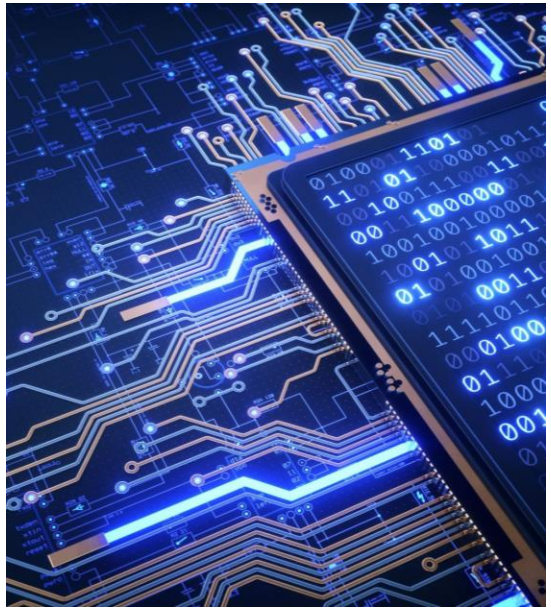

100+ Days of
Cyber Security



# 1.Computer Basics

**Fundamental** concepts of computer hardware, software, and input/output operations

**Introduces** key elements related to web and internet technologies and networking

**Familiarizing** yourself with computer hardware components, such as the CPU, RAM, and storage devices

# 2.General Coding

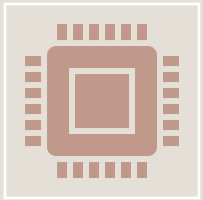
**General** coding focuses on learning a programming language and the foundational concepts required for coding

In this case, the recommended language is C

Progress in understanding control flow structures like loops and conditional statements

# 3. Script Writing

**Introduces** scripting using the Python programming language



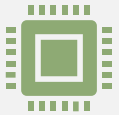
Python is widely used in cybersecurity for its simplicity and versatility

**Basics** of Python programming, including variables, lists, and dictionaries

# 4. Web Application Testing

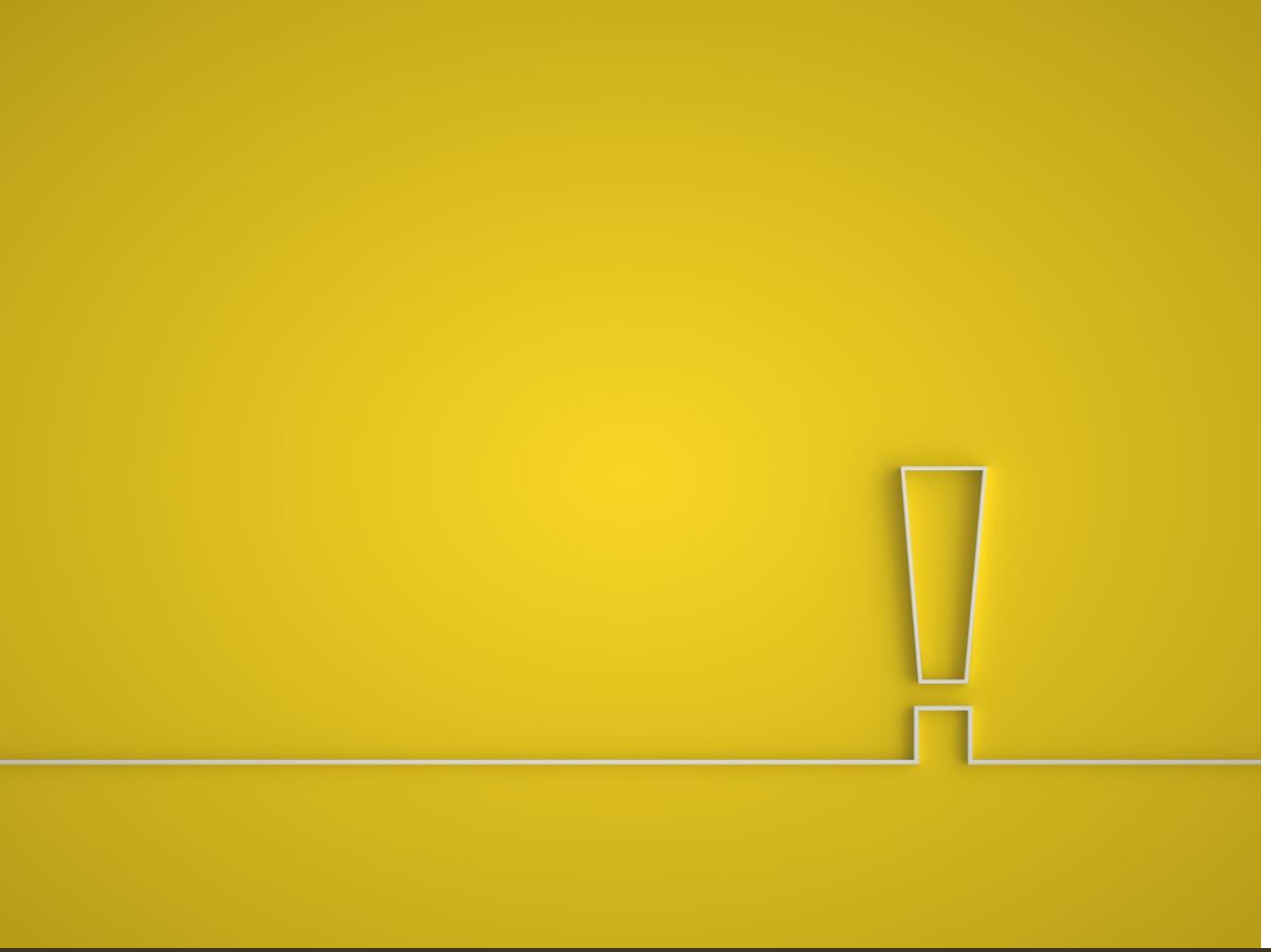
**Involves** assessing the security of web applications, including identifying vulnerabilities and ensuring secure coding practices

