Mandiant

DATASHEET

Purple Team Assessment

Benefits

- Prepare your security team for real world cyber incidents—without real risk or business impact
- Assess and enhance your security team's ability to prevent, detect and respond to authentic, relevant and active attack scenarios in a controlled, realistic environment
- Test and tune technical defenses to increase breach detection and response effectiveness
- Align with MITRE ATT&CK framework
- Identify gaps in your active and passive security controls
- Improve your organization's ability to respond to future incidents

Coach your security team to improve detection and response to relevant and active attack scenarios

Why Mandiant

Mandiant has been at the forefront of cybersecurity and cyber threat intelligence since 2004. Our incident responders are on the frontlines of the most complex breaches worldwide. We have a deep understanding of both existing and emerging threat actors, as well as their rapidly changing tools, tactics and procedures.

Service overview

The Mandiant Purple Team Assessment evaluate your security organization's ability to prevent, detect, and respond to attack scenarios by using the latest threat intelligence and the Mandiant Security Validation technology. They focus on highly realistic scenarios relevant to your industry.

To expose shortcomings in your current technology stack, the purple team does not assume that your security operations work as intended. Unlike adversarial penetration testing designed to identify misconfigurations or unpatched systems in your network infrastructure, the Purple Team Assessment, which incorporates Mandiant controls validation technology, is a collaborative assessment which provides quantifiable evidence of security effectiveness.

A Purple Team Assessment is recommended for organizations that want to test and develop the ability of their security team, processes and technology to detect, prevent, and respond to targeted attack across all phases of the attack lifecycle.

Our approach

The purple team begins by analyzing intelligence to determine the data breaches and threat groups most active in your industry vertical. They then identify what threats are relevant and create validation content to challenge your security infrastructure to capture data on how your security controls behave to authentic and active attack TTPs. They use those TTPs to test your security team's ability to detect and respond to industry-relevant threats in realistic scenarios.

The Purple Team Assessment consists of multiple step-by-step, scenario-based exercises to test your team's performance in phase of the attack lifecycle.

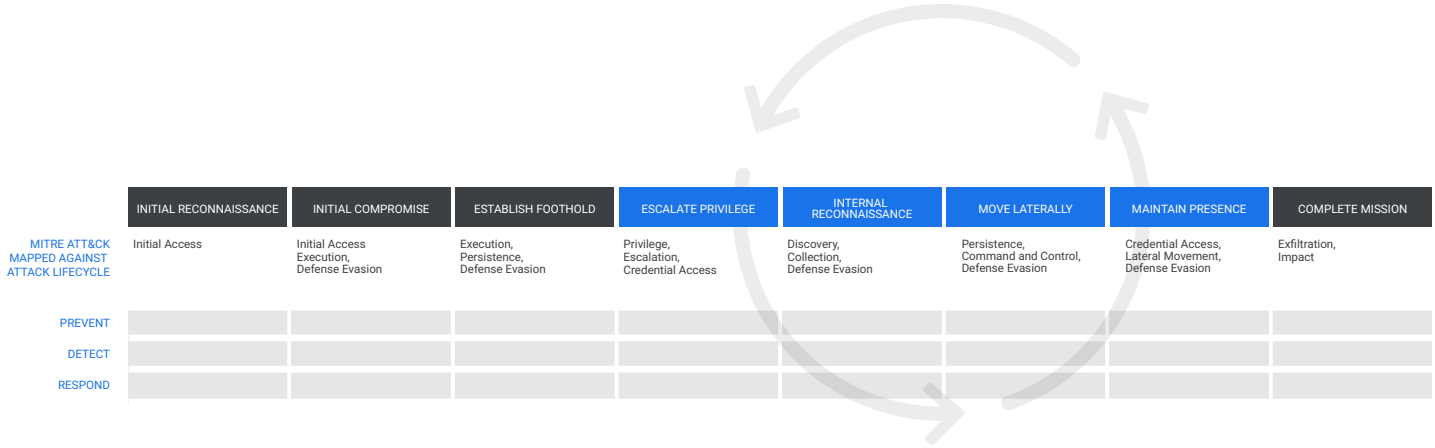

FIGURE 1. The Mandiant purple team tests the client security team's capabilities against every phase of the attack lifecycle.

Your security team works directly with a Mandiant incident response consultant and red team consultant at each phase to participate in the exercise and attempt to detect scenario activities. If malicious activity is detected, the purple team works with your security team to ensure an appropriate response to the detected activity and the existence of procedures to ensure continued success. If the malicious activity is not detected, our consultants work with your security team on how to better use existing logging, monitoring, and alerting detection technologies during the next simulation attempt. They may also identify areas for technological improvement.

Engagement timeline and deliverables

A Purple Team Assessment generally takes a total of three weeks to complete—two weeks for testing, and one week to assemble and deliver a report.

Deliverables

Detailed report that includes:

- A scorecard containing metrics related to detection of the simulated incidents
- Executive summary
- Walkthrough of technical details and capability evaluation with step-by-step instructions on how to recreate our findings
- Evidence-supported findings and remediation strategies
- Strategic recommendations for long-term operational improvements
- Technical and executive-level briefs can be produced upon request.