GOOGLE CYBER SECURITY
Course 1: Foundations of Cyber Security

SKILLS: Cybersecurity, Security Information and Event Management (SIEM), Network Analysis, Security Controls, Security Management, Cyber Security Strategy, Incident Response, Data Ethics, Ethical Standards And Conduct, Cyber Attacks, Information Assurance, Cyber Risk

Module 1

Welcome to exciting world of Cyber

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

A threat actor is any person or group who presents a security risk.

What Is Cybersecurity?

- It's the practice of protecting **confidentiality**, **integrity**, and **availability** of data.
- It involves securing **networks, devices, people, and data** from threats or attacks.

Key Cybersecurity Terms:

Term	Simple Meaning
Compliance	Following laws and rules to avoid fines or security issues.
Security Frameworks	Guidelines or blueprints for building a secure environment.
Security Controls	Tools or actions (like firewalls, policies) to reduce risks.
Security Posture	How strong your overall cybersecurity is and how well you respond to threats.
Threat Actor	Anyone (person or group) trying to cause harm to systems or data.
Internal Threat	A security risk from someone inside (employee, vendor, partner) — accidental or intentional.
Network Security	Protecting an organization's internal network (devices, systems, data).
Cloud Security	Protecting data and apps stored on cloud servers (remote data centers).
Programming	Writing code to automate tasks, detect threats, or secure systems.

Key Takeaways:

- Knowing these terms helps you become a better **security analyst**.
- Helps in **detecting, preventing, and responding** to cyber threats.
- Stay updated using trusted glossaries like the **NIST glossary**.

Transferable Skills (soft skills from other areas)

Skill	Why It's Important in Cybersecurity
Communication	Explaining technical issues clearly to both tech and non-tech people
Problem-solving	Finding smart, quick solutions to threats and vulnerabilities
Time management	Prioritizing urgent tasks during security incidents
Growth mindset	Always learning — because tech and threats constantly evolve
Diverse perspectives	Respecting different viewpoints to solve problems more effectively

Technical Skills (hard skills specific to cybersecurity)

Skill	What It Helps With
Programming	Automating tasks like data searching and log analysis
SIEM tools	Collecting and analyzing logs to detect suspicious activity
IDS (Intrusion Detection)	Monitoring systems for unauthorized access or malware activity
Threat landscape knowledge	Understanding current hacker tactics and malware trends
Incident response	Following proper steps during and after a security breach

Core Cybersecurity Terms:

- **Cybersecurity (or security):**
  Protecting confidentiality, integrity, and availability of data, networks, devices, and people from unauthorized access or threats.
- **Cloud security:**
  Securing data and systems stored in cloud environments by configuring access for authorized users only.
- **Internal threat:**
  Security risk from a current/former employee, vendor, or partner—whether intentional or accidental.
- **Network security:**
  Protecting an organization's network infrastructure (devices, systems, data) from unauthorized access.
- **Personally Identifiable Information (PII):**
  Any data that can be used to identify a person (e.g., name, ID number, email).
- **Sensitive PII (SPII):**
  A more protected type of PII—like medical records or bank account numbers—that requires stricter handling.
- **Security posture:**
  How well an organization can protect itself and adapt to cybersecurity threats.

Module 2

Evolution of Cybersecurity

Love Letter Attack

What Was the Love Letter Attack?

- **Name**: ILOVEYOU virus (also called "Love Bug")
- **Date**: May 2000
- **Type**: Worm (self-replicating malware)
- **Attack Vector**: Social engineering via email
- **Subject Line**: ILOVEYOU
- **Attachment**: LOVE-LETTER-FOR-YOU.txt.vbs

How It Worked:

1. **Email bait**: Victims received an email with the subject **"ILOVEYOU"**, which intrigued many people.
2. **Deceptive file**: The attachment appeared to be a harmless text file, but was actually a **Visual Basic Script (.vbs)** containing malicious code.
3. **Execution**: When the victim opened the file, the worm:
    - Overwrote files (images, music, docs)
    - Sent copies of itself to all contacts in the victim's Microsoft Outlook address book
    - Spread rapidly around the world

Impact:

- **Over 10 million computers infected globally**
- **Estimated damage**: $5.5 to $8.7 billion
- Forced governments and corporations to shut down email systems temporarily

Key Lesson:

The ILOVEYOU virus showed how **human curiosity and trust can be exploited**, making **social engineering one of the most dangerous tools** in cyberattacks—even more than technical exploits.

