Training Course on Red Team and Blue Team Operations for Threat Hunters

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Training Course on Red Team and Blue Team Operations for Threat Hunters provides **cybersecurity professionals** with the **cutting-edge knowledge** and **hands-on skills** required to excel in modern **threat hunting**. Participants will gain a deep understanding of both **offensive (Red Team)** and **defensive (Blue Team)** strategies, enabling them to proactively identify, analyze, and neutralize advanced persistent threats (APTs) and sophisticated cyberattacks. Through **practical labs** and **real-world case studies**, attendees will learn to anticipate adversary tactics, enhance detection capabilities, and strengthen organizational resilience against evolving cyber threats.

The curriculum emphasizes a **purple teaming mindset**, fostering collaboration between offensive and defensive security functions. This holistic approach empowers **threat hunters** to not only uncover hidden vulnerabilities but also to develop robust **incident response** plans and implement **proactive defense mechanisms**. Graduates will be equipped to lead **security operations**, conduct advanced **digital forensics**, and contribute significantly to their organization's overall **cybersecurity posture** in an increasingly hostile digital landscape.

Programme Curriculum

Training Course on Red Team and Blue Team Operations for Threat Hunters

Introduction

Training Course on Red Team and Blue Team Operations for Threat Hunters provides **cybersecurity professionals** with the **cutting-edge knowledge** and **hands-on skills** required to excel in modern **threat hunting**. Participants will gain a deep understanding of both **offensive (Red Team)** and **defensive (Blue Team)** strategies, enabling them to proactively identify, analyze, and neutralize advanced persistent threats (APTs) and sophisticated cyberattacks. Through **practical labs** and **real-world case studies**, attendees will learn to anticipate adversary tactics, enhance detection capabilities, and strengthen organizational resilience against evolving cyber threats.

The curriculum emphasizes a **purple teaming mindset**, fostering collaboration between offensive and defensive security functions. This holistic approach empowers **threat hunters** to not only uncover hidden vulnerabilities but also to develop robust **incident response** plans and implement **proactive defense mechanisms**. Graduates will be equipped to lead **security operations**, conduct advanced **digital forensics**, and contribute significantly to their organization's overall **cybersecurity posture** in an increasingly hostile digital landscape.

Course Duration

10 days

Course Objectives

1. Understand and replicate **attacker methodologies**, including the **MITRE ATT&CK framework**, for realistic **Red Team engagements**.
2. Employ **proactive search techniques** across networks and endpoints to uncover **stealthy threats** and **zero-day exploits**.
3. Improve **detection, containment, eradication, and recovery** processes for rapid **breach mitigation**.
4. Design and deploy **resilient security architectures**, including **SIEM optimization** and **endpoint detection and response (EDR)**.
5. Acquire proficiency in **forensic investigation** and **malicious code analysis** to understand attack impacts.
6. Bridge the gap between offensive and defensive teams to create a **continuous feedback loop** for security improvement.
7. Streamline **alert triage**, automate **response playbooks**, and improve **threat intelligence integration**.
8. Identify vulnerabilities and apply **secure configurations** in **cloud environments (AWS, Azure, GCP)**.
9. Recognize and counter **phishing, pretexting, and social engineering attacks** through awareness and technical controls.
10. Identify and remediate **web application vulnerabilities** and **API security flaws**.
11. Utilize **packet analysis** and **flow data** to detect **anomalous behavior** and **network intrusions**.
12. Understand how **secure development lifecycles** can prevent vulnerabilities from the source.
13. Ensure adherence to **data privacy regulations (GDPR, CCPA)** and effectively report security posture to stakeholders.

Organizational Benefits

- Significantly reduce the risk of successful cyberattacks by identifying and addressing vulnerabilities before exploitation.
- Improve the speed and effectiveness of breach detection, containment, and recovery, minimizing business disruption and financial losses.
- Build a more resilient and adaptable defense against evolving threats, leading to increased organizational trust and continuity.
- Maximize the effectiveness of existing security tools and technologies through better integration and utilization.
- Ensure adherence to industry regulations and reduce overall cybersecurity risk exposure.
- Cultivate a highly skilled cybersecurity workforce capable of independently handling complex security challenges.
- Drastically cut down the time it takes to identify and remediate security incidents.
- Promote a strong, collaborative security-first mindset across the organization.

