Introduction to Cybersecurity

Introduction to cybersecurity

Imagine that you're preparing for a storm. You've received notification that a storm is coming. You prepare by gathering the tools and materials you'll need to stay safe. You make sure your windows and doors are secure. You assemble a first aid kit, tools, food and water. You're prepared. The storm hits and there are powerful winds and heavy rain. The storm is using its force to try and breach your home. You notice some water leaks and begin patching them quickly in order to minimize any risk or potential damage.

:39

Handling a security incident is no different. Organizations must prepare for the storm by ensuring they have the tools to mitigate and quickly respond to outside threats. The objective is to minimize risk and potential damage.

:56

As a security analyst, you'll work to protect your organization and the people it serves from a variety of risks and outside threats. And if a threat does get through, you and your team will provide a solution to remedy the situation.

:11

To help you better understand what this means, we'll define security and discuss the roles of security professionals in organizations.

:19

Let's start with some definitions: Cybersecurity, or security, is the practice of ensuring confidentiality, integrity, and availability of information by protecting networks, devices, people, and data from unauthorized access or criminal exploitation.

:39

For example, requiring complex passwords to access sites and services improves confidentiality by making it much more difficult for a threat actor to compromise them. A threat actor is any person or group who presents a security risk.

:57

Now that you know the definition of security, let's discuss what security teams do for an organization.

:03

Security protects against external and internal threats. An external threat is someone outside of the organization trying to gain access to private information, networks or devices.

1:16

An internal threat comes from current or former employees, external vendors, or trusted partners. Often these internal threats are accidental, such as an employee clicking on a compromised link in an email. Other times, the internal actor intentionally engages in activities such as unauthorized data access or abusing systems for personal use.

1:40

Experienced security professionals will help organizations mitigate or reduce the impact of threats like these.

1:48

Security teams also ensure an organization meets regulatory compliance, or laws and guidelines, that require the implementation of specific security standards.

1:59

Ensuring that organizations are in compliance may allow them to avoid fines and audits, while also upholding their ethical obligation to protect users.

2:09

Security teams also maintain and improve business productivity. By establishing a plan for business continuity, security teams allow people to do their jobs, even in the case of something like a data breach.

2:22

Being security conscious can also reduce expenses associated with risks, such as recovering from data loss or operational downtime, and potentially avoiding fines. The last benefit of security that we'll discuss is maintaining brand trust. If services or customer data are compromised, this can lower trust in the organization, damage the brand, and hurt the business in the long term. Loss of customer trust may also lead to less revenue for the business.

2:51

Now, let's go over some common security-based roles. After completing this certificate program, here are some job titles you may want to search for: Security analyst or specialist, Cybersecurity analyst or specialist, Security operation center or SOC analyst, Information security analyst.

3:12

You'll also learn more about the responsibilities associated with some of these job titles later in the program.

k:19

As you may now realize, the field of security includes many topics and concepts and every activity you complete in this program moves you one step closer to a new job. Let's keep learning together.

