Cybersecurity Fundamentals

A Career in Cybersecurity

Job market

5 Minutes

Module overview

This module focuses on the current and growing need for cybersecurity professionals around the world. You will learn about these topics:

- The demand for cybersecurity professionals in the current job market
- Core attributes and skills that cybersecurity professionals should possess
- Primary responsibilities of common cybersecurity job roles
- Cybersecurity certifications that are available
- Resources to learn more and potential options to consider to get started in a cybersecurity career

Learning objectives

After completing this module, learners should be able to:

- Summarize the job market for cybersecurity professionals
- Identify core attributes and skills that cybersecurity professionals should possess
- Describe the primary responsibilities involved in typical cybersecurity job roles
- Discuss some of the common cybersecurity certifications available
- List resources and options to consider for those starting a cybersecurity career

Current job market

Cybersecurity is a fascinating and ever-growing field that lives at the intersection of established technologies and emerging cybersecurity threats. As a career path, it requires a variety of skills and personal characteristics, some of which you may already have. Cybersecurity professionals do not always have a traditional four-year university degree. They come from very diverse backgrounds. You may be in a position where you are just starting out in your career, transitioning jobs, or beginning a second career.

If you are considering a career in cybersecurity, it is important to know about today's job market and projections, skills you need to start out and succeed in a cybersecurity job, and some common job roles. Let's learn more about the great demand for cybersecurity professionals around the world.

If there is one trend that everyone can agree on, it is that cybersecurity is a fast-growing market with tremendous career opportunities. No matter how you crunch the numbers, there’s a huge need for cybersecurity professionals over the next decade. Here are some fast facts.

> Cybersecurity job opportunities will **grow 35%** from 2021 to 2031, much faster than the average growth rate for all occupations.
>
> **– US Bureau of Labor Statistics (https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm)**

> It's estimated that there are **4.19 million cybersecurity professionals worldwide**, which is an increase of more than 700,000 compared to 2020 data.
>
> **– 2021 (ISC)2 Cybersecurity Workforce Study (https://www.isc2.org/-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx)**

> There will be **3.5 million unfilled cybersecurity jobs** globally by 2025. Of these open positions, India is expected to have more than 1.5 million job vacancies in cybersecurity by 2025.
>
> **– Cybersecurity Ventures (https://cybersecurityventures.com/jobs/?utm_source=skillsbuild.org)**

Core attributes and skills

15 Minutes

The short supply of qualified cybersecurity professionals has led to unfilled positions and a widening work skills gap. You might be wondering what skills you need to face down security threats. If you like a challenge and solving hard problems, then this could be a great area of work for you!

Let's explore the typical personal characteristics and skills you need to succeed in cybersecurity.

