1. 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.

- ***Security posture:***

  An organization's ability to manage its defense of critical assets and data and react to change, leading to lower risk.

- ***Network security:***

  The practice of keeping an organization's network infrastructure secure from unauthorized access.
- ***Cloud security:***

  The process of ensuring that assets stored in the cloud are properly configured and access is limited to authorized users.
- ***Security frameworks:***

  Guidelines used for building plans to help mitigate risks and threats to data and privacy.
- ***Compliance:***

  The process of adhering to internal standards and external regulations to avoid fines and security breaches.
- ***Programming:***

  The process of creating a specific set of instructions for a computer to execute tasks, including automation and alerting suspicious activity.
- ***Security controls:***

  Safeguards designed to reduce specific security risks, used with security frameworks to establish a strong security posture.

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.

- ***CompTIA Security+***

  An industry-leading certification that validates foundational cybersecurity skills and enhances job prospects.
- ***Communication***

  The ability to convey information clearly to both technical and non-technical audiences, essential for collaboration in cybersecurity.
- ***Technical skills***

  Specific skills and knowledge related to tools and procedures in cybersecurity, necessary for effective performance in the field.
- ***Transferable skills***

  Skills developed through life experiences that can be applied across various careers, crucial for success in cybersecurity.
- ***Problem-solving***

  The capacity to identify and resolve issues proactively, a key responsibility of cybersecurity analysts.

Glossary terms from module 1

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

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.**

Key takeaways

In this reading, you learned about some common attacks and their impacts. You also learned about social engineering and why it's so successful. While this is only a brief introduction to attack types, you will have many opportunities throughout the program to further develop your understanding of how to identify and defend against cybersecurity attacks.

- ***Ransomware3***

  A type of malware that encrypts an organization's data and demands payment for restoration.
- ***Phishing3***

  Phishing is the use of digital communications to trick individuals into revealing sensitive data or deploying malicious software.
- ***USB Baiting3***

  A social engineering tactic where a malware-infected USB stick is left for an employee to find and install.

- ***Malware***

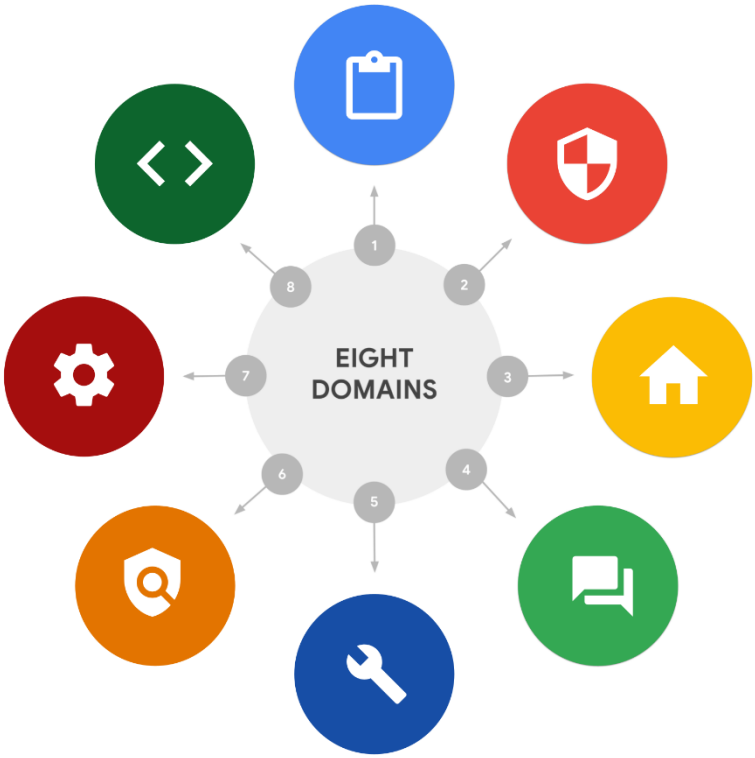
  Malware is software designed to harm devices or networks, with various types including viruses, worms, and ransomware.
- ***Social Engineering***

  Social engineering is a manipulation technique that exploits human error to gain private information or access.
- ***Business Email Compromise (BEC)***

  A phishing attack where a threat actor sends an email that appears to be from a known source to request sensitive information.

