

No. 126

CYBERSECURITY

Red Teaming and Purple Teaming

Testing and improving your defences through realistic adversary simulation

oJAYo.com

oJAYo

FREE SAMPLE · ojayo.com

SECTRAININGNOW SERIES · NO. 126

Red Teaming and Purple Teaming

Testing and improving your defences through realistic adversary simulation

oJAYo
Published by oJAYo.com

FREE SAMPLE · ojayo.com

Red Teaming and Purple Teaming

Testing and improving your defences through realistic adversary simulation

First edition, 2026. Copyright © 2026 oJAYo. Published by oJAYo.com. All rights reserved. No part of this book may be reproduced or shared without written permission, except for brief quotations in reviews.

This book is an independent publication. Product, framework and tool names mentioned in this book are trademarks of their respective owners. All other product names are trademarks of their respective owners. oJAYo.com is not affiliated with, sponsored by or endorsed by any vendor named in this book.

The information in this book is provided for general education. AI products, features, plans, prices and policies change frequently; always confirm details in the vendor's current documentation. Screens marked “Illustration” are simplified drawings, not captures of real software. Company and person names in examples are fictional.

[ISBN: add if registered]

FREE SAMPLE · ojayo.com

CONTENTS

How to use this book 1

PART I · FOUNDATIONS

1 What red teaming is 5
2 What purple teaming is 6
3 Pen tests, red teams and purple teams 7
4 Why it matters 8
5 The teams 9
6 Threat-led testing 10
7 Objectives 11
8 Safety 12
9 Legal and ethical rules 13
10 Frameworks and schemes 14

PART II · RED TEAM EXERCISES

11 The lifecycle 16
12 Planning 17
13 Threat intelligence 18
14 Scenarios 19
15 How attacks unfold 20
16 Detection opportunities 21
17 Stealth 22
18 Measuring response 23
19 Reporting 24
20 Replay and remediation 25

PART III · PURPLE TEAMING

21 The purple team loop 27
22 Mapping with MITRE ATT&CK 28
23 Adversary emulation plans 29

FREE SAMPLE · ojayo.com

24 Test libraries 30
25 Running a session 31
26 Measuring coverage 32
27 Detection engineering 34
28 Metrics 35
29 Continuous testing 36
30 Tabletop exercises 37

PART IV · PRACTICE

31 For smaller organizations 39
32 Tools 40
33 AI in red and purple teaming 41
34 Culture 42
35 Careers 43
36 Common mistakes 44
37 Worked example: red team 45
38 Worked example: purple team 46
39 A maturity path 47
40 A learning path 48
Checklists 49
Glossary 50
Further reading 51

FREE SAMPLE · ojayo.com

BEFORE YOU BEGIN

How to use this book

What this book covers, who it is for, and how to use it.

A **red team** plays the part of a real attacker, with permission, to test whether an organization can detect and respond to an attack. A **purple team** brings attackers and defenders into the same room so they can improve detections together, technique by technique.

This beginner's book explains both practices from the defender's point of view: why they exist, how exercises are planned and kept safe, how threat intelligence shapes them, how purple teams measure and improve detection coverage, and how organizations of different sizes can start. It explains concepts and process, not attack techniques.

What this book covers

- Red teams, blue teams, purple teams and control teams.
- Objectives, rules of engagement, safety and the law.
- Threat-led frameworks such as TIBER-EU and DORA TLPT.
- The red team lifecycle and reporting.
- Purple teaming with MITRE ATT&CK, test libraries and metrics.
- Tools, AI, culture, careers and a maturity path.

Who this book is for

- **SOC analysts and detection engineers.**
- **Security managers** commissioning exercises.
- **Testers** moving towards adversary simulation.

FREE SAMPLE · ojayo.com

How the book is organized

- **Part I — Foundations** (Chapters 1–10): red teams, purple teams, how they differ from penetration tests, why they matter, the teams involved, threat intelligence, objectives, safety, the law, and frameworks.
- **Part II — Red team exercises** (Chapters 11–20): lifecycle, planning, intelligence, scenarios, how attacks unfold, detection opportunities, stealth, measuring response, reporting and replay.
- **Part III — Purple teaming** (Chapters 21–30): the purple loop, ATT&CK mapping, emulation plans, test libraries, running a session, coverage, detection engineering, metrics, continuous testing and tabletop exercises.
- **Part IV — Practice** (Chapters 31–40): smaller organizations, tools, AI, culture, careers, mistakes, two worked examples, maturity and a learning path.
- **Reference**: checklists, glossary and further reading.