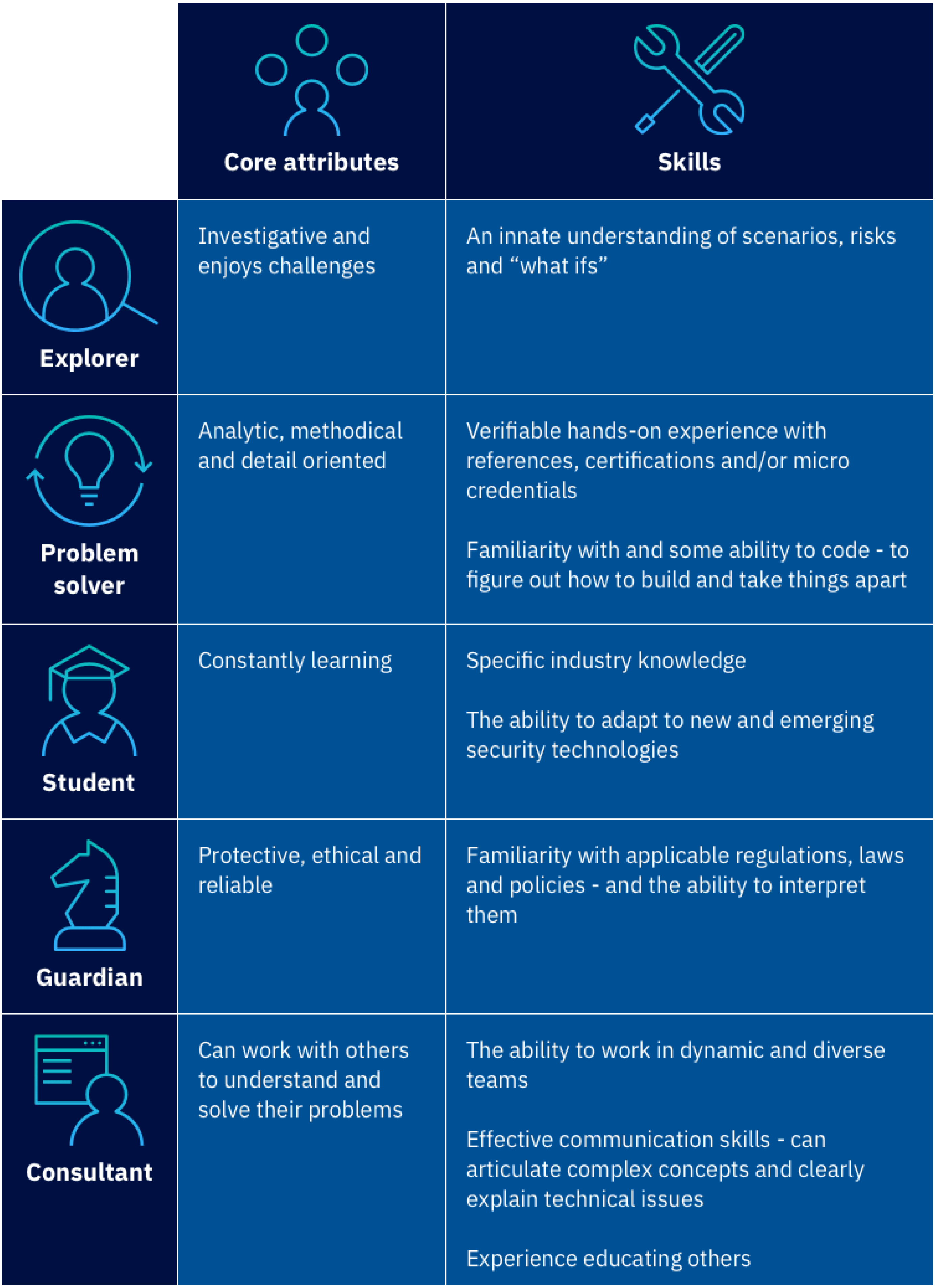
What skills should new cybersecurity professionals focus on? No matter the educational background of the professional, there are some essential elements. These elements can be classified into two groups: core attributes and skills.

- **Core attributes** can be considered a general disposition beneficial to security professionals — a set of common personality traits and learned behaviors.
- **Skills** include both technical and workplace-related abilities.

A new security professional may not have all these skills at first, but focusing on them over time will provide greater career path flexibility and the foundation for technical or business-focused leadership positions.

This table shows the core attributes and skills cybersecurity professionals should have. Does this sound like you? Take a moment to please review.

Cookie Preferences



	Core attributes	Skills
Explorer	Investigative and enjoys challenges	An innate understanding of scenarios, risks and “what ifs”
Problem solver	Analytic, methodical and detail oriented	Verifiable hands-on experience with references, certifications and/or micro credentials Familiarity with and some ability to code - to figure out how to build and take things apart
Student	Constantly learning	Specific industry knowledge The ability to adapt to new and emerging security technologies
Guardian	Protective, ethical and reliable	Familiarity with applicable regulations, laws and policies - and the ability to interpret them
Consultant	Can work with others to understand and solve their problems	The ability to work in dynamic and diverse teams Effective communication skills - can articulate complex concepts and clearly explain technical issues Experience educating others

Source: **It’s not where you start – it’s how you finish: Addressing the cybersecurity skills gap with a new collar approach (https://securityintelligence.com/events/its-not-where-you-start-its-how-you-finish-addressing-the-cybersecurity-skills-gap-with-a-new-collar-approach/)**, IBM Institute for Business Value, 2017

What do you think?

Here are some questions to think about. Please type your answer to each question in the boxes. Reflecting and typing an answer is a good way to process your thoughts. Your answers are just for you and are only saved in this course for you. Be sure to click **Save Text**.

In terms of core attributes:

- Are you an **Explorer** who is investigative in nature and enjoys challenges? Do you like that every day is different and presents new challenges, versus following routines?