Determine the type of attack

Previously, you learned about the eight Certified Information Systems Security Professional (CISSP) security domains. The domains can help you better understand how a security analyst's job duties can be organized into categories. Additionally, the domains can help establish an understanding of how to manage risk. In this reading, you will learn about additional methods of attack. You'll also be able to recognize the types of risk these attacks present.



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 (Universal Serial Bus) 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.

Key takeaways

The eight CISSP security domains can help an organization and its security team fortify against and prepare for a data breach. Data breaches range from simple to complex and fall under one or more domains. Note that the methods of attack discussed are only a few of many. These and other types of attacks will be discussed throughout the certificate program.

Resources for more information

To view detailed information and definitions of terms covered in this reading, visit the National Institute of Standards and Technology (NIST) glossary.

Pro tip: If you cannot find a term in the NIST glossary, enter the appropriate search term (e.g., "cybersecurity birthday attack") into your preferred search engine to locate the definition in another reliable source such as a .edu or .gov site.

- ***Social Engineering Attacks***

  A manipulation technique that exploits human error to gain private information, with forms including phishing, smishing, and vishing.
- ***Password Attacks***

  An attempt to access password-secured devices, systems, networks, or data, including methods like brute force and rainbow table attacks.
- ***Adversarial Artificial Intelligence***

  A technique that manipulates AI and machine learning technologies to conduct attacks more efficiently.
- ***Supply İChain Attacks***

  Targets vulnerabilities in systems, applications, or hardware throughout the supply chain, potentially affecting multiple organizations.
- ***Cryptographic Attacks***

  Affects secure communication between a sender and recipient, including methods like birthday and collision attacks.
- ***Physical Attacks***

  A security incident affecting both digital and physical environments, such as malicious USB devices and card cloning.

Understand attackers

Previously, you were introduced to the concept of threat actors. As a reminder, a threat actor is any person or group who presents a security risk. In this reading, you'll learn about different types of threat actors. You will also learn about their motivations, intentions, and how they've influenced the security industry.

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.

Key takeaways

Threat actors are defined by their malicious intent and hackers are defined by their technical skills and motivations. Understanding their motivations and intentions will help you be better prepared to protect your organization and the people it serves from malicious attacks carried out by some of these individuals and groups.

Resources for more information

To learn more about how security teams work to keep organizations and people safe, explore the Hacking Google series of videos.

- ***Insider Threats***

  Insider threats are individuals within an organization who misuse their access to harm the organization, motivated by sabotage, espionage, or corruption.
- ***Threat Actor***

  A threat actor is any person or group who presents a security risk, influencing the security industry through their actions.
- ***Hacktivists***

  Hacktivists are motivated by political agendas, using digital means to promote social change or political causes.
- ***Advanced Persistent Threats (APTs)***

  APTs are skilled individuals or groups that infiltrate networks undetected, often targeting critical infrastructure or intellectual property.

- ***Hacker Types3***

  Hackers can be categorized as ethical, semi-authorized, or unauthorized, based on their motivations and adherence to legal standards.

Glossary terms from module 2

Terms and definitions from Course 1, Module 2

Adversarial artificial intelligence (AI): A technique that manipulates artificial intelligence (AI) and machine learning (ML) technology to conduct attacks more efficiently

Business Email Compromise (BEC): A type of phishing attack where a threat actor impersonates a known source to obtain financial advantage

CISSP: Certified Information Systems Security Professional is a globally recognized and highly sought-after information security certification, awarded by the International Information Systems Security Certification Consortium

Computer virus: Malicious code written to interfere with computer operations and cause damage to data and software

Cryptographic attack: An attack that affects secure forms of communication between a sender and intended recipient

Hacker: Any person who uses computers to gain access to computer systems, networks, or data

