Core Skills for cyber security Professionals

Core skills for cybersecurity professionals

In this video, we'll discuss both transferable and technical skills that are particularly useful for a security analyst.

Transferable skills are skills from other areas that can apply to different careers.

Technical skills may apply to several professions as well. However, at times they may require knowledge of specific tools, procedures, and policies.

Let's discuss some core transferable skills you may already have that will benefit you in a career as a security analyst. Communication is a transferable skill for a security analyst. They will often need to describe certain threats, risks, or vulnerabilities to people who may not have a technical background.

For example, security analysts may be tasked with interpreting and communicating policies and procedures to other employees. Or analysts may be asked to report findings to their supervisors, so the appropriate actions can be taken to secure the organization.

Another transferable skill is collaboration. Security analysts often work in teams with engineers, digital forensic investigators, and program managers. For example, if you are working to roll out a new security feature, you will likely have a project manager, an engineer, and an ethical hacker on your team. Security analysts also need to be able to analyze complex scenarios that they may encounter. For example, a security analyst may need to make recommendations about how different tools can support efficiency and safeguard an organization's internal network.

The last transferable skill that we'll discuss is problem-solving. Identifying a security problem and then diagnosing it and providing solutions is a necessary skill to keep business operations safe. Understanding threat actors and identifying trends can provide insight on how to handle future threats.

Okay, now that we've covered some important transferable skills, let's discuss some technical skills that security analysts need to develop. A basic understanding of programming languages is an important skill to develop because security analysts can use programming to automate tasks and identify error messages.

Like learning any other language, learning a programming language may seem challenging at first. However, this certificate program assumes no prior programming experience, so we'll start at the very beginning and provide several opportunities for hands-on practice with languages like Python

and SQL.

Another important technical skill is knowing how to use security information and event management, or SIEM, tools. Security professionals use SIEM tools to identify and analyze security threats, risks, and vulnerabilities. For example, a SIEM tool may alert you that an unknown user has accessed the system. In the event of an unknown user accessing the system, you may use computer forensics to investigate the incident.

Now, let's discuss computer forensics. Similar to an investigator and a forensic scientist working in the criminal justice system, digital forensic investigators will attempt to identify, analyze, and preserve criminal evidence within networks, computers, and electronic devices.

Keep in mind that you may already have some of the core skills we've discussed. And if you don't have the technical skills, that's okay! This program is designed to support you in learning those skills.

For example, over the past seven years working in cybersecurity, I've learned that security analysts need to have intellectual curiosity and the motivation to keep learning in order to succeed. Personally, I dedicate time on a regular basis towards learning more Python and SQL skills in order to meet the demands of the projects I'm working on. You'll get to learn about Python and SQL later in this program.

As you continue this journey, you'll build the knowledge and skills you need to enter the security field.

Veronica: My path to working in cybersecurity

Hi, I'm Veronica and I'm a security engineer at Google. My journey into cybersecurity has changed my life for the better in so many ways. The most important part is fulfilling work. I get to do something that I absolutely love and that I'm super interested in, and I feel very lucky that this is what I get to do for work. Before I entered my current field, I had no idea what cybersecurity was. My knowledge of cybersecurity was using secure passwords, and that was about it. So if you asked me, you know, would I be in cybersecurity five years ago? I would've said, what is that? Someone without a technical background can 100% be successful in cybersecurity. My path to my current role in cybersecurity started as an IT resident here at Google staff in Techstop. I learned a lot of analytical thinking skills, working on a help desk, troubleshooting, debugging. I didn't realize I had transferable skills until I got into my role in cybersecurity. And from there, I took it upon myself to bug a bunch of security engineers, interviewed a lot of them. I didn't get here alone. It took a village of mentors to get me here, so don't be afraid to ask for help. I don't think someone needs a college degree to go into cybersecurity. Some of the brightest minds that I get to work with don't have a college degree, so I think that's one of the best parts about the industry. Looking back at my career, I wish I would have known that I don't have to check all the boxes, that I don't have to be an expert in the area to shoot my shot, and I also wish I would've known that perfectionism can get in the way of what you want to achieve.

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.

The importance of cybersecurity

As we've discussed, security professionals protect many physical and digital assets. These skills are desired by organizations and government entities because risk needs to be managed. Let's continue to discuss why security matters.
Play video starting at ::17 and follow transcript0:17
Security is essential for ensuring an organization's business continuity and ethical standing. There are both legal implications and moral considerations to maintaining an organization's security. A data breach, for example, affects everyone that is associated with the organization. This is because data losses or leaks can affect an organization's reputation as well as the lives and reputations of their users, clients, and customers. By maintaining strong security measures, organizations can increase user trust. This may lead to financial growth and ongoing business referrals.

As previously mentioned, organizations are not the only ones that suffer during a data breach. Maintaining and securing user, customer, and vendor data is an important part of preventing incidents that may expose people's personally identifiable information.

Personally identifiable information, known as PII, is any information used to infer an individual's identity. PII includes someone's full name, date of birth, physical address, phone number, email address, internet protocol, or IP address and similar information.

Sensitive personally identifiable information, known as SPII, is a specific type of PII that falls under stricter handling guidelines and may include social security numbers, medical or financial information, and biometric data, such as facial recognition. If SPII is stolen, this has the potential to be significantly more damaging to an individual than if PII is stolen.

PII and SPII data are key assets that a threat actor will look for if an organization experiences a breach. When a person's identifiable information is compromised, leaked, or stolen, identity theft is the primary concern.

Identity theft is the act of stealing personal information to commit fraud while impersonating a victim. And the primary objective of identity theft is financial gain.

We've explored several reasons why security matters. Employers need security analysts like you to fill the current and future demand to protect data, products, and people while ensuring confidentiality, integrity, and safe access to information. This is why the U.S. Bureau of Labor Statistics expects the demand for security professionals to grow by more than 30% by the year 2030.

So keep learning, and eventually you'll be able to do your part to create a safer and more secure environment for organizations and people alike!

Wrap-up

Congratulations on completing the first section of this course! Let's quickly review what we've covered so far, before moving on.

We defined security and introduced the benefits of implementing security in an organization. Then, we discussed different job responsibilities, such as managing threats and installing prevention software. We also introduced some important core skills, like collaboration and computer forensics. We finished by discussing the value of security and how it supports critical business functions.

I hope you've gained a greater understanding of security. If you feel like you need a refresher before moving on, you can always go back and review any content you're unsure about.

By learning the basics, you are laying the foundation for the rest of your security career.

Coming up, we'll explore some well-known attacks that shaped the security industry. I'm excited to continue this journey with you!