- Are you a **Problem solver** who is detailed oriented and methodical in your thinking?

- Are you a **Student** who is a lifetime learner and can stay on top of the latest developments, threats, and trends in cybersecurity? Are you good at building up a network of contacts to have your own community of knowledge (e.g., colleagues, conference participants).

- Are you a **Guardian** who is protective and reliable? Do you want to uphold your reputation and that of your company so you are not the one who let the threat "get by you"?

- Are you a **Consultant** in nature who is a team player and wants to work to solve business problems?

1. Think about your **core attributes**. What core attributes do you have today and what core attributes would you want to work on developing?

From a young age i have always helped my friends to solve their problems (technical problems ie math) .I always eager to learn new technologies and love the thrill of solving problems. The core attributes i want to work on developing are being protective ,ethical and detail oriented.

Save Text

In terms of skills:

- Are you an **Explorer** who could understand scenarios, risks, and "what if's"?

- Are you a **Problem solver** who could gains skills in coding, figure out how things are built, and get some hands-on experience and/or certifications?

- Are you a **Student** who could grow your cybersecurity industry knowledge and adapt to emerging security technologies?

- Are you a **Guardian** who could become more acquainted and knowledgeable about laws and regulations to uphold?

- Are you a **Consultant** who could effectively communicate complex, technical concepts and work with diverse teams?

Cookie Preferences

2. Think about your **skills**. What skills do you have today and what skills would you want to work on developing?

I have excellent communication skills and good at grasping new concepts fast. I want to work on my exploratory skills and learn about laws and regulations and how to uphold them.

Save Text

Skill areas to build

Cybersecurity professionals have a diverse set of backgrounds, some of them in the IT field and some from totally different fields. The key is to **build up** a set of relevant technical skills and workplace-related abilities that can give you the basics you need to launch into a cybersecurity role. Here are some skill areas to consider. This is not an exhaustive list, but it covers the foundational skills to think about.

Skill area	**Description**
System administration	For Linux, UNIX, and/or Windows operating systems, you need to know the basics of installing, configuring, and maintaining client and server systems. You need to understand the underlying models for user management, permissions, file systems, and command scripts.
Network administration	You need to understand protocols such as TCP/IP, FTP, and SMTP. In particular, you need to know what they mean and how they're used at a practical, hands-on level.
Customer service	You need the ability to interact with clients to help them through diagnosing and remediating security issues.
Communications	You need the ability to succinctly communicate, using verbal and written communications, technical information about security incidents and remediation of these incidents.
Aptitude for investigation	You need the curiosity and mindset for detecting and probing into unusual behavior. This can be demonstrated through experience in troubleshooting IT issues or in a totally different field such as military intelligence. The key is to demonstrate the initiative to do the requisite detective work to get to the bottom of suspicious situations.

Someone who works in cybersecurity should be inventive and able to come up with solutions quickly to stop breaches from becoming massive problems for an organization. Remember, thinking creatively is probably how the cyber attackers got in. A cybersecurity professional must be just as creative to realize how they got inside the system.

Overall, you can see having key technical skills, being a critical thinker, interacting with people, and having a "detective mindset" can help you succeed.