Target Audience

1. Threat Hunters
2. SOC Analysts
3. Incident Responders
4. Security Engineers
5. Penetration Testers
6. Security Architects
7. Cybersecurity Consultants
8. IT Security Managers

Course Outline

Module 1: Introduction to Red Team & Blue Team Fundamentals

- Defining Red Team, Blue Team, and Purple Team roles and objectives.
- Understanding the adversarial mindset and defensive strategies.
- Overview of the cyber kill chain and common attack vectors.
- Introduction to legal and ethical considerations in offensive security.
- **Case Study:** The NotPetya Ransomware Attack: Analyzing the initial compromise and the defensive failures.

Module 2: Threat Intelligence and Adversary Profiling

- Sources and types of **threat intelligence (Strategic, Tactical, Operational)**.
- Collecting and analyzing **OSINT (Open-Source Intelligence)** for target reconnaissance.
- Building **adversary profiles** and understanding their **TTPs (Tactics, Techniques, and Procedures)**.
- Integrating threat intelligence into security operations.
- **Case Study:** APT28 (Fancy Bear) Operations: Dissecting their intelligence gathering and targeting methods.

Module 3: Advanced Network Reconnaissance & Mapping

- Passive and active **network scanning** techniques.
- Identifying exposed services, vulnerabilities, and attack surfaces.
- Utilizing tools like Nmap, Shodan, and Censys for network discovery.
- Mapping network topography and identifying critical assets.
- **Case Study:** A corporate network compromise due to unpatched public-facing services discovered via OSINT.

Module 4: Initial Access Techniques (Red Team Focus)

- **Phishing and spear-phishing** campaigns for credential harvesting.
- Exploiting **client-side vulnerabilities** in browsers and applications.
- Utilizing **supply chain attacks** and trusted relationships.
- Bypassing common **perimeter defenses** like firewalls and IPS.
- **Case Study:** The SolarWinds Supply Chain Attack: How adversaries gained initial access through a trusted vendor.

Module 5: Command & Control (C2) and Persistence

- Establishing **covert communication channels** with compromised systems.
- Implementing various **persistence mechanisms** (registry, scheduled tasks, services).
- Evading **C2 detection** by network monitoring tools.

- Understanding **domain fronting** and other evasion techniques.
- **Case Study:** A banking trojan maintaining persistence and C2 channels within a financial institution's network.

Module 6: Lateral Movement and Privilege Escalation (Red Team Focus)

- Techniques for moving laterally across network segments (Pass-the-Hash, Kerberoasting).
- Exploiting **Active Directory vulnerabilities** for domain dominance.
- Leveraging **local privilege escalation** techniques on Windows and Linux.
- Using tools like Mimikatz, BloodHound, and CrackMapExec.
- **Case Study:** A ransomware group's rapid lateral movement and privilege escalation to encrypt an entire enterprise network.

Module 7: Data Exfiltration and Impact (Red Team Focus)

- Techniques for **data staging and exfiltration** (DNS tunneling, encrypted channels).
- Methods for **destroying or encrypting data** for impact.
- Understanding the exfiltration lifecycle and detection points.
- Simulating **data breach scenarios** and their potential consequences.
- **Case Study:** A nation-state actor exfiltrating sensitive intellectual property from a research firm.

Module 8: Endpoint Detection & Response (EDR) for Threat Hunters (Blue Team Focus)

- Understanding EDR capabilities for **real-time monitoring** and **threat detection**.
- Analyzing **endpoint telemetry** (process activity, file changes, network connections).
- Developing **custom detection rules** and **behavioral analytics**.
- Utilizing EDR tools to **contain and remediate** endpoint compromises.
- **Case Study:** Using EDR to detect and respond to fileless malware attacks that bypassed traditional antivirus.

Module 9: Network Security Monitoring and Traffic Analysis (Blue Team Focus)

- Deploying and configuring **IDS/IPS (Intrusion Detection/Prevention Systems)**.
- Deep packet inspection and **network flow analysis (NetFlow, IPFIX)**.
- Identifying **anomalous network traffic patterns** and known indicators of compromise (IOCs).
- Utilizing Wireshark, Zeek, and other network analysis tools.
- **Case Study:** Detecting C2 communication and data exfiltration attempts through DNS tunneling.

