Plurilock
CRITICAL SERVICES

**Continuous Red and Purple Teaming**

# Continuous Red Teaming and Purple Teaming Services

## Adversary Simulation. Collaborative Defense Enhancement.

**94%** of organizations running red team testing face successful penetration.

This engagement simulates real-world adversary behavior to test your organization's defenses end to end. Using a collaborative purple-team approach, we help you understand attack paths while improving detection and response capabilities. Through continuous testing aligned to PTEF and MITRE ATTandCK frameworks, combined with real-time visibility via Plurilock's integrated portal, we identify exploitable weaknesses before adversaries do.

## Objective-Driven Adversary Simulation Engagements

### Attack Simulation Services

**Full-Scope Red Team Engagements**

Multi-vector attack campaigns combining physical security testing, social engineering, application testing, network penetration, and cloud security assessments

**Assumed Breach Scenarios**

Testing your detection and response capabilities from an already-compromised position within your environment

**Physical Security Testing**

Attempts to gain unauthorized physical access to facilities, data centers, or restricted areas

**Wireless and Network Exploitation**

Identification and exploitation of vulnerabilities in wireless networks, network segmentation, and perimeter defenses

### Advanced Threat Operations

**Cloud Infrastructure Testing**

Red team operations targeting cloud environments including AWS, Azure, GCP, and hybrid infrastructure

**Active Directory and Identity Exploitation**

Attacks targeting identity management systems, Active Directory, and authentication mechanisms

**Command and Control (C2) Operations**

Establishing covert communication channels and demonstrating advanced persistent threat (APT) techniques

**Custom Malware and Tool Development**

Creation of custom exploitation tools and payloads designed to evade detection by your security controls

**Ongoing Attack Simulations**

Continuous red team operations that adapt to your evolving environment and security controls

## Collaborative Defense Enhancement Exercises

### Team Collaboration & Training

Purple teaming bridges the gap between offensive red team operations and defensive blue team capabilities, creating a collaborative environment focused on measurable security improvements.

**Threat-Informed Defense Workshops**

Collaborative sessions where red and blue teams work together to understand attack techniques and enhance detection capabilities

**MITRE ATT&CK Mapping and Coverage Analysis**

Assessment of your security control coverage against MITRE ATTandCK framework with gap identification

**Detection Engineering**

Collaborative development and tuning of security detection rules, SIEM use cases, and threat hunting queries


## Contact Us

**+1 (888) 776-9234 (Plurilock)**
**+1 (310) 530-8260 (USA)**
**+1 (613) 526-4945 (Canada)**


Advanced cybersecurity and Zero Trust
Security assessments and consulting
IT products and solutions
Professional services
Managed services

## Practical Security Testing

### Tabletop Exercises

Scenario-based discussions simulating attack campaigns to evaluate response procedures and decision-making

### Live-Fire Exercises

Controlled attack simulations where defensive teams practice detection, analysis, and response in real-time

### Security Control Validation

Testing the effectiveness of specific security technologies, including EDR, SIEM, DLP, WAF, and other defense-in-depth controls

### Incident Response Testing

Validation of incident response playbooks, escalation procedures, and communication protocols under realistic attack scenarios

### Threat Hunting Enablement

Training and collaboration to enhance proactive threat hunting capabilities within your security operations team

## Typical Assessment Deliverable

### Red Team Purple Team Exercise Report:

- **Overview**: attack paths, exploited vulnerabilities, and achieved objectives
- **Attack Chain Documentation**: detailed technical write-ups of successful attack paths, including indicators of compromise (IOCs)
- **Security Control Effectiveness Matrix**: evaluation of defensive technology effectiveness and bypass techniques discovered
- **Security Improvement Roadmap:** Prioritized recommendations for enhancing detection, prevention, and response capabilities
- **Incident Response Enhancement Plan**: recommendations for improving incident response procedures based on exercise findings
- **Remediation Guidance**: specific technical recommendations for addressing identified vulnerabilities and security gaps

**Test your defenses before attackers do.**
**Schedule your red team assessment today**

sales@plurilock.com


## Contact Us

**+1 (888) 776-9234 (Plurilock)**
**+1 (310) 530-8260 (USA)**
**+1 (613) 526-4945 (Canada)**


Advanced cybersecurity and Zero Trust
Security assessments and consulting
IT products and solutions
Professional services
Managed services

# Plurilock Services

### Zero Trust

Design and implementation of zero trust architectures (ZTAs)

### Data Protection

Protection of intellectual property and digital assets

### Identity and Access Management

Design, implementation, and integration of complete identity and access management (IAM)

### Public Key Infrastructure

Design and implementation of modern public key infrastructure (PKI) deployments

### Offensive Security

Security assessments and tests with a hacker mindset

### Penetration Testing as a Service (PTaaS)

Managed service providing continuous penetration testing to rapidly surface emerging vulnerabilities

### Data Protection as a Service (DPaaS)

Managed data protection service to operate DLP and insider threat capabilities as a service

### Emergency Support

Immediate, cross functional team for urgent and high impact IT and cyber problems


*Selection of current and past customers that can be publicly represented*

Plurilock CRITICAL SERVICES