Cybersecurity job roles

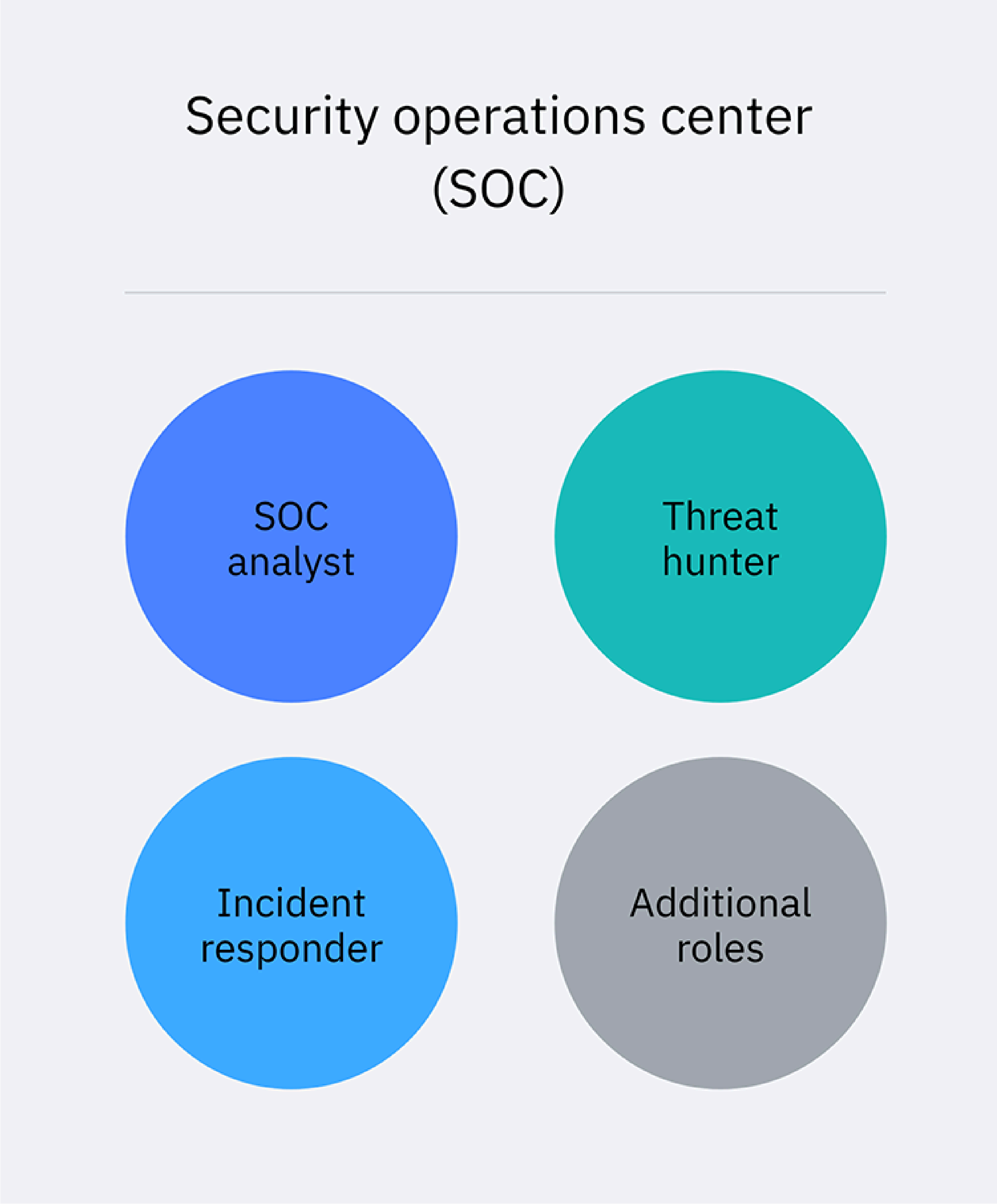
25 Minutes

Cookie Preferences

Cybersecurity professionals are on the front line of cyber crime defense to protect vital computer systems from internal and external threats such as malware, hackers, and social engineering.

All organizations have some form of information security needs. Data needs to be protected everywhere! Cybersecurity crosses all industries. Financial institutions as well as government, education, and retail sectors are some of the biggest players because of their size.

There are many different cybersecurity opportunities, and within those areas are dozens of positions requiring different skills and experience. Some roles may require travel while others are at a fixed location such as a security operations center (SOC). This centralized team monitors an organization for potential security incidents, investigates these incidents, and (if necessary) remediates such incidents. In this lesson, we will go over some of the interesting job roles in cybersecurity.



> **Note:** There are many more job roles in the field of cybersecurity. This is not a complete list. Job roles vary by company and security area, as well as by name. These are some common roles.

SOC analyst

In the company's security operations center (SOC), there is an **entry level** job role called the **SOC analyst.**

-

Cookie Preferences

It is also known as a cybersecurity analyst or triage analyst.

- This role is "reactive" in that the SOC analyst responds to individual alerts and investigates, as if being a detective, based on the evidence.
- You may see references to a SOC analyst role being a "Level 1" position. The increasing numbered levels are usually used to indicate levels of responsibility and corresponding experience requirements. You may also see reference to a "Junior" position.

What do they do on a typical day?

