Cybersecurity & Networking Basics: Foundations

Day 1: Cybersecurity Foundations

Module Overview

- Introduction to Cybersecurity
- Types of Cyber Attacks
- The CIA Triad

What is Cybersecurity?

- Protection of systems, networks, and data
  - Defense against unauthorized access and damage
  - Core pillar of modern digital society

Why Cybersecurity Matters

Financial Losses

Breaches lead to direct costs from recovery, legal fees, and regulatory fines, plus indirect costs from lost business and reputational damage.

Reputational Damage

Loss of customer trust and public perception can take years to rebuild, severely impacting future growth and market position.

Data Privacy Violations

Compromised personal data can result in identity theft, fraud, and severe legal repercussions under data protection laws like GDPR and CCPA.

Operational Disruptions

Cyber attacks can halt business operations, crippling essential services and leading to significant downtime and economic impact.

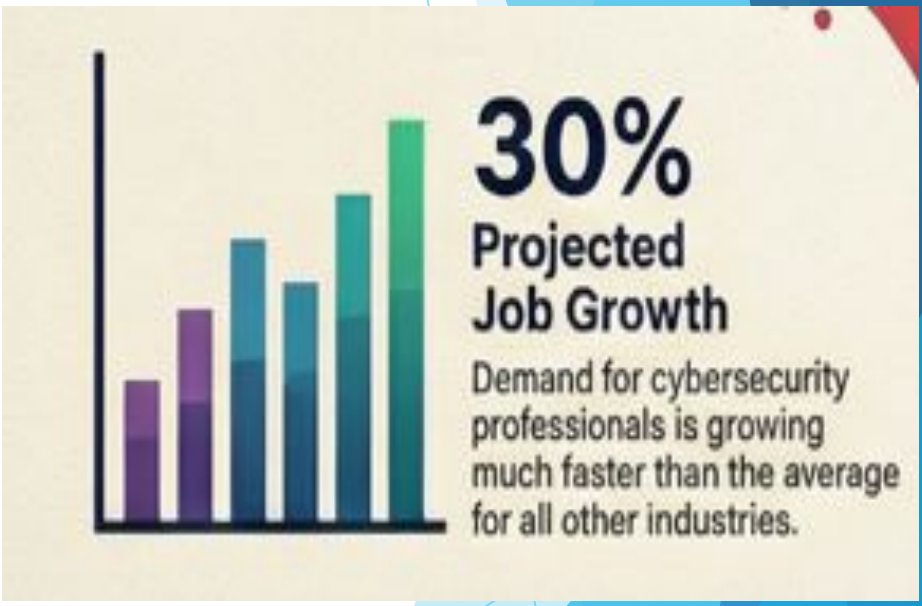
Economic Impact of Cybercrime

Famous Real-World Cybersecurity Incidents

Incident	Year	Country	What Happened	Attack Type	Impact	Reference
Equifax Data Breach	2017	USA	Hackers exploited unpatched web vulnerability to access sensitive consumer data	Data Breach	~147 million people affected; personal info (SSN, birth dates, addresses) stolen	https://en.wikipedia.org/wiki/2017_Equifax_data_breach?utm_source=chatgpt.com
WannaCry Ransomware	2017	UK	Ransomware spread using Windows vulnerability; NHS hospitals forced to shut down operations	Ransomware	~200,000 computers infected globally; hospitals disrupted	https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs/
SolarWinds Supply Chain Attack	2020	USA	Hackers inserted malicious code into trusted SolarWinds software updates; compromised government & private networks	Supply Chain Attack	Thousands of organizations affected; espionage & sensitive data access	https://en.wikipedia.org/wiki/SolarWinds

Cybersecurity Careers

- The U.S. Bureau of Labor Statistics predicts a growth rate of over 30% for cybersecurity jobs by 2030.
- Example: Microsoft and other tech companies rely heavily on cybersecurity experts to secure sensitive data.
- Skills required: Beyond technical expertise, professionals also need strong communication and collaboration abilities.



Navigating Your Career in Cybersecurity: A Beginner's Roadmap

30% Projected Industry Growth

The U.S. Bureau of Labor Statistics expects security roles to grow significantly by 2030.

Diverse Backgrounds are an Asset

Skills like critical thinking, communication, and curiosity are more valuable than prior technical experience.

