GRYPHON SECURITY

# Purple Team Testing

**Detection Validation. Operational Readiness. Defensible Outcomes.**

A collaborative adversary simulation designed to evaluate an organization's ability to detect, analyze, and respond to real-world attacker behavior where sensitive data, system integrity, and operational continuity are mission-critical.

Modern organizations face persistent threats that rarely succeed because controls are entirely absent, but because malicious activity is not detected or acted upon in time. Purple Team Testing provides leadership with a clear, defensible understanding of how effectively the organization can identify and respond to attacker behavior using a structured methodology aligned to the MITRE ATT&CK.

Unlike traditional penetration testing, Purple Team engagements emphasize shared visibility, collaboration, and operational improvement rather than stealth or point-in-time exploitation.

## What We Do

We conduct a structured Purple Team engagement where adversarial techniques are executed transparently while defensive teams monitor, detect, and respond in real time.

Testing focuses on attacker behaviors across identity systems, endpoints, networks, and privileged workflows. Each technique is mapped to the MITRE ATT&CK Framework and evaluated based on whether it was detected, partially detected, or missed entirely. The result is a practical assessment of defensive effectiveness, not a theoretical maturity score.

## Why This Matters

Detection and response failures can allow attackers to operate undetected, escalate access, and cause material harm long before an incident is formally identified.

Unlike vulnerability-centric testing, Purple Team Testing demonstrates whether security tools, telemetry, and response procedures function effectively during realistic attack scenarios. This allows leadership to understand where meaningful detection gaps exist, how quickly incidents would be identified, and whether response actions would be timely, coordinated, and defensible.

## Our Testing Approach

This service uses a structured, collaborative methodology grounded in real attacker tradecraft.

The engagement is not a certification, attestation, or compliance audit. Instead, it is designed to answer one core question:

**“If an attacker is active in the environment, will we see it, and will we respond effectively?”**

Findings are contextualized to the organization’s size, staffing model, technology stack, and threat exposure so improvements are achievable and prioritized.

## What’s Tested

Purple Team Testing evaluates defensive capability across attacker behaviors most relevant to real-world threats, including:

- **Detection & Alerting**
  Visibility into malicious activity across endpoints, identity systems, and networks
- **Response Workflows**
  Escalation paths, investigation steps, and coordination during simulated attacks
- **Identity & Credential Abuse**
  Detection of credential harvesting, misuse, and privilege escalation
- **Lateral Movement & Persistence**
  Ability to identify attacker movement and long-term footholds
- **Logging & Telemetry Coverage**
  Completeness and usefulness of logs supporting detection and investigation

Each area is assessed through observed attacker actions rather than checklist validation.

## What You Receive

Clients receive a comprehensive Purple Team Test Report, including:

- Executive-level summary written in plain language
- MITRE-mapped findings showing detection outcomes
- Evidence-backed narratives for each tested technique
- Screenshots and artifacts supporting each tested technique
- A prioritized Remediation Roadmap (30 / 60 / 90-day recommendations)
- TTP reference table for ongoing detection engineering

The report is suitable for leadership briefings, remediation planning, and audit or compliance support.

## Who This Service Is For

This service is designed for:

- Organizations with active detection and response capabilities
- Security teams seeking to validate monitoring and alerting effectiveness
- Environments operating a SOC or centralized security monitoring
- Organizations seeking to improve incident readiness before a real breach occurs

## This Service Is *Not* Designed For

- Organizations seeking a checkbox compliance assessment
- Organizations looking for managed SOC services or tool resale
- Environments without leadership commitment to remediation and risk ownership

Gryphon Security focuses on clarity, collaboration, and defensible outcomes.

## Why Gryphon Security

- **Real-World Tradecraft**
  Testing aligned to active attacker behavior and MITRE ATT&CK.
- **Operational Improvement Focus**
  Engagements strengthen detection and response capabilities.
- **Evidence-Driven Execution**
  Findings based on observed outcomes, not assumptions
- **Clear Reporting**
  Evidence-based results written for leaders and practitioners.
- **Independent & Vendor Neutral**
  No product resale or vendor bias.

## Next Steps

An initial conversation is structured, confidential, and obligation-free.

We will:

- Confirm scope and environment
- Discuss key detection and response concerns
- Explain exactly what testing will and will not include

We will not pressure you into tools, managed services, or long-term contracts.

**Gryphon Security, LLC**
Offensive Security & Adversary Simulation
info@gryphonsec.com | www.gryphonsec.com