Toni: My path to cybersecurity

Hi, I'm Toni, I'm a Security Engineering Manager. Our teams protect Google and its users from serious threats. Usually government-backed attackers, coordinated influence operations and serious cybercrime threat actors. I grew up as an army brat. My dad was in the military and we moved around a lot. I've always had an interest in security sort of generally. I got really hooked on international relations when I was in high school. I did a lot of Model United Nations. And that really sort of brought these two things together for me, the way that security works in the world. I come from a big family. I knew I was going to need financial assistance to go to college. And the Department of Defense provides a lot of educational opportunities that are tied to service. So this was a natural fit for me. I knew I was interested in this area and this was going to provide a career path into something I was passionate about. I started as an intelligence analyst, but not focused on cybersecurity. I worked counterinsurgency for a number of years and geopolitical intelligence issues. Eventually, as I looked and saw that the way that cybersecurity was starting to have an impact both in our daily lives and in that world of international relations, I got more and more drawn to it. Transitioning into cybersecurity was a huge shift for me. I came in without a solid technical background, had to learn a lot of that on the job and through self-paced learning in different types of courses, I needed to learn programming languages like Python and SQL, two of the things that we cover in this certificate, I needed to learn a whole new language about the vocabulary of threats and the different components and how those manifest technically. One of the things that I had to figure out very early in this journey is what kind of learner I was. I work best with a structured learning style. So turning to a lot of these online courses and resources that took this material and structured it sort of from first principles through application resonated very well for me. A lot of this was also learned on the job by co-workers who were willing to share and invest time in helping me understand this. I asked a lot of questions and I still do. Most of cybersecurity work is going to be learned on the job in the specific environment that you're protecting. So you have to work well with your teammates in order to be able to build that knowledge base. My advice would be to stay curious and keep learning, especially focusing on your technical skills and growing those throughout your career. It's really easy to get imposter syndrome in cybersecurity because it's so broad and mastery of all these different areas is a lifetime's work. And sometimes that imposter syndrome can shut us down and make it feel like, why bother trying to keep growing. I'm never going to be able to master this instead of motivating us. So keep learning, push through that fear. The efforts always going to be rewarded.

Responsibilities of an entry-level cybersecurity analyst

Technology is rapidly changing and so are the tactics and techniques that attackers use. As digital infrastructure evolves, security professionals are expected to continually grow their skills in order to protect and secure sensitive information. In this video, we'll discuss some job responsibilities of an entry-level security analyst.

So, what do security analysts do? Security analysts are responsible for monitoring and protecting information and systems.

Now, we'll discuss three primary responsibilities of a security analyst, starting with protecting computer and network systems. Protecting computer and network systems requires an analyst to monitor an organization's internal network. If a threat is detected, then an analyst is generally the first to respond. Analysts also often take part in exercises to search for weaknesses in an organization's own systems.

For example, a security analyst may contribute to penetration testing or ethical hacking. The goal is to penetrate or hack their own organization's internal network to identify vulnerabilities and suggest ways to strengthen their security measures.

Think of it like this. After you lock your car, you check the door handles to make sure no one can access any valuables you keep inside.

Security analysts also proactively work to prevent threats from happening in the first place. One way they do this is by working with information technology, or IT, teams to install prevention software for the purposes of identifying risks and vulnerabilities.

Analysts may also be involved in software and hardware development. They'll often work with development teams to support product security by setting up appropriate processes and systems to meet the organization's data protection needs.

The last task we'll discuss is conducting periodic security audits. A security audit is a review of an organization's security records, activities, and other related documents. For example, an analyst may examine in-house security issues, such as making sure that confidential information, like individual computer passwords, isn't available to all employees.

Phew, that was a lot to cover! But hopefully you have a general idea of what entry-level security analysts do on a day-to-day basis.

Security analysts are an important part of any organization. Their daily tasks protect small businesses, large companies, nonprofit organizations, and government agencies. They also help to ensure that the people served by those organizations remain safe.

