MANDIANT
NOW PART OF Google Cloud

DATASHEET

# Red Team Operations (RTO)

**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

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

## Why Mandiant

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 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.

Red Team Operations engagements follow the phases of the attack lifecycle.

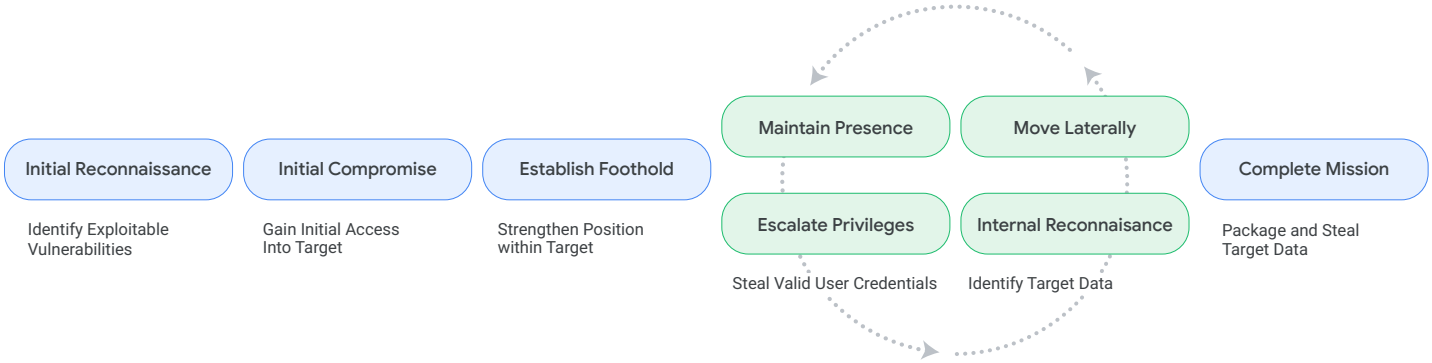


**FIGURE 1.** Attack lifecycle.

Once the objectives are set, the red team starts by conducting initial reconnaissance. Mandiant leverages a combination of proprietary intelligence repositories as well as open-source intelligence (OSINT) tools and techniques to perform reconnaissance of the target environment.

Mandiant attempts to gain initial access to the target environment by exploiting vulnerabilities or conducting a social engineering attack. Mandiant leverages techniques used by real-world attackers to gain privileged access to these systems.

Once access is gained, the red team attempts to escalate privileges to establish and maintain persistence within the environment by deploying a command and control infrastructure, just like an attacker would.

After persistence and command and control systems are established within the environment, the red team attempts to accomplish its objectives through any non-disruptive means necessary.

## Why Choose Red Team Operations

Red Team Operations are recommended for organizations that want to:

- **Test detection and response capabilities.** Security teams prepare for real world incidents, but you need to confirm that they can respond properly — without real risk.
- **Raise awareness and show impact.** The Mandiant red team behaves like real-world attackers, working to compromise your environment from the Internet by using information only available to the Internet. Successful red team engagements can help justify increased security budgets and identify gaps that require further investment.

### 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 long-term improvement
- Invaluable experience responding to a real-world incident without the pressure of a potential headline-causing breach