Malware: Software designed to harm devices or networks

Password attack: An attempt to access password secured devices, systems, networks, or data

Phishing: The use of digital communications to trick people into revealing sensitive data or deploying malicious software

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

Physical social engineering: An attack in which a threat actor impersonates an employee, customer, or vendor to obtain unauthorized access to a physical location

Social engineering: A manipulation technique that exploits human error to gain private information, access, or valuables

Social media phishing: A type of attack where a threat actor collects detailed information about their target on social media sites before initiating the attack

Spear phishing: A malicious email attack targeting a specific user or group of users, appearing to originate from a trusted source

Supply-chain attack: An attack that targets systems, applications, hardware, and/or software to locate a vulnerability where malware can be deployed

USB baiting: An attack in which a threat actor strategically leaves a malware USB stick for an employee to find and install to unknowingly infect a network

Virus: refer to "computer virus"

Vishing: The exploitation of electronic voice communication to obtain sensitive information or to impersonate a known source

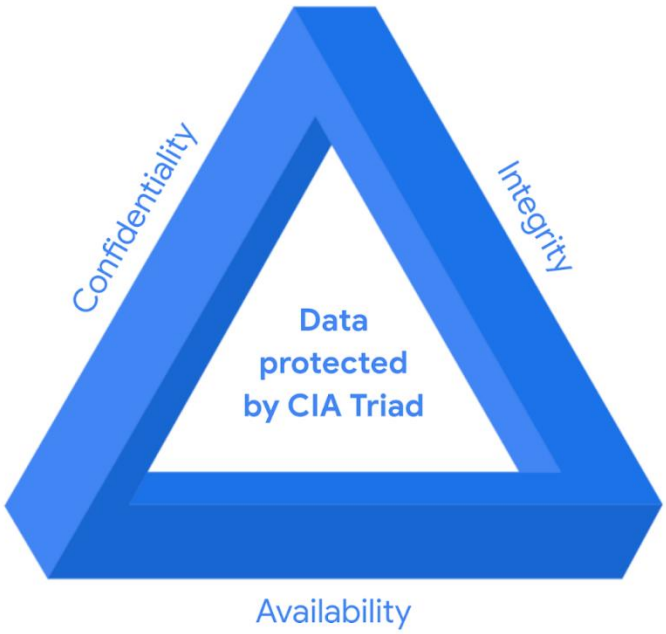
Watering hole attack: A type of attack when a threat actor compromises a website frequently visited by a specific group of users

Controls, frameworks, and compliance

Previously, you were introduced to security frameworks and how they provide a structured approach to implementing a security lifecycle. As a reminder, a security lifecycle is a constantly evolving set of policies and standards. In this reading, you will learn more about how security frameworks, controls, and compliance regulations—or laws—are used together to manage security and make sure everyone does their part to minimize 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.

Key takeaways

In this reading you learned more about controls, frameworks, and compliance. You also learned how they work together to help organizations maintain a low level of risk.

As a security analyst, it's important to stay up-to-date on common frameworks, controls, and compliance regulations and be aware of changes to the cybersecurity landscape to help ensure the safety of both organizations and people.

- ***HIPAA[3]***

  The Health Insurance Portability and Accountability Act is a U.S. federal law that protects patients' health information and mandates specific compliance requirements for organizations handling such data.
- ***CIA Triad[3]***

  The CIA triad consists of confidentiality, integrity, and availability, which are foundational principles used to inform risk management in cybersecurity.
- ***Security Controls[3]***

  Security controls are safeguards designed to reduce specific security risks, ensuring that security goals and processes are effectively implemented.
- ***Security Frameworks[3]***

  Security frameworks are guidelines that help organizations build plans to mitigate risks and threats to data and privacy, consisting of identifying goals, setting guidelines, implementing processes, and monitoring results.
- ***Compliance[3]***

  Compliance refers to the process of adhering to internal standards and external regulations, which is crucial for managing security risks.
- ***NIST Cybersecurity Framework[3]***

  The NIST Cybersecurity Framework is a voluntary compliance framework developed by the National Institute of Standards and Technology to help organizations manage risk effectively.
- ***GDPR[3]***

  The General Data Protection Regulation is a European Union regulation that protects the data and privacy rights of E.U. residents, imposing strict requirements on organizations handling such data.

