CYBERGUARDX

Network & Security Engineer Diploma

Cyber Security

https://academy.cyberguardx.org/network-security-diploma

About Us

CyberGuardX Academy is a cutting-edge cybersecurity training platform dedicated to nurturing the next generation of cybersecurity professionals. With a focus on practical learning and industry-relevant skills, we aim to empower individuals with the tools they need to excel in today's rapidly evolving digital landscape. Our academy provides a comprehensive curriculum, combining hands-on experience, globally recognized certifications, and real-world scenarios to prepare students for the challenges of modern cybersecurity. At CyberGuardX, we pride ourselves on offering flexible learning options, expert instructors with real-world experience, and a community-driven approach to education. Join us to take your cybersecurity knowledge to the next level and become a trusted expert in the field.

https://academy.cyberguardx.org/network-security-diploma

Objective

The Network & Security Engineer Diploma aims to provide participants with the critical skills required to excel in networking and cybersecurity roles. This diploma focuses on equipping learners with the expertise to design, configure, and secure networks while mastering cybersecurity principles such as risk management, encryption, and threat detection.

Participants will gain hands-on experience in implementing secure networks using firewalls, VPNs, and advanced routing techniques. They will also learn to detect and respond to security incidents with SIEM platforms like QRadar and Splunk, perform vulnerability assessments, and execute compliance-driven projects.

Additionally, the program aligns with globally recognized certifications such as Cisco CCNA, CompTIA Security+, Fortinet NSE4, and ISC^2 Certified in Cybersecurity (CC), empowering learners to confidently achieve these credentials. By completing this diploma, participants will be prepared for roles such as Network Engineer, SOC Analyst, Firewall Administrator, and Security Operations Specialist, combining theoretical knowledge with real-world, hands-on expertise to thrive in the cybersecurity job market.

https://academy.cyberguardx.org/network-security-diploma

Diploma Outline

01 Network Essentials

02 Cybersecurity Fundamentals

03 Ethical Hacking Basics

04 Firewall Management

05 SIEM & Threat Detection

About the Network & Security Engineer Diploma

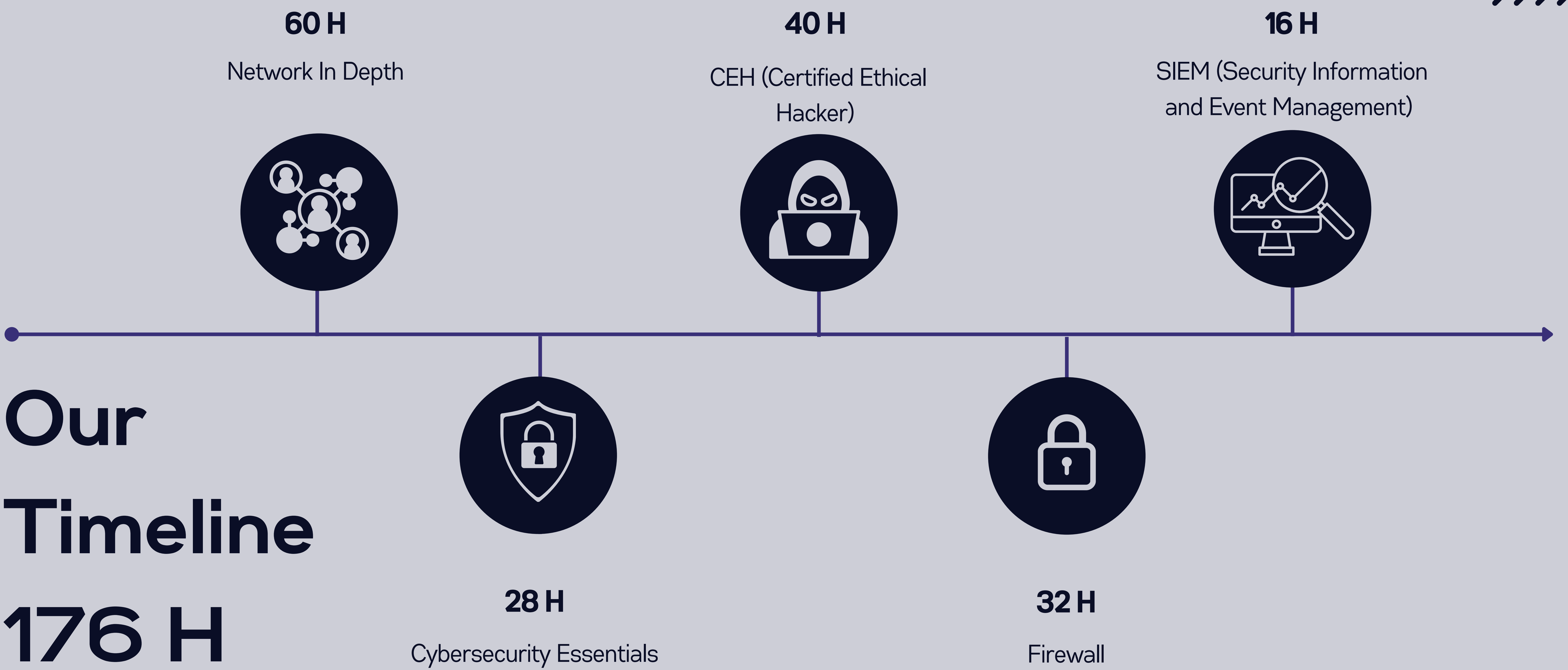
The Network & Security Engineer Diploma at CyberGuardX Academy is a comprehensive training program tailored for individuals aspiring to excel in modern networking and cybersecurity roles. This 175-hour diploma equips participants with the essential knowledge and practical skills required to design, implement, and secure advanced network infrastructures.

