Advanced Network Security and Threat Mitigation Training Course

26 - 30 Oct 2026

Kuala Lumpur

5200 € (Per Person)

Ref: #NO6858_118057

Course Introduction / Overview:

In today's hyper-connected digital landscape, the sophistication of cyber threats is evolving at an unprecedented rate, making robust network security and proactive threat mitigation non-negotiable for any organization. This intensive training course is designed to move beyond theoretical knowledge, providing participants with the advanced skills required to design, implement, and manage a resilient security posture. We will delve deep into the principles outlined by leading academics like William Stallings in his seminal work, "Cryptography and Network Security: Principles and Practice," to build a foundational understanding of modern defense mechanisms. This program, offered by BIG BEN Training Center, covers the entire lifecycle of network security, from establishing a secure network architecture and configuring advanced defense systems like firewalls and IDS/IPS, to mastering the art of threat hunting, vulnerability assessment, and effective incident response. Participants will learn to analyze network traffic, identify indicators of compromise, and apply threat intelligence to preemptively neutralize attacks before they cause significant damage. The curriculum is meticulously crafted to address contemporary challenges, including cloud security vulnerabilities and the implementation of zero-trust frameworks, ensuring that attendees are prepared to protect critical digital assets against the most advanced persistent threats.

Target Audience / This training course is suitable for:

- Network Security Engineers.
- Cybersecurity Analysts.
- IT Managers and Team Leaders.
- Security Operations Center (SOC) Personnel.
- System Administrators.
- Information Security Consultants.
- IT Professionals seeking to specialize in security.
- Incident Responders.
- Network Architects.

Target Sectors and Industries:

- Banking and Financial Services.
- Healthcare and Medical Institutions.
- Information Technology and Telecommunications.
- Governmental bodies and Public Sector agencies.
- E-commerce and Retail.
- Energy and Utilities.
- Consulting and Professional Services.
- Education and Research Institutions.

Target Organizations Departments:

- Information Technology (IT) Department.
- Information Security (InfoSec) Department.
- Network Operations Center (NOC).
- Security Operations Center (SOC).
- Risk Management and Compliance.
- Internal Audit and Governance.
- Technical Support and Help Desk.
- Research and Development.

Course Offerings:

By the end of this course, the participants will have able to:

- Design and implement a secure network architecture using segmentation and layering.
- Configure and manage advanced firewalls, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS).
- Conduct comprehensive vulnerability assessments and interpret penetration testing results.
- Analyze network traffic and system logs to detect and investigate security incidents.
- Develop and execute a structured incident response plan according to industry best practices.
- Utilize threat intelligence to proactively identify and mitigate emerging cyber threats.
- Apply cryptographic principles to secure data in transit and at rest.
- Implement security controls for cloud environments and remote access solutions.
- Understand the principles of the MITRE ATT&CK framework and the cyber kill chain.
- Evaluate and apply zero-trust security models within an enterprise environment.

Course Methodology:

The training methodology at BIG BEN Training Center is centered on immersive and practical learning to ensure participants can apply their knowledge directly to real-world scenarios. This course adopts a blended approach that combines expert-led instruction with hands-on, interactive exercises. Mornings are typically dedicated to exploring core concepts, advanced security frameworks, and threat mitigation strategies, supported by detailed presentations and real-life case studies of major security breaches. The afternoons are focused on practical application, where participants engage in simulated lab environments to configure security devices, analyze packet captures, and respond to mock security incidents. We foster a collaborative learning environment through group discussions, brainstorming sessions, and team-based problem-solving activities. This allows participants to share insights and learn from the diverse experiences of their peers. Continuous feedback is provided by the instructor throughout the sessions to reinforce learning and address individual challenges. Our goal is to move beyond passive listening, empowering attendees with the confidence and competence to effectively manage and defend complex network infrastructures against sophisticated cyber threats.

Course Agenda (Course Units):

Unit One: Foundations of Modern Network Security

- Network Security Principles and the CIA Triad.
- Deep Dive into TCP/IP Vulnerabilities.
- Understanding the Cyber Kill Chain and MITRE ATT&CK Framework.
- Common Attack Vectors: Phishing, Malware, Ransomware, and DDoS.
- Introduction to Cryptography and Public Key Infrastructure (PKI).
- Developing Effective Security Policies and Procedures.
- Legal, Ethical, and Compliance Considerations in Cybersecurity.

Unit Two: Designing and Implementing Perimeter Defenses

- Advanced Firewall Architectures and Rule-Based Policies.
- Configuring and Tuning Intrusion Detection and Prevention Systems (IDS/IPS).
- Implementing Secure Virtual Private Networks (VPNs) and Remote Access.
- Network Segmentation and Micro-segmentation Strategies.
- Securing Wireless Networks (WPA3 and Enterprise Authentication).
- Unified Threat Management (UTM) Solutions.
- Hardening Network Devices: Routers, Switches, and Access Points.

Unit Three: Threat Detection, Analysis, and Intelligence

- Security Information and Event Management (SIEM) Systems.
- Advanced Log Analysis and Correlation Techniques.
- Network Traffic Analysis and Packet Inspection.
- Introduction to Threat Hunting Methodologies.
- Leveraging Cyber Threat Intelligence (CTI) Feeds.
- Fundamentals of Malware Analysis and Reverse Engineering.
- Detecting Advanced Persistent Threats (APTs).

Unit Four: Vulnerability Management and Offensive Security

- Conducting Network Vulnerability Scanning and Assessment.
- Interpreting Scan Results and Prioritizing Remediation.
- Fundamentals of Penetration Testing and Ethical Hacking.
- Web Application Security Vulnerabilities (OWASP Top 10).
- Social Engineering Techniques and Countermeasures.
- Managing the Patch and Vulnerability Lifecycle.
- Developing a Robust Remediation and Mitigation Strategy.

Unit Five: Incident Response and Advanced Security Architectures

- Building a Comprehensive Incident Response Plan (IRP).
- Incident Triage, Containment, Eradication, and Recovery.
- Introduction to Digital Forensics and Evidence Handling.
- Securing Cloud Environments (IaaS, PaaS, SaaS).
- Implementing a Zero-Trust Security Model.
- Future Trends in Network Security: AI, Machine Learning, and Automation.
- Final Capstone Project: Responding to a Simulated Multi-Stage Cyber Attack.

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

In an era of increasingly sophisticated state-sponsored cyber-attacks, how can organizations balance the principles of a zero-trust architecture with the operational need for seamless data flow and user accessibility?

What unique qualities does this course offer compared to other courses?

This training course distinguishes itself by focusing on the strategic mindset required for modern cybersecurity, rather than merely providing a procedural guide to specific software or tools. While participants will gain hands-on experience, the core emphasis is on understanding the "why" behind security decisions, enabling them to architect adaptable and resilient defense systems. We move beyond standard curriculum by integrating advanced concepts such as proactive threat hunting, the practical application of the MITRE ATT&CK framework, and the strategic implementation of zero-trust models. The course content is continuously updated to reflect the latest threat intelligence and attack vectors, ensuring relevance in a rapidly changing field. Unlike other programs that may focus narrowly on either offensive or defensive tactics, this course provides a holistic view, teaching participants how to think like an attacker to build stronger defenses. The capstone project, a simulated multi-stage attack, provides an unparalleled opportunity to integrate all learned skills from initial detection to final forensic analysis in a high-pressure, realistic environment, cementing knowledge and building true professional competence.