



DATA SHEET

Red Team Operations (RTO)

Test your ability to protect your most critical assets from a real-world targeted attack



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
- Test your internal security team’s ability to prevent, detect and respond to incidents in a controlled and realistic environment
- Identify and mitigate complex security vulnerabilities before an attacker exploits them
- Get fact-based risk analyses and recommendations for improving security posture

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

The Red Team Operations engagement consists of a realistic, “no-holds-barred” attack scenario in your environment. The Mandiant red team uses any non-destructive methods necessary to accomplish a set of jointly agreed upon mission objectives while simulating attacker behavior. The red team closely mimics a real attacker’s active and stealthy attack methods by using TTPs seen on real, recent incident response engagements. This helps assess your security team’s ability to detect and respond to an active attacker scenario.

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

Red Team Operations begin by jointly determining whether the red team should have some or no knowledge of your environment. Mandiant applies its industry experience to identify objectives that represent primary risks to your core business functions.