Datastat Research
Building Capacity in Training and Research

DATASTAT TRAINING IN

OFFICIAL COURSE PROSPECTUS

Center for Advanced Research & Professional Development

Nairobi Training Center • Global Virtual Academy • Corporate On-Site

DEFENSE AND SECURITY

Red Team Operations and Adversarial Simulation Training Course

Comprehensive Course Syllabus, Practical Modules & Upcoming Schedules

PROGRAM SPECIFICATIONS & HIGHLIGHTS

DURATION
5 Days Practical Hands-on

DELIVERY MODES
In-Person Class & Live Virtual

CERTIFICATION
Accredited Certificate of Completion

INTAKES / DATES
Multiple Cohort Schedules Included

PREPARED FOR:

Valued Participant

Email: training@datastatresearch.org | Issued: November 21, 2026

Academic & Professional Training Year: 2026

DATASTAT TRAINING INSTITUTE

P.O. Box 102802-00101, Nairobi, Kenya

Training Centers: Nairobi • Mombasa • Kigali • Dubai • Live Virtual Academy

Tel: +254 724 527 104 | +254 734 969 612

Email: training@datastatresearch.org

www.datastatresearch.org

Red Team Operations and Adversarial Simulation Training Course

Defense and Security • 5 Days Intensive • Accredited Certification

Course Overview

Red Team Operations and Adversarial Simulation Training Course provides an advanced framework for organizations to assess, enhance, and test their cybersecurity, operational resilience, and strategic defense capabilities.

Key Skills & Software Tools Covered

MS Word • CALDERA • Cobalt Strike • and Metasploit

Upcoming Training Schedules

Confirmed cohort intakes and venues. Both physical in-person classroom and live virtual online seats are available.

TRAINING DATES	LOCATION / VENUE	FORMAT / DURATION	INVESTMENT (FEE)
29 Dec 2025 – 2 Jan 2026	Nairobi	Classroom / 5d	**$1,500 USD / KES 110,000**
29 Dec 2025 – 2 Jan 2026	Kigali	Classroom / 5d	**$3,000 USD / KES 90,000**
29 Dec 2025 – 2 Jan 2026	Dubai	Classroom / 5d	**$5,000 USD / KES 90,000**
29 Dec 2025 – 2 Jan 2026	Cape Town	Classroom / 5d	**$4,500 USD / KES 90,000**
29 Dec 2025 – 2 Jan 2026	Addis Ababa	Classroom / 5d	**$3,000 USD / KES 90,000**
29 Dec 2025 – 2 Jan 2026	Singapore	Classroom / 5d	**$5,000 USD / KES 90,000**
29 Dec 2025 – 2 Jan 2026	Istanbul	Classroom / 5d	**$5,000 USD / KES 90,000**
29 Dec 2025 – 2 Jan 2026	Bangkok	Classroom / 5d	**$5,000 USD / KES 90,000**
29 Dec 2025 – 2 Jan 2026	Accra	Classroom / 5d	**$4,000 USD / KES 90,000**
5 Jan 2026 – 9 Jan 2026	Nairobi	Classroom / 5d	**$1,500 USD / KES 110,000**
5 Jan 2026 – 9 Jan 2026	Kigali	Classroom / 5d	**$3,000 USD / KES 90,000**
5 Jan 2026 – 9 Jan 2026	Dubai	Classroom / 5d	**$5,000 USD / KES 90,000**

* Corporate discounts and customized cohort scheduling are available for teams of 3 or more participants.

Course Curriculum & Modules

Red Team Operations and Adversarial Simulation Training Course

Introduction

Red Team Operations and Adversarial Simulation Training Course provides an advanced framework for organizations to assess, enhance, and test their cybersecurity, operational resilience, and strategic defense capabilities. This course equips participants with the knowledge and practical tools to emulate realistic threat actors, perform adversarial simulations, and identify systemic vulnerabilities in both digital and physical environments. Participants will learn how Red Teams operate to anticipate attacks, exploit weaknesses, and provide actionable recommendations to improve organizational preparedness, risk management, and decision-making under high-pressure scenarios.

The course emphasizes the integration of threat intelligence, attack simulation frameworks, and organizational risk assessment methodologies to strengthen defenses and proactively mitigate threats. Participants will gain hands-on experience in planning and executing Red Team operations, understanding attacker TTPs (tactics, techniques, and procedures), and designing adversarial exercises that enhance situational awareness. By linking simulated operations with strategic security planning, learners will develop the skills to anticipate, detect, and respond to evolving threats while improving cross-functional collaboration and resilience.

Course Objectives

- Understand the fundamentals of Red Team operations and adversarial simulation.

- Apply threat intelligence to anticipate potential attack vectors.
- Identify organizational vulnerabilities across digital and physical domains.
- Plan, execute, and report on realistic adversarial exercises.
- Integrate attack simulation frameworks into security governance structures.
- Analyze attack patterns, TTPs, and threat actor behaviors.
- Evaluate organizational risk management and incident response capabilities.
- Design scenarios to test both technical and human factors vulnerabilities.
- Apply ethical hacking principles in controlled, simulated environments.
- Enhance cross-functional coordination during security assessments.
- Develop actionable recommendations for strengthening defenses.
- Assess the effectiveness of existing cybersecurity tools and protocols.
- Foster a culture of proactive security awareness and continuous improvement.

