BLACKBIRD FOR TRAINING

# Red Team Operations (CRTO) Training Course

18 – 22 January 2027
Kuala Lumpur (Malaysia)



# Red Team Operations (CRTO) Training Course

**Ref:** 3254925_182182 **Date:** 18 – 22 January 2027 **Location:** Kuala Lumpur (Malaysia) **Fees:** 4900 GBP

## Introduction

In today's rapidly evolving digital environment, cyber threats are becoming more sophisticated and persistent. Organizations across the Middle East and North Africa need proactive, advanced solutions to strengthen their security defenses. The Certified Red Team Operations CRTO certification provides the expertise needed to simulate real-world attacks, identify vulnerabilities, and build a robust security posture.

This course is designed for a wide range of professionals, from junior and mid-level team members looking to build core technical skills, to senior and executive-level decision-makers aiming to enhance strategic oversight of security operations. It caters to various sectors, including oil and gas, banking and financial services, telecommunications, government, human resources, project management, marketing, and sales.

Through in-depth instruction and practical exercises, this certification empowers participants to understand and execute Red Team operations effectively. By mastering the latest techniques and methodologies, participants will be better prepared to address security challenges and contribute to organizational resilience and productivity.

## Course Objectives

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

- Understand the core principles and purpose of Red Team Operations.
- Apply ethical attack simulation techniques and advanced testing methodologies.
- Use tools and processes to perform comprehensive Red Team engagements.
- Identify, document, and communicate security vulnerabilities effectively.
- Develop actionable plans to improve security posture and reduce risk.
- Collaborate with Blue Teams and other stakeholders to integrate defenses.
- Create structured reports to support executive decision-making.
- Stay informed of the latest trends and threats in ethical hacking and Red Teaming.



# Course Outlines

## Day 1: Introduction to Red Team Operations

- Define Red Teaming and its strategic role in cybersecurity programs.
- Differentiate Red Team Operations from traditional penetration testing.
- Identify the organizational goals and security priorities for Red Team initiatives.
- Discuss the current landscape of cyber threats and attacker tactics.
- Review core tools and frameworks for conducting ethical attack simulations.
- Understand legal and ethical considerations in Red Team activities.

## Day 2: Tools and Techniques for Attack Simulation

- Explore methods for network reconnaissance and data gathering.
- Analyze target environments to understand vulnerabilities and potential entry points.
- Study evasion techniques for bypassing intrusion detection and prevention systems.
- Learn about managing sessions and maintaining control during simulations.
- Evaluate exploitation methods and post-exploitation practices.
- Participate in exercises focused on foundational attack simulations in a controlled environment.

## Day 3: Advanced Exploitation and Control

- Learn techniques to escalate privileges and access sensitive data.
- Explore methods for bypassing advanced security defenses.
- Practice the use of remote administration and command tools.
- Identify vulnerabilities in real-world applications and systems.
- Analyze operational impacts and risk implications of exploitation.
- Conduct practical exercises simulating complex attack scenarios.

## Day 4: Integration and Collaboration with Defensive Teams

- Develop processes for integrating Red Team findings into organizational security.
- Understand how to communicate and collaborate with Blue Teams.
- Apply methods to avoid detection and maintain operational stealth.
- Practice documenting attack simulations and creating structured reports.
- Analyze performance data to identify gaps and recommend improvements.
- Review case studies on successful Red Team engagements.



### Day 5: Project Management and Final Assessment

- Create a complete Red Team Operations plan with defined objectives.
- Assign roles and responsibilities within the team and project scope.
- Develop communication strategies for engaging stakeholders and leadership.
- Address organizational, legal, and ethical considerations.
- Conduct a final assessment exercise to apply all learned skills.
- Present findings and participate in a wrap-up discussion with certification awarded upon completion.

## Why Attend this Course: Wins & Losses!

- Gain practical skills in real-world attack simulation and risk analysis.
- Build an in-depth understanding of Red Team methodologies and best practices.
- Identify vulnerabilities and develop actionable strategies to address them.
- Strengthen collaboration with defensive teams and improve organizational security.
- Achieve certification that demonstrates advanced skills and professional credibility.
- Access to hands-on exercises to reinforce skills and confidence.
- Learn from real-world examples and advanced case studies.
- Enhance organizational resilience and security awareness.
- Challenges include the need for foundational cybersecurity knowledge and possible implementation barriers without executive support.

## Conclusion

The Certified Red Team Operations CRTO certification provides a strategic and practical pathway for security professionals and leaders to strengthen their organizations' defenses against evolving cyber threats. Through a comprehensive curriculum that covers Red Team planning, execution, and analysis, participants gain the knowledge and experience needed to address vulnerabilities and enhance security readiness.

**This certification offers significant value to executives seeking to strengthen security strategies, team leaders aiming to build better integration with defensive teams, and specialists wanting to expand their expertise in advanced attack simulation. By completing this course, participants position themselves as trusted resources in building secure and resilient digital environments.**