The 8 Security Domains

CIA Triad

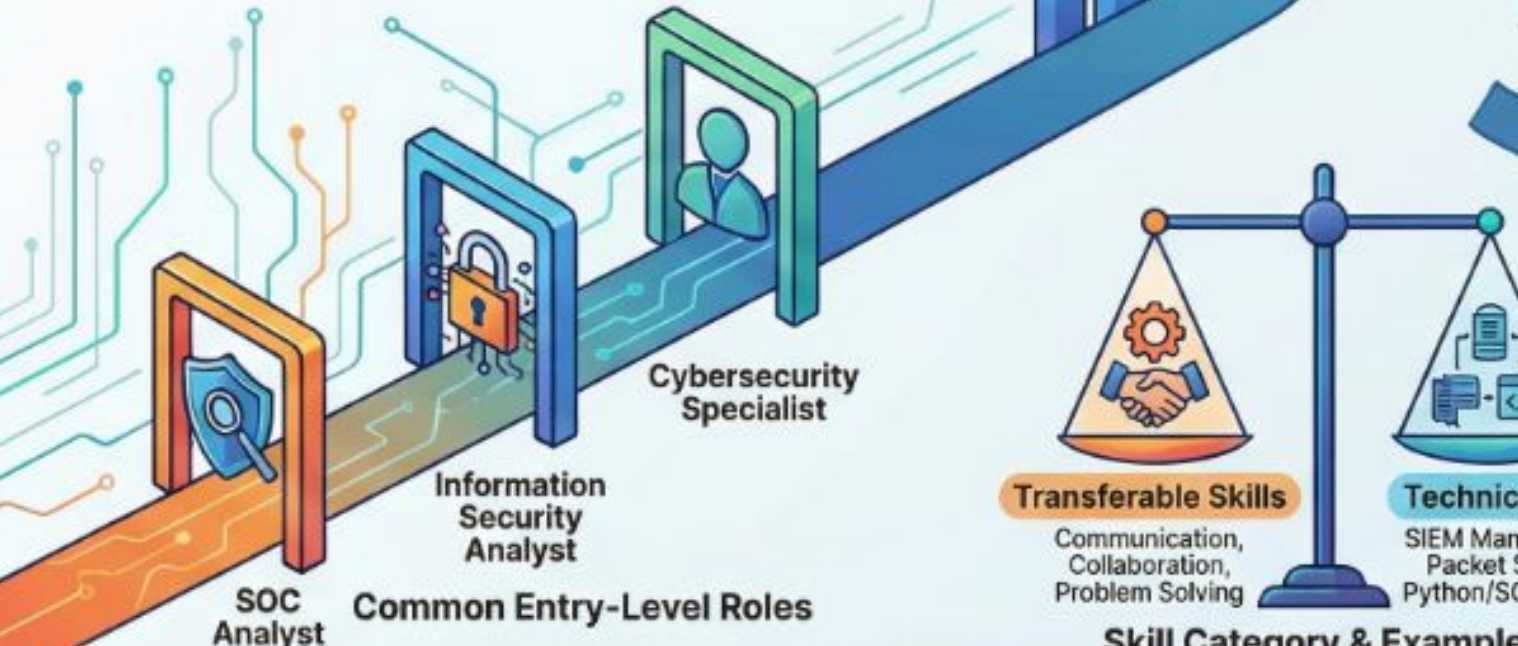
The foundational model ensuring the Confidentiality, integrity, and Availability of sensitive data.

Essential Technical Tools

SIEM Tools (Splunk/Chronicle)

Programming (Python/SQL)

