleshooting security events that come into the SOC. Often this is the tier that communicates with the affected party. Responsibilities include detection, classification, and escalation of events.

Tier/Level 2 (L2)

A second-tier analyst may have mitigation responsibilities over any event escalated by a first-tier SOC analyst. If the event requires even further support, a more experienced third-tier analyst may be involved to remediate the situation.

Tier/Level 3 (L3)

The third-tier analyst might also build tools and processes to improve capabilities within the SOC, including the processes followed by lower-tier analysts. Higher tier roles have higher compensation but require deeper technical skills and experience.

SKILLS REQUIREMENTS

Networking

It will be helpful to know the various common port numbers and the difference between TCP and UDP. TCP relies on an established connection called a three-way handshake and the UDP protocol. Think of UDP as the “Unreliable Dang Protocol” because the UDP protocol just sends messages and doesn’t care if they get them there or not, whereas in the TCP connection if a piece of data is missed in transit, it will resend the missed packet and then put them back together in order. UDP services are mainly used for things such as video streaming where a glitch in the movie because of dropped packets wouldn’t matter a lot. TCP connections are used when every bit of data needs to arrive at the destination, such as in a file transfer. If you are transferring a file, if all bits and bytes do not get to the destination, the file will not be able to be run.

Next is the TCP three-way handshake process. This is important because this three-way handshake process establishes a connection between two hosts for a TCP connection.

Network Security

The basic tenets of security revolved around the concept of CIA Triad, not the Central Intelligence Agency but confidentiality, integrity, and availability. All security can be broken down from these three high-level categories. Confidentiality is the secrecy of the information, making sure that the information can only be seen by the intended people, no more no less. Integrity revolves around the correctness of the data, making sure that the information you are consuming is the data that you intend to consume, complete and unaltered. Availability consists of making sure that the data can be used when it needs to be used.

Cryptography

There are a few cryptography principles that you will need to know as well. The first is the difference between encryption vs. hashing. Basically, encrypting is changing the data in a way that makes it unreadable, but it is intended to be changed back in a way to make the message readable again. Hashing is the process of taking a set of data and creating a unique fingerprint out of it. For instance, if you had a thousand lines of code, you could save it to a file and hash that file to a 128-bit MD5 hash that would look something similar to this:

97fbca75e134639d48bd83270ae9e045

The main difference between a hash and an encryption is that a hash is one way. There is not any viable way to turn the string above back into the characters.

Endpoint Security
The front lines of the cybersecurity war are on your network endpoints. User laptops, smart phones, and printers are only a few of the targeted devices that attackers can compromise. The difficulty with endpoint security is the plethora of devices on the market. Most of all devices run on one of these three operating system (OS) families: Windows, Unix, and MacOS.

TOOLS

SIEM
Other than collecting logs, the SIEM also normalizes logs, which means to put them into the correct chronological order. Because of the varying time zones across the world configured in your devices, the timestamps, or date and time, on each log need to be accounted for. Also in normalization, when the logs are ingested into the SIEM platform, they must meet a certain standard and format.

Each SIEM has a proprietary technique that is used to take in billions of logs and picks out the things that are suspicious, but at a basic level, either the vendor or the users (or both) create rules that if any of the logs match a given criteria, it will sound the alarm.

Firewalls
Additional to SIEM and SOAR, you will likely come across firewalls. Firewall and firewall engineering is a specialty all on its own, but it's important jargon to understand the biggest players in the firewall space are Cisco, Checkpoint, Fortinet, Palo Alto, Juniper, and SonicWall. As a security analyst, you might be responsible for performing a firewall block on an IP address or requesting to have it done. What this means is you have used the tools and techniques of a security analyst and determined that it was bad, and you want to block that IP address from being communicated with from your internal network.

IDS/IPS
Intrusion detection systems can either be placed in line or through a network tap. Intrusion detection systems are designed to detect and not take preventative measures. Tapping the network allows the device to see the network traffic but not affect bandwidth. IDS placed through a tap cannot take preventative action because they cannot control the flow of traffic.

The IPS has the ability to change the flow of traffic between the two devices because of the way it sits on the network. Intrusion prevention systems must be placed. Placing an IPS in line allows it to control the flow of traffic and take preventative actions to protect it.

IDS can be placed in line as well. Most modern IPS will have some rules set to "take action" and some set to monitor only. These are called intrusion detection and prevention systems (IDPS).

