TLP: CLEAR

Enhancing Organizational Cyber Resilience Through Red Team Exercise

Abrão Ximenes

abraoximenes@nog.tl

TLNO2 Conference

November 21, 2025

TLP: CLEAR

Abstract

This paper highlights how Red Team exercises play a vital role in enhancing cyber resilience by simulating realistic attacks on people, processes, and technology. It covers the cyber threat landscape, cyber resilience frameworks, the differences between Red Team exercises and penetration testing, communication flows among involved teams, the Red Team exercise lifecycle, and the essential frameworks and competency certifications required. A demonstration of Red Team infrastructure is presented as a critical component of the exercise, emphasizing its importance in enabling realistic attack simulations, managing compromised targets, and ensuring the effectiveness of Red Team operations. Overall, the presentation underscores how proactive Red Team exercises help organizations identify vulnerabilities, strengthen defenses, and improve response capabilities against sophisticated cyber threats

TLP: CLEAR

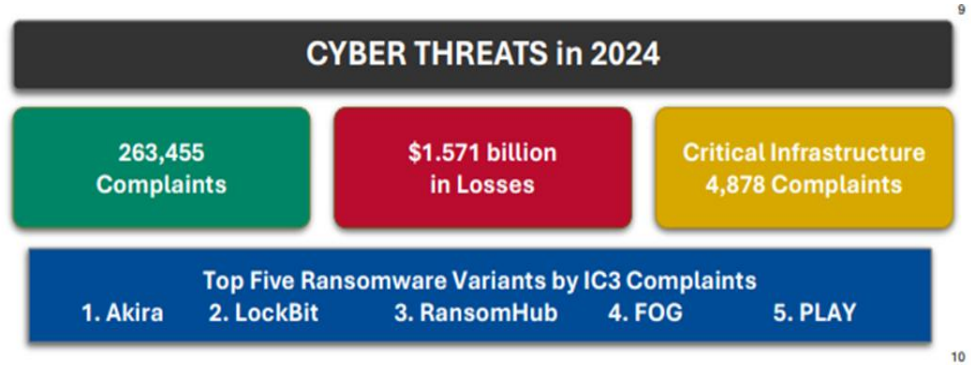
Agenda

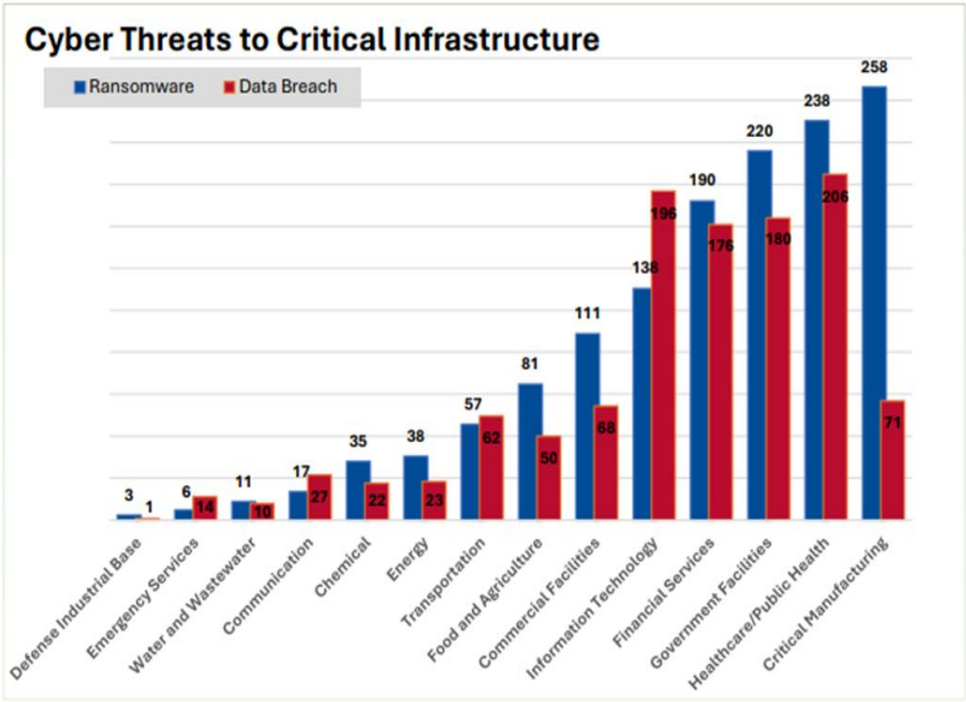
- Cyber Threat Landscape
- Cybersecurity and Cyber Resilience Framework
- Cyber Resilience Testing and Assessment Framework
- What Is Red Team? Role of Red Team Exercise in Cyber Resilience
- Difference between Red Team and Penetration Testing
- Communication Flow in Red Team Exercise
- Red Team Exercise Lifecycle
- Red Team Frameworks
- Certification Body and Qualification
- Demo Red Team Infrastructure