Ethical concepts that guide cybersecurity decisions

Previously, you were introduced to the concept of security ethics. Security ethics are guidelines for making appropriate decisions as a security professional. Being ethical requires that security professionals remain unbiased and maintain the security and confidentiality of private data. Having a strong sense of ethics can help you navigate your decisions as a cybersecurity professional so you're able to mitigate threats posed by threat actors' constantly evolving tactics and techniques. In this reading, you'll learn about more ethical concepts that are essential to know so you can make

appropriate decisions about how to legally and ethically respond to attacks in a way that protects organizations and people alike.

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.

Key takeaways

As a future security professional, ethics will play a large role in your daily work. Understanding ethics and laws will help you make the correct choices if and when you encounter a security threat or an incident that results in a breach.

- ***Counterattacks[3]***

  Actions taken against threat actors, which are illegal in the U.S. and can lead to serious consequences, including escalation of attacks.
- ***Privacy Protection[3]***

  The safeguarding of personal information from unauthorized use, particularly concerning PII and SPII data.
- ***Security Ethics[3]***

  Guidelines for making appropriate decisions as a security professional, emphasizing the importance of remaining unbiased and maintaining confidentiality.
- ***Confidentiality[3]***

  The principle that only authorized users can access specific assets or data, requiring respect for privacy to safeguard private information.
- ***Laws[3]***

  Rules recognized by a community and enforced by a governing entity, which security professionals must adhere to in their practice.

Glossary terms from module 3

Terms and definitions from Course 1, Module 3

Asset: An item perceived as having value to an organization

Availability: The idea that data is accessible to those who are authorized to access it

Compliance: The process of adhering to internal standards and external regulations

Confidentiality: The idea that only authorized users can access specific assets or data

Confidentiality, integrity, availability (CIA) triad: A model that helps inform how organizations consider risk when setting up systems and security policies

Hacktivist: A person who uses hacking to achieve a political goal

Health Insurance Portability and Accountability Act (HIPAA): A U.S. federal law established to protect patients' health information

Integrity: The idea that the data is correct, authentic, and reliable

National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF): A voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk

Privacy protection: The act of safeguarding personal information from unauthorized use

Protected health information (PHI): Information that relates to the past, present, or future physical or mental health or condition of an individual

Security architecture: A type of security design composed of multiple components, such as tools and processes, that are used to protect an organization from risks and external threats

Security controls: Safeguards designed to reduce specific security risks

Security ethics: Guidelines for making appropriate decisions as a security professional

Security frameworks: Guidelines used for building plans to help mitigate risk and threats to data and privacy

Security governance: Practices that help support, define, and direct security efforts of an organization

