Foundations of Cybersecurity

Module 1: Foundations of Cybersecurity

Tools for the course:

- Microsoft Word: Help and learning: Microsoft Support page for Word
- Google Docs: Help Center page for Google Docs
- Microsoft Excel: Help and learning: Microsoft Support page for Excel
- Google Sheets: Help Center page for Google Sheets
- Microsoft PowerPoint: Help and learning: Microsoft Support page for PowerPoint
- How to use Google Slides: Help Center page for Google Slides
- Common problems with labs: Troubleshooting help for Labs activities

Course Overview

- Core Security Concepts
- Security Domains
- Network Security
- Computing Basics
- Assets, threats, and vulnerabilities
- Incident detection and response
- Python Security Tasks

Entry Level Jobs this course prepares for:

- Cybersecurity Analyst
- Security Analyst
- Security Operations Center (SOC) Analyst

The course list:

- Foundations of Cybersecurity — (current course) Explore the cybersecurity profession, including significant events that led to the development of the cybersecurity field and its continued importance to organizational operations. Learn about entry-level cybersecurity roles and responsibilities.
- Play It Safe: Manage Security Risks — Identify how cybersecurity professionals use frameworks and controls to protect business operations, and explore common cybersecurity tools.
- Connect and Protect: Networks and Network Security — Gain an understanding of network-level vulnerabilities and how to secure networks.
- Tools of the Trade: Linux and SQL — Explore foundational computing skills, including communicating with the Linux operating system through the command line and querying databases with SQL.
- Assets, Threats, and Vulnerabilities — Learn about the importance of security controls and developing a threat actor mindset to protect and defend an organization's assets from various threats, risks, and vulnerabilities.
- Sound the Alarm: Detection and Response — Understand the incident response lifecycle and practice using tools to detect and respond to cybersecurity incidents.
- Automate Cybersecurity Tasks with Python — Explore the Python programming language and write code to automate cybersecurity tasks.
- Put It to Work: Prepare for Cybersecurity Jobs — Learn about incident classification, escalation, and ways to communicate with stakeholders. This course closes out the program with tips on how to engage with the cybersecurity community and an introduction to AI in cybersecurity.
- Accelerate Your Job Search with AI — Gain practical job search strategies and learn how to leverage AI tools (like Gemini and NotebookLM) to uncover your most valuable skills, create a job search plan, manage your applications, and practice for interviews as you navigate your path to your next role.

Common 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

Transferable and Technical Cybersecurity 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.

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.

Module 2: The evolution of Cybersecurity

Common attacks and their effectiveness

Previously, you learned about past and present attacks that helped shape the cybersecurity industry. These included the LoveLetter attack, also called the ILOVEYOU virus, and the Morris worm. One outcome was the establishment of response teams, which are now commonly referred to as computer security incident response teams (CSIRTs). In this reading, you will learn more about common methods of attack. Becoming familiar with different attack methods, and the evolving tactics and techniques threat actors use, will help you better protect organizations and people.

Phishing

Phishing is the use of digital communications to trick people into revealing sensitive data or deploying malicious software.

Some of the most common types of phishing attacks today include:

- **Business Email Compromise (BEC)**: A threat actor sends an email message that seems to be from a known source to make a seemingly legitimate request for information, in order to obtain a financial advantage.
- **Spear phishing**: A malicious email attack that targets a specific user or group of users. The email seems to originate from a trusted source.
- **Whaling**: A form of spear phishing. Threat actors target company executives to gain access to sensitive data.
- **Vishing**: The exploitation of electronic voice communication to obtain sensitive information or to impersonate a known source.
- **Smishing**: The use of text messages to trick users, in order to obtain sensitive information or to impersonate a known source.

Malware

Malware is software designed to harm devices or networks. There are many types of malware. The primary purpose of malware is to obtain money, or in some cases, an intelligence advantage that can be used against a person, an organization, or a territory.

Some of the most common types of malware attacks today include:

- **Viruses**: Malicious code written to interfere with computer operations and cause damage to data and software. A virus needs to be initiated by a user (i.e., a threat actor), who transmits the virus via a malicious attachment or file download.
    - When someone opens the malicious attachment or download, the virus hides itself in other files in the now infected system. When the infected files are opened, it allows the virus to insert its own code to damage and/or destroy data in the system.
- **Worms**: Malware that can duplicate and spread itself across systems on its own.
    - In contrast to a virus, a worm does not need to be downloaded by a user. Instead, it self-replicates and spreads from an already infected computer to other devices on the same network.
- **Ransomware**: A malicious attack where threat actors encrypt an organization's data and demand payment to restore access.
- **Spyware**: Malware that's used to gather and sell information without consent.
    - Spyware can be used to access devices. This allows threat actors to collect personal data, such as private emails, texts, voice and image recordings, and locations.