TLP: CLEAR

Cyber Threat Landscape

	Motivations (%)			
Sector	**Espionage**	**Sabotage**	**Cybercrime**	**Hacktivism**
Aerospace and Defence	72	8	17	3
Asset and Wealth Management	31	0	69	0
Automotive	22	0	72	6
Construction	12	9	76	3
Education	56	1	42	1
Energy	44	17	34	5
Financial Services	35	2	59	4
Food and Agriculture	44	4	48	4
Government	73	9	15	3
Healthcare	31	3	66	0
Hospitality and Leisure	21	3	73	3
Legal	36	2	57	5
Manufacturing	31	3	63	3
Media and Entertainment	50	5	40	5
Pharmaceuticals and Life Sciences	38	3	59	0
Professional Services	24	5	69	5
Resources and Mining	35	5	55	5
Retail	9	2	89	2
Technology	55	5	38	2
Telecommunications	66	5	28	1
Transport and Logistics	37	8	51	4



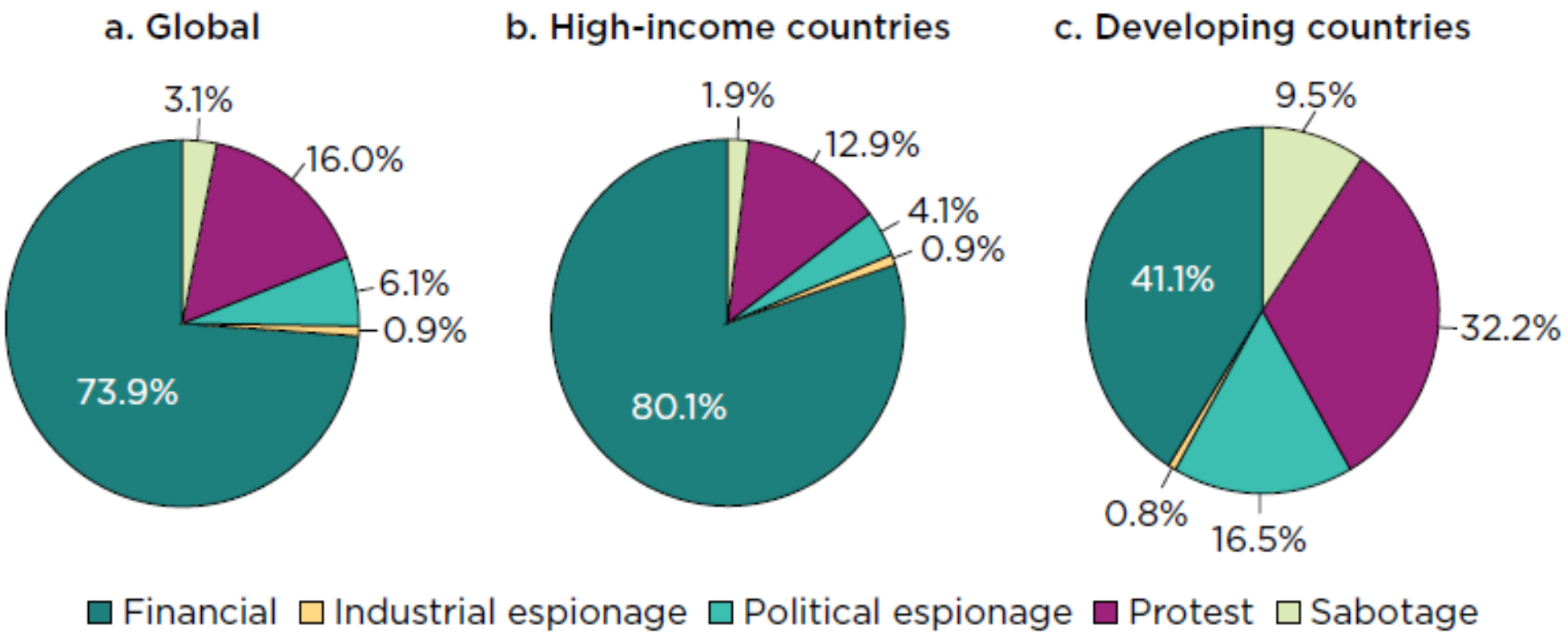


https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect.html

Source: FBI Internet Crime Report 2024

TLP: CLEAR

FIGURE 1.11 Distribution of disclosed cyber incidents, by motive and income group, 2014–23



World Bank Group Publication 2024: Cybersecurity Economics for Emerging Markets https://openknowledge.worldbank.org/entities/publication/4ec1bf22-3658-4d69-b9d3-43122254bc66

TLP: CLEAR

Cyber Security & Cyber Resilience

- Cyber security focuses on **protecting** information systems, networks, and data from attacks, unauthorized access, damage, or theft
- **Prevent** incidents from occurring
- **Cyber Security**: Firewalls, antivirus, and patch management, Intrusion detection and prevention, access control and encryption, Security policies and awareness training
- Cyber resilience focuses on organization's ability to continue operating even when facing cyberattacks
- Cyber Resilience includes cybersecurity but goes beyond it by emphasizing **continuity, response, and recovery**
- **Cyber resilience:** BCP, DRP, Red Team Exercise, Crisis Communication and Coordination, CTI and adaptive defense

TLP: CLEAR

- **Cybersecurity:** make sure the ship doesn’t leak and no pirates can board
- **Cyber Resilience:** ensure that even if the ship leaks or is attacked, it can stay afloat, repair itself, and reach its destination