- **Monitor** computer network traffic to detect suspicious activity that may indicate the presence of hackers or malware such as trojans and ransomware.
- **Investigate** alerts that are triggered by a security incident and event monitoring (SIEM) tool (such as **IBM Security QRadar (https://www.ibm.com/security/security-intelligence/qradar)**) when it detects suspicious events to determine if the alert is a false positive (a false alarm) or a true positive (a real-life security incident that needs to be addressed). If a true positive alert, then this involves identifying the context, cause, and impacted user(s).
- **Evaluate** the severity of security incident and assign the appropriate risk rating to these incidents (e.g., low or high severity).
- **Escalate** high severity incidents to the incident responder.

What is an example of what a SOC analyst will do?

Let's say an alert comes in on the SIEM tool. The SOC analyst determines that it is regarding a malware infection on the computer of one of the executives in the organization. Upon investigation, the SOC analyst concludes it is a true positive. Since it is an attack that impacts an executive who has access to highly sensitive information, the SOC analyst assigns it a high severity.

What are key skills to have for this job role?

- Computer networking and systems administration skills
    - For instance, how does the connection flow through an IP address, and flow through a network, router, and devices associated with networking? How to administer a Windows server and Linux server? What is a database server? How to look at and understand system logs of all events and transactions for a device, router, firewall, and so on?

Note: This role does not require skills in computer programming. Coding is not a requirement for this role.

Incident responder

Next, also in the SOC, is a **mid level** job role called the **incident responder**.

- It is also known as incident response analyst.
- This role determines if a reported alert is an organizational attack or a persistent threat on a company's network and ensures it is remediated.

What do they do on a typical day?
• **Scope** the extent of a cybersecurity incident. For example, if malware is detected on one person's workstation computer in a human resources department, then has it spread to any other computers in that department? Has it spread to other parts of the company? Has its malicious behavior been contained by automated defenses (such as anti-virus software and firewalls) or has it compromised company assets? • **Plan remediation** based on the scope of the cybersecurity incident. This involves researching the nature of the incident (e.g., what type of malicious behavior is targeted by malware) and determining how best to respond to it. • **Implement remediation** with appropriate teams such as opening IT tickets to re-image infected computers, educating end users on how to avoid clicking on phishing email attachments, or communicating the extent of a data breach to appropriate executives in a timely manner.
What is an example of what an incident responder will do?
Let's say a high severity incident of malware is reported on an executive's computer. The incident responder determines if other employees are impacted by the malware, how best to respond to it, and collaborates with others to remediate.
What are key skills to have for this job role?
• Computer networking and systems administration skills • Familiarity with the company and corporate policies (e.g., data, privacy, legal) • Remediation skills to select the right technical and non-technical corrective actions

Threat hunter

Next, also in the SOC, is another **mid level** job role called the **threat hunter.**

- It is also known as a threat analyst.
- This role is "proactive" in that the threat hunter does research to stay current about latest threats, how they have evolved, and codes rules for triggering alerts in the SIEM tool for the company.

What do they do on a typical day?
• **Proactively research** the "threat landscape" by continuously monitoring various threat resources, such as **IBM X-Force Exchange (https://exchange.xforce.ibmcloud.com/)**. • **Evaluate** which new and emerging threats are highest risk to their organization based on criteria such as the industries targeted, vulnerabilities exploited, and tactics employed by the threats. • **Respond** to these threats by: • Implementing system configuration changes.   • Programming automation in security tools to automatically detect activity that is characteristic of these threats.   • Sensitizing the organization to potential attacks.
What is an example of what a threat hunter will do?
Let's say a brand new ransomware threat has been publicized. A threat hunter will research this threat and implement automation to help prevent the threat from penetrating the organization and detect the threat if it manages to penetrate.
What are key skills to have for this job role?
• Computer networking and systems administration skills • Understanding sources of threat intelligence information and implementing automation to detect suspicious behavior **Note**: Threat hunters often have experience in other security roles such as a SOC analyst, incident responder, penetration tester, or vulnerability testing analyst.

Possible career progression

It is possible to enter the cybersecurity profession without a degree by starting in an entry-level IT position. You could then work your way up to a cybersecurity role.

In terms of career progression, there are various scenarios that could play out. For instance:

- You could start out as a systems administrator and, over time, make a lateral move into a SOC analyst role.
- You could begin as a SOC analyst and continue in that career for a long time.
- You could begin as a SOC analyst and perhaps become a SOC team lead or advance to becoming an incident responder.
- You could potentially perform a combination of the responsibilities of a SOC analyst, incident responder, and threat hunter.