Social Engineering

Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. Human error is usually a result of trusting someone without question. It's the mission of a threat actor, acting as a social engineer, to create an environment of false trust and lies to exploit as many people as possible.

Some of the most common types of social engineering attacks today include:

- **Social media phishing**: A threat actor collects detailed information about their target from social media sites. Then, they initiate an attack.
- **Watering hole attack**: A threat actor attacks a website frequently visited by a specific group of users.
- USB baiting: A threat actor strategically leaves a malware USB stick for an employee to find and install, to unknowingly infect a network.
- **Physical social engineering**: A threat actor impersonates an employee, customer, or vendor to obtain unauthorized access to a physical location.

Social engineering principles

Social engineering is incredibly effective. This is because people are generally trusting and conditioned to respect authority. The number of social engineering attacks is increasing with every new social media application that allows public access to people's data. Although sharing personal data—such as your location or photos—can be convenient, it's also a risk.

Reasons why social engineering attacks are effective include:

- **Authority**: Threat actors impersonate individuals with power. This is because people, in general, have been conditioned to respect and follow authority figures.
- **Intimidation**: Threat actors use bullying tactics. This includes persuading and intimidating victims into doing what they're told.
- **Consensus/Social proof**: Because people sometimes do things that they believe many others are doing, threat actors use others' trust to pretend they are legitimate.
    - For example, a threat actor might try to gain access to private data by telling an employee that other people at the company have given them access to that data in the past.
- **Scarcity**: A tactic used to imply that goods or services are in limited supply.
- **Familiarity**: Threat actors establish a fake emotional connection with users that can be exploited.
- **Trust**: Threat actors establish an emotional relationship with users that can be exploited over time. They use this relationship to develop trust and gain personal information.
- **Urgency**: A threat actor persuades others to respond quickly and without questioning.

The 8 CISSP Security Domains

- Security and Risk Management
    - Defines security goals and objectives, risk mitigation, compliance, business continuity, and the law.
- Asset Security
    - Secures digital and physical assets. It's also related to the storage, maintenance, retention, and destruction of data.
- Security Architecture and Engineering
    - Optimizes data security by ensuring effective tools, systems, and processes are in place.
- Communications and Network Security

    - Manage and secure physical networks and wireless communications.
- Identity and Access Management
    - Keeps data secure, by ensuring users follow established policies to control and manage physical assets, like office spaces, and logical assets, such as networks and applications.
- Security Assessment and Testing
    - Conducting security control testing, collecting and analyzing data, and conducting security audits to monitor for risks, threats, and vulnerabilities.
- Security Operations
    - Conducting investigations and implementing preventative measures.
- Software Development Security
    - Uses secure coding practices, which are a set of recommended guidelines that are used to create secure applications and services.

Attack types

Password attack

A password attack is an attempt to access password-secured devices, systems, networks, or data. Some forms of password attacks that you'll learn about later in the certificate program are:

- Brute force
- Rainbow table

Password attacks fall under the communication and network security domain.

Social engineering attack

Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables.

Some forms of social engineering attacks that you will continue to learn about throughout the program are:

- Phishing
- Smishing
- Vishing
- Spear phishing
- Whaling
- Social media phishing
- Business Email Compromise (BEC)
- Watering hole attack
- USB baiting
- Physical social engineering

- Social engineering attacks are related to the security and risk management domain.

Physical attack

A physical attack is a security incident that affects not only digital but also physical environments where the incident is deployed.

Some forms of physical attacks are:

- Malicious USB cable
- Malicious flash drive

- Card cloning and skimming

  Physical attacks fall under the asset security domain.

Adversarial artificial intelligence

Adversarial artificial intelligence is a technique that manipulates artificial intelligence and machine learning technology to conduct attacks more efficiently.

- Adversarial artificial intelligence falls under **both** the communication and network security and the identity and access management domains.

Supply-chain attack

A supply-chain attack targets systems, applications, hardware, and/or software to locate a vulnerability where malware can be deployed. Because every item sold undergoes a process that involves third parties, this means that the security breach can occur at any point in the supply chain. These attacks are costly because they can affect multiple organizations and the individuals who work for them.

