DATA SHEET

Red Team for Security Operations (RTSO)

Coach your security team to improve detection and response to realistic attack scenarios

BENEFITS

- Assess the state of your detection and response capabilities
- Make sure you are prepared with all the right people, processes and technology needed to respond to an incident
- Enhance your internal security team's ability to prevent, detect and respond to incidents in a controlled and realistic environment
- Test your security tools and procedures in a controlled, non-destructive attack scenario
- Decrease response time and effectiveness
- Mature incident response procedures
- Ensure that preventative measures are in place to prevent various attack scenarios

Why Mandiant

Mandiant, a FireEye company, 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

Red Team for Security Operations (RTSO), also known as "Purple Team," is designed to test your internal security team's ability to prevent, detect, respond and contain an advanced targeted attack in your network. This is accomplished by using realistic attack scenarios through each phase of the attacker lifecycle.

The Mandiant red team determines the threat groups most active in your industry and create signatures that would emulate the tools, tactics, and procedures (TTPs) such groups use to target your environment. These signatures are then built into RTSO scenarios so your security team can experience realistic TTPs.

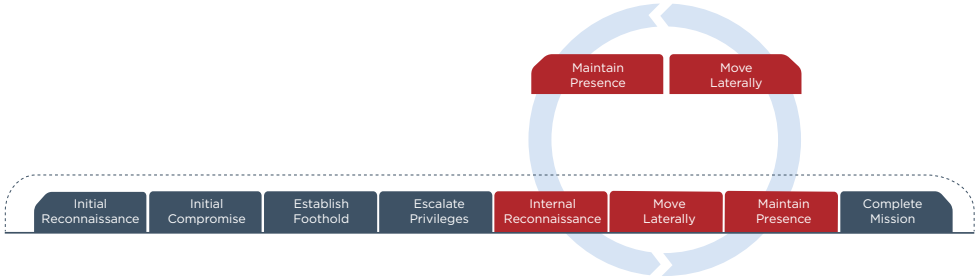
RTSO helps enhance overall detection and alerting capabilities. It is not designed to identify vulnerabilities or misconfigurations in your network infrastructure.

Red Team for Security Operations vs. standard Red Team Operations

	Red Team for Security Operations	Red Team Operations
Objective	Evaluate detect, prevent, respond capabilities across each phase of the attack lifecycle	Pursue goal-oriented, sample objectives such as stealing executive's email and accessing critical business data
Differentiation	Mandiant incident responder works side-by-side with customer's security team, coaching along the way	Emulate goal-oriented real-world targeted attack. Mandiant team will do whatever is necessary to accomplish the objective
Attack Simulated	Can simulate multiple attack groups at each phase of the attack lifecycle	Execute ongoing attack working toward the agreed-upon goal
Customer security team involvement	Respond to attack scenarios with Mandiant incident responder observing and coaching	No direct involvement with Mandiant team. Work to detect, prevent and respond to the red team attack. Option for security team to not know they are in an exercise

Methodology

The Red Team for Security Operations methodology is a step-by-step scenario-based exercise applied to each phase of the attack lifecycle.



	Initial Reconnaissance	Initial Compromise	Establish Foothold	Escalate Privileges	Internal Reconnaissance	Move Laterally	Maintain Presence	Complete Mission
Detect	—	✓	✓	✓	✗	✗	✗	✓
Inhibit	✓	✓	✓	✓	✗	✓	✗	✗
Respond	✗	✓	✗	✗	✗	✗	✗	✗

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

These phases include reconnaissance, initial compromise, establish foothold, escalate privileges, internal reconnaissance and complete mission. The assessment includes an incident responder who works with your internal security team or security operations center (SOC) to detect each scenario performed by the red team.

At each step, if malicious activity is detected, Mandiant works with the internal security team to ensure that the response to the detection is appropriate and that procedures exist to ensure continued success. If the malicious activity is not detected, the red team works with a Mandiant incident response consultant to either better utilize existing detection technologies during the next simulation or to identify an area for technological improvement.

As the security team detects and responds to red team activity, the incident response consultant observes their incident response processes and procedures in action and helps drive improved detection and response time. Mandiant consultants also review existing logs to determine if they are sufficient for detecting red team activity.

Why Choose Red Team for Security Operations

RTSO 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.

DELIVEREABLES

- Summary for executives and senior-level management
- Technical details with step-by-step information for each scenario performed
- Tactical recommendations for immediate improvement
- Strategic recommendations for long-term improvement
- Invaluable experience working directly with security professionals with years of experience responding to the large breaches

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.