**Understanding** JavaScript for frontend testing, including its role in manipulating the Document Object Model



Progress to learning SQL for backend testing

**Understanding** how to perform security testing using tools like OWASP ZAP



- **Description:** Shell scripting involves automating tasks and executing commands in a command-line environment using shell scripts.
- The recommended shell scripting language here is **Bash.**
- **Where to Start:** Begin with an introduction to Bash scripting, including command line utilities and script execution.

# 5. Shell Scripting

# 6. Application Security

**Understanding** common vulnerabilities in software applications and implementing secure coding practices to mitigate risks

**Common** application vulnerabilities, such as the OWASP Top **10**

**Delve** into secure coding practices, input validation techniques, and the importance of web application firewalls and security headers

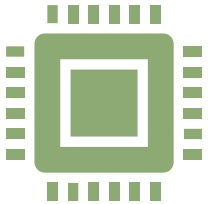
# 7. Cloud Security

## Cloud

**Unique** challenges and best practices for securing cloud computing environments and services

## Explore

**Different** cloud service models and their security implications



## Focus on

**Identity** and access management in the cloud and learn how to secure cloud infrastructure and data

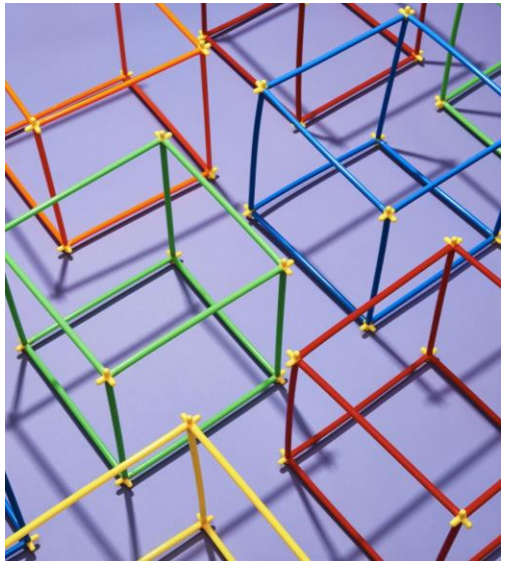
# 8. Threat Intelligence

**Involves** gathering, analyzing, and utilizing information about potential cybersecurity threats to enhance proactive security measures

**Understanding** the importance of threat intelligence and various sources for gathering threat information

Learn techniques for analyzing and utilizing threat intelligence data

# 9. Security Operations



- Focus on managing **security incidents**, **monitoring systems**, and ensuring effective **Incident response** within an organization
- Where to Start: Begin by understanding **Security Information and Event Management (SIEM)** and its role in monitoring and detecting security incidents
- Insights into **Security Operations Center (SOC)** functions and the tools used in security operations

# 10. Risk Management and Assessment

01

**RMA** involve identifying, evaluating, and mitigating cybersecurity risks within an organization

02

**Understanding** the fundamentals of risk management and assessment, including risk identification, analysis, and mitigation strategies

03

**Explore** techniques for conducting risk assessments in cybersecurity

# 11. Endpoint Security and Device Protection

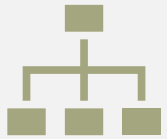
**EPS** focuses on securing individual devices, such as laptops, desktops, and mobile devices, from various threats and vulnerabilities

