ABAD آباد
معهد شبكة آباد للتدريب
ABAD NETWORK FOR TRAINING

معسكر الأمن السيبراني - المستوى الثاني

CyberSecurity Bootcamp Level 2

Certified Incident Responder "eCIR Certification"

Threat Detection & SIEM Operations (20%)

- Construct and execute custom SIEM queries to identify suspicious and malicious activity. (Apply)
- Correlate and analyze multi-source log data to detect indicators of compromise (IOCs). (Analyze)
- Interpret log entries, alerts, and endpoint activity to recognize signs of initial access. (Understand)

Endpoint & Network Analysis (35%)

- Analyze endpoint telemetry and audit logs to identify local user, group, and system enumeration activity. (Analyze)
- Differentiate privilege escalation techniques, such as exploit use, token manipulation, and UAC bypass, based on endpoint behavior. (Understand)
- Evaluate persistence mechanisms—including service creation, registry modifications, scheduled tasks, and startup artifacts—to determine attacker footholds. (Evaluate)
- Monitor and detect credential access behaviors such as memory scraping, SAM/LSASS access, and credential dumping tools. (Apply)
- Analyze and correlate PCAP data to trace attack chains, C2 communication, lateral movement, and authentication-based anomalies. (Analyze)
- Investigate data exfiltration and unauthorized access by analyzing protocol behavior, traffic patterns, and endpoint interactions. (Analyze)

ABAD آباد
معهد شبكة آباد للتدريب
ABAD NETWORK FOR TRAINING

معسكر الأمن السيبراني - المستوى الثاني

CyberSecurity Bootcamp Level 2

Certified Incident Responder "eCIR Certification"

Digital Forensics & Evidence-Based Analysis (20%)

- Deconstruct malicious macro-enabled documents and extract VBA code to identify embedded payloads and execution logic. (Analyze)
- Perform static analysis on PE files to isolate suspicious imports, metadata, and indicators of compromise. (Analyze)
- Examine Windows Registry artifacts to uncover evidence of persistence, execution history, and system configuration changes. (Analyze)

Threat Intelligence & Attribution (10%)

- Map detected behaviors to known threat actor TTPs using frameworks like MITRE ATT&CK. (Apply)
- Assess behavioral patterns to attribute activity to known APT groups. (Evaluate)

Reporting & Communication (15%)

- Compose a clear investigation report including a timeline, impact assessment, and response actions. (Apply)
- Document and convey technical findings (e.g., IOCs, tools, payloads) to relevant stakeholders and response teams. (Apply)
- Translate forensic and analytical data into actionable containment, eradication, and recovery recommendations. (Evaluate)

ABAD آباد
معهد شبكة آباد للتدريب
ABAD NETWORK FOR TRAINING

معسكر الأمن السيبراني - المستوى الثاني

CyberSecurity Bootcamp Level 2

Certified Digital Forensics Professional "eCDFP Certification"

Preservation of Evidence (20%)

- Understanding the methodology of collection
- Execute the steps of collection plan based on best practices
- Preserve and maintain the integrity of evidence

Fundamentals of Digital Forensics (33%)

- Analyze digital forensics artifacts on Windows operating systems
- Identify evidence of execution on Windows operating systems
- Understand the basic structure of a digital forensic report

Storage Device Fundamentals (20%)

- Demonstrate how to analyze physical device characteristics
- Demonstrate how to analyze logical storage characteristics

Digital Forensics Tools and Techniques (27%)

- Demonstrate appropriate usage of digital forensic analysis tools and techniques
- Demonstrate appropriate usage of network analysis tools and techniques
- Demonstrate appropriate usage of log and timeline tools and techniques

ABAD آباد
معهد شبكة آباد للتدريب
ABAD NETWORK FOR TRAINING

معسكر الأمن السيبراني - المستوى الثاني

CyberSecurity Bootcamp Level 2

Certified Threat Hunting Professional "eCTHP Certification"

Threat Hunting Methodology (10-15%)

- Apply foundational threat hunting concepts to evaluate the most effective methods and tools for a given hunting scenario
- Apply industry-standard frameworks (e.g., MITRE ATT&CK, Cyber Kill Chain) to identify and categorize adversary behaviors during threat hunts
- Analyze organizational readiness and assess the maturity level of threat hunting programs using structured methods

Threat Hunting Strategies (10-15%)

- Evaluate potential threat actors targeting various organizations and analyze common infiltration techniques
- Construct valid and actionable hypotheses to initiate different types of threat hunting activities
- Determine the most effective hunting technique based on current threat intelligence and context

Cyber Threat Intelligence (10-15%)

- Select the most appropriate type of Cyber Threat Intelligence (CTI) source based on specific hunting scenarios
- Evaluate the credibility and accuracy of Indicators of Compromise (IOCs) and other data in intelligence reports
- Extract relevant and actionable data from CTI sources for use in active threat hunting
- Explain intelligence sharing models and determine appropriate opportunities and methods for sharing threat data

ABAD آباد
معهد شبكة آباد للتدريب
ABAD NETWORK FOR TRAINING

معسكر الأمن السيبراني - المستوى الثاني

CyberSecurity Bootcamp Level 2

Certified Threat Hunting Professional "eCTHP Certification"

Network Threat Hunting (25-30%)

- Identify and interpret different types of network-based IOCs relevant to specific threat hunts
- Demonstrate the use of capture and display filters in tools like Wireshark and tcpdump to collect and analyze network traffic
- Use Wireshark to examine packet captures and detect indicators of malicious network activity
- Evaluate packet captures to identify anomalous, suspicious, or malicious network traffic patterns

Endpoint Threat Hunting (30-40%)

- Use platforms like Splunk and ELK to construct and execute investigations that identify specific IOCs and TTPs in endpoint logs
- Detect hidden malicious processes and behaviors on Windows and Linux endpoints through targeted analysis
- Distinguish between legitimate and malicious files, processes, registry entries, and scheduled tasks in Windows environments
- Build and optimize queries to trace potential malicious activity across stages of the Cyber Kill Chain