- As a SOC analyst you can make a lateral move into a systems administrator or identity and access management (IAM) administrator role.

> **Note:** This depends on the maturity of the company. More mature organizations may hire for all three job roles (SOC analyst, incident responder, threat analyst). A less mature organization might have one individual dedicated to a combination of all three job roles.

Additional job roles

Here are some other roles to be familiar with.

Expand each job role to view a description.

Security consultant ✕

- An entry-level or mid-level position who is responsible for solving cybersecurity problems under the guidance of a senior consultant.
- Perform tasks that are needed throughout the life cycle of a project.
- Often hired outside of the company as a source of expertise.
- There are many specializations, such as a strategy consultant, operations consultant, and so on.

Security administrator ✕

- A mid-level position that also works in the SOC, but this role is quite different than a SOC analyst.
- Like a systems administrator, but this role works with security tools, like SIEM tools.
- Keeps the security tools maintained by applying patches and tuning them to properly perform.
- Writes scripts to automate tasks in the security systems.
- Does not investigate incidents.

Identity and access management (IAM) administrator ✕

-

Cookie Preferences

An entry-level or mid-level position that supports different groups in a company.

- Responsible for managing application/system authorities and privileges, single sign-on, reporting on applications, and working with developers to implement identity and access management capabilities for new applications.
- Must be skilled in using IAM tools and networking administration.

Penetration tester ⊗

- A more advanced position that is also called pen tester who emulates the "bad guys".
- Responsible for testing a computer system, network, or application to find security vulnerabilities that a hacker could potentially exploit.
- Often hired outside of the company to "break into" the company's system to provide a level of quality control and external assessment.

Mobile administrator ⊗

- An entry-level position that manages the security protection for employees' mobile devices.
- Need a system administrator background.

Compliance analyst ⊗

- An entry-level position in a large company that does internal auditing of whether a company is following its security policies, privacy policies, and country laws.
- Also helps organizations get ready for an external audit, which are required depending on the industry (e.g., healthcare, finance, and so on).

This is the end of the lesson. Be sure to select the "**I've checked it out**" box to take a mini quiz to check your understanding of this lesson. You will be presented with three on-the-job scenarios to then identify the correct cybersecurity job role. This is required for lesson completion.

Cookie Preferences

Understanding certifications

10 Minutes

There are a lot of cybersecurity related certifications out there and many are being developed. Staying on top of these qualifications might require studying itself!

Certifications may be product-specific or they may relate to industry concepts. Certifications exist within the industry to allow standards to be maintained with regards to skills and knowledge. Roles requiring specific qualifications tend to be more specialist. If a role requires a certain skill set, you may see certifications listed in its job posting.

Having a certification can increase the range of job roles available and be a good way to demonstrate certain levels of proficiency when applying for jobs.

Let's help make sense of some of the common certifications that are available in this field.

> **Note:** Some of the following certifications are for industry professionals with years of experience. These are qualifications you could consider working towards in the years after you get a security-related role. They are included here to highlight the progression pathway.

Expand each certification to learn key information.

CompTIA Security+ ⊗

- This is a global certification that validates the baseline skills practitioners need to perform core security functions and pursue an IT security career.
- This is the best certification for entry level cybersecurity job roles.
- CompTIA Security+ certification is targeted at these job roles: systems administrator, network administrator, security administrator, junior IT auditor or penetration tester, security specialist, security consultant, and security engineer.
- Recommended experience is to have CompTIA Network+ and two years of experience in IT administration with a security focus.

Find out more information about CompTIA Security+. (https://www.comptia.org/certifications/security) (https://www.comptia.org/certifications/security)

CompTIA Cybersecurity Analyst (CySA+) ⊗

Cookie Preferences

- This is an IT workforce certification that applies behavioral analytics to networks and devices to prevent, detect, and combat cybersecurity threats.
- CySA+ is the most up-to-date security analyst certification that covers advanced persistent threats in a post-2014 cybersecurity environment.
- CompTIA CySA+ certification is targeted at these job roles: IT security analyst, SOC analyst, vulnerability analyst, cybersecurity specialist, threat intelligence analyst, security engineer, cybersecurity analyst, and security monitoring.
- Recommended experience is to have Network+, Security+ or equivalent knowledge. Minimum of 3-4 years of hands-on information security or related experience. While there is no required prerequisite, CySA+ is intended to follow CompTIA Security+ or equivalent experience and has a technical, hands-on focus.