**The** importance of endpoint security and the types of threats that target individual devices

Explore different **security measures** and best practices to protect endpoints, including antivirus software, firewalls, and encryption techniques

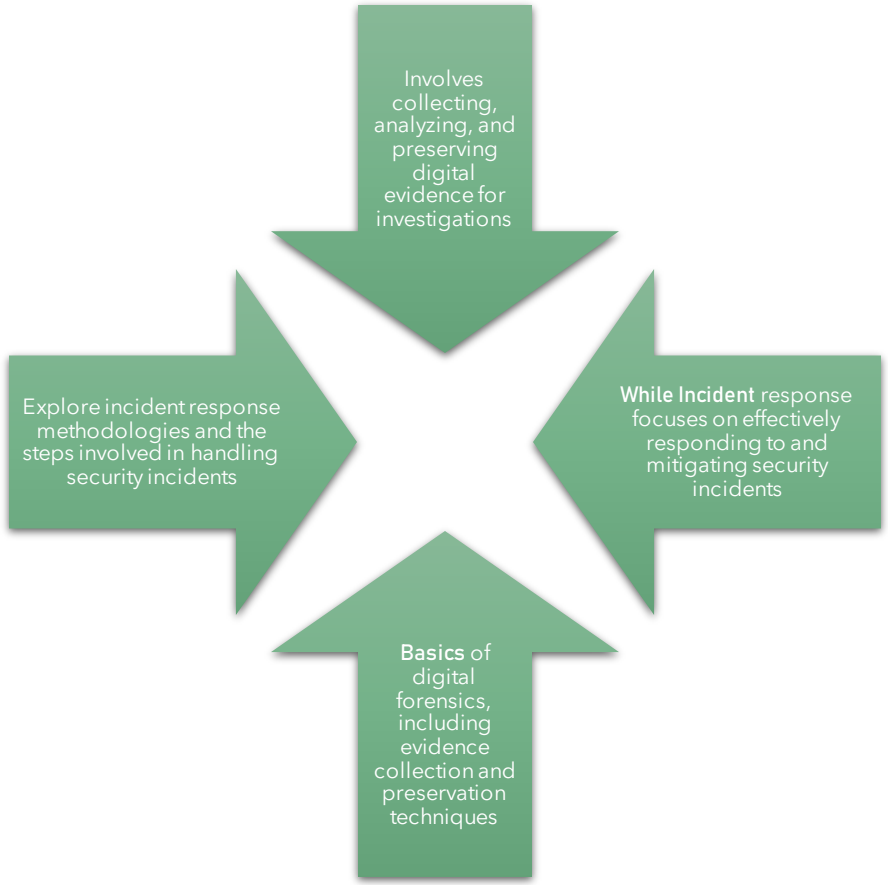
# 12. Identity and Access Management

**IAM** involves managing user identities and controlling access to systems and resources to ensure proper authorization and authentication



**Understanding** the fundamentals of IAM and its role in ensuring secure access control

**Explore** concepts such as user provisioning, authentication mechanisms, and access management



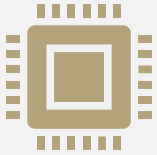

# 13. Digital Forensics and Incident Response

# 14. Introduction to Job Profiles and Designations

- Overview of various job roles and designations in the cybersecurity field, giving insights into the responsibilities and skill requirements of each role
- Where to Start: Start by exploring different job profiles in cybersecurity, such as security analyst, digital forensic investigator, penetration tester, security consultant, Red teamer/Blue teamer, malware analyst, SOC analyst, and security auditor
- Research the responsibilities, required skills, and career paths associated with each role to gain a comprehensive understanding




# 15. Projects combining Cybersecurity with Machine Learning, Web 3, Blockchain



Description: This topic explores the intersection of cybersecurity with emerging technologies such as machine learning , Web 3.0, and blockchain

It focuses on understanding how these technologies can enhance cybersecurity practices

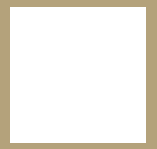
Where to Start: Begin by learning the basics of ML and its applications in cybersecurity, such as anomaly detection and threat intelligence

# 16. Bug Bounty Programs and Capture the Flag Challenges

**Bug** bounty **programs** and **CTF challenges** provide opportunities to practice and showcase cybersecurity skills by identifying vulnerabilities in systems and networks

**Understanding** the concept of bug bounty programs and how they work

**Explore** CTF challenges, which simulate real-world security scenarios



**Participate** in online CTF competitions or platforms to improve your skills and knowledge