Equifax Breach

he **Equifax breach** was a massive cybersecurity incident in **2017** that exposed the personal data of **147 million people**, making it one of the worst data breaches in U.S. history.

What Happened?

- **Date**: Discovered in **July 2017** (occurred between **May–July 2017**)
- **Company**: Equifax – a major U.S. credit reporting agency
- **Cause**: A **known vulnerability** in Apache Struts (CVE-2017-5638) was **not patched**
- **Exploit**: Hackers used the unpatched vulnerability to gain access to Equifax's systems

What Was Exposed?

- Names
- Social Security Numbers (SSNs)
- Birth dates
- Addresses
- Driver's license numbers
- Credit card information (for ~200,000 people)

Why It Was Serious

- Affected nearly **half the U.S. population**
- Involved **highly sensitive PII (Personally Identifiable Information)**
- Could lead to **identity theft, fraud**, and long-term personal and financial risks

Consequences

- **$700 million** settlement (with the FTC, CFPB, and states)
- Major **reputational damage** to Equifax
- Sparked global **calls for stronger data privacy laws**
- Led to increased awareness around **patch management and incident response**

Lessons Learned

- **Always patch known vulnerabilities promptly**
- **Encrypt sensitive data** and monitor systems
- Implement strong **incident response plans**
- Prioritize **transparency and communication** during a breach\

Brain Virus (1986)

- **What was it?**
  The **first PC virus**, created by two Pakistani brothers, **Basit and Amjad Farooq Alvi**.
- **How it worked:**
  It infected the **boot sector** of MS-DOS computers through floppy disks. When the computer started, the virus loaded into memory and could spread to other disks inserted into the drive.
- **Purpose:**
  The creators claimed it was not meant to harm but to **prevent software piracy** of their medical software.
- **Impact:**
  It unintentionally spread globally, showing how fast malware could propagate—even without the internet.

Morris Worm (1988)

- **What was it?**
  The **first worm** to spread extensively over the **early internet (ARPANET)**, created by **Robert Tappan Morris**, a student at Cornell.
- **How it worked:**
  It exploited **vulnerabilities in UNIX systems**, such as:
  - **Sendmail** (email service flaw)
  - **Finger daemon**
  - **Weak passwords**
- **Purpose:**
  Morris claimed it was meant to **measure the size of the internet**, not cause harm.
- **Impact:**
  It **slowed down thousands of systems**, causing major disruption. Estimated cost of damages: **$100,000 to $10 million**.
- **Aftermath:**
  - Morris was the **first person convicted under the U.S. Computer Fraud and Abuse Act**.
  - Led to the creation of the **first CSIRT (Computer Security Incident Response Team)**.

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.

Types of attacks and which CISSP security domain they relate to

Password Attacks

What it is: Trying to guess or crack passwords to gain access.
Examples:

- Brute Force
- Rainbow Table
  CISSP Domain: *Communication and Network Security*

Social Engineering Attacks

What it is: Tricking people into giving up private information.
Examples:

- Phishing, Smishing, Vishing
- Spear Phishing, Whaling
- Social Media Phishing, BEC
- Watering Hole, USB Baiting
- Physical Social Engineering
  CISSP Domain: *Security and Risk Management*

Physical Attacks

What it is: Attacks that target the physical hardware.
Examples:

- Malicious USB cable
- Malicious Flash Drive
- Card Cloning & Skimming
  CISSP Domain: *Asset Security*

Adversarial Artificial Intelligence

What it is: Misusing AI to launch smarter attacks.
CISSP Domains:

- *Communication and Network Security*
- *Identity and Access Management*

Supply-Chain Attack

What it is: Inserting malware or vulnerabilities in the supply process.
CISSP Domains:

- *Security and Risk Management*
- *Security Architecture and Engineering*
- *Security Operations*

Cryptographic Attacks

What it is: Breaking encryption or secure communications.
Examples:

- Birthday Attack
- Collision Attack
- Downgrade Attack
  CISSP Domain: *Communication and Network Security*

Threat Actor Types

1. Advanced Persistent Threats (APTs)

Highly skilled groups that secretly infiltrate networks and stay hidden for a long time.
Motivations:

- Sabotage of critical infrastructure (e.g., power grids)
- Theft of intellectual property (e.g., trade secrets, patents)

2. Insider Threats

Individuals within an organization who misuse their authorized access.
Motivations:

Sabotage

- Corruption
- Espionage
- Data leaks or unauthorized access

3. Hacktivists

Threat actors driven by political or social motives.
Motivations:

- Political protests
- Propaganda
- Campaigning for social change
- Gaining public attention

Hacker Categories

1. ***Authorized Hackers (Ethical Hackers)***

- Work legally and follow a code of ethics
- Help protect systems by finding and fixing vulnerabilities

2. ***Semi-Authorized Hackers (Researchers)***

- Explore systems and find weaknesses
- Do not exploit the vulnerabilities they discover

3. ***Unauthorized Hackers (Unethical Hackers)***

- Operate illegally
- Aim to steal and sell sensitive data for financial gain

Other Hacker Types

- **New/Unskilled Threat Actors (Script Kiddies):** Use existing tools to attack systems. Motivated by curiosity, revenge, or fun.
- **Contracted Hackers:** Work for pay. May take on both legal and illegal jobs.
- **Vigilante Hackers:** Claim to fight against unethical hackers. May act outside the law.

Key Takeaway

- **Threat actors** are defined by **intent** (harmful purpose).
- **Hackers** are defined by **technical skills** and **motivations** (ethical or unethical). Understanding both helps you better prepare and defend against cyber threats.

Module 3

Frameworks and Controls

Security frameworks

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

NIST Cybersecurity Framework

The NIST Cybersecurity Framework is a voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk.

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.

A triangle representing the CIA (confidentiality, integrity, availability) triad
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:

- Identifying and documenting security goals
- Setting guidelines to achieve security goals
- Implementing strong security processes
- 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:

- Privacy
- Security
- 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.

Key Ethical Concepts in Cybersecurity

1. ***Counterattacks Are Illegal in the U.S.***

- You **can defend**, but **you cannot legally attack back** (counterattack).
- Why? Because of laws like:
  - **Computer Fraud and Abuse Act (1986)**
  - **Cybersecurity Information Sharing Act (2015)**
- Counterattacks = Vigilantism = Illegal

*2. **Why Counterattacks Are Risky***

- May escalate the situation
- Can cause more damage
- May involve **state-sponsored** attackers (international problem)
- Only **federal employees or military** can legally respond this way

International Perspective

- The **International Court of Justice (ICJ)** allows counterattacks only if:
  - It targets only the original attacker
  - It tries to stop the attack, not escalate it
  - Effects are reversible
- But it's still risky and unclear, so **most organizations avoid it**

Ethical Principles

▪ ***Confidentiality***

- Only authorized people should access certain data.
- You must respect people's **privacy**.

▪ ***Privacy Protection***

- You're responsible for protecting personal data like:
  - **PII (name, phone number)**
  - **SPII (SSN, credit card number)**
- If mishandled, it can seriously harm individuals.

▪ ***Law***

- You must:
  - Follow the law
  - Work honestly and without bias
  - Be responsible and transparent
  - Stay updated in your skills

Example Law: HIPAA (USA)

- Protects patient health data (PHI)
- Organizations **must notify** patients if their data is leaked

Key Takeaways

- **Don't counterattack** — defend instead.
- **Protect private data** and **follow the law**.
- Ethics = honesty, fairness, responsibility.
- Stay educated and help improve the cyber world.