The curriculum integrates a blend of theoretical foundations and hands-on experience, covering key areas such as network essentials, operating systems, network security devices, attack prevention, cybersecurity tools, and advanced SIEM solutions. Through real-world projects and interactive labs, participants will develop expertise in creating secure networks, managing firewalls, and responding to cybersecurity incidents.

By the end of this diploma, learners will be prepared for globally recognized certifications like CCNA, Security+, Fortinet NSE4, and Palo Alto PCNSA. Graduates will be equipped to tackle roles such as Network Security Engineer, SOC Analyst, Firewall Specialist, and more, making them valuable assets in today’s cybersecurity landscape.

CyberGuardX Academy ensures that students gain robust, industry-aligned education through flexible learning formats and experienced instructors, preparing them to meet the challenges of modern digital security demands.

Our Timeline 176 H



60 H

Network In Depth

28 H

Cybersecurity Essentials

40 H

CEH (Certified Ethical Hacker)

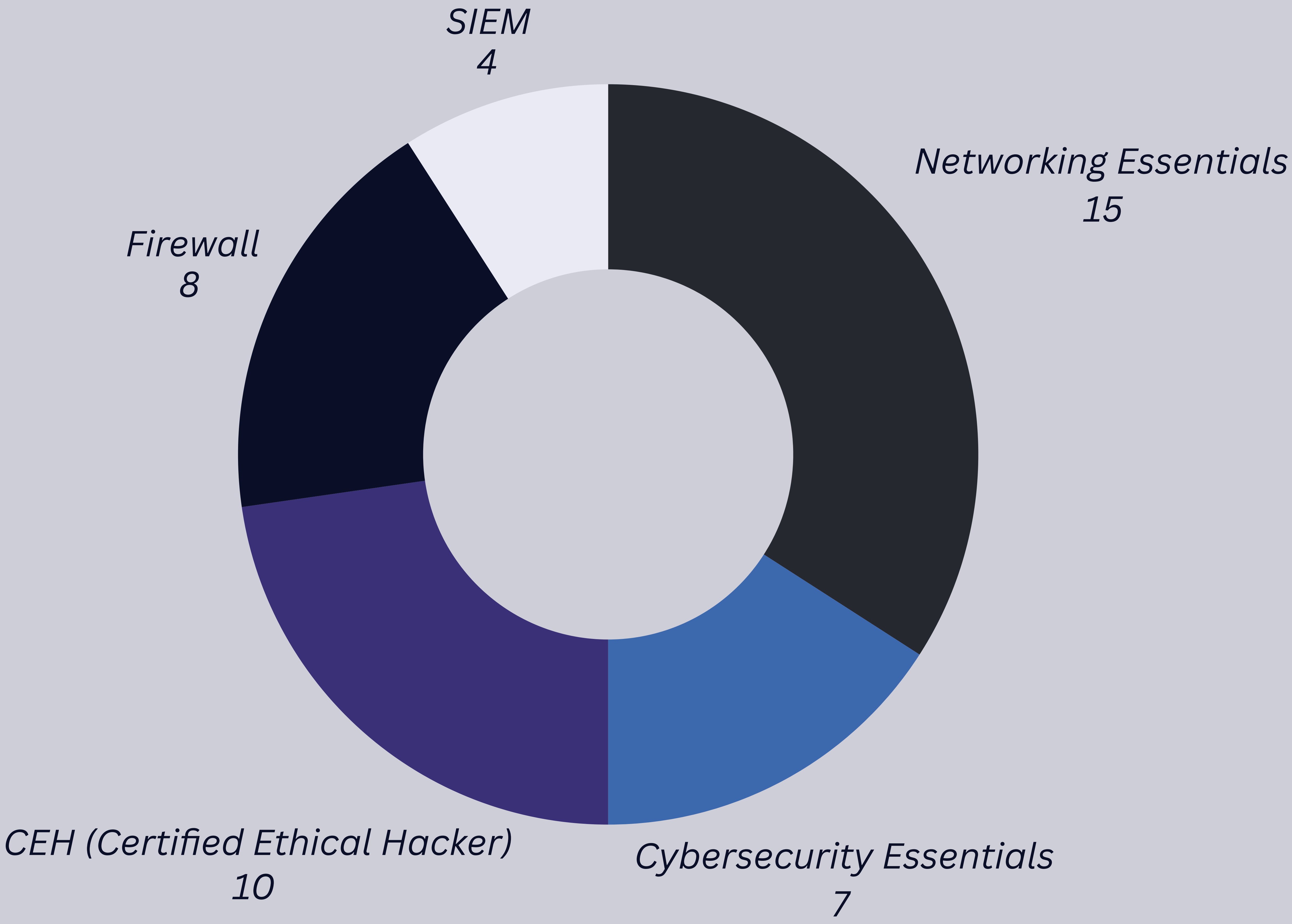
32 H

Firewall

16 H

SIEM (Security Information and Event Management)

176 HOUR / 44 SESSION



Course 1: Network Essentials

◆ Overview: This module provides an in-depth exploration of networking principles, covering network design, configuration, and troubleshooting. It offers a strong foundation for advanced networking concepts and real-world applications, focusing on best practices and industry standards.

◆ Key Topics:

- OSI Model & TCP/IP Protocol Suite: Detailed analysis of network communication layers, data encapsulation, and protocol interactions.
- IP Addressing & Subnetting: Comprehensive coverage of IPv4 and IPv6 addressing schemes, subnet masks, CIDR notation, and advanced subnetting techniques.
- VLANs & Trunking: Network segmentation concepts, VLAN tagging (802.1Q), inter-VLAN routing, and spanning tree protocol (STP) for loop prevention.
- Routing Protocols: Static vs. dynamic routing, including RIP, OSPF, EIGRP, and BGP fundamentals, with real-world implementation examples.
- Switching Mechanisms: MAC address tables, ARP, port security, spanning tree variations (RSTP, MSTP), and Layer 3 switching techniques.
- Network Topologies & Architectures: Enterprise network design, hybrid cloud networking, SDN basics, and best practices for scalable, secure infrastructures.
- DNS, DHCP & NAT: Detailed configuration, troubleshooting, and security considerations for name resolution and dynamic address allocation.
- Packet Analysis & Troubleshooting: Hands-on experience with Wireshark for analyzing network traffic, diagnosing issues, and optimizing performance.

◆ Career Impact: Prepares students for roles such as Network Engineer, IT Administrator, and certifications like CCNA and CompTIA Network+.

Course 2: Cybersecurity Essentials

🔹 Overview: This module focuses on cybersecurity fundamentals, risk management, and defensive strategies to mitigate modern cyber threats effectively. It covers security policies, encryption, system hardening, and regulatory compliance.

