Transferable and technical cybersecurity skills

Previously, you learned that cybersecurity analysts need to develop certain core skills to be successful at work. **Transferable skills** are skills from other areas of study or practice that can apply to different careers. **Technical skills** may apply to several professions, as well; however, they typically require knowledge of specific tools, procedures, and policies. In this reading, you'll explore both transferable skills and technical skills further.

Transferable skills

You have probably developed many transferable skills through life experiences; some of those skills will help you thrive as a cybersecurity professional. These include:

- **Communication:** As a cybersecurity analyst, you will need to communicate and collaborate with others. Understanding others' questions or concerns and communicating information clearly to individuals with technical and non-technical knowledge will help you mitigate security issues quickly.

- **Problem-solving:** One of your main tasks as a cybersecurity analyst will be to proactively identify and solve problems. You can do this by recognizing attack patterns, then determining the most efficient solution to minimize risk. Don't be afraid to take risks, and try new things. Also, understand that it's rare to find a perfect solution to a problem. You'll likely need to compromise.

- **Time management:** Having a heightened sense of urgency and prioritizing tasks appropriately is essential in the cybersecurity field. So, effective time management will

help you minimize potential damage and risk to critical assets and data. Additionally, it will be important to prioritize tasks and stay focused on the most urgent issue.

- **Growth mindset:** This is an evolving industry, so an important transferable skill is a willingness to learn. Technology moves fast, and that's a great thing! It doesn't mean you will need to learn it all, but it does mean that you'll need to continue to learn throughout your career. Fortunately, you will be able to apply much of what you learn in this program to your ongoing professional development.

- **Diverse perspectives:** The only way to go far is together. By having respect for each other and encouraging diverse perspectives and mutual respect, you'll undoubtedly find multiple and better solutions to security problems.

Technical skills

There are many technical skills that will help you be successful in the cybersecurity field. You'll learn and practice these skills as you progress through the certificate program. Some of the tools and concepts you'll need to use and be able to understand include:

- **Programming languages:** By understanding how to use programming languages, cybersecurity analysts can automate tasks that would otherwise be very time consuming. Examples of tasks that programming can be used for include searching data to identify potential threats or organizing and analyzing information to identify patterns related to security issues.

- **Security information and event management (SIEM) tools:** SIEM tools collect and analyze log data, or records of events such as unusual login behavior, and support

analysts' ability to monitor critical activities in an organization. This helps cybersecurity professionals identify and analyze potential security threats, risks, and vulnerabilities more efficiently.

- **Intrusion detection systems (IDSs):** Cybersecurity analysts use IDSs to monitor system activity and alerts for possible intrusions. It's important to become familiar with IDSs because they're a key tool that every organization uses to protect assets and data. For example, you might use an IDS to monitor networks for signs of malicious activity, like unauthorized access to a network.

- **Threat landscape knowledge:** Being aware of current trends related to threat actors, malware, or threat methodologies is vital. This knowledge allows security teams to build stronger defenses against threat actor tactics and techniques. By staying up to date on attack trends and patterns, security professionals are better able to recognize when new types of threats emerge such as a new ransomware variant.

- **Incident response:** Cybersecurity analysts need to be able to follow established policies and procedures to respond to incidents appropriately. For example, a security analyst might receive an alert about a possible malware attack, then follow the organization's outlined procedures to start the incident response process. This could involve conducting an investigation to identify the root issue and establishing ways to remediate it.

CompTIA Security+

In addition to gaining skills that will help you succeed as a cybersecurity professional, the Google Cybersecurity Certificate helps prepare you for the CompTIA Security+ exam, the industry leading certification for cybersecurity roles. You'll earn a dual credential when you complete both, which can be shared with potential employers. After completing all eight courses in the Google Cybersecurity Certificate, you will unlock a 30% discount for the CompTIA Security+ exam and

additional practice materials.

Key takeaways

Understanding the benefits of core transferable and technical skills can help prepare you to successfully enter the cybersecurity workforce. Throughout this program, you'll have multiple opportunities to develop these and other key cybersecurity analyst skills.

Revision #1
Created 30 May 2023 14:43:51 by naruzkurai
Updated 30 May 2023 21:56:57 by naruzkurai