Sandboxing
Quite a few endpoints detection software will detonate the file on your behalf so it can know whether it is bad or not, but nothing comes as close as a good report from Cuckoo, Hybrid Analysis, or Joe Sandbox. These tools are designed to twist every knob and press every button to squeeze as much

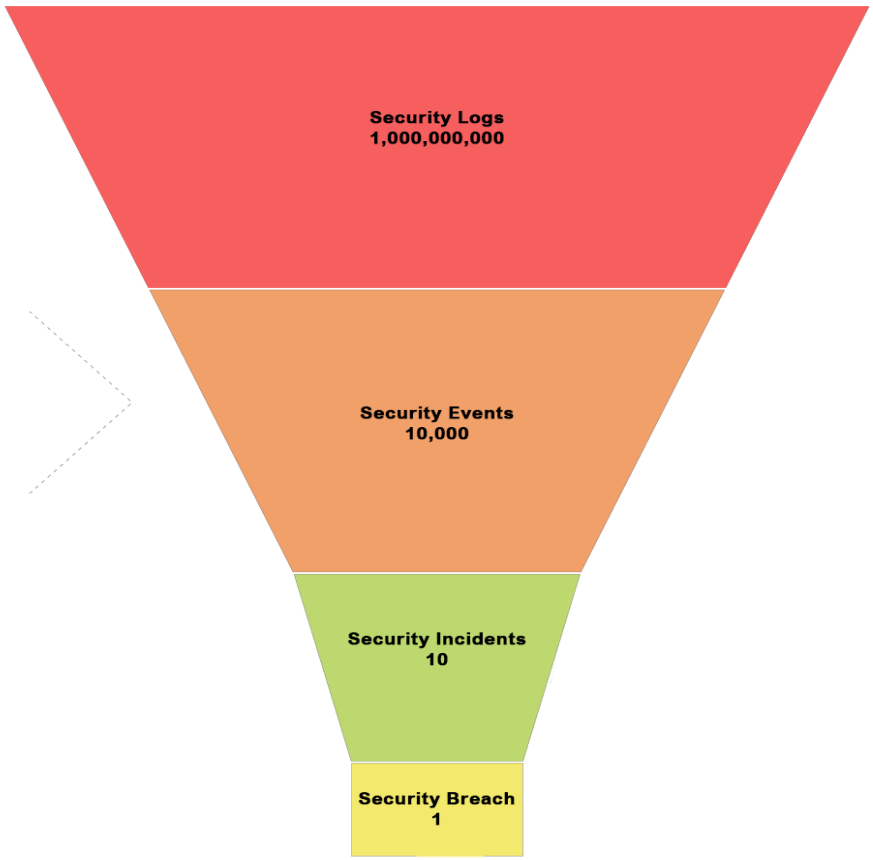
execution information as they can out of it. As a SOC analyst, you mainly use these tools to get out indicators of compromise like hashes of files that it drops, or IP addresses and domains it contacts to run these through your SIEM to see if there are any historical connections.

There are a few online sandbox tools but be wary to now execute proprietary files in a public sandbox to be shared with the community. Other online tools to take note of are:

- Virustotal.com: VirusTotal is perhaps the most useful online tool for a SOC analyst. You visit the website and punch in a URL or hash, and you will, most of the time, have a good idea if the IoC is good or bad.
- Domain Tools: The whois tool at domain tools I always found very easy to use. While there are plenty of very good online whois searches available, I always like to use domain tools.
- Talos Intelligence: Use this tool to conduct reputational checks on IP addresses and URLs.
- IPVoid: Use this tool to check blacklists for a particular IP address.
- URLVoid: Use this tool to check URLs for safety reputations.
- Threat Crowd: Use this tool as a search engine for threats. Threat Crowd is a system fo finding and researching artifacts relating to cyber threats.
- TOR Exit Node List: Check to see if the IP address is on a TOR exit node.
- IBM X-Force Exchange: Check the IoC for information in X-Force Exchange.
- Search Engine: Always check a search engine when looking for suspicious items. Some gems are more hidden!

COMMON DEFINITON IN SOC

As you go through your day as a SOC analyst, you will come across terms that aren't always agreed on, and the meanings are a bit vague. From the best of our combined experience, these are the best definitions for these terms.



Security Logs

At the very base of a security program are security logs. These logs could be from anything and everything and about anything and everything. Once they are ingested into a SIEM, they become a security log. An example of important security logs that a SOC would want to capture are network flow logs, Windows Event Logs, Unix Syslog's, and firewall logs. Security events can string together many security logs.

Security Event

Security events are the day-to-day routine security monitoring from the tooling. They are very common, and almost all security tooling notifications start as a security event generated from security logs, except for vulnerability scanners, and are escalated as needed. A security event must be escalated to a security incident before becoming a breach. When a security event is escalated to become an incident, the incident response process triggers, and an incident handler is assigned.

Incident

Security incidents are uncommon but happen more frequently than a security breach. An incident is declared, and the incident response process starts if there is suspected loss of sensitive data.

What is not an incident: security events and vulnerabilities that have not been escalated.

Security Breaches

Security breaches are rare and contain a verified loss of data containing sensitive personal information. In most cases to utter the words something is a breach; it requires the legal department and the CISO to declare a breach. As a new analyst, it is good practice to not use this term anywhere unless told otherwise. In most cases, breaches require a breach notification to clients and sometimes the public and are handled with extra sensitivity. All breaches start as incidents.