Linux Operating System



Common Entry-Level Roles

Transferable Skills

Communication, Collaboration, Problem Solving

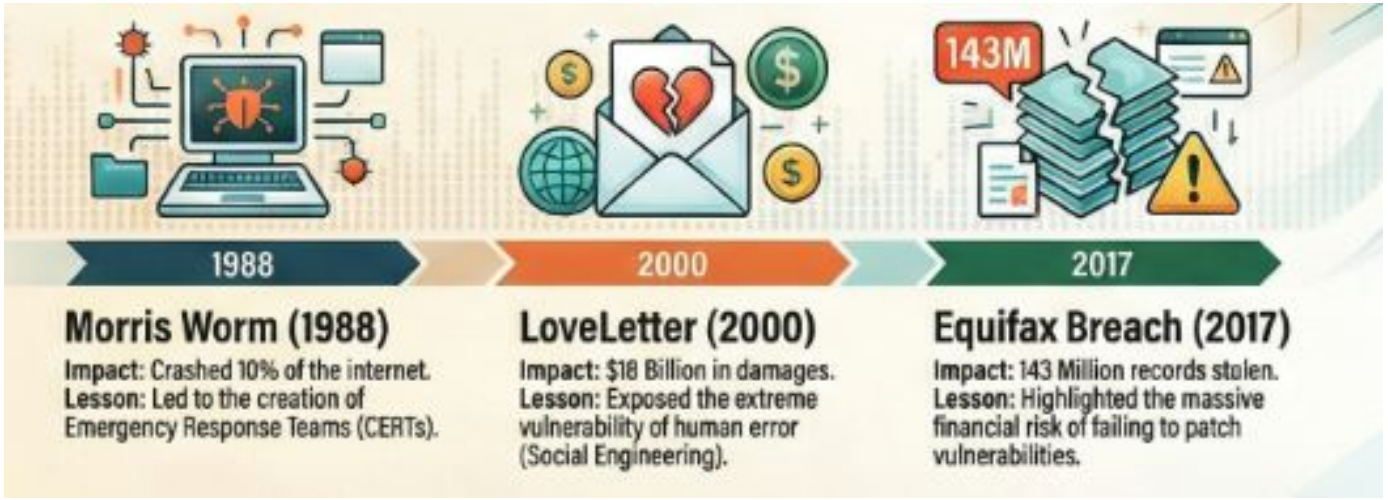
Technical Skills

SIEM Management, Packet Sniffing, Python/SQL Coding

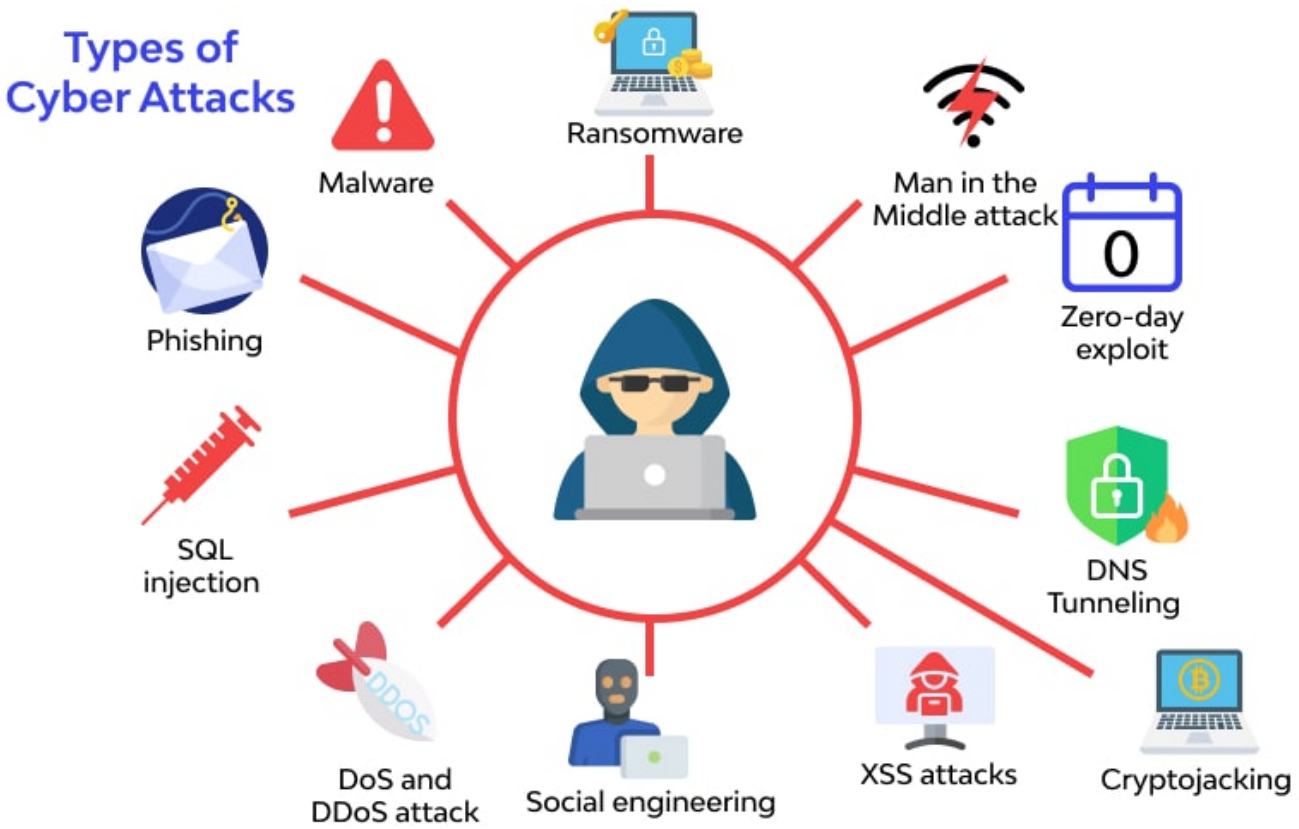
Skill Category & Examples

Why Attacks Succeed

- Software vulnerabilities
  - Human error
  - Poor security policies



Types of Cyber Attacks



Ransomware

- Malware that encrypts files and locks users out until a ransom is paid.
- Example: WannaCry (2017) crippled the UK National Health Service and 200k+ devices.
- Average incidents cost organizations over $4.5 million in payments and downtime.

