
BREAKING IN
TO BUILD TRUST
AN SDG EBOOK ON
CONTINUOUS RED TEAMING

TABLE OF

CONTENTS

Introduction

In a world where digital threats evolve faster than compliance checklists and breach headlines dominate the news cycle, organizations must rethink how they assess and defend their security posture. What once sufficed as an annual or semi-annual penetration test is no longer enough. Enter ***Continuous Red Teaming (CRT)****: a modern, proactive evolution of offensive security that's becoming the new foundation of digital trust and resilience.*

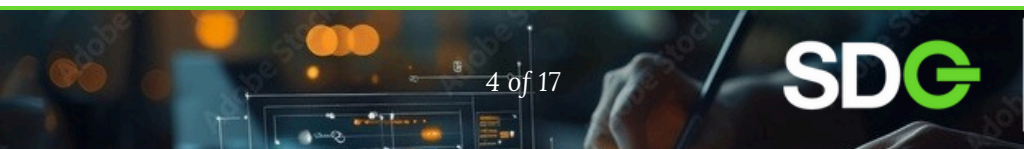
CHAPTER I

Penetration Testing Tactical, But Limited

Penetration Testing has been the basis of offensive security assessments for over two decades. It involves simulating attacks on a system or application to uncover exploitable vulnerabilities. Most pentests follow a structured process:

Penetration Testing Process:

1. **Scoping:** Define limits (external/internal, web apps, APIs, network layers).
2. **Reconnaissance:** Passive and active information gathering.
3. **Vulnerability Discovery:** Scanning, manual enumeration.
4. **Exploitation:** Attempt to gain unauthorized access using known weaknesses.
5. **Post-Exploitation:** Lateral movement or privilege escalation (if scoped).
6. **Reporting:** Documenting findings, severity, and remediation guidance.



Despite its value, **pentesting is fundamentally constrained:**

1. **Time-bound:** Often conducted annually or bi-annually.
2. **Tool-driven:** Limited to what tools or techniques are in the tester's kit.
3. **Not stealthy:** Rarely tests detection capabilities.
4. **Compliance-focused:** Designed for checkbox compliance, not resilience.
5. **Predictable:** Internal teams often know when it's happening.

In essence, penetration testing provides a snapshot in time, not a continuous risk view.

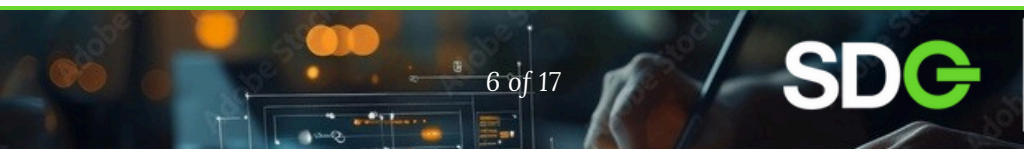
CHAPTER II

Red Teaming: Simulating Real-World Adversaries

Red Teaming is a deeper, goal-oriented assessment method that simulates advanced attacker behavior across the full cyber kill chain. The objective isn't just to identify vulnerabilities, but to determine how far a threat actor could go while evading detection and response mechanisms.

Red Teaming Methodology:

1. **Threat Modeling:** Define objectives aligned with business risks (e.g., access customer PII).
2. **Attack Path Design:** Plan tactics using frameworks like MITRE ATT&CK.
3. **Initial Access:** Through phishing, credential stuffing, or exposed services.
4. **Persistence & Evasion:** Use living-off-the-land binaries (LOLBins), C2 channels.
5. **Lateral Movement:** Pivot using pass-the-hash, token impersonation.



6. **Objective Completion:** Exfiltrate data, gain Domain Admin, or compromise critical systems.

7. **Debrief:** Technical walkthrough, defensive blind spots, recommendations.

Unlike PT, Red Team engagements are stealthy, multi-phase, and often nondisclosed to the Blue Team. The goal is to test not just technology, but the people and processes of detection and response.

However, Red Teaming is resource-intensive, typically periodic, and still not frequent enough to validate resilience against rapidly evolving threats.

