Advanced attackers recognize that the organizations they target have basic network tools in place – firewalls, intrusion prevention systems and even “next gen” firewalls. These attackers probe to identify preventative measures and circumvent these defenses either through social engineering or exploiting vulnerabilities. Mandiant pairs the most advanced intelligence on these adversaries with a team of expert analysts who tell you when you are under attack and what you should do to respond.

All alerts are not equal. Mandiant’s Network Threat Detection service identifies and analyzes the activity of high-risk threat actors on your network so you can act immediately.

Mandiant’s Network Threat Detection service alerts you to attacker activity at every phase of an attack and directs your response.

OVERVIEW

Mandiant’s Network Threat Detection service combines our network sensor with analysis by Mandiant experts and our extensive proprietary intelligence to give you unequalled visibility into when and where high-risk threat actors are active on your network.

Detect Active Attacker Activity
Uncover all types of attacker behavior, including command and control, malware beacons, spear phishing attacks, and data theft.

Identification of Data Leaving Your Network
When Mandiant identifies an attack, we capture information like usernames and passwords, hashes and actual files leaving the network.

Analysis by Mandiant Experts
Mandiant’s threat experts analyze, investigate and classify the threat level for each incident and provide specific recommendations on what actions you should take.

IP Reputation Based Monitoring
In addition to our intelligence on advanced threat actors, we alert you to other high-risk threats including botnets and Russian Business Network (RBN) style attacks.

HIGHLIGHTS

Unlike other network security products we don’t just drop a box on your network and light it up with alerts. Mandiant analysts investigate and confirm attacks.

Intel on Advanced Threats
Utilizes the most up-to-date threat intel gathered from hundreds of thousands of hours responding to advanced threat actors.

Comprehensive Monitoring
Sees both sides of the proxy server and the VPN, as well as the general network.

Spear Phishing Detection
Identifies spear phishing attacks so you can detect and kill the first attacks when they begin.

Attack Confirmation
Our experts investigate to confirm who is attacking you and what they are doing.

Analysis by Experts
Experts include malware reverse engineers, network & intel analysts and forensics specialists.

Insight into Attacker Activity
Data analysis of attacker communications shows you exactly what the attacker is doing, including what data they are stealing.
**Mandiant Network Threat Detection**

Mandiant’s unique combination of intelligence, expert analysis and post-processing is designed to combat the tactics of advanced attackers. With Mandiant you find attacks other network security solutions miss.

**CAPABILITIES**

The Mandiant Network Threat Detection service utilizes Mandiant’s proprietary network intelligence to identify active attacker activity such as command & control communications and data theft. When an attack is identified, Mandiant’s MCIRT® analysts investigate and provide visibility into what attackers are doing.

**Spear Phish Data Correlation**
- Spear phising detection identifies potential attacks when they are in their earliest stages
- Reconstruct e-mails from spear-phishing attacks

**Capture & Record Attacker Activity**
- Captures network traffic when attacker activity is observed
- Automated post processing and review by Mandiant analysts reveals attacker behavior

**Mandiant Intelligence**
- Attacker command & control infrastructure
- Advanced threat actor protocols and methods
- Malware analysis & behavior
- Centralized analysis leads to spread of new intelligence

**Insight into Attacker Communications**
- Visibility into attacker activity down to a single keystroke to see username/password and hashes