Find out more information about the CompTIA Cybersecurity Analyst (CySA+). (https://www.comptia.org/certifications/cybersecurity-analyst)

IT Infrastructure Library (ITIL) Certification

- ITIL is a globally accepted framework of best practice for IT Service Management (ITSM).
- The ITIL certification scheme provides a modular approach to the ITIL framework. There is a tiered structure of multiple certifications, for instance from Foundation to Master level. This offers flexibility relating to the different disciplines and areas of ITIL and the ability to focus studies on key areas of interest.
- There are entry level certifications to consider that are relevant only if a particular role requires it.

Find out more about IT Infrastructure Library (ITIL) Certification. (https://www.axelos.com/certifications/itil-service-management)

Certified Ethical Hacker (CEH)

- A Certified Ethical Hacker is a skilled professional who understands and knows how to look for weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to assess the security posture of a target system(s).
- The CEH credential certifies individuals in the specific network security discipline of Ethical Hacking from a vendor-neutral perspective.
- This trusted and respected program can benefit any cybersecurity professional.

Find out more information about the Certified Ethical Hacker (CEH). (https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/)

Cookie Preferences

Certified Information Systems Security Professional (CISSP)

- The CISSP certification validates a practitioner's skills and expertise to effectively design, implement, and manage a cybersecurity program.
- It is ideal for experienced security practitioners, managers, and executives interested in proving their knowledge across a wide array of security practices and principles, including those in the following positions: chief information security officer, director of security, security analyst, security architect, security consultant, and many more.
- **Note**: Five years of experience is required.

Find out more information about the Certified Information Systems Security Professional (CISSP). (https://www.isc2.org/Certifications/CISSP#)

Certified Information Security Manager (CISM)

- ISACA offers the CISM certification for practitioners to demonstrate their proven, multifaceted expertise and ability to understand complex, challenging security management issues for enterprises.
- Recent independent studies consistently rank CISM as one of the highest paying and sought after IT certifications.
- **Note**: Five years of experience is required.

Find out more about the Certified Information Security Manager (CISM). (https://www.isaca.org/credentialing/cism)

Security clearance

In addition to certifications, many roles within government agencies or organizations working with the public sector may require individuals to undergo a set of background checks. These vary by countries and have different levels depending on the sensitivity of the job role. If a clearance check is required, then this will typically be highlighted in the job listing.

In certain countries, if an individual already holds a previously issued clearance, then the re-application process is slightly streamlined. Or, at least the individual is more likely to pass the required checks. Due to the costs around certain checks and the reluctance or inability of individuals to get checked, there is a measurable salary premium in the marketplace for those with security clearance.

Helpful resources and getting started

10 Minutes

Hopefully you've found this course to be informative, interesting, and educational in equal measures. This can be a part of your cybersecurity journey. This lesson will provide you with inspiration for future exploration.

Helpful resources

First, here are some resources you can check out, bookmark, and keep in mind if you would like to explore more about cybersecurity and stay in touch with the latest developments in the field. This is a curated listing. There are a lot of organizations and websites out there to check out depending on your interests.

Cybersecurity organizations

- The **National Institute of Standards and Technology (NIST) (https://www.nist.gov/topics/cybersecurity)** is a unit of the U.S. Commerce Department that maintains measurement standards. It has a program to implement practical cybersecurity and privacy through outreach and effective application of standards and best practices necessary for the US to adopt cybersecurity capabilities.
- The **National Cyber Security Centre (NCSC) (https://www.ncsc.gov.uk/)** is the UK's leading authority on cybersecurity issues. The website contains a lot of advice documents and guidance for specific industries.
- The **Open Web Application Security Project (OWASP) (https://www.owasp.org/index.php/Main_Page)** is a worldwide, non-profit, charitable organization focused on improving the security of software. It provides an unbiased source of information on best practices as well as an active body advocating open standards.
- The **Information Systems Security Association (ISSA) (https://www.issa.org/)** is a non-profit organization for the information security profession. It is committed to promoting a secure digital world. Most resources from ISSA are for members. You can review the benefits of becoming a member and if there are any local chapters near you. Search if there is a local chapter near you and take a look at the chapter's website.
- **Women in Cybersecurity (WiCyS) (https://www.wicys.org/about-wicys)** is a US-based non-profit membership organization that is dedicated to bringing together women in cybersecurity from academia, research and industry to share knowledge, experience, networking, and mentoring.
- The **Forum of Incident Response and Security Teams (FIRST) (https://www.first.org/)** is a global forum and recognized global leader in incident response. FIRST provides up-to-date best practice documents, publications, and so on.