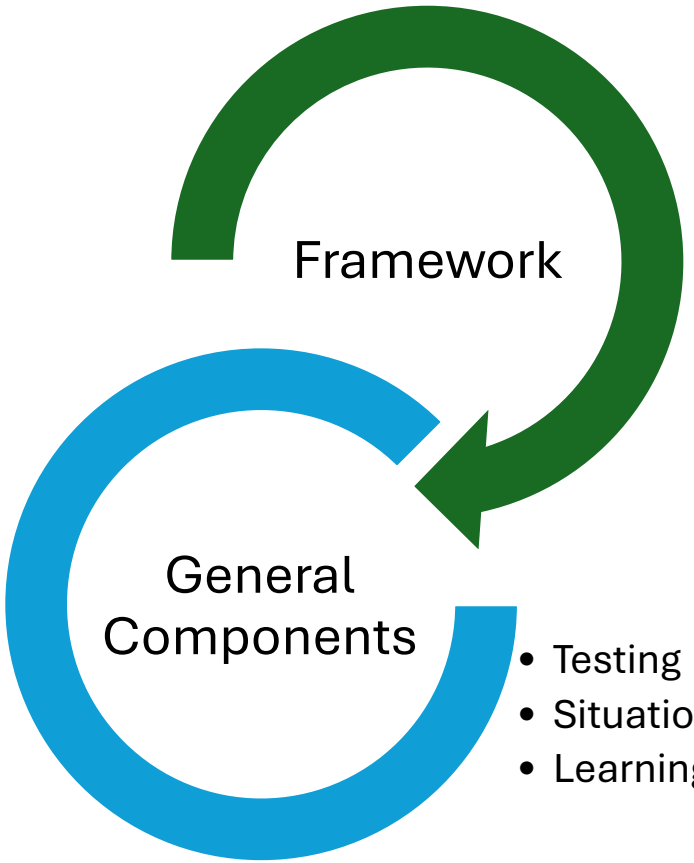
TLP: CLEAR

Cyber Security & Cyber Resilience

Aspects	Cyber Security	Cyber Resilience
Focus	Protect and prevent attacks	Maintain operations during and after attacks
Approach	Defensive and control-based	Adaptive and response-oriented
Scope	Technical (IT protection controls)	Holistic (people, process, technology, governance)