CHAPTER III

The Rise of Continuous Red Teaming (CRT)

CRT evolves red teaming into a persistent, real-time security validation capability. It continuously simulates adversarial behavior to uncover detection gaps, validate controls, and improve incident response.

How CRT Works:

1. **Scope Definition:** Identify critical assets and threats
2. **Threat Simulation Platform:** Use BAS tools and frameworks like Cobalt Strike, Sliver, Mythic, etc.
3. **Persistent Attack Scenarios:** Run over weeks or months to mimic APT dwell time
4. **Continuous Monitoring:** Assess SOC visibility, reduce false positives
5. **Adaptive Tactics:** CRT evolves as detections improve
6. **Feedback Loop:** Tune controls based on results

7. **Reporting & Metrics:**
    - Time to Detect (TTD)
    - Time to Contain (TTC)
    - Coverage Gaps
    - Playbook Efficiency

CRT Benefits:

- Validates detection and response
- Trains Blue Teams continuously
- Reduces the attack surface in real time
- Aligns with threat-informed defense frameworks
- Feeds into executive governance dashboards

CRT is often delivered as a managed service or via in-house adversary emulation teams with automation pipelines for daily/weekly campaigns. It helps security teams move from being reactive to resilient. It uncovers gaps that traditional security tools and controls miss, especially in areas like lateral movement, credential abuse, and social engineering.

CHAPTER IV

CRT vs. Traditional Testing

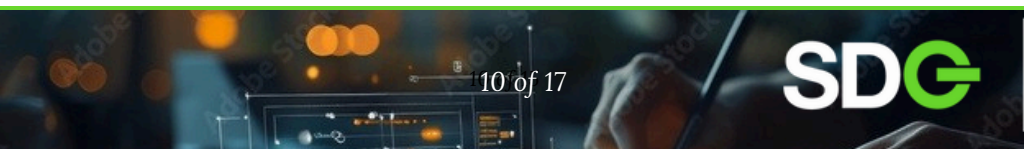
Why CRT Outpaces Penetration Testing

Penetration Testing

Capability	Penetration Testing
Frequency	1-2x/year
Objective	Find vulnerabilities
Detection Test	No
Coverage	Scoped tools
Digital Trust	Low

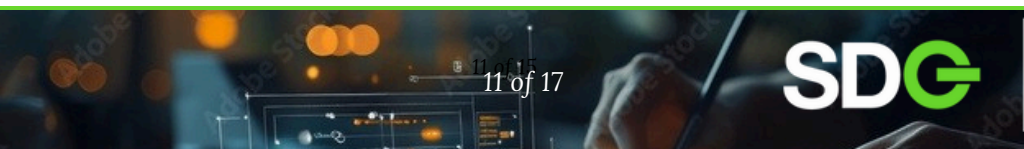
Red Teaming

Capability	Red Teaming
Frequency	Annually
Objective	Emulate attacker
Detection Test	Partial
Coverage	Multi-vector
Digital Trust	Medium



Continuous Red Teaming

Capability	Continuous Red Teaming
Frequency	Daily/Weekly
Objective	Validate resilience
Detection Test	Yes
Coverage	Full kill chain
Digital Trust	High



CHAPTER V

Blue Teaming The Unsung Hero

While Red Teams break in, Blue Teams defend. Their responsibilities include:

- Security Monitoring (SIEM, EDR, NDR)
- Threat Detection & Correlation
- Incident Response & Containment
- Threat Hunting & Log Analysis
- Control Tuning (e.g., adjusting alert thresholds, behavior analytics)

In a CRT program, Blue Teams are **continuously challenged.** This results in:

- Faster Mean Time to Detect (MTTD)
- Stronger playbooks and response strategies
- Mature attack surface management
- Deeper threat hunting capabilities

They are essential to close the loop on Red Team simulations. CRT without a capable Blue Team is just noise.

CHAPTER VI

Purple Teaming
The Feedback Engine

Purple Teaming formalizes collaboration between Red and Blue Teams. It transforms an adversarial exercise into an educational one, where insights are shared in real-time to enhance detection and defense.