- Supply-chain attacks can fall under several domains, including but not limited to the security and risk management, security architecture and engineering, and security operations domains.

Cryptographic attack

A cryptographic attack affects secure forms of communication between a sender and intended recipient. Some forms of cryptographic attacks are:

- Birthday
- Collision
- Downgrade

- Cryptographic attacks fall under the communication and network security domain.

Threat actor types

Advanced persistent threats

Advanced persistent threats (**APTs**) have significant expertise accessing an organization's network without authorization. APTs tend to research their targets (e.g., large corporations or government entities) in advance and can remain undetected for an extended period of time. Their intentions and motivations can include:

- Damaging critical infrastructure, such as the power grid and natural resources
- Gaining access to intellectual property, such as trade secrets or patents

Insider threats

Insider threats abuse their authorized access to obtain data that may harm an organization. Their intentions and motivations can include:

- Sabotage
- Corruption
- Espionage
- Unauthorized data access or leaks

Hacktivists

Hacktivists are threat actors that are driven by a political agenda. They abuse digital technology to accomplish their goals, which may include:

- Demonstrations
- Propaganda
- Social change campaigns
- Fame

Hacker Types

A hacker is any person who uses computers to gain access to computer systems, networks, or data. They can be beginner or advanced technology professionals who use their skills for a variety of reasons.

There are three main categories of hackers:

- Authorized hackers are also called **ethical hackers**. They follow a code of ethics and adhere to the law to conduct organizational risk evaluations. They are motivated to safeguard people and organizations from malicious threat actors.
- Semi-authorized hackers are considered **researchers**. They search for vulnerabilities but don't take advantage of the vulnerabilities they find.
- Unauthorized hackers are also called **unethical hackers**. They are malicious threat actors who do not follow or respect the law. Their goal is to collect and sell confidential data for financial gain.

- Note: There are multiple hacker types that fall into one or more of these three categories.

New and unskilled threat actors have various goals, including:

- To learn and enhance their hacking skills
- To seek revenge
- To exploit security weaknesses by using existing malware, programming scripts, and other tactics

Other types of hackers are not motivated by any particular agenda other than completing the job they were contracted to do. These types of hackers can be considered unethical or ethical hackers. They have been known to work on both illegal and legal tasks for pay.

There are also hackers who consider themselves vigilantes. Their main goal is to protect the world from unethical hackers.

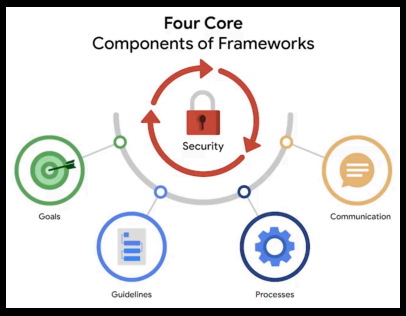
Module 3: Protect against threats, risks, and vulnerabilities

Introduction to security frameworks and controls

Security Frameworks
Guidelines used for building plans to help mitigate risk and threats to data and privacy.

GDPR - General Data Protection Regulation (European Law) grants citizens more control over their personal data.

Purpose of security Frameworks
- Protecting PII
- Securing financial information
- Identifying security weaknesses
- Managing organizational risks
- Aligning security with business goals



4 Core Components of Frameworks
1. Identifying and documenting security goals.
2. Setting guidelines to achieve security goals.
3. Implementing strong security processes.
4. Monitoring and communicating results.

Security Controls
Safeguards designed to reduce specific security risks.

Secure Design

CIA Triad (Confidentiality, Integrity, Availability**)**
A foundation model that helps inform how organizations consider risk when setting up systems and security policies.

- Confidentiality
  - Only authorized users can access specific assets or data.

- Integrity
  - Data is correct, authentic, and reliable.

- Availability
  - Data is accessible to those who are authorized to access it.

Asset
An item perceived as having value to an organization.

NIST CSF (Cyber Security Framework)
A voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk.

How controls, frameworks, and compliance are related

The confidentiality, integrity, and availability (CIA) triad is a model that helps inform how organizations consider risk when setting up systems and security policies.

CIA are the three foundational principles used by cybersecurity professionals to establish appropriate controls that mitigate threats, risks, and vulnerabilities.

As you may recall, security controls are safeguards designed to reduce specific security risks. So they are used alongside frameworks to ensure that security goals and processes are implemented correctly and that organizations meet regulatory compliance requirements.

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

They have four core components:

1. Identifying and documenting security goals
2. Setting guidelines to achieve security goals
3. Implementing strong security processes
4. Monitoring and communicating results

Compliance is the process of adhering to internal standards and external regulations.

