



Defeating Advanced Adversaries - Purple Team Tactics and Kill Chain Defenses

Course Introduction:

In an increasingly complex cybersecurity landscape, organizations face sophisticated adversaries that employ advanced tactics to compromise systems and data. To effectively combat these threats, a collaborative approach is essential. This 5-day course, "Defeating Advanced Adversaries - Purple Team Tactics and Kill Chain Defenses," is designed to bridge the gap between offensive and defensive strategies through the integration of Red and Blue team methodologies.

Throughout this course, participants will gain a comprehensive understanding of Purple Teaming, where teams work together to enhance security posture by simulating real-world attacks while simultaneously improving defense mechanisms. We will explore the Cyber Kill Chain, a framework that outlines the stages of a cyber-attack, and learn how to identify and mitigate threats at each phase.

Participants will engage in exercises, utilizing threat intelligence and adversary emulation techniques to experience the dynamics of a Purple Team environment. By the end of this course, attendees will be equipped with skills and strategies to effectively defend against advanced adversaries, ensuring a more resilient cybersecurity framework for their organizations.

Course Objectives:

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

- Understand the concepts of Purple Teaming and the Cyber Kill Chain framework.
 - Analyze threat intelligence to identify and anticipate adversary tactics.
 - Emulate real-world attack scenarios using adversary emulation techniques.
 - Implement layered defensive strategies to mitigate threats at each Kill Chain phase.
 - Develop and refine incident response plans to effectively handle cyber incidents.
 - Collaborate effectively within Purple Teams to enhance organizational security posture.
 - Explore emerging trends and techniques in cybersecurity for future preparedness.
-

Who Should Attend?

This course is suitable for Cybersecurity Professionals, Security Analysts, Incident Responders, Penetration Testers, IT Managers and Directors, and DevOps and SRE Teams.

Course Outline:

Day 1: Introduction to Purple Teaming and the Cyber Kill Chain

- **Overview of Purple Teaming**
 - Understanding the concept of Purple Teaming
 - Roles and responsibilities of Red, Blue, and Purple teams
 - Benefits of a collaborative approach
- **The Cyber Kill Chain**
 - Introduction to the Kill Chain model
 - Phases of the Kill Chain: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command & Control, and Actions on Objectives
 - Case studies on successful and thwarted attacks

Day 2: Threat Intelligence and Adversary Emulation

- **Gathering and Analyzing Threat Intelligence**
 - Sources of threat intelligence (OSINT, commercial feeds, etc.)
 - Analyzing and leveraging threat intelligence for proactive defense
- **Adversary Emulation Techniques**
 - Techniques for simulating real-world attacks
 - Tools for adversary emulation (e.g., MITRE ATT&CK framework)
 - Developing scenarios for training and testing

Day 3: Defensive Strategies and Tools

- **Implementing Defensive Tactics**
 - Layered security approaches and defense-in-depth strategies
 - Endpoint detection and response (EDR) solutions
 - Network monitoring and intrusion detection systems (IDS)
- **Purple Team Exercises**
 - Exercises simulating real attack scenarios
 - Collaboration between Red and Blue teams during exercises
 - Debriefing and analyzing outcomes

Day 4: Incident Response and Mitigation Strategies

- **Incident Response Planning**
 - Developing and refining incident response plans
 - Roles and responsibilities during an incident
 - Communication strategies during incidents
- **Mitigation Techniques**
 - Techniques for mitigating attacks at different Kill Chain phases

- Post-incident analysis and lessons learned
- Continuous improvement of defensive strategies

Day 5: Advanced Tactics and Future Trends

- **Advanced Adversary Tactics**
 - Understanding advanced persistent threats (APTs)
 - Emerging tactics, techniques, and procedures (TTPs) from adversaries
- **Future of Cyber Defense**
 - Trends in cybersecurity and evolving threat landscapes
 - Preparing for the future: AI, machine learning, and automation in defense
 - Final collaborative exercise and course wrap-up

Course Methodology:

A variety of methodologies will be used during the course that including:

- (30%) Based on Case Studies
- (30%) Techniques
- (30%) Role Play
- (10%) Concepts
- Pre-test and Post-test
- Variety of Learning Methods
- Lectures
- Case Studies and Self Questionnaires
- Group Work
- Discussion
- Presentation

Course Certificate:

International Center for Training & Development (ICTD) will award an internationally recognized certificate(s) for each delegate on completion of training.

Course Fees:

To be advised as per course location. This rate includes participant's manual, Hand-Outs, buffet lunch, coffee/tea on arrival, morning & afternoon of each day.

Course Timings:

Daily Course Timings:

08:00 - 08:20	Morning Coffee / Tea
08:20 - 10:00	First Session
10:00 - 10:20	Coffee / Tea / Snacks
10:20 - 12:20	Second Session
12:20 - 13:30	Lunch Break & Prayer Break
13:30 - 15:00	Last Session