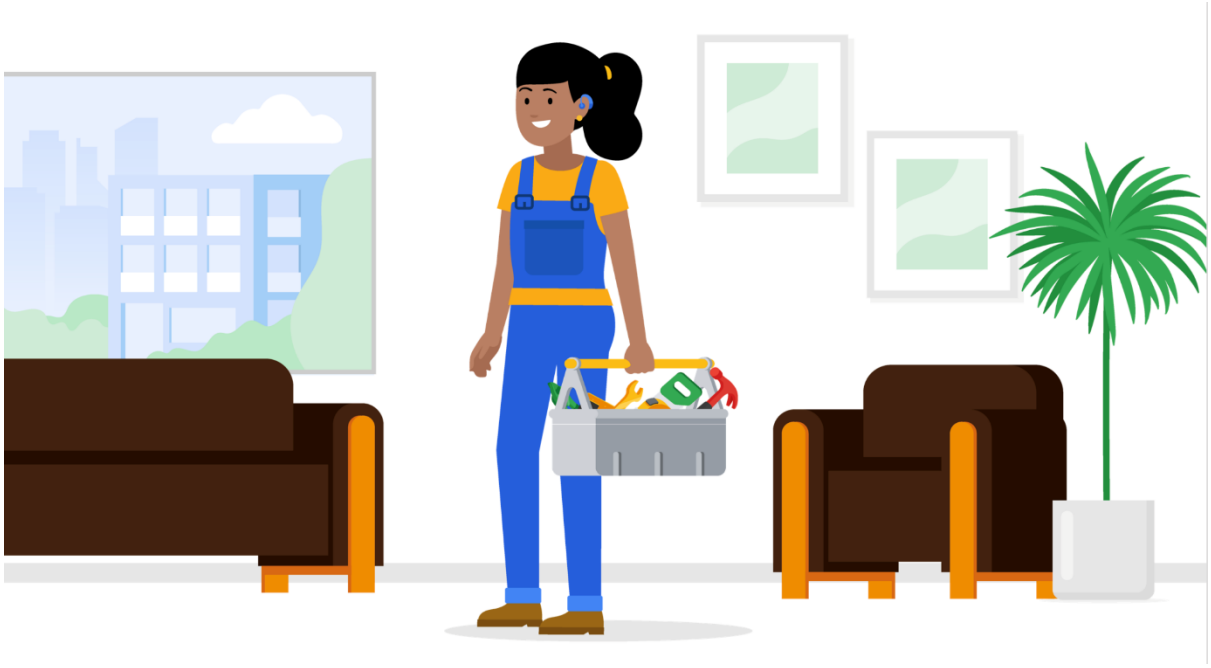
Sensitive personally identifiable information (SPII): A specific type of PII that falls under stricter handling guidelines

Tools for protecting business operations

Previously, you were introduced to several technical skills that security analysts need to develop. You were also introduced to some tools entry-level security analysts may have in their toolkit. In this reading, you'll learn more about how technical skills and tools help security analysts mitigate risks.

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. The 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.**

Key takeaways

In this reading, you learned about a few tools a security analyst may have in their toolkit, depending on where they work. You also explored two important types of playbooks: chain of custody and protecting and preserving evidence. However, these are only two procedures that occur at the beginning of a forensic investigation. If forensic investigations interest you, you are encouraged to further explore this career path or security practice. In the process, you may learn about forensic tools that you want to add to your toolkit. While all of the forensic components that make

up an investigation will not be covered in this certificate program, some forensic concepts will be discussed in later courses.

Resources for more information

The Google Cybersecurity Action Team's Threat Horizon Report provides strategic intelligence for dealing with threats to cloud enterprise.

The Cybersecurity & Infrastructure Security Agency (CISA) has a list of Free Cybersecurity Services and Tools. Review the list to learn more about open-source cybersecurity tools.

- ***SIEM Tools[3]***

  SIEM tools collect and analyze log data to monitor critical activities, providing alerts for specific threats and vulnerabilities.
- ***Protecting and Preserving Evidence[3]***

  This involves proper management of digital evidence to prevent alteration or loss, prioritizing volatile data during investigations.
- ***Playbooks[3]***

  Playbooks are manuals that guide analysts through operational actions, ensuring proper procedures are followed during security incidents.
- ***Chain of Custody[3]***

  This process documents evidence possession and control during an incident lifecycle, crucial for maintaining the integrity of evidence.
- ***Network Protocol Analyzers[3]***

  Also known as packet sniffers, these tools capture and analyze data traffic within a network, essential for monitoring and troubleshooting.

Use tools to protect business operations

Previously, you were introduced to programming, operating systems, and tools commonly used by cybersecurity professionals. In this reading, you'll learn more about programming and operating systems, as well as other tools that entry-level analysts use to help protect organizations and the people they serve.

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. You will learn more about Linux, including the Linux kernel and GNU, in a later course.

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 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.

Key takeaways

In this reading, you learned more about programming and operating systems. You were also introduced to several new tools and processes. Every organization selects their own set of tools. Therefore, the more tools you know, the more valuable you are to an organization. Tools help security analysts complete their tasks more efficiently and effectively.