Nikki: A day in the life of a security engineer

My name is Nikki and I'm a security engineer at Google. I am part of the insider threat detection team at Google, so my role is more focused on catching insider threats or insider suspicious activity within the company. My first experience with cybersecurity was when I was interning at the aquarium. I learned a lot of network security there, they had a lot of phishing attempts, of course, you know, at the aquarium. My manager was really focused on making sure that our networks were secure and I learned a lot from him and that really sparked my interest in cybersecurity. The main reason I chose to pursue a career in cybersecurity is just how flexible the career path is. Once you're in security, there's so many different fields you can dive into. Whether it's through the blue team, protecting the user or the red team, which is just, you know, poking holes in other people's defenses and letting them know where they're going wrong. A day in the life as a entry- level security professional? Um, it can change day to day, but there's two basic parts to it. There's the operation side, which is responding to detections and doing investigations. And then there's the project side where you're working with other teams to build new detections or improve the current detections. The difference between this entry- level cybersecurity analyst and an entry-level cybersecurity engineer is pretty much that the analyst is more focused on operations and the engineer, while they can do operations, they also build the, the detections and they do more project focused work. My favorite task is probably the operations side doing investigations because we can sometimes get something like this actor did such and such on this day. And we're supposed to then dive into what they've been doing, what they've been working on to figure out if there's any suspicious activity or if it was just a false positive. One of the biggest ways I've made an impact as an entry-level cybersecurity professional is actually working on the playbooks that, um, our team uses. A playbook is a list of how to go through a certain detection, and what the analyst needs to look at in order to investigate those incidents. I was really proud of those, those playbooks that I've made so far because a lot of my teammates have even said how helpful they've been to them. If you love solving problems, if you love protecting user data, being at the front lines of a lot of headlines, then this is definitely the role for you.

Common cybersecurity terminology

As you've learned, **cybersecurity** (also known as security) is the practice of ensuring confidentiality, integrity, and availability of information by protecting networks, devices, people, and data from unauthorized access or criminal exploitation. In this reading, you'll be introduced to some key terms used in the cybersecurity profession. Then, you'll be provided with a resource that's useful for staying informed about changes to cybersecurity terminology.

Key cybersecurity terms and concepts

There are many terms and concepts that are important for security professionals to know. Being familiar with them can help you better identify the threats that can harm organizations and people alike. A security analyst or cybersecurity analyst focuses on monitoring networks for breaches. They also help develop strategies to secure an organization and research information technology (IT) security trends to remain alert and informed about potential threats. Additionally, an analyst works to prevent incidents. In order for analysts to effectively do these types of tasks, they need to develop knowledge of the following key concepts.

Compliance is the process of adhering to internal standards and external regulations and enables organizations to avoid fines and security breaches.

Security frameworks are guidelines used for building plans to help mitigate risks and threats to data and privacy.

Security controls are safeguards designed to reduce specific security risks. They are used with security frameworks to establish a strong security posture.

Security posture is an organization's ability to manage its defense of critical assets and data and react to change. A strong security posture leads to lower risk for the organization.

A **threat actor**, or malicious attacker, is any person or group who presents a security risk. This risk can relate to computers, applications, networks, and data.

An **internal threat** can be a current or former employee, an external vendor, or a trusted partner who poses a security risk. At times, an internal threat is accidental. For example, an employee who accidentally clicks on a malicious email link would be considered an accidental threat. Other times, the internal threat actor *intentionally* engages in risky activities, such as unauthorized data access.

Network security is the practice of keeping an organization's network infrastructure secure from unauthorized access. This includes data, services, systems, and devices that are stored in an organization’s network.

Cloud security is the process of ensuring that assets stored in the cloud are properly configured, or set up correctly, and access to those assets is limited to authorized users. The cloud is a network made up of a collection of servers or computers that store resources and data in remote physical locations known as data centers that can be accessed via the internet. Cloud security is a growing subfield of cybersecurity that specifically focuses on the protection of data, applications, and infrastructure in the cloud.

Programming is a process that can be used to create a specific set of instructions for a computer to execute tasks. These tasks can include:

- Automation of repetitive tasks (e.g., searching a list of malicious domains)
- Reviewing web traffic
- Alerting suspicious activity

Key takeaways

Understanding key technical terms and concepts used in the security field will help prepare you for your role as a security analyst. Knowing these terms can help you identify common threats, risks,

and vulnerabilities. To explore a variety of cybersecurity terms, visit the National Institute of Standards and Technology glossary. Or use your browser to search for high-quality, reliable cybersecurity glossaries from research institutes or governmental authorities. Glossaries are available in multiple languages.
i also have a bunch of data in this glossary search on this site

https://library.naruzkurai.tk/search?term=glossary