🔹 Key Topics:

- Cybersecurity Frameworks: Detailed study of NIST, ISO 27001, CIS Controls, and their implementation in enterprise environments.
- Risk Assessment & Threat Modeling: Identifying vulnerabilities, calculating risk impact, and implementing effective mitigation strategies.
- Authentication & Access Control: Role-based access control (RBAC), multi-factor authentication (MFA), and identity & access management (IAM) methodologies.
- Windows & Linux Security Hardening: Advanced system protection techniques, patch management strategies, and security baseline configurations.
- Encryption & Cryptography: In-depth exploration of symmetric vs. asymmetric encryption, hashing algorithms, PKI infrastructure, and SSL/TLS security protocols.
- SIEM & Incident Response: Implementation of security event monitoring, attack vector analysis, and structured incident response methodologies.
- Malware Analysis & Endpoint Protection: Understanding rootkits, ransomware, advanced persistent threats (APTs), and endpoint detection and response (EDR) solutions.

🔹 Career Impact: Equips learners for roles like Security Analyst, Cybersecurity Engineer, and prepares them for certifications such as Security+ and CISSP (entry-level knowledge).

Course 3: CEH (Certified Ethical Hacker) Basics

🔹 Overview: This module provides a comprehensive introduction to ethical hacking methodologies, penetration testing techniques, and vulnerability assessments through hands-on labs.

🔹 Key Topics:

- Ethical Hacking Lifecycle: Covering reconnaissance, scanning, exploitation, maintaining access, and covering tracks.
- Passive & Active Reconnaissance: OSINT, footprinting, and enumeration techniques for effective target profiling.
- Social Engineering Techniques: Phishing, pretexting, baiting, and psychological manipulation tactics.
- Metasploit Framework & Exploitation Tools: Automating exploits, payload generation, and privilege escalation.
- Web Application Security: Detailed analysis of SQL injection, XSS, CSRF, and OWASP security misconfigurations.
- Wireless Network Attacks: WPA2 cracking, rogue AP detection, and strategies for securing enterprise Wi-Fi.
- Post-Exploitation & Lateral Movement: Techniques for privilege escalation, persistence mechanisms, and credential dumping.

🔹 Career Impact: Develops skills for Penetration Tester, Red Team Specialist, and certifications such as CEH and OSCP (fundamentals).

Course 4: Network Security Operation and Implementation (Firewall Management)

🔹 Overview: This module provides hands-on training in configuring and managing enterprise firewalls, securing network traffic, and implementing VPN solutions.

🔹 Key Topics:

- Firewall Fundamentals: Stateful vs. stateless filtering, deep packet inspection (DPI), and zone-based security models.
- Enterprise Firewall Configurations: Best practices for configuring FortiGate, Cisco ASA, and Palo Alto firewalls.
- NAT, ACLs, & Security Policies: Implementing granular access controls, traffic filtering, and secure network segmentation.
- IPS/IDS Integration: Threat detection methods, signature-based vs. anomaly-based analysis, and automated response mechanisms.
- VPN Deployment: Configuring site-to-site and remote access VPNs (IPSec & SSL), encryption standards, and secure tunneling.
- Zero Trust Security Models: Implementing micro-segmentation, least privilege access, and continuous authentication strategies.
- Cloud Firewall Solutions: Configuring AWS, Azure, and Google Cloud firewall solutions to secure cloud-based workloads.

🔹 Career Impact: Supports roles like Firewall Specialist, Network Security Engineer, and vendor-specific certifications such as Fortinet NSE and Palo Alto PCNSA.

Course 5: SIEM & Threat Detection

🔹 Overview: This module focuses on security event monitoring, log analysis, and incident response using industry-standard SIEM platforms.

🔹 Key Topics:

- Security Log Analysis: Techniques for collecting, parsing, and interpreting system logs for security insights.
- Threat Intelligence & Incident Response: Correlating data sources, detecting anomalies, and responding to security threats.
- Correlation Rules & SIEM Customization: Creating actionable alerts, dashboards, and automated security workflows.
- SIEM Administration: Hands-on experience with QRadar, Splunk, and other SIEM solutions.
- Security Automation (SOAR): Orchestrating automated response mechanisms for proactive threat mitigation.
- Forensic Analysis: Investigating breach incidents, collecting digital evidence, and conducting malware reverse engineering.

🔹 Career Impact: Prepares students for roles such as SOC Analyst, Incident Responder, and SIEM-related certifications like Splunk Core Certified User and IBM QRadar SIEM Certification.

To register Click on the Photo

Thanks