Glossary terms from Module 3

1. **Asset**: An item perceived as having value to an organization
2. **Availability**: The idea that data is accessible to those who are authorized to access it
3. **Compliance**: The process of adhering to internal standards and external regulations
4. **Confidentiality**: The idea that only authorized users can access specific assets or data
5. **Confidentiality, Integrity, Availability (CIA) Triad**: A model that helps inform how organizations consider risk when setting up systems and security policies
6. **Hacktivist**: A person who uses hacking to achieve a political goal
7. **Health Insurance Portability and Accountability Act (HIPAA)**: A U.S. federal law established to protect patients' health information
8. **Integrity**: The idea that the data is correct, authentic, and reliable
9. **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
10. **Privacy Protection**: The act of safeguarding personal information from unauthorized use
11. **Protected Health Information (PHI)**: Information that relates to the past, present, or future physical or mental health or condition of an individual
12. **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
13. **Security Controls**: Safeguards designed to reduce specific security risks
14. **Security Ethics**: Guidelines for making appropriate decisions as a security professional
15. **Security Frameworks**: Guidelines used for building plans to help mitigate risk and threats to data and privacy
16. **Security Governance**: Practices that help support, define, and direct security efforts of an organization
17. **Sensitive Personally Identifiable Information (SPII)**: A specific type of PII that falls under stricter handling guidelines

Module 4

Important Cybersecurity Tools

What you'll learn

- SIEM tools
- Playbooks
- Network protocol analyzers
- Linux operating system

1. Understand Logs First

- **Logs** are records of events in a system (e.g., login attempts).
- These are the **raw data** used by security tools to detect problems or attacks.

2. Use SIEM Tools

SIEM (Security Information and Event Management) tools help:

- **Collect**, **analyze**, and **monitor** log data in **real-time**.
- Reduce manual work by **alerting** you only when something unusual happens.

Common SIEM tools:

- **Splunk Enterprise** – self-hosted tool to search & analyze logs.
- **Google Chronicle** – cloud-native SIEM for fast access and updates.

3. Work With Playbooks

- A **playbook** is a written guide that tells you exactly what steps to take in response to an incident.
- Examples: How to react to a phishing attack or handle access reviews.

Two important types of playbooks:

a. Chain of Custody

- Track who had the evidence, when, where, and why.
- Ensures **accountability** and **integrity** of evidence.

b. Protecting and Preserving Evidence

- Prioritize **volatile data** (temporary data that disappears if power goes off).
- Make **copies** and use those for analysis to protect original evidence.

4. Use Network Protocol Analyzers (Packet Sniffers)

- Tools that **capture and analyze** network traffic.
- Examples:
  - **Wireshark**
  - **tcpdump**

These help you **see data packets** moving through the network and detect suspicious activity.

5. Build Skills Over Time

- You **don't need to be an expert** right away.
- As you continue learning, you'll **practice with these tools** and understand how to:
  - Spot threats
  - Investigate incidents
  - Reduce risks

Tools Beyond SIEM and Playbooks:

Security analysts **also use programming languages and operating systems** to manage and automate security tasks.

1. Linux (Operating System)

- **Open-source** operating system.
- Uses **command-line interface (CLI)** instead of a graphical one.
- Not a programming language, but allows direct system interaction through **commands**.
- Common Use: Reviewing **logs**, especially for errors or suspicious network traffic.

2. SQL (Structured Query Language)

- Used to **create, manage, and query databases**.
- Helps analysts **filter massive amounts of data** to retrieve specific details, such as login attempts or user actions.

3. Python (Programming Language)

- Used to **automate repetitive tasks**.
- Useful for **data parsing**, **log analysis**, **scripting tools**, and **performing investigations** with speed and accuracy.

Tools & Concepts for Cybersecurity Analysts

Programming

- **Python**: Automates repetitive tasks (e.g., log analysis, scanning).
- **SQL**: Helps retrieve specific information from large databases (e.g., user login history).

