RED TEAM OPERATIONS

TEST THE EFFICACY OF YOUR SECURITY STAFF, PROCESSES AND TECHNOLOGY

MANDIANT
A FireEye® Company

Proactively identify and mitigate complex security vulnerabilities that can lead to critical data loss.

BENEFITS

- Know whether your critical data is at risk and how easily it may be obtained by a malicious actor
- Assess the security of your environment against a realistic "no-holds-barred" attacker
- 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 attack scenario
- Identify and mitigate complex security vulnerabilities before an attacker exploits them
- Attain fact-based risk analysis findings and recommendations for improvement

WHY MANDIANT

Mandiant is a trusted advisor to organizations globally with over 10 years of experience dealing with advanced threat actors from around the world. We support organizations during the most critical times after a security breach has been identified and proactively help them improve their detection, response and containment capabilities. Our Red Team Operations leverage our deep knowledge of advanced persistent threats and attacker behavior. We seek to achieve a pre-determined set of objectives by simulating the tools, tactics and procedures (TTPs) of real-world attackers.

Overview

We offer two types of Red Team Operations: Red Team Assessments and Red Teaming for Security Operations. Both assessments are objective-oriented and realistic — they focus only on the assets you define as most critical to your business.

Red Team Assessments

The Red Team Assessment consists of a "no-holds-barred" realistic attack scenario in your environment. Our red team uses any methods necessary (without damaging the business) to accomplish a set of jointly agreed upon objectives, simulating attacker behavior. These objectives focus on the most critical areas of the business that represent the greatest risk.

Sample Objectives

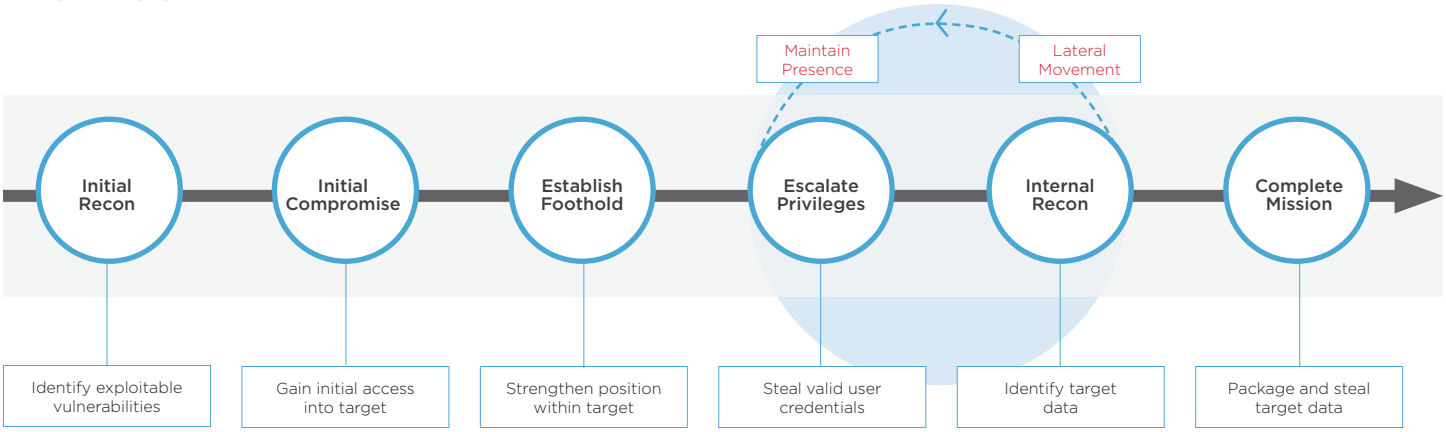
Steal executive or developer emails	**Break into a segmented environment that contains business critical or sensitive data**	**Take control of an automated device such as an IoT device, a medical device or a manufacturing device**

Methodology

We start by jointly determining whether the work should be performed white box (with knowledge) or black box (without knowledge). Leveraging Mandiant's industry intelligence, we work with your team to determine three to five objectives that represent key risks to areas considered critical to the business. The intent is to determine the likelihood of these risks occurring. Once the objectives have been agreed upon, the red team starts conducting its operations. The red team attempts to

FireEye®

ATTACK LIFECYCLE



break into the environment to perform internal reconnaissance. Once access is gained, the red team attempts to escalate privileges and maintain persistence by deploying multiple unique backdoors, just like an attacker would. The red team then attempts to accomplish its objectives through any non-disruptive means necessary.

Red Teaming for Security Operations

Red Teaming for Security Operations is designed to test both your organization's security posture and the capabilities of your internal security team. This is accomplished by using a realistic scenario prior to an attacker breaching your environment, potentially causing unwanted headlines.

Red Teaming for Security Operations builds on the Red Team Assessment by also focusing on the prevention, detection and response capabilities of your internal security team. An incident responder works with your security team to help detect the red team while the assessment is in progress and to advise on appropriate response tactics if activity is detected. Once the assessment is completed, members of the red team and the embedded incident responder work with your internal security team to build a plan to enhance prevention, detection and response to future attacks.

Methodology

The Red Teaming for Security Operations methodology is identical to the Red Team Assessment methodology, except that it includes an incident responder with your internal security team or Security Operations Center (SOC) to work on detecting the red team's activity. Once the assessment has been completed, members of the red team and the incident responder work with your internal team to develop a recommendations document detailing additional prevention, detection and response actions to enhance your security posture based on the Red Team Assessment and our experience responding to complex intrusions. The findings are based on our assessment of your security posture within the phases of the attack lifecycle.

WHAT YOU GET

- Summary for executives and senior-level management
- Technical details with step-by-step information that allows you to recreate our findings
- Fact-based risk analysis so you know a critical finding is relevant to your environment
- Tactical recommendations for immediate improvement
- Strategic recommendations for longer-term improvement
- Invaluable experience responding to a real-world incident without the pressure of a potential headline-causing breach

For more information on Mandiant consulting services, visit:
www.FireEye.com/services.html

Mandiant, a FireEye Company
1440 McCarthy Blvd. Milpitas, CA 95035
(703) 935 1701 | 800.647.7020 | info@mandiant.com

www.FireEye.com

FireEye