Organizational Benefits

- Improved detection of operational and cybersecurity vulnerabilities
- Enhanced threat anticipation and proactive mitigation strategies
- Increased organizational resilience and readiness against attacks
- Better-informed decision-making through actionable simulation insights
- Strengthened incident response capabilities
- Optimized allocation of security resources
- Enhanced staff awareness and preparedness
- Improved compliance with industry and regulatory standards
- Stronger collaboration between IT, security, and operational teams
- Increased confidence in organizational risk management frameworks

Target Audiences

- Security analysts and cyber defense teams
- Risk management and compliance officers
- IT and cybersecurity managers
- Critical infrastructure operators
- Incident response and SOC personnel
- Penetration testers and ethical hackers
- Executive leadership and strategy teams
- Security consultants and auditors

Course Duration: 5 days

Course Modules

Module 1: Introduction to Red Team Operations

- Fundamentals of Red Teaming and its role in organizational security
- Differences between Red, Blue, and Purple Teams
- Legal, ethical, and regulatory considerations
- Overview of adversarial simulation methodologies
- Planning Red Team exercises aligned with organizational goals
- Case Study: Red Team engagement uncovering critical operational weaknesses

Module 2: Threat Intelligence and Attack Simulation

- Gathering and analyzing threat intelligence
- Mapping attacker profiles and TTPs
- Threat modeling for digital and physical environments
- Leveraging intelligence to guide Red Team planning
- Prioritizing high-risk assets and systems
- Case Study: Simulating APT attacks on financial institutions

Module 3: Vulnerability Assessment and Reconnaissance

- Techniques for open-source intelligence (OSINT) collection
- Network and system reconnaissance tools
- Social engineering and human factors analysis
- Identifying physical and procedural vulnerabilities
- Risk prioritization based on vulnerability impact
- Case Study: Reconnaissance uncovering gaps in enterprise security

Module 4: Planning and Executing Red Team Operations

- Designing realistic attack scenarios
- Defining objectives, rules of engagement, and success metrics
- Coordinating multi-domain operations
- Contingency planning and operational risk management
- Reporting and documenting operational findings
- Case Study: Multi-stage penetration exercise on a corporate network

Module 5: Social Engineering and Human Factor Exploitation

- Phishing, vishing, and pretexting techniques
- Behavioral analysis and manipulation strategies
- Assessing employee awareness and response protocols
- Mitigating risks associated with human vulnerabilities
- Integrating social engineering into broader Red Team exercises
- Case Study: Social engineering attack revealing insider weaknesses

Module 6: Technical Exploitation and Cyber Attack Simulation

- Network penetration testing and exploitation methods
- Application-level vulnerabilities and attack vectors
- Bypassing security controls and defenses
- Logging, monitoring, and evasion techniques
- Integrating technical exploits with operational simulations
- Case Study: Red Team technical breach in a simulated cloud environment

Module 7: Reporting, Debriefing and Recommendations

- Structuring actionable Red Team reports
- Communicating findings to technical and executive stakeholders
- Prioritizing recommendations based on risk and impact
- Lessons learned for continuous improvement
- Aligning simulation results with governance and compliance frameworks
- Case Study: Executive briefing transforming security policies

Module 8: Continuous Improvement and Security Culture

- Measuring effectiveness of Red Team operations
- Integrating findings into incident response and risk management
- Enhancing cross-team collaboration and awareness
- Developing long-term strategies for adversarial preparedness
- Building a proactive security culture organization-wide
- Case Study: Institutionalizing Red Team exercises in a multinational company

Training Methodology

- Instructor-led lectures and scenario discussions
- Hands-on simulation exercises in controlled environments
- Case study analysis and group problem-solving
- Collaborative planning and execution of Red Team exercises
- Practical templates for vulnerability assessment, reporting, and mitigation
- Feedback sessions and debriefings to reinforce learning

Register as a group from 3 participants for a Discount

Send us an email: info@datastatresearch.org or call +254724527104

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.

f. Payment should be done at least a week before commence of the training, to DATASTAT CONSULTANCY LTD account, as indicated in the invoice so as to enable us prepare better for you.

Certification & Learning Methodology

- Hands-on practical delivery with real-world datasets, case studies, and lab exercises.
- Post-training mentorship, access to class resources, and customized follow-up support.
- Participants who successfully complete the course receive an accredited Datastat Certificate of Completion.

How to Enroll & Reserve Your Seat

1. Online Registration: Visit https://datastatresearch.org/courses/red-team-operations-and-adversarial-simulation-training-course to register online.
2. Email Booking: Send participant details to training@datastatresearch.org for official invoice & reservation.
3. Support & Assistance: Inquire via phone +254 724 527 104 | +254 734 969 612.