- ***Programming3***

  Programming is the process of creating instructions for a computer to execute tasks, often using languages like Python for automation.
- ***Encryption3***

  Encryption converts readable data into a secure format to ensure confidentiality, making it unreadable to unauthorized users.
- ***Penetration Testing3***

  Penetration testing simulates attacks to identify vulnerabilities in systems and processes, serving as a thorough risk assessment.
- ***Operating Systems3***

  Operating systems like Linux, macOS, and Windows serve as the interface between computer hardware and users, each offering unique functionalities.
- ***Web Vulnerability3***

  A web vulnerability is a flaw in a web application that can be exploited by threat actors to gain unauthorized access or deploy malware.
- ***Antivirus Software3***

  Antivirus software is designed to prevent, detect, and eliminate malware and viruses, scanning for patterns indicative of threats.
- ***Intrusion Detection System ídSĝ3***

  An IDS monitors system activity and alerts on potential intrusions by analyzing network packets for signs of threats.

Create a cybersecurity portfolio

Throughout this certificate program, you will have multiple opportunities to develop a professional cybersecurity portfolio to showcase your security skills and knowledge.

In this reading, you'll learn what a portfolio is and why it's important to develop a professional cybersecurity portfolio. You'll also learn about options for creating an online or self-hosted portfolio that you can share with potential employers when you begin to look for cybersecurity jobs.

What is a portfolio, and why is it necessary?

Cybersecurity professionals use portfolios to demonstrate their security education, skills, and knowledge. Professionals typically use portfolios when they apply for jobs to show potential employers that they are passionate about their work and can do the job they are applying for. Portfolios are more in depth than a resume, which is typically a one-to-two page summary of relevant education, work experience, and accomplishments. You will have the opportunity to develop a resume, and finalize your portfolio, in the last course of this program.

Options for creating your portfolio

There are many ways to present a portfolio, including self-hosted and online options such as:

- **Documents folder**
- **Google Drive or Dropbox™**
- **Google Sites**
- **Git repository**

Option 1: Documents folder

Description: A documents folder is a folder created and saved to your computer's hard drive. You manage the folder, subfolders, documents, and images within it.

Document folders allow you to have direct access to your documentation. Ensuring that your professional documents, images, and other information are well organized can save you a lot of time when you're ready to apply for jobs. For example, you may want to create a main folder titled something like "Professional documents." Then, within your main folder, you could create subfolders with titles such as:

- **Resume**

- **Education**
- **Portfolio documents**
- **Cybersecurity tools**
- **Programming**

Setup: Document folders can be created in multiple ways, depending on the type of computer you are using. If you're unsure about how to create a folder on your device, you can search the internet for instructional videos or documents related to the type of computer you use.

Option 2: Google Drive or Dropbox

Description: Google Drive and Dropbox offer similar features that allow you to store your professional documentation on a cloud platform. Both options also have file-sharing features, so you can easily share your portfolio documents with potential employers. Any additions or changes you make to a document within that folder will be updated automatically for anyone with access to your portfolio.

Similar to a documents folder, keeping your Google Drive or Dropbox-based portfolio well organized will be helpful as you begin or progress through your career.

Setup: To learn how to upload and share files on these applications, visit the Google Drive and Dropbox websites for more information.

Option 3: Google Sites

Description: Google Sites and similar website hosting options have a variety of easy-to-use features to help you present your portfolio items, including customizable layouts, responsive webpages, embedded content capabilities, and web publishing.

Responsive webpages automatically adjust their content to fit a variety of devices and screen sizes. This is helpful because potential employers can review your content using any device and your media will display just as you intend. When you're ready, you can publish your website and receive a unique URL. You can add this link to your resume so hiring managers can easily access your work.

Setup: To learn how to create a website in Google Sites, visit the Google Sites website.