Cybersecurity publications and platforms

- **Cybersecurity Ventures (https://cybersecurityventures.com/)** is the home of **Cybercrime Magazine**. Cybersecurity Ventures is the world's leading researcher for the global cyber economy, and a trusted source for cybersecurity facts, figures, and statistics. It provides the latest cyber economic market data, insights, and ground-breaking predictions to a global audience of cybersecurity professionals.
- **Security Intelligence (https://securityintelligence.com/)** is a site that provides analysis and insights from across the cybersecurity industry. You will find the latest news, research, podcasts, and so on.

Cookie Preferences

- **SC Media (https://www.scmagazine.com/about-sc-media/)** shares industry expert guidance and insight, in-depth features and timely news, and independent product reviews in various content forms in partnership with and for top-level information security executives and their technical teams.
- **Wired Threat Level (https://www.wired.com/category/threatlevel/)** is a series of cybersecurity articles from **Wired magazine (https://www.wired.com/)**.
- The **IBM X-Force Exchange (https://exchange.xforce.ibmcloud.com/)** is a public threat intelligence platform that advises about critical alerts regarding new attacks, vulnerabilities, and campaigns. It provides a real-time geographic view of live threat activity. You can search or submit a file to scan, keep your own investigations, and see what others are sharing.

Cybersecurity blogs

- **Krebs on Security (https://krebsonsecurity.com/)** is a collection of blogs about computer security and cyber crime authored by Brian Krebs, an American journalist and investigative reporter.
- **Graham Cluley (https://www.grahamcluley.com/)** is a collection of blogs about the latest computer security news, opinion, and advice authored by Graham Cluley, a British speaker and independent analyst.
- The **Recorded Future blog (https://www.recordedfuture.com/blog/)** provides cyber threat intelligence analysis, industry perspectives, Recorded Future company updates, and more.

Getting started in the industry

What's next? What can you do to perhaps get started in the cybersecurity industry? Depending on your interest and experience, if you are considering a career in cybersecurity, then you could explore these different options.

- **Expand your knowledge!** The more you become familiar with cybersecurity, the more avenues will open up for you to explore. Try following up your interests and discover new roles and industries that you may not have considered before.

- **Continue learning!** This is the beginning of your learning experience. You can continue learning by searching online for additional cybersecurity topics and consider some of these educational resources.
  - The **Cyber Security Body Of Knowledge (Cybok) (https://www.cybok.org/)** aims to be a comprehensive body of knowledge to inform and underpin education and professional training for the cyber security sector. It acts as an excellent reference guide for security topics
  - The **SANS Institute (https://www.sans.org/)** is a cooperative research and education institution. At the heart of SANS are the many security practitioners in varied global organizations from corporations to universities working together to help the entire information security community. SANS is a trusted and large source for **information security training (https://www.sans.org/find-training/)** and **security certification (https://www.giac.org/)**.
  - The **IBM Security Learning Academy (https://www.securitylearningacademy.com/)** provides free technical training on IBM Security products. You can explore the **course catalog (https://www.securitylearningacademy.com/local/navigator/index.php)** and build your own curriculum by enrolling in courses.
    - Please note that you would need to create an IBM ID account.
  -

Cookie Preferences

The **National Institute of Standards and Technology (NIST) (https://www.nist.gov/itl/applied-cybersecurity/nice/resources/online-learning-content)** offers free and low cost online cybersecurity learning content for career and professional development.

  - And, stay tuned for more education offerings in this program!

- **Explore opportunities!** If you are seeking employment, you can start exploring the job marketplace. Check out job postings to identify common requests and qualifications. Get a sense for which jobs might appeal to you in the future, and work to meet the qualifications.

Cookie Preferences