Objective	Security of systems and data	Continuity of services and public trust
Examples	Firewalls, patching, IAM, IDS/IPS	BCP, DRP, RT, crisis simulation
Mindset	We must not be attacked	Attacks will happen, but we must keep going

TLP: CLEAR

Cyber Resilience



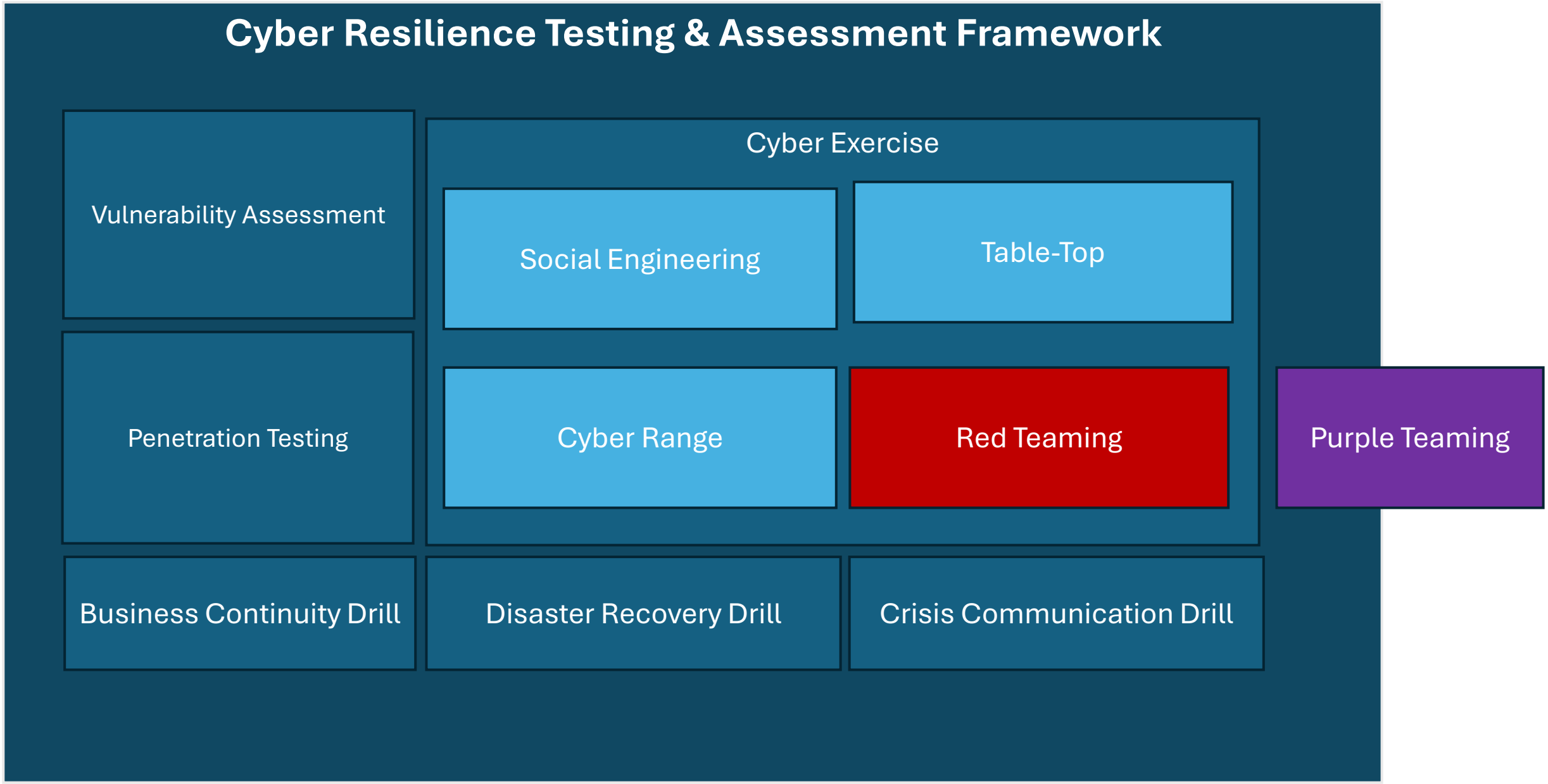
- Governance
- Identification
- Protection
- Detection
- Response
- Recovery

