THROUGHSEC

Blue Team Course

Course Overview

The Blue Team course is designed to provide foundational skills and practical knowledge in defensive cybersecurity. This course introduces participants to critical tools, techniques, and methodologies for monitoring, analyzing, and defending IT systems against cyber threats. Through hands-on labs and scenarios, learners will gain real-world experience in securing modern IT infrastructures.

Course Modules

Module 1: Cybersecurity Basics

Overview:
This module introduces the fundamental principles of cybersecurity and the core concepts of blue team operations. Participants will learn about common threats, the CIA triad, and the roles of a blue team in protecting organizational assets.

Content:

- **Introduction to Cybersecurity**:
    - What is cybersecurity?
    - The importance of blue teams in cybersecurity operations.
- **Core Cybersecurity Concepts**:
    - CIA Triad (Confidentiality, Integrity, Availability)
    - Types of cyber threats (Malware, Phishing, Ransomware, Insider threats)
- **Defensive Security Frameworks**:
    - NIST Cybersecurity Framework
    - CIS Critical Security Controls

Module 2: Networking Fundamentals for Blue Teams

Overview:
Networking is the backbone of cybersecurity. This module covers essential networking concepts,

including protocols, packet analysis, and defensive mechanisms such as firewalls and VPNs. Participants will also learn how to use tools like Wireshark to analyze network traffic.

Content:

- **OSI Model & Networking Basics**:
    - Overview of the OSI Model (Application, Transport, Network, Data Link, Physical)
    - Common networking protocols (HTTP, DNS, TCP/IP, ICMP, UDP)
- **Packet Analysis**:
    - Introduction to Wireshark and other packet capture tools
    - Understanding packet capture (PCAP) files and analyzing network traffic
- **Network Defense Mechanisms**:
    - Firewalls and IDS/IPS systems
    - VPNs and Network Segmentation
    - Basic principles of NAT, port forwarding, and DMZ

Module 3: Security Information and Event Management (SIEM)

Overview:
SIEM systems are critical for collecting, analyzing, and correlating logs from diverse sources. This module introduces participants to popular SIEM tools and teaches them how to parse logs, write queries, and build dashboards for monitoring and threat detection.

Content:

- **SIEM Basics**:
    - What is SIEM and its role in cybersecurity defense?
    - Overview of popular SIEM tools (Splunk, ELK Stack, Graylog)
- **Log Management**:
    - Types of logs (System logs, Application logs, Network logs)
    - Collecting logs from different platforms (Windows, Linux, Networking Devices)
- **Log Parsing & Analysis**:
    - Log parsing techniques and filtering logs for relevant data
    - Creating custom SIEM queries to detect malicious activity

- **Building Dashboards**:
    - How to create dashboards and visualizations in SIEM tools
    - Using dashboards for proactive monitoring and alerting

Module 4: Endpoint Security

Overview:
Endpoints are a primary target for attackers. This module focuses on securing Windows and Linux systems by analyzing logs, monitoring activities, and implementing system hardening techniques to mitigate threats effectively.

Content:

- **Windows Endpoint Security**:
    - Windows Event Logs (Application, Security, System logs)
    - Detecting suspicious activity in Windows logs (Failed login attempts, privilege escalation)
    - Security configurations (Group Policies, Windows Defender)
- **Linux Endpoint Security**:
    - Linux log files (Syslog, auth.log, kern.log)
    - Monitoring user activity and process tracking (top, ps, netstat)
    - Hardening Linux systems: disabling unnecessary services, securing SSH
- **Endpoint Protection Tools**:
    - Antivirus/Antimalware solutions (Windows Defender, ClamAV)
    - Endpoint Detection and Response (EDR) solutions

Module 5: Threat Intelligence and Malware Analysis

Overview:
Understanding the threat landscape is crucial for proactive defense. This module introduces the basics of threat intelligence and malware analysis, helping participants recognize indicators of compromise and use frameworks like MITRE ATT&CK to inform defensive strategies.

Content:

- **Threat Intelligence Basics**:
    - What is threat intelligence?

    - Types of threat intelligence (Tactical, Operational, Strategic)
    - Using threat intelligence feeds to enhance defense
- **Indicators of Compromise (IoC)**:
    - What are IoCs and how to detect them?
    - Common IoCs: IP addresses, URLs, file hashes, and domain names
- **Malware Basics**:
    - Types of malware (Viruses, Trojans, Ransomware, Rootkits)
    - Tools and techniques for basic malware analysis
    - Using sandboxes for malware analysis
- **MITRE ATT&CK Framework**:
    - Introduction to MITRE ATT&CK and its relevance to blue teams
    - Mapping attack techniques to detection and mitigation

Module 6: Incident Response Fundamentals

Overview:
Incident response is at the heart of blue team operations. This module covers the lifecycle of incident response, from preparation to recovery. Participants will practice responding to simulated incidents, using playbooks and standardized methodologies to handle threats effectively.

Content:

- **Incident Response Lifecycle**:
    - Phases of incident response (Preparation, Detection, Containment, Eradication, Recovery)
    - Incident response best practices and playbooks
- **Initial Incident Detection**:
    - Recognizing signs of a security incident (e.g., unusual network traffic, alerts)
    - Using SIEM and other tools for incident detection
- **Containment & Eradication**:
    - Containment strategies (Isolating infected systems, blocking malicious IPs)
    - Removing malware and compromised accounts

- **Post-Incident Activities**:
    - Forensic analysis and evidence collection
    - Reporting and lessons learned to improve future defenses

---

Key Learning Outcomes

By the end of this course, participants will:

1. Understand the fundamentals of defensive cybersecurity operations.
2. Analyze and defend against network and endpoint threats.
3. Use SIEM tools for log analysis and threat detection.
4. Apply threat intelligence to enhance security posture.
5. Conduct incident response operations in simulated scenarios.

The **Blue Team Course** is designed for individuals seeking to develop defensive cybersecurity skills. Here are some key groups who would benefit from this course:

1. **Aspiring Cybersecurity Professionals**: Those new to the field of cybersecurity who want to specialize in defensive security roles such as SOC Analyst, Incident Responder, or Security Engineer.
2. **IT Professionals**: Individuals already working in IT roles like system administrators, network engineers, or IT support, looking to shift to a cybersecurity-focused role with an emphasis on defending systems and networks.
3. **Students in Cybersecurity**: College students pursuing a degree in cybersecurity, IT, or related fields who want to gain practical, hands-on experience in blue team operations.
4. **Incident Responders and SOC Analysts**: Those aiming to specialize in responding to security incidents, analyzing system logs, detecting anomalies, and maintaining the security of IT infrastructures.
5. **Network and System Security Engineers**: IT professionals who want to deepen their understanding of defensive security, particularly focusing on network defense mechanisms, endpoint protection, and incident response.
6. **Cybersecurity Consultants**: Freelancers or consultants who wish to add defensive security strategies to their toolkit, offering security assessments and incident response planning to organizations.