Coursera : Foundation of Cybersecurity Course

Module 1 :Welcome to the exciting world of Cybersecurity

Cybersecurity (or security) :
The practice of ensuring confidentiality, integrity, and availability of information by protecting networks, devices, people, and data from unauthorized access or criminal exploitation.

For example :
Requiring complex passwords to access sites and services improves confidentiality by making it much more difficult fora threat actor to compromise them.

A Threat Actor :
Any person or group who represents a security risk.

Benefits of security :

- Protects against external and internal threats :

➔ External Threats : An external threat is someone outside of the organization trying to gain access to private information, networks or devices.

➔ Internal threats : An internal threat comes from current or former employees, external vendors, or trusted partners.

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

- Meets regulatory compliance : Security team ensures an organization meets regulatory compliance, or laws and guidelines, that require the implementation of specific security standards. Ensuring that organizations are in compliance may allow them to avoid fines and audits, while also upholding their ethical obligation to protect users.

- Maintains and improves the business productivity : Security team also maintain and improve business productivity. By establishing a plan for a business continuity, security teams allow people to do their jobs, even in the case of something like a data breach.
- Reduces Expenses : Being security conscious can also reduce expenses associated with risks, such as recovering from data loss or operational downtime, and potentially avoiding fines.
- Maintains Brand Trust : If services or data of customers are compromised, this can lower trust in the organisation, damage the brand, and hurt the business in the long term. Loss of customer trust may also lead to less revenue for the business.

After completing this certificate the job roles I can search for :

- Security analyst or specialist.
- Cybersecurity analyst or specialist.
- Security Operations Centre (SOC) analyst.
- Information security analyst.

“ Most of cybersecurity work is going to be learned on the job in the specific environment that you’re protecting.”

Job Responsibilities :

1. **Entry-level security analyst :**

What do security analysts do?
> Security analysts are responsible for monitoring and protecting information systems.

<u>Three Primary Responsibilities :</u>

- Protecting networks and computer 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.

- Install Prevention software.

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.

- 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.

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?
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.

Difference between entry-level cybersecurity analyst and entry-level cybersecurity engineer.

Entry-level cybersecurity analyst	Entry-Level Cybersecurity Engineer
The analyst is more focused on operations	While they can do operations, they can also build the detections and they do more project focused work.

What do you need for job?
For any job, you need certain skills to be successful, and many of these core skills are transferable from one role to the next. No matter what job you currently have, you likely have many core skills already. Having a diverse background enhances your core skills, which means your personal experiences and perspectives are especially valuable.
Two types of important skills :

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.

Why security matters?

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.

- **Personally Identifiable Information (PII)**

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 (SPII)**

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.

What we covered until now :

- Defined security
- Job responsibilities
- Core skills
- Value of security

Terms and definitions from Course 1, Module 1 :

Cybersecurity (or security): The practice of ensuring confidentiality, integrity, and availability of information by protecting networks, devices, people, and data from unauthorized access or criminal exploitation

Cloud security: The process of ensuring that assets stored in the cloud are properly configured and access to those assets is limited to authorized users

Internal threat: A current or former employee, external vendor, or trusted partner who poses a security risk

Network security: The practice of keeping an organization's network infrastructure secure from unauthorized access

Personally identifiable information (PII): Any information used to infer an individual’s identity

Security posture: An organization’s ability to manage its defense of critical assets and data and react to change

Sensitive personally identifiable information (SPII): A specific type of PII that falls under stricter handling guidelines

Technical skills: Skills that require knowledge of specific tools, procedures, and policies

Threat: Any circumstance or event that can negatively impact assets

Threat actor: Any person or group who presents a security risk

Transferable skills: Skills from other areas that can apply to different careers