- Testing
- Situational Awareness
- Learning and Evolving

Global Policy and Regulatory Trends

- BIS Guidance on Cyber Resilience for Financial Market Infrastructures
- IMF & World Bank Cyber Resilience Framework for Financial Institutions
- NIST Cybersecurity Framework 2.0 emphasizes Governance and Resilience
- EU Digital Operational Resilience Act (DORA, 2022)

TLP: CLEAR


Cyber Resilience Testing & Assessment Framework
Vulnerability Assessment
Penetration Testing
Cyber Exercise
Social Engineering
Table-Top
Cyber Range
Red Teaming
Purple Teaming
Business Continuity Drill
Disaster Recovery Drill
Crisis Communication Drill

TLP: CLEAR

What Is Red Team? Role in Cyber Resilience

- A proactive and realistic cybersecurity simulation designed to measure and enhance an organization's resilience
- Red Teaming adopts a broader, intelligence-driven approach to evaluate an organization's overall security posture and resilience
- Testing Security Controls in Realistic Scenarios
- Improving Detection and Response Capabilities
- Strengthening Policies, Procedures, and Governance
- Encouraging Collaboration and a Purple Team Approach
- Enhancing Threat Awareness and Preparedness

TLP: CLEAR

Red Team Vs Pentest

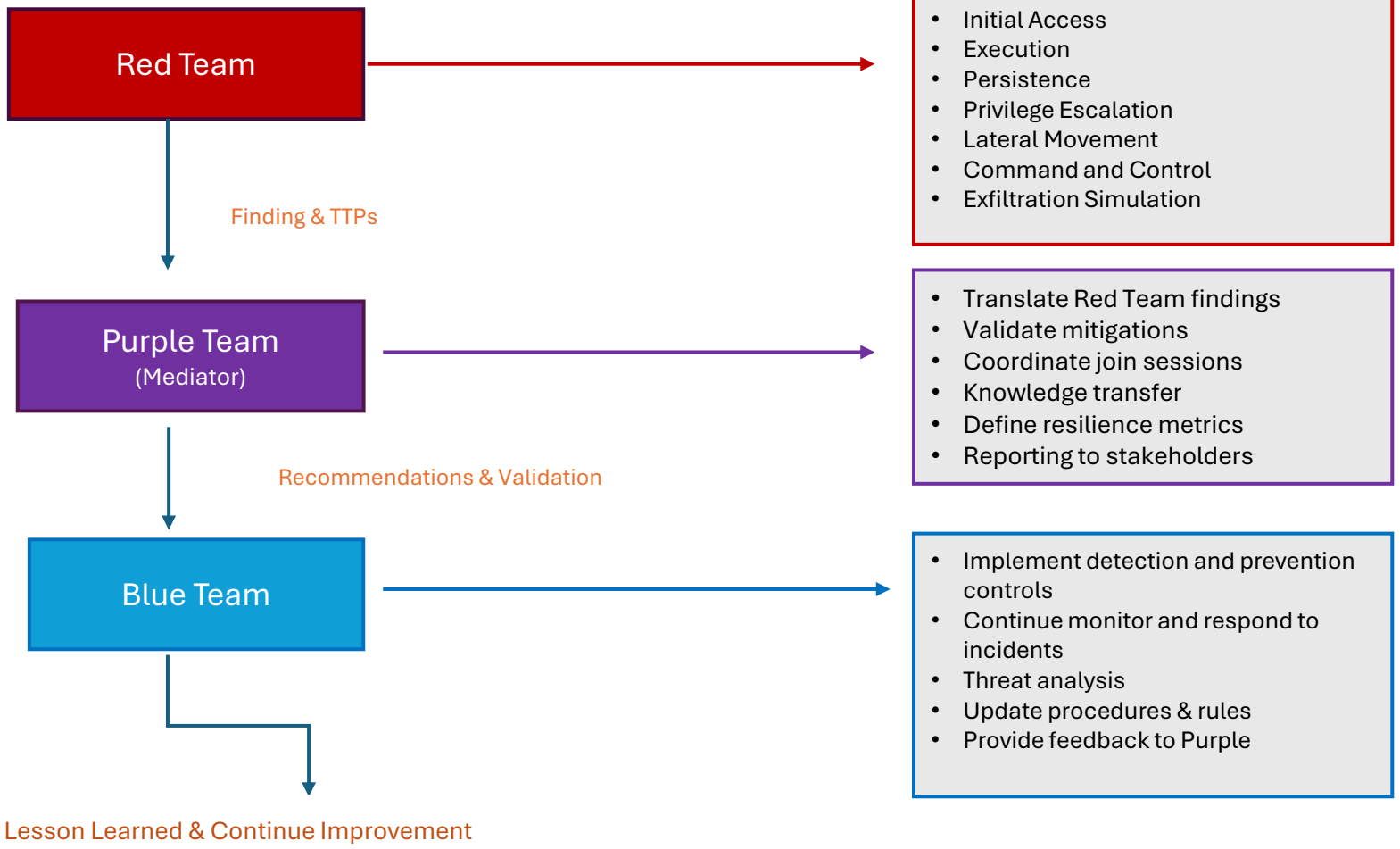
Characteristics	Red Team	Pentest
Objective	Test resilience against realistic attacks in order to identify potential weaknesses of protection, detection and response capabilities	Gain insight into system vulnerabilities
Scope	Broad → people, processes, technology	Network, applications, Configurations, patch level
Defensive informed	Covert and unknown to Blue Team	Open and known to Blue Team
Post-exploitation	Extensive focus on critical assets and functions	Very limited
Methods	Focus on realistic simulation; testing includes technical, human and physical factors	Focus on efficiency; testing includes mostly technical factors
Techniques	Tactics, techniques and procedures (TTP)	Mapping, scanning and exploiting

TLP: CLEAR

Characteristics	Red Team	Pentest
environment	Live production systems	Typically, limited interaction with live production systems
Duration	Months	Weeks
Physical Security	May be tested	Not be tested
Social Engineering	may be used	Not used
Advantage	Demonstrates real business impact, tests organizational response, improves processes and detection	Fast, measurable, technically focused
Limitation	More costly, longer duration, requires extensive approval and coordination	Less testing of humans and processes; may not reveal cross-domain attack paths
Outcome	List of vulnerabilities	Assessment of resilience and real-world readiness

