**What is cyber security**

Cybersecurity is the branch of technology that aims to protect computers, mobile devices, and information from malicious actors who want to gain unauthorized access to them or cause harm.

Cybersecurity protects data, devices, and networks from potential threats such as hackers, criminals, and malicious code.

**Types of cybersecurity**

### 1. Application security

### 2. Cloud security

### 3. Critical infrastructure security

### 4. Information security (InfoSec)

### 5. Network security

## Common cyber threats

Password attacks, Phishing attacks, DOS attacks, Man-in-the-middle attacks, Malware

## What is a threat in cybersecurity?

In cybersecurity, a threat is any kind of action that has the potential to negatively impact an organization’s operations, procedures, systems, or data.

## Common types of cyberattacks

### 1. Malware 2. Phishing 3. Man-in-the-middle (MitM) 4. Denial of Service (DoS)5. Injection attacks

**Malware**

Trojans, Adware, Spyware, Ransomware

**Man-in-the-middle (MitM)**

HTTPS spoofing, IP spoofing, SSL hijacking

**Injection attacks**

Code injection , SQL Injection , XML Injection

## What does a cybersecurity analyst do?

* Monitor network traffic for security incidents and events.
* Investigate incidents and respond to events in real time.
* Write detailed incident response reports.
* Install and operate [firewalls](https://www.coursera.org/articles/what-is-firewall), [encryption programs](https://www.coursera.org/articles/types-of-encryption), and other security software.
* Fix vulnerabilities.
* Develop and promote best practices for [information security](https://www.coursera.org/articles/infosec).
* Conduct threat research.
* Perform periodic risk assessments and [penetration tests](https://www.coursera.org/articles/how-to-become-a-penetration-tester).

#### **Cybersecurity technical skills**

* **Intrusion detection:** While the ultimate goal of cybersecurity is to prevent attacks, you’ll need to know how to detect them when they do happen. This can include network monitoring, event log analysis, and familiarity with SIEMs.
* **Endpoint management:** As more and more people work from home, companies need security professionals who know how to secure multiple endpoints, like computers, phones, and [Internet of Things](https://www.coursera.org/articles/internet-of-things) devices. Tools might include firewalls, antivirus software, network access controls, and virtual private networks (VPNs).
* **Data security:** Data represents a valuable resource for most organizations. Knowing how to protect it involves understanding encryption, access management, transmission control and internet protocols (TCPs and IPs), and the [CIA Triad](https://www.coursera.org/articles/cia-triad) (confidentiality, integrity, accessibility).
* **Networking and network security:** Most attacks occur on networked systems. To protect against these types of threats, you’ll need to know how networks work, as well as their particular vulnerabilities.
* **Programming:** While advances in technology are enabling cybersecurity analysts to perform their work without having to write code, a foundational understanding of languages like [JavaScript](https://www.coursera.org/articles/java-vs-javascript), [Python](https://www.coursera.org/articles/what-is-python-used-for-a-beginners-guide-to-using-python), and [C/C++](https://www.coursera.org/articles/what-is-c-plus-plus) could give you a competitive edge.

#### **Cybersecurity workplace skills**

* **Attention to detail:** Noticing a small anomaly could mean saving your company from a big data loss.
* **Communication:** When security events happen, you’ll need to coordinate with your security team and document the process of investigation and recovery. You may be tasked with training your fellow employees in best security practices.
* **Critical thinking:** Whether you’re responding to a threat, patching a vulnerability, or recommending new security protocols, critical thinking skills empower you to make data-driven decisions.
* **Curiosity:** Technology continues to evolve, and cybercriminals continue to come up with new ways to steal or destroy data. Curiosity will help you stay up to date on new threats and security best practices.
* **Calm under pressure:** Responding to a security event means acting fast and prioritizing the tasks that will shut down the attack or isolate the data breach quickly to minimize damage.

Cyber Security Domains

GRC, SOC, Cloud Security,Netowrk Security,Incident Response,Ethical Hacker

1. GRC

….Governance Risk and compliance…. Setting security principle , documentation…not technical domand….NIST framework… **Course** ComTIA sec+

1. SOC Analyst

Read logs, real time monitoring, alerts, SIEM Tools like splunk…**Course** CompTIA SEC+

1. Cloud Security Engineer

To protect data, network and app on cloud ….. **Course** Certified cloud sec professional, AWS security speclity , Azure security Engineer…..first network engerning , cloud engering

1. Network Security

Network engineer , **Course** CCNA , firwalls ,

1. Incident Response and Digital Forensics (DFIR)

Threats ko find karna , response karna ,find karna ,….autospy , volatitly …. **Course** GIAC Incident handler ….GIAC Fronice Handler

1. Penetration Tester or Ethical Hacker

Defend organization , attach organization …red team , blue team…. **Course** CEH…OSCP

| **Domain** | **Learning Duration (Est.)** | **Key Certifications** |
| --- | --- | --- |
| **GRC** (Governance, Risk, Compliance) | 4–6 months | ISO 27001, CISA, CRISC |
| **SOC Analyst** (SIEM, log analysis) | 6–9 months | CompTIA CySA+, Splunk, Blue Team certs |
| **Cloud Security** | 6–9 months | AWS/Azure Security, CCSP |
| **Network Security** | 4–6 months | CompTIA Network+, Cisco CCNA Security |
| **Incident Response** | 6–9 months | SANS GCIH, CompTIA CySA+ |
| **Ethical Hacking(Pen Tester)** | 9–12 months | CEH, eJPT, OSCP (advanced) |