Specific controls, frameworks, and compliance

The National Institute of Standards and Technology (NIST) is a U.S.-based agency that develops multiple voluntary compliance frameworks that organizations worldwide can use to help manage risk. The more aligned an organization is with compliance, the lower the risk.

Examples of frameworks include the NIST Cybersecurity Framework (CSF) and the NIST Risk Management Framework (RMF).

Note: Specifications and guidelines can change depending on the type of organization you work for.

In addition to the NIST CSF and NIST RMF, there are several other controls, frameworks, and compliance standards that are important for security professionals to be familiar with to help keep organizations and the people they serve safe.

The Federal Energy Regulatory Commission - North American Electric Reliability Corporation (**FERC-NERC**)

FERC-NERC is a regulation that applies to organizations that work with electricity or that are involved with the U.S. and North American power grid.

- These types of organizations have an obligation to prepare for, mitigate, and report any potential security incident that can negatively affect the power grid.
- They are also legally required to adhere to the Critical Infrastructure Protection (CIP) Reliability Standards defined by the FERC.

The Federal Risk and Authorization Management Program (FedRAMP®)

FedRAMP is a U.S. federal government program that standardizes security assessment, authorization, monitoring, and handling of cloud services and product offerings.

- Its purpose is to provide consistency across the government sector and third-party cloud providers.

Center for Internet Security (CIS®)

CIS is a nonprofit with multiple areas of emphasis. It provides a set of controls that can be used to safeguard systems and networks against attacks.

- Its purpose is to help organizations establish a better plan of defense.
- CIS also provides actionable controls that security professionals may follow if a security incident occurs.

General Data Protection Regulation (GDPR)

GDPR is a European Union (E.U.) general data regulation that protects the processing of E.U. residents' data and their right to privacy in and out of E.U. territory.

- For example, if an organization is not being transparent about the data they are holding about an E.U. citizen and why they are holding that data, this is an infringement that can result in a fine to the organization.
- Additionally, if a breach occurs and an E.U. citizen's data is compromised, they must be informed.
- The affected organization has 72 hours to notify the E.U. citizen about the breach.

Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS is an international security standard meant to ensure that organizations storing, accepting, processing, and transmitting credit card information do so in a secure environment. The objective of this compliance standard is to reduce credit card fraud.

The Health Insurance Portability and Accountability Act (HIPAA)

HIPAA is a U.S. federal law established in 1996 to protect patients' health information. This law prohibits patient information from being shared without their consent.

It is governed by three rules:

1. Privacy
2. Security
3. Breach notification

Organizations that store patient data have a legal obligation to inform patients of a breach because if patients' Protected Health Information (PHI) is exposed, it can lead to identity theft and insurance fraud.

PHI relates to the past, present, or future physical or mental health or condition of an individual, whether it's a plan of care or payments for care.

- Along with understanding HIPAA as a law, security professionals also need to be familiar with the Health Information Trust Alliance (**HITRUST®**), which is a security framework and assurance program that helps institutions meet HIPAA compliance.

International Organization for Standardization (ISO)

ISO was created to establish international standards related to technology, manufacturing, and management across borders. It helps organizations improve their processes and procedures for staff retention, planning, waste, and services.

System and Organizations Controls (SOC type 1, SOC type 2)

The American Institute of Certified Public Accountants® (AICPA) auditing standards board developed this standard. The SOC1 and SOC2 are a series of reports that focus on an organization's user access policies at different organizational levels such as:

- Associate
- Supervisor
- Manager
- Executive
- Vendor
- Others

They are used to assess an organization's financial compliance and levels of risk. They also cover confidentiality, privacy, integrity, availability, security, and overall data safety. Control failures in these areas can lead to fraud.

Pro tip: There are a number of regulations that are frequently revised. You are encouraged to keep up-to-date with changes and explore more frameworks, controls, and compliance. Two suggestions to research: the Gramm-Leach-Bliley Act and the Sarbanes-Oxley Act.

Ethical concerns and laws related to counterattacks

United States standpoint on counterattacks

In the U.S., deploying a counterattack on a threat actor is illegal because of laws like the Computer Fraud and Abuse Act of 1986 and the Cybersecurity Information Sharing Act of 2015, among others. You can only defend. The act of counterattacking in the U.S. is perceived as an act of vigilantism. A vigilante is a person who is not a member of law enforcement who decides to stop a crime on their own. And because threat actors are criminals, counterattacks can lead to further escalation of the attack, which can cause even more damage and harm. Lastly, if the threat actor in question is a state-sponsored hacktivist, a counterattack can lead to serious international implications. A hacktivist is a person who uses hacking to achieve a political goal. The political goal may be to promote social change or civil disobedience.