Callouts

TIP

Practical advice you can use straight away.

IN PRACTICE

How an idea looks in real exercises.

WATCH OUT

Common mistakes and risks.

KEY IDEA

The one thing to remember from a section.

FREE SAMPLE · ojayo.com

A note on authorization

Red and purple team activity is only legitimate with written authorization from the organization being tested. Screens are **simplified illustrations**.

FREE SAMPLE · ojayo.com

PART I

Foundations

These chapters explain what red and purple teams are, why they exist and the rules that keep them safe.

FREE SAMPLE · ojayo.com

CHAPTER 1

What red teaming is

A red team simulates a real adversary.

A definition

Red teaming is an authorized, goal-based simulation of a realistic attacker. Instead of listing every weakness, the red team tries to achieve a specific objective, such as reaching a sensitive system, while most defenders do not know an exercise is happening.

What it tests

A red team tests the whole defence: technology, processes and people. The key questions are whether the attack is noticed, how quickly, and whether the response stops it.

KEY IDEA

A red team exercise measures your ability to detect and respond, not just your weaknesses.

FREE SAMPLE · ojayo.com

CHAPTER 2

What purple teaming is

Purple teaming is collaboration.

Purple teaming combines red (attack) and blue (defence). The red side runs a technique openly; the blue side checks whether it was prevented, detected or missed; both improve the defence and test again. It turns findings into better detections immediately.

A mandatory step in some schemes

The updated **TIBER-EU** framework, published by the European Central Bank in February 2025, made purple teaming a mandatory part of its tests, in line with the EU's DORA rules.

FREE SAMPLE · ojayo.com

CHAPTER 3

Pen tests, red teams and purple teams

Three related activities.

Activity	Main question	Defenders know?
Penetration test	what weaknesses exist?	usually yes
Red team	can we detect and respond?	few people
Purple team	how do we detect this better?	yes, together

Figure 3.1 Penetration test, red team and purple team

Which first

Most organizations should run penetration tests and fix basic weaknesses first. Red team exercises give most value once logging, EDR and an incident response process exist.

FREE SAMPLE · ojayo.com

The oJAYo library

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

SAP SECURITY · 67 BOOKS

SAP Role Design Handbook
Access Control Field Guide
Signavio Process Governance
ABAC in Practice
Auditing SAP Systems
Securing SAP BTP
Securing SAP Fiori
SAP User Training Playbook
SAP Basis Essentials
SAP HANA Security
SAP Authorization Troubleshooting
HR and Payroll Security
Finance and Procurement Authorizations
BW and BusinessObjects Security
SAP Network and Web Security
SAP Security Interview Guide
SAP Cloud ALM Security
SAP Data Services Security
SAP Architecture Explained
SAP SD Security
SAP CRM Security
SAP SRM Security
SAP Ariba Security
SailPoint for SAP
SAP PP Security
SAP QM Security
PI/PO and Integration Suite Security
SAPUI5 Security
Testing in SAP Cloud ALM with Jira
SAP SLT Security
SAP PS Security
SAP Plant Maintenance Security
SAP EWM Security
SAP Digital Manufacturing Security
SAP SuccessFactors Security
Security in SAP Activate
SAP Concur Security
SAP Fieldglass Security
SAP Analytics Cloud Security
SAP Datasphere and Business Data Cloud Security
SAP Build and Work Zone Security
Joule and SAP Business AI Security
SAP MDG Security
SAP TM Security
SAP IBP Security
SAP GTS Security
SAP Sales, Service and Commerce Cloud Security
SAP S/4HANA Cloud Public Edition Security
SAP Business One and ByDesign Security
SAP Identity Management Migration
SAP Security Patching
Threat Detection and SIEM for SAP
Data Privacy (GDPR) for SAP
RISE with SAP Security
Ransomware and Incident Response for SAP
Compliance Mapping for SAP
Third-Party and Support Access for SAP
SAP Process Control and Risk Management
SAP Cloud Identity Access Governance
SAP Cloud Identity Services
SAP System Hardening
SAP Certificates and Encryption
SAP Penetration Testing
SAP Security Roadmap
Secure Development on SAP BTP
SAP Data Custodian and Data Sovereignty
Threat Intelligence for SAP