Module 10: SIEM Operations and Log Analysis for Threat Hunters (Blue Team Focus)

- Centralized **log collection and aggregation** from diverse sources.
- Developing effective **SIEM use cases** and **correlation rules**.
- Performing **advanced queries** and **data visualization** for threat hunting.
- Integrating **threat intelligence feeds** into SIEM for proactive alerting.
- **Case Study:** Correlating SIEM alerts to identify a multi-stage attack campaign, from initial access to lateral movement.

Module 11: Digital Forensics and Incident Response (DFIR) Essentials

- **Incident response lifecycle**: Preparation, Identification, Containment, Eradication, Recovery, Post-Incident Analysis.
- **Memory forensics** and volatile data acquisition.

- **Disk forensics** and artifact analysis.
- Chain of custody and legal considerations in digital investigations.
- **Case Study:** Post-breach analysis of a server compromised by a web shell, identifying the initial exploit and subsequent activities.

Module 12: Malware Analysis Fundamentals

- **Static and dynamic malware analysis** techniques.
- Identifying **malicious functionalities** and **packer detection**.
- Utilizing sandboxes and virtual environments for safe analysis.
- Extracting **IOCs** from malware samples.
- **Case Study:** Analyzing a custom backdoor used in a targeted attack to understand its capabilities and identify its C2 infrastructure.

Module 13: Cloud Security for Threat Hunters (AWS, Azure, GCP)

- Understanding **cloud attack vectors** and misconfigurations.
- Monitoring **cloud security logs** and events (CloudTrail, Azure Monitor).
- Implementing **Identity and Access Management (IAM)** best practices.
- Securing **containerized environments** (Docker, Kubernetes).
- **Case Study:** A public cloud account compromise due to weak IAM policies, leading to data exfiltration from storage buckets.

Module 14: Purple Teaming and Red/Blue Team Exercises

- Designing and executing effective **purple teaming exercises**.
- Developing **measurable metrics** for Red and Blue Team performance.
- Constructive feedback loops and continuous improvement processes.
- Simulating **realistic adversary scenarios** in a controlled environment.
- **Case Study:** A series of purple team exercises leading to a significant reduction in detection time for common attack patterns.

Module 15: Building a Threat Hunting Program & Future Trends

- Establishing a **dedicated threat hunting team** within an organization.
- Integrating threat hunting into existing **security operations**.
- Measuring the **maturity of a threat hunting program**.
- Emerging threats and future trends in cybersecurity (AI/ML in security, Quantum Computing threats).
- **Case Study:** A small organization successfully building out a foundational threat hunting capability with limited resources, leveraging open-source tools.

Training Methodology

This course adopts a highly interactive and practical training methodology, combining theoretical instruction with extensive hands-on labs and realistic simulations. The approach includes:

- **Instructor-Led Sessions**: Expert-led discussions on core concepts, methodologies, and best practices.
- **Hands-on Labs**: Practical exercises in a dedicated cyber range environment, allowing participants to apply learned techniques in real-world scenarios.
- **Case Studies and War Games**: Analysis of actual cyberattack scenarios and participation in simulated Red Team vs. Blue Team engagements to reinforce learning.

- **Tool Demonstrations and Usage**: Practical exposure to industry-standard offensive and defensive security tools.
- **Group Discussions and Collaboration**: Encouraging peer-to-peer learning and fostering a purple teaming mindset.
- **Capstone Project**: A comprehensive, simulated Red Team/Blue Team exercise to demonstrate integrated skills.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.com or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
07 Sep 2026	18 Sep 2026	Physical	$3,000
14 Sep 2026	25 Sep 2026	Physical	$3,000
21 Sep 2026	02 Oct 2026	Physical	$3,000
28 Sep 2026	09 Oct 2026	Physical	$3,000

Start Date	End Date	Location	Price
05 Oct 2026	16 Oct 2026	Physical	$3,000
12 Oct 2026	23 Oct 2026	Physical	$3,000
19 Oct 2026	30 Oct 2026	Physical	$3,000
26 Oct 2026	06 Nov 2026	Physical	$3,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com