Option 4: Git repository

Description: A Git repository is a folder within a project. In this instance, the project is your portfolio, and you can use your repository to store the documents, labs, and screenshots you complete during each course of the certificate program. There are several Git repository sites you can use, including:

- **GitLab**
- **Bitbucket™**
- **GitHub**

Each Git repository allows you to showcase your skills and knowledge in a customizable space. To create an online project portfolio on any of the repositories listed, you need to use a version of Markdown.

Setup: To learn about how to create a GitHub account and use Markdown, follow the steps outlined in the document Get started with GitHub.

Portfolio projects

As previously mentioned, you will have multiple opportunities throughout the certificate program to develop items to include in your portfolio. These opportunities include:

- **Drafting a professional statement**
- **Conducting a security audit**
- **Analyzing network structure and security**
- **Using Linux commands to manage file permissions**
- **Applying filters to SQL queries**
- **Identifying vulnerabilities for a small business**
- **Documenting incidents with an incident handler's journal**
- **Importing and parsing a text file in a security-related scenario**
- **Creating or revising a resume**

Note: Do not include any private, copyrighted, or proprietary documents in your portfolio. Also, if you use one of the sites described in this reading, keep your site set to "private" until it is finalized.

Key takeaways

Now that you're aware of some options for creating and hosting a professional portfolio, you can consider these as you develop items for your portfolio throughout the certificate program. The more proactive you are about creating a polished portfolio, the higher your chances of impressing a potential employer and obtaining a new job opportunity in the cybersecurity profession.

- ***Document Folder***

  A document folder is a local storage option on a computer where professionals can organize their portfolio documents and images for easy access.
- ***Cloud Storage (Google Drive, Dropbox)***

  Cloud storage services like Google Drive and Dropbox allow users to store and share portfolio documents online, providing easy access and collaboration features.
- ***Google Sites***

  Google Sites is a website hosting platform that enables users to create customizable portfolio websites that can be shared with potential employers.
- ***Git Repository***

  A Git repository is a version-controlled space where professionals can store and showcase their portfolio projects, including code and documentation.
- ***Cybersecurity Portfolio***

  A cybersecurity portfolio is a collection of documents and projects that demonstrate a professional's education, skills, and knowledge in the field of cybersecurity.

Create a cybersecurity portfolio

Throughout this certificate program, you will have multiple opportunities to develop a professional cybersecurity portfolio to showcase your security skills and knowledge.

In this reading, you'll learn what a portfolio is and why it's important to develop a professional cybersecurity portfolio. You'll also learn about options for creating an online or self-hosted portfolio that you can share with potential employers when you begin to look for cybersecurity jobs.

What is a portfolio, and why is it necessary?

Cybersecurity professionals use portfolios to demonstrate their security education, skills, and knowledge. Professionals typically use portfolios when they apply for jobs to show potential employers that they are passionate about their work and can do the job they are applying for. Portfolios are more in depth than a resume, which is typically a one-to-two page summary of relevant education, work experience, and accomplishments. You will have the opportunity to develop a resume, and finalize your portfolio, in the last course of this program.

Options for creating your portfolio

There are many ways to present a portfolio, including self-hosted and online options such as:

- **Documents folder**
- **Google Drive or Dropbox™**
- **Google Sites**
- **Git repository**

Option 1: Documents folder

Description: A documents folder is a folder created and saved to your computer's hard drive. You manage the folder, subfolders, documents, and images within it.

Document folders allow you to have direct access to your documentation. Ensuring that your professional documents, images, and other information are well organized can save you a lot of time when you're ready to apply for jobs. For example, you may want to create a main folder titled something like "Professional documents." Then, within your main folder, you could create subfolders with titles such as:

- **Resume**

- **Education**
- **Portfolio documents**
- **Cybersecurity tools**
- **Programming**

Setup: Document folders can be created in multiple ways, depending on the type of computer you are using. If you're unsure about how to create a folder on your device, you can search the internet for instructional videos or documents related to the type of computer you use.

Option 2: Google Drive or Dropbox

Description: Google Drive and Dropbox offer similar features that allow you to store your professional documentation on a cloud platform. Both options also have file-sharing features, so you can easily share your portfolio documents with potential employers. Any additions or changes you make to a document within that folder will be updated automatically for anyone with access to your portfolio.