CYBERSECURITY · 64 BOOKS

Zero Trust Networks
Productivity at Work
ABAP Custom Code Security
S/4HANA Conversion Role Redesign
Getting Started with Canva AI
Getting Started with Character.AI
Getting Started with DeepL
Getting Started with Perplexity
Prompt Engineering
Cybersecurity Basics
Python for Beginners
JavaScript for Beginners
DevOps and Platform Engineering
AI-Powered Cyber Attacks
Securing AI Agents and Shadow AI
Ransomware
Phishing and Social Engineering
Deepfakes and Identity Fraud
Post-Quantum Cryptography
Software Supply Chain Security and DevSecOps
OT and Industrial Security
Sovereign Cloud and Data Sovereignty
Geopolitical Cyber Risk
Cloud Security and Identity Protection
Identity and Access Management Basics
Privileged Access Management
Passwordless and Passkeys
Identity Threat Detection and Response
SSO and Federation
AWS Security Fundamentals
Microsoft Azure and Entra ID Security
Google Cloud Security
Kubernetes and Container Security

FREE SAMPLE · ojayo.com

The oJAYo library (continued)

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

Cloud Security Posture Management
Serverless Security
OWASP Top 10 for Web Applications
API Security
Secure Coding Practices
Threat Modeling
Mobile App Security
SOC Fundamentals
Incident Response Planning
Digital Forensics
Threat Hunting
EDR and XDR
Malware Analysis Basics
Ethical Hacking for Beginners
Red Teaming and Purple Teaming (you are read…
Bug Bounty Hunting
CTF for Beginners
Data Loss Prevention
Encryption Basics
Privacy Engineering and Privacy by Design
Data Classification and Governance
NIST CSF 2.0
ISO 27001
SOC 2 for Startups
PCI DSS 4.0
HIPAA Security for Healthcare
Third-Party and Vendor Risk Management
Email Security: DMARC, SPF and DKIM
IoT and Smart Device Security
Cyber Insurance
Security Awareness Training Programs

AI · 11 BOOKS

Working with Claude
Working with ChatGPT
Getting Started with Google Gemini
Getting Started with DeepSeek
Getting Started with Grok
Getting Started with Microsoft Copilot
Agentic AI Explained
MCP: The Model Context Protocol
Vibe Coding
AI Coding Tools
AI Detection

CERTIFICATION GUIDES · 28 BOOKS

CompTIA Security+ Study Guide
ISC2 CC Study Guide
ISC2 CISSP Study Guide
ISACA CISM Study Guide
ISACA CISA Study Guide
ISACA CRISC Study Guide
ISC2 CCSP Study Guide
CompTIA CySA+ Study Guide
CompTIA PenTest+ Study Guide
EC-Council CEH Study Guide
OffSec OSCP+ Study Guide
CompTIA SecurityX Study Guide
GIAC GSEC Study Guide
AWS Certified Security - Specialty Study Guide
Microsoft Security Certifications Study Guide
CompTIA SecAI+ Study Guide
ISACA AAISM Study Guide
ISACA AAIA Study Guide
ISACA AAIR Study Guide
IAPP AIGP Study Guide
ISO/IEC 42001 Lead Implementer and Lead Auditor…
AWS Certified AI Practitioner Study Guide
AWS Certified Machine Learning Engineer - Associ…
AWS Certified Generative AI Developer - Profession…
Microsoft AI-901 Study Guide
Microsoft AI-103 Study Guide
Google Cloud Generative AI Leader Study Guide
Google Cloud Professional Machine Learning Engin…

BUNDLES · 18 PACKS, SAVE UP TO $145

SAP Security Starter Pack (5 books, $149)
SAP GRC and Audit Pack (5 books, $129)
S/4HANA Migration Security Pack (4 books, $109)
SAP Cloud Security Pack (5 books, $129)
SAP Threat Defense Pack (5 books, $129)
Cybersecurity Starter Pack (5 books, $129)
Identity and Access Pack (5 books, $129)
Cloud Security Pack (6 books, $149)
SOC and Incident Response Pack (5 books, $129)
Application Security Pack (5 books, $129)
Security Compliance Pack (5 books, $129)
Ethical Hacking Pack (5 books, $129)
AI at Work Pack (5 books, $129)
AI Developer Pack (5 books, $129)
AI Security and Governance Pack (5 books, $129)
CISSP + Security+ Exam Pack (2 books, $79)
ISACA Exam Pack (3 books, $99)
AI Certification Pack (4 books, $109)

END OF FREE SAMPLE

Red Teaming and Purple Teaming

Enjoyed it? The full book has 56 pages and 40 chapters.
Instant PDF download, $49.

Get the full book

ojayo.com · Created by the oJAYo expert team

This sample may be shared freely. The full book is licensed to one reader.