IITC
IT PROFESSIONAL ACADEMY

מיישם הגנת סייבר

לפרטים והרשמה
055-2780865

IITC
החילזון 3, רמת גן | 077-4123211

www.iitc.co.il
avivab@iitc.co.il

IITC
IT PROFESSIONAL ACADEMY

תוכן עיניינים

נושא	היקף שעות
Introduction	5
Network Technologies	50
Microsoft Technologies	50
Linux - introduction course	60
Cloud	30
Ethical Hacking & Web Hacking	95
Security Operation Center (SOC), EDR and Endpoint Security, SIEM	100
Firewall	30
Forensics	30

סה"כ 450 שעות

IITC
IT PROFESSIONAL ACADEMY

סילבוס התוכנית

Module 1: Network Technologies

50 שעות

- Networking devices
- LAN/WAN, network topologies
- The OSI reference model, TCP/IP
- Physical layer and ethernet
- ARP and ICMP
- IP addressing: IPv4, VLSM, IPv6

- TCP three-way handshake and UDP protocol
- Application layer: HTPP, SSH, DNS
- IP routing
- DHCP and NAT
- Network monitoring with Wireshark

IITC
IT PROFESSIONAL ACADEMY

50 שעות

Module 2: Microsoft Technologies

- Introduction to Windows
- Introduction to Windows, domains, and the Azure cloud
- Building a Windows client machine and cloud computing
- Cloud services, resources and solutions
- Managing processes and services

- Windows and cloud networking and security
- Microsoft Active Directory and identity
- Group policies
- Windows services (RDP, DNS, DHCP, File and printer sharing)
- Intro to cmd and powershell scripting

IITC
IT PROFESSIONAL ACADEMY

50 שעות

Module 3: Linux - Introduction Course

- Introduction to Linux and Linux distributions
- Building a Linux virtual machine
- The Linux file system
- Text processing and regular expressions
- Access control and file permissions
- Searching for specific files

- Linux networking
- Managing processes
- Installing programs and services (webserver, mysql, ssh, dhcp)
- Bash scripting

www.iitc.co.il
avivab@iitc.co.il
IITC
החילזון 3, רמת גן | 077-4123211
לפרטים והרשמה
055-2780865

IITC
IT PROFESSIONAL ACADEMY

Module 4: Cloud

30 שעות

- Cloud Computing
- Cloud Models (Public/Private/Hybrid)
- Types of Cloud (IaaS/PaaS/SaaS)
- Introduction to Azure, Azure Services
- Virtual Machines
- Account & Subscription
- Azure Services, Azure Portal, Azure PowerShell
- CLI & Cloud Shell

Module 5: Ethical Hacking & Web Hacking

95 שעות

- OSINT, WHOIS and DNS enumeration
- Discovering live hosts
- Network, port scanning and OS fingerprinting (Nmap)
- Vulnerability analysis
- Remote control
- The Metasploit database
- Brute force attacks
- Privilege escalation: Windows
- Privilege escalation: Linux
- Lateral movement
- HTTP and the web stack
- OWASP top 10
- SQL injection
- Client-side injections (XSS, CSRF)
- OS command injections
- Denial of Service
- Local File Execution (LFI) and Remote File Inclusion (RFI)
- Working with Burp Suite

IITC
IT PROFESSIONAL ACADEMY

100 שעות

Module 6: Security Operation Center (SOC), EDR and Endpoint Security, SIEM

- SOC Services, SOC Types, SOC Rules, SOC Playbooks
- IP Investigation / Public Tools
- MITRE Attack – Tactics & Techniques
- Sandbox Solution
- LAB: IP Investigation & Report Creation
- How to Response to a Cyber Attack (NIST 800-61)
- Incident Response Plan
- Table Top Exercise - Ransomware Infection
- LAB: Creating Incident Response Plan
- Denial of Service
- Phishing Investigation
- Malware & Ransomware & RAT
- LAB: Simulation of RAT Investigation
- What is Event Viewer?
- Registry
- Task Scheduler & Persistance
- What is EDR?
- XDR, EDR, MDR - What are the differences
- EDR Installation and Configuration
- What is SIEM
- SIEM Types
- Data Collection: Syslog, CEF, API
- Wazuh Installation
- Wazuh Architecture - Elasticsearch, Logstash & Kibana
- Wazuh Configuration
- Kibana Query Language
- Rule Definition & Log Level

IITC
IT PROFESSIONAL ACADEMY

Module 7: Firewall

30 שעות

- Introduction to firewall Technologies and architecture
- Deployment Platforms
- Security Policy, rules and order of processing
- Logs and Monitoring Traffic and Connections
- Network Address Translation
- User Management and Authentication
- Application layer defenses

Module 8: Forensics

30 שעות

- What is digital forensics?
- What is an evidence?
- Evidence life cycle
- Files and File Systems
- Digital Forensics and Common Artifact
- Malware Analysts - Static and Dynamic
- Persistence (WMI/Startup/Schedule task/Registry)
- MITRE Attack – Tactics & Techniques