Operating Systems

- **Linux**: Open-source OS commonly used by analysts.
  - Uses **command-line interface (CLI)** for tasks like checking logs.
- **macOS® & Windows®**: Also used, but Linux is preferred for many security tasks.

Web Vulnerabilities

- Weak points in web apps that can be exploited (e.g., XSS, SQLi).
- To stay current, check the **OWASP Top 10** list of most critical web application security risks.

Antivirus Software

- Detects and removes malware.
- Can scan memory to find patterns indicating infection.

Intrusion Detection System (IDS)

- Monitors network traffic for suspicious behavior.
- Alerts when a threat (like unauthorized access) is detected.

Encryption

- Protects confidentiality by converting **plaintext → ciphertext**.
- Ensures data can't be read by unauthorized users.

Penetration Testing (Pen Testing)

- Simulated cyberattack to find security holes.
- Helps assess both **internal and external** threats.

Cybersecurity portfolio

Step 1: Understand What a Portfolio Is

- A **cybersecurity portfolio** is a **collection of your work, skills, and knowledge**.
- It goes **beyond a resume** by showing what you can actually do—like hands-on labs, tools used, and case studies.
- You'll build it **throughout your certificate program**.

Step 2: Choose How You Want to Host Your Portfolio

You can pick one of the following 4 options:

Option 1: Documents Folder (Offline)

- Create a folder on your computer called **"Professional Documents."**
- Add subfolders like:
  - Resume
  - Cybersecurity Tools
  - Programming
  - Portfolio Projects
  - Education
- Easy to organize, but not instantly shareable online.

Option 2: Google Drive or Dropbox (Cloud Storage)

- Upload and organize your documents in folders like above.
- You can share **specific files/folders** with employers.
- Automatically updates any edits.
- Make sure file permissions are set to **"View only"** when sharing.

Option 3: Google Sites (Online Website Portfolio)

- Create a **simple website** to showcase your work visually.
- Add text, images, and embedded documents.
- Create sections like:
  - About Me
  - Resume
  - Projects
  - Certifications
  - Contact
- **Publish your site** and add the link to your resume.
- Keep it private until it's ready.

Option 4: GitHub / GitLab / Bitbucket (Git Repository)

- Create a **GitHub repo** named something like cybersecurity-portfolio.
- Add folders for:
  - Projects
  - Labs
  - Reports
  - Screenshots
- Use **Markdown** to make your portfolio readable and organized.
- Use version control to track your progress over time.

Step 3: Add These Projects to Your Portfolio

As you move through the program, include:

- A **professional statement** about your goals
- A **security audit report**
- A **network security analysis**
- **Linux commands** for managing permissions
- **SQL filters** in queries
- A **vulnerability assessment** for a small business
- An **incident handler's journal**
- A script or log parsing activity
- Your **updated resume**

Step 4: Follow Best Practices

- Don't include any **private**, **confidential**, or **copyrighted** content.
- Keep your site or repository **private until it's complete**.
- Be **organized** and **professional**—this is your proof of skills!

Glossary terms from Module 4

1. **Antivirus software**: A software program used to prevent, detect, and eliminate malware and viruses
2. **Database**: An organized collection of information or data
3. **Data point**: A specific piece of information
4. **Intrusion detection system (IDS)**: An application that monitors system activity and alerts on possible intrusions
5. **Linux**: An open-source operating system
6. **Log**: A record of events that occur within an organization's systems
7. **Network protocol analyzer (packet sniffer)**: A tool designed to capture and analyze data traffic within a network
8. **Order of volatility**: A sequence outlining the order of data that must be preserved from first to last
9. **Programming**: A process that can be used to create a specific set of instructions for a computer to execute tasks
10. **Protecting and preserving evidence**: The process of properly working with fragile and volatile digital evidence
11. **Security information and event management (SIEM)**: An application that collects and analyzes log data to monitor critical activities in an organization
12. **SQL (Structured Query Language)**: A query language used to create, interact with, and request information from a database