For these reasons, the only individuals in the U.S. who are allowed to counterattack are approved employees of the federal government or military personnel.

International standpoint on counterattacks

The International Court of Justice (**ICJ**), which updates its guidance regularly, states that a person or group can counterattack if:

- The counterattack will only affect the party that attacked first.
- The counterattack is a direct communication asking the initial attacker to stop.
- The counterattack does not escalate the situation.
- The counterattack effects can be reversed.

Organizations typically do not counterattack because the above scenarios and parameters are hard to measure. There is a lot of uncertainty dictating what is and is not lawful, and at times negative outcomes are very difficult to control.

- Counterattack actions generally lead to a worse outcome, especially when you are not an experienced professional in the field.

To learn more about specific scenarios and ethical concerns from an international perspective, review updates provided in the Tallinn Manual online.

Ethical principles and methodologies

Because counterattacks are generally disapproved of or illegal, the security realm has created frameworks and controls—such as the confidentiality, integrity, and availability (CIA) triad and others discussed earlier in the program—to address issues of confidentiality, privacy protections, and laws. To better understand the relationship between these issues and the ethical obligations of cybersecurity professionals, review the following key concepts as they relate to using ethics to protect organizations and the people they serve.

Confidentiality means that only authorized users can access specific assets or data. Confidentiality as it relates to professional ethics means that there needs to be a high level of respect for privacy to safeguard private assets and data.

Privacy protection means safeguarding personal information from unauthorized use. Personally identifiable information (PII) and sensitive personally identifiable information (SPII) are types of personal data that can cause people harm if they are stolen. PII data is any information used to infer an individual's identity, like their name and phone number. SPII data is a specific type of PII that falls under stricter handling guidelines, including social

security numbers and credit card numbers. To effectively safeguard PII and SPII data, security professionals hold an ethical obligation to secure private information, identify security vulnerabilities, manage organizational risks, and align security with business goals.

Laws are rules that are recognized by a community and enforced by a governing entity. As a security professional, you will have an ethical obligation to protect your organization, its internal infrastructure, and the people involved with the organization.

To do this:

- You must remain unbiased and conduct your work honestly, responsibly, and with the highest respect for the law.
- Be transparent and just, and rely on evidence.
- Ensure that you are consistently invested in the work you are doing, so you can appropriately and ethically address issues that arise.
- Stay informed and strive to advance your skills, so you can contribute to the betterment of the cyber landscape.

As an example, consider the Health Insurance Portability and Accountability Act (HIPAA), which is a U.S. federal law established to protect patients' health information, also known as PHI, or protected health information. This law prohibits patient information from being shared without their consent. So, as a security professional, you might help ensure that the organization you work for adheres to both its legal and ethical obligation to inform patients of a breach if their health care data is exposed.

Module 4: Cybersecurity Tools and Programming Languages

Tools for protecting business operations

An entry-level analyst's toolkit Every organization may provide a different toolkit, depending on its security needs. As a future analyst, it's important that you are familiar with industry standard tools and can demonstrate your ability to learn how to use similar tools in a potential workplace.

Security information and event management (SIEM) tools

A SIEM tool is an application that collects and analyzes log data to monitor critical activities in an organization. A log is a record of events that occur within an organization's systems. Depending on the amount of data you're working with, it could take hours or days to filter through log data on your own. SIEM tools reduce the amount of data an analyst must review by providing alerts for specific types of threats, risks, and vulnerabilities.

SIEM tools provide a series of dashboards that visually organize data into categories, allowing users to select the data they wish to analyze. Different SIEM tools have different dashboard types that display the information you have access to.

SIEM tools also come with different hosting options, including on-premise and cloud. Organizations may choose one hosting option over another based on a security team member's expertise. For example, because a cloud-hosted version tends to be easier to set up, use, and maintain than an on-premise version, a less experienced security team may choose this option for their organization.

Network protocol analyzers (packet sniffers)

A network protocol analyzer, also known as a packet sniffer, is a tool designed to capture and analyze data traffic in a network. This means that the tool keeps a record of all the data that a computer within an organization's network encounters. Later in the program, you'll have an opportunity to practice using some common network protocol analyzer (packet sniffer) tools.