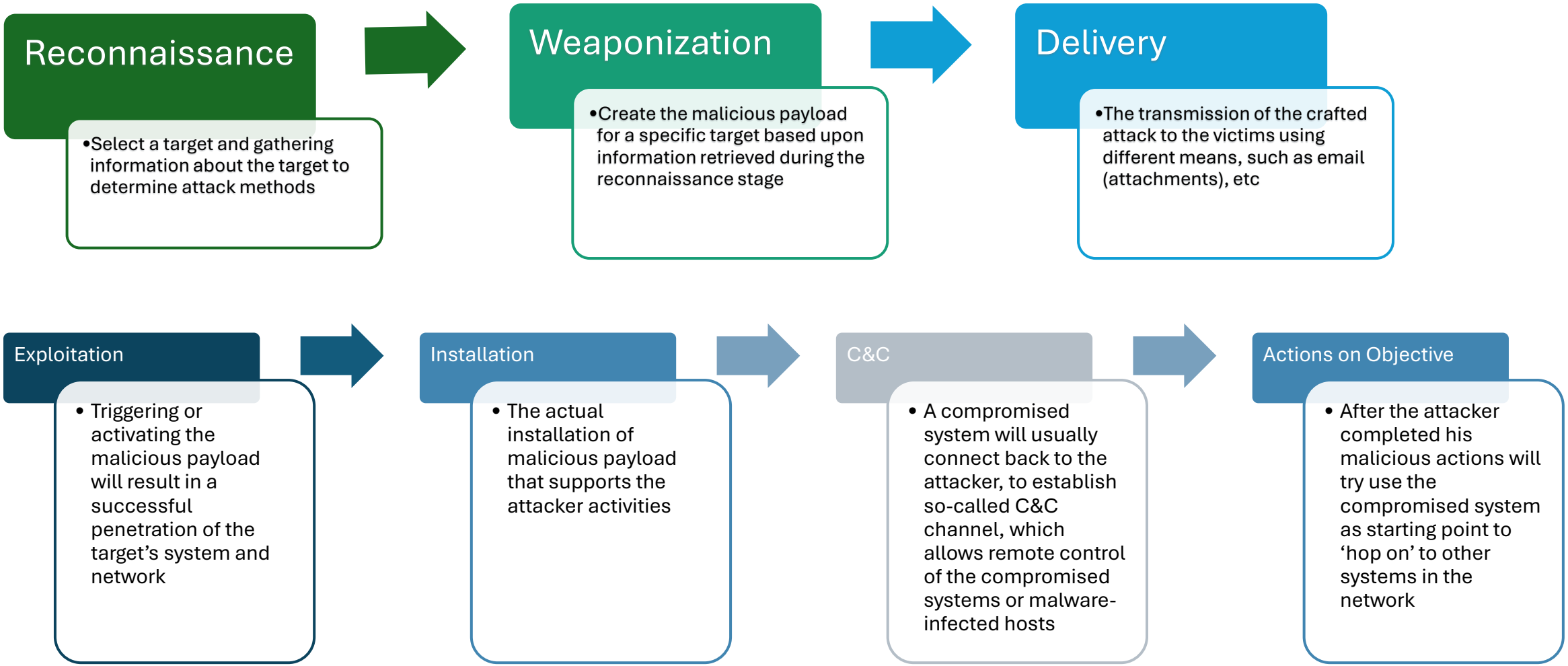
TLP: CLEAR

Communication Flow in Red Team Exercise



TLP: CLEAR

Red Team Exercise Lifecycle



TLP: CLEAR

Red Team Framework

- Lockheed Martin Cyber Kill Chain Framework
- The MITRE ATT&CK
- Threat Intelligence Based Ethical Red Teaming (TIBER-EU)
- The Saudi Arabian Financial Entities Ethical Red Teaming Framework
- Hongkong iCAST – Intelligence-Led Cyber Attack Simulation Testing
- Singapore Red Team – Adversarial Attack Simulation Exercise

TLP: CLEAR

Certification Body and Qualification

Certification Body	Qualification
CREST	• CREST Certified Threat Intelligence Manager (CCTIM) • CREST Certified Simulated Attack Manager (CCSAM) • CREST Certified Simulated Attack Specialist (CCSAS)
ISACA	• Cybersecurity Nexus (CSX
(ISC)2	• Certified Information Systems Security Professional (CISSP) • Systems Security Certified Practitioner (SSCP)
SANS	• GIAC Red Team Professional (GRTP) • GIAC Penetration Tester (GPEN) • GIAC Web Application Penetration Tester (GWAPT) • GIAC Exploit Researcher and Advanced Penetration Tester (GXPN) • GIAC Cloud Penetration Tester (GCPN) • GIAC Experienced Penetration Tester (GX-PT) • GIAC Enterprise Vulnerability Assessor Certification (GEVA)
Offensive Security	• OffSec Certified Professional (OSCP) • OffSec Experienced Penetration Tester (OSEP) • OffSec Web Expert (OSWE) • OffSec Exploit Developer (OSED)
Others .. etc	• eLearn Security Certified Professional Penetration Tester (eCPPT) • Certified Penetration Testing Professional (CPENT) • Certified Ethical Hacker (CEH)

TLP: RED

Demo Red Team Infrastructure

Q&A