Similar to a documents folder, keeping your Google Drive or Dropbox-based portfolio well organized will be helpful as you begin or progress through your career.

Setup: To learn how to upload and share files on these applications, visit the Google Drive and Dropbox websites for more information.

Option 3: Google Sites

Description: Google Sites and similar website hosting options have a variety of easy-to-use features to help you present your portfolio items, including customizable layouts, responsive webpages, embedded content capabilities, and web publishing.

Responsive webpages automatically adjust their content to fit a variety of devices and screen sizes. This is helpful because potential employers can review your content using any device and your media will display just as you intend. When you're ready, you can publish your website and receive a unique URL. You can add this link to your resume so hiring managers can easily access your work.

Setup: To learn how to create a website in Google Sites, visit the Google Sites website.

Option 4: Git repository

Description: A Git repository is a folder within a project. In this instance, the project is your portfolio, and you can use your repository to store the documents, labs, and screenshots you complete during each course of the certificate program. There are several Git repository sites you can use, including:

- **GitLab**
- **Bitbucket™**
- **GitHub**

Each Git repository allows you to showcase your skills and knowledge in a customizable space. To create an online project portfolio on any of the repositories listed, you need to use a version of Markdown.

Setup: To learn about how to create a GitHub account and use Markdown, follow the steps outlined in the document Get started with GitHub.

Portfolio projects

As previously mentioned, you will have multiple opportunities throughout the certificate program to develop items to include in your portfolio. These opportunities include:

- **Drafting a professional statement**
- **Conducting a security audit**
- **Analyzing network structure and security**
- **Using Linux commands to manage file permissions**
- **Applying filters to SQL queries**
- **Identifying vulnerabilities for a small business**
- **Documenting incidents with an incident handler's journal**
- **Importing and parsing a text file in a security-related scenario**
- **Creating or revising a resume**

Note: Do not include any private, copyrighted, or proprietary documents in your portfolio. Also, if you use one of the sites described in this reading, keep your site set to "private" until it is finalized.

Key takeaways

Now that you're aware of some options for creating and hosting a professional portfolio, you can consider these as you develop items for your portfolio throughout the certificate program. The more proactive you are about creating a polished portfolio, the higher your chances of impressing a potential employer and obtaining a new job opportunity in the cybersecurity profession.

- ***Document Folder***

  A document folder is a local storage option on a computer where professionals can organize their portfolio documents and images for easy access.
- ***Cloud Storage (Google Drive, Dropbox)***

  Cloud storage services like Google Drive and Dropbox allow users to store and share portfolio documents online, providing easy access and collaboration features.
- ***Google Sites***

  Google Sites is a website hosting platform that enables users to create customizable portfolio websites that can be shared with potential employers.
- ***Git Repository***

  A Git repository is a version-controlled space where professionals can store and showcase their portfolio projects, including code and documentation.
- ***Cybersecurity Portfolio***

  A cybersecurity portfolio is a collection of documents and projects that demonstrate a professional's education, skills, and knowledge in the field of cybersecurity.

Glossary terms from module 4

Terms and definitions from Course 1, Module 4

Antivirus software: A software program used to prevent, detect, and eliminate malware and viruses

Database: An organized collection of information or data

Data point: A specific piece of information

Intrusion detection system (IDS): An application that monitors system activity and alerts on possible intrusions

Linux: An open-source operating system

Log: A record of events that occur within an organization's systems

Network protocol analyzer (packet sniffer): A tool designed to capture and analyze data traffic within a network

Order of volatility: A sequence outlining the order of data that must be preserved from first to last

Programming: A process that can be used to create a specific set of instructions for a computer to execute tasks

Protecting and preserving evidence: The process of properly working with fragile and volatile digital evidence

Security information and event management (SIEM): An application that collects and analyzes log data to monitor critical activities in an organization

SQL (Structured Query Language): A query language used to create, interact with, and request information from a database