Purple Teaming Process:

1. J**oint Scenario Planning:** Red proposes TTPs; Blue identifies expected telemetry.
2. **Live Simulation:** Execution with simultaneous monitoring.
3. **Data Correlation:** Blue shows what was detected vs. missed.
4. **Tuning:** Adjust SIEM, EDR rules, response triggers.
5. **Documentation:** Update playbooks, enrich threat intel

Purple teaming can be embedded within CRT or run as sprint-based collaborative exercises.

CHAPTER VII

Implementing CRT: A Maturity Model

Adopting CRT doesn't happen overnight. It evolves through progressive levels:

Level 1 - Ad Hoc Red Team Engagements

- Annual exercises
- Manual emulation, no continuous feedback

Level 2 - Integrated Red/Blue Collaboration

- Purple teaming initiated
- SOC involved in debriefs

Level 3 - Automated Adversary Simulation

- BAS tools for daily attack emulation
- Threat library mapped to MITRE

Level 4 - Threat Informed Defense

- CRT drives threat modeling, detection engineering
- Real-time metrics to leadership

Level 5 - Business Risk-Aligned CRT

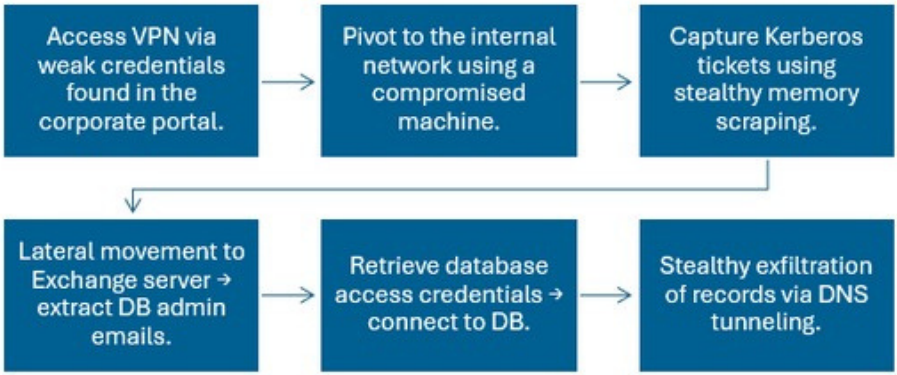
- TTPs prioritized by impact on business processes
- Executive-level dashboards for resilience

CHAPTER VIII

Real-World CRT Use Case

Objective: Exfiltrate sensitive records from a production database without triggering alerts.

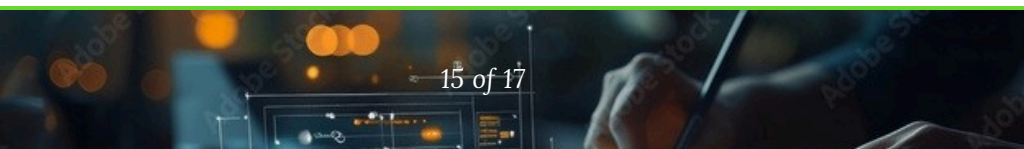
Flow:



Outcome: Attack undetected for 14 days; CRT revealed that logging existed but lacked correlation rules.

Fixes:

- Enhanced alerting on unusual outbound DNS patterns.
- Hardening of OWA portal with MFA and IP filtering.
- Playbook created for DNS anomaly investigation.



Conclusion

The security paradigm is shifting from **audit-driven validation** to **threat-driven resilience**. In this shift, **Continuous Red Teaming becomes the core capability.** It allows organizations to:

- Continuously stress-test their defenses.
- Validate whether investments in detection and response actually work.
- Move from hypothetical risk to real, measurable assurance.

While Penetration Testing remains valuable in compliance, CRT reflects the realties of today's threat landscape. When Red, Blue, and Purple teams operate in concert, organizations gain the only thing that truly matters in cybersecurity today: **Digital Trust.**

SDG

Partner with SDG to enhance your resilience and build digital trust.

solutions@sdgc.com

(203) 866-8886

Did you enjoy this eBook?

Be sure to check out:

FINDING YOUR **SASE MATCH**

AN SDG EBOOK ON

The Ultimate Guide to Choosing Your SASE-as-a-Service Provider

www.sdgc.com