Man-in-the-Middle (MITM)

- Attackers secretly intercept and relay communications between two parties.
- Often uses insecure public Wi-Fi to 'listen' and capture private credentials.
- Example: DarkHotel campaign targeted executives via luxury hotel networks.
- Costs companies hundreds of millions in stolen trade secrets and intellectual property.

Zero-Day Exploit

- Targets software vulnerabilities unknown to the vendor (zero days to fix).
- Example: Stuxnet used four zero-day flaws to sabotage nuclear centrifuges.
- High-value exploits sell for $2.5 million, while victims face millions in emergency fixes.

DNS Tunneling

- Encodes sensitive data into DNS queries to sneak past firewalls.
- Example: OilRig (APT34) used this to steal data from Middle Eastern governments.
- Leads to stealthy breaches costing an average of $160 per stolen record.

Cryptojacking

- Unauthorized use of a victim’s hardware to mine cryptocurrency.
- Example: Hackers hijacked Tesla’s public cloud to run mining scripts.
- Increases energy bills and infrastructure wear, raising operational costs by 10-30%.

Cross-Site Scripting (XSS)

- Injects malicious scripts into trusted websites to execute in a visitor's browser.
- Example: British Airways payment page was hacked to skim 380k credit cards.
- Results in massive regulatory fines (e.g., £20 million) and fraud liability.

Social Engineering

- Manipulates humans into breaking security rules rather than hacking code.
- Example: 2020 Twitter Hack tricked staff to hijack accounts like Elon Musk's.
- Business Email Compromise (BEC) scams have cost global businesses over $43 billion.

DoS and DDoS Attacks

- Floods a server with junk traffic to make it unavailable to legitimate users.
- Example: Dyn Attack (2016) used IoT botnets to take down Netflix and Twitter.
- Downtime for online businesses costs roughly $5,600 per minute in lost revenue.

SQL Injection (SQLi)

- Inserts malicious commands into database inputs to reveal private data.
- Example: Heartland Payment Systems breach compromised 130 million cards.
- One of the most expensive attacks, with US data breaches averaging $9.5 million.

Phishing

- Fraudulent emails disguised as reputable sources to steal login credentials.
- Example: 2016 DNC Leak began with a fake Google 'Change Password' email.
- The entry point for 90% of attacks, contributing to trillions in global damages.

Malware

- Broad term for harmful software like viruses, trojans, and spyware.
- Example: Emotet evolved from a banking trojan to a global malware distributor.
- 'Cleaning' a network after infection costs mid-sized enterprises ~ $2.7 million.

The CIA Triad

- The foundational concept of cybersecurity.
- Three core principles:
  - Confidentiality
    - Privacy of sensitive data.
  - Integrity
    - Accuracy and reliability of data.
  - Availability.
    - Accessibility of data when required.

1. Confidentiality

- Ensures sensitive data is accessible only to authorized users.
- Crucial for healthcare (medical records) and banking (account details).
- Prevents identity theft, blackmail, and fraudulent activities.

Confidentiality: Methods of Protection

- Encryption: Transforms data into unreadable formats (e.g., WhatsApp messages).
- Access Control Lists (ACLs): Permissions defining who can see what (e.g., HR salary data).
- Multi-Factor Authentication (MFA): Verifying identity via passwords + SMS/Fingerprints.

2. Integrity

- Ensures information remains accurate, complete, and unaltered.
- Protects against unauthorized modification that could lead to poor decisions.
- Critical for tax filings and medical administration records (MAR).

Integrity: Methods of Protection

- Hashing (SHA256): Generates a unique digital fingerprint to detect changes.
- Digital Signatures: Verifies authenticity of documents and prevents tampering.
- Checksums: Used during file transfers to ensure data isn't corrupted or incomplete.

3. Availability

- Guarantees that data and systems are accessible when needed.
- Crucial for services requiring 24/7 uptime like hospitals or banks.
- System downtime leads to lost productivity and potential life-threatening delays.

Availability: Methods of Protection

- Backup Systems: Regular data copies stored in multiple locations for recovery.
- Redundancy: Having 'spare' systems or servers ready to take over if one fails.
- Load Balancing: Distributing traffic across servers to prevent overloads (e.g., Amazon sales).