Playbooks

A playbook is a manual that provides details about any operational action, such as how to respond to a security incident. Organizations usually have multiple playbooks documenting processes and procedures for their teams to follow. Playbooks vary from one organization to the next, but they all have a similar purpose: To guide analysts through a series of steps to complete specific security-related tasks.

For example, consider the following scenario: You are working as a security analyst for an incident response firm. You are given a case involving a small medical practice that has suffered a security breach. Your job is to help with the forensic investigation and provide evidence to a cybersecurity insurance company. They will then use your investigative findings to determine whether the medical practice will receive their insurance payout.

In this scenario, playbooks would outline the specific actions you need to take to conduct the investigation. Playbooks also help ensure that you are following proper protocols and procedures. When working on a forensic case, there are two playbooks you might follow:

- The first type of playbook you might consult is called the chain of custody playbook. Chain of custody is the process of documenting evidence possession and control during an incident lifecycle. As a security analyst involved in a forensic analysis, you will work with the computer data that was breached. You and the forensic team will also need to document who, what, where, and why you have the collected evidence. wesThe evidence is your responsibility while it is in your possession. Evidence must be kept safe and tracked. Every time evidence is moved, it should be reported. This allows all parties involved to know exactly where the evidence is at all times.

- The second playbook your team might use is called the protecting and preserving evidence playbook. Protecting and preserving evidence is the process of properly working with fragile and volatile digital evidence. As a security analyst, understanding what fragile and volatile digital evidence is, along with why there is a procedure, is critical. As you follow this playbook, you will consult the order of volatility, which is a sequence outlining the order of data that must be preserved from first to last. It prioritizes volatile data, which is data that may be lost if the device in question powers off, regardless of the reason. While conducting an investigation, improper management of digital evidence can compromise and alter that evidence. When evidence is improperly managed during an investigation, it can no longer be used. For this reason, the first priority in any investigation is to properly preserve the data. You can preserve the data by making copies and conducting your investigation using those copies.

Tools and their purposes

Programming

Programming is a process that can be used to create a specific set of instructions for a computer to execute tasks. Security analysts use programming languages, such as Python, to execute automation.

- Automation is the use of technology to reduce human and manual effort in performing common and repetitive tasks.
- Automation also helps reduce the risk of human error.

Another programming language used by analysts is called Structured Query Language (**SQL**). SQL is used to create, interact with, and request information from a database.

- A database is an organized collection of information or data.
- There can be millions of data points in a database.
- A data point is a specific piece of information.

Operating systems

An operating system is the interface between computer hardware and the user. Linux®, macOS®, and Windows are operating systems. They each offer different functionality and user experiences.

Previously, you were introduced to Linux as an open-source operating system. Open source means that the code is available to the public and allows people to make contributions to improve the software.

- Linux is not a programming language; however, it does involve the use of a command line within the operating system.
- A command is an instruction telling the computer to do something.
- A command-line interface is a text-based user interface that uses commands to interact with the computer.

Web vulnerability

A web vulnerability is a unique flaw in a web application that a threat actor could exploit by using malicious code or behavior, to allow unauthorized access, data theft, and malware deployment.

To stay up-to-date on the most critical risks to web applications, review the Open Web Application Security Project (OWASP) Top 10.

Antivirus/Antimalware software

Antivirus software is a software program used to prevent, detect, and eliminate malware and viruses. It is also called anti-malware. Depending on the type of antivirus software, it can scan the memory of a device to find patterns that indicate the presence of malware.

Intrusion detection system

An intrusion detection system (IDS) is an application that monitors system activity and alerts on possible intrusions.

- The system scans and analyzes network packets, which carry small amounts of data through a network.
    - The small amount of data makes the detection process easier for an IDS to identify potential threats to sensitive data.
- Other occurrences an IDS might detect can include theft and unauthorized access.

Encryption

Encryption makes data unreadable and difficult to decode for an unauthorized user; its main goal is to ensure confidentiality of private data.

- Encryption is the process of converting data from a readable format to a cryptographically encoded format.
- Cryptographic encoding means converting plaintext into secure ciphertext.
- Plaintext is unencrypted information and secure ciphertext is the result of encryption.

Note: Encoding and encryption serve different purposes.

- Encoding uses a public conversion algorithm to enable systems that use different data representations to share information.

Penetration testing

Penetration testing, also called pen testing, is the act of participating in a simulated attack that helps identify vulnerabilities in systems, networks, websites, applications, and processes. It is a thorough risk assessment that can evaluate and identify external and internal threats as well as weaknesses.