DATA SHEET

Continuous Purple Team Assessment

Refine and mature your attack responses with an iterative, repeatable coaching regimen

KEY BENEFITS

- Demonstrate technology stack and/or security budget ROI with scorecard with effectiveness metrics
- Enhance your security team's practical skills
- Mature incident response procedures
- Assess the impact of ongoing changes to people, processes and technology within your security program
- Address gaps in active and passive security controls
- Discover previously undetected gaps in your security program
- Align with the MITRE ATT&CK framework

Why FireEye Mandiant

FireEye Mandiant has been at the forefront of cyber security and cyber threat intelligence since 2004. Our incident responders have been on the frontlines of the world's 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 FireEye Mandiant Continuous Purple Team Assessment enables you to improve your security organization's ability to prevent, detect and respond to the latest attack techniques observed in data breaches. This offering uses coaching sessions (with regularly scheduled assessment intervals) that incorporate the latest FireEye threat intelligence, scenarios based on actual frontline incident response experiences and the FireEye Verodin Security Instrumentation Platform (SIP). This potent combination generates highly realistic scenarios relevant to your industry.

The iterative emulated threat scenarios will increase in complexity as testing progresses. Failed scenarios will be repeated so your organization can learn to successfully respond to threats by focusing on what matters most during a data breach:

- Dwell time
- Mean time to detect
- Mean time to respond
- Mean time to contain

This engagement is best suited for organizations that have an established cyber security capability and seek to improve incident response detections and capabilities over a period of time. Such organizations typically have a SIEM, security team and endpoint detection and response (EDR) solution in place.

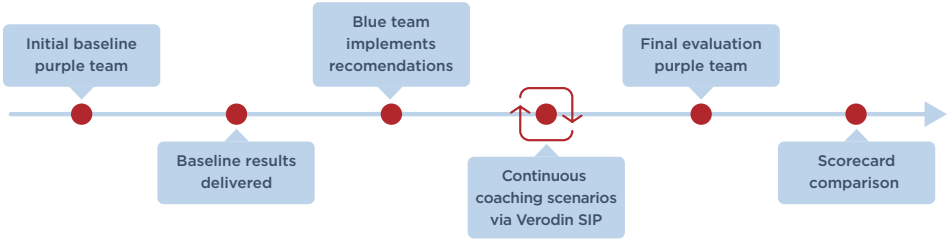

Figure 1. Phases of Continuous Purple Team Assessment engagement.

Our Approach

The Mandiant team begins by performing intelligence analysis to determine the data breaches and threat groups most active in your industry. The Mandiant team uses this analysis to create Verodin SIP scenarios to emulate the threat groups' tools, tactics and procedures (TTPs). Your security team's ability to prevent, detect and respond to threats known to target your industry is tested in realistic and relevant scenarios.

The Continuous Purple Team Assessment consists of multiple step-by-step, scenario-based stacked exercises at each phase of the attack lifecycle and MITRE ATT&CK™ framework.

The first assessment phase baselines your organization's ability to detect, prevent and respond to emulated and relevant attack scenarios, and identifies areas for improvement.

Following the baseline assessment, your team is provided with the Verodin SIP to practice responding to realistic attack scenarios. Your organization's progress is re-assessed at regular intervals to track improvement.

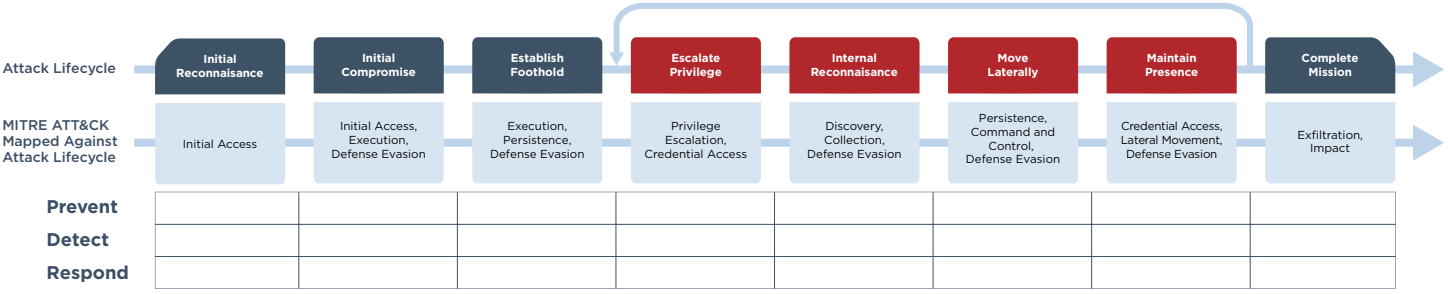

Figure 2. The Mandiant purple team tests the client security team's capabilities against every phase of the attack lifecycle.

Your security team works directly with a FireEye Mandiant incident response consultant and red team consultant at each phase of the exercise. Scenarios will begin with common TTPs relevant to your industry. Testing will be repeated to measure improvement in your organization's detection and response capabilities. Scorecards will be provided periodically throughout testing to report on the effectiveness of changes implemented within your security controls and team.

Our consultants will work with your security team to help fine-tune any processes and controls that are not contributing to your incident response function. You will have time to implement changes before the next round of the Continuous Purple Team Assessment.

A final purple team exercise is conducted at conclusion to measure improvements made during the course of the Continuous Purple Team Assessment.

Engagement Timeline

A Continuous Purple Team Assessment is typically three months, but can be extended if requested. Each testing cycle takes three weeks to complete: two weeks for testing and one week for reporting. At least three weeks of lead time is required to schedule each testing cycle.

DELIVERABLES

Detailed Continuous Purple Team Assessment report including:

- A scorecard containing metrics related to detection of the emulated incidents
- Executive summary
- Walkthrough of technical details and evaluation of capabilities with step-by-step information to recreate findings
- Evidence-supported findings and remediation strategies
- Risk and impact analysis to prioritize findings based on relevancy to your environment
- Strategic recommendations for long-term operational improvements

Technical- and executive-level briefs available upon request.

To learn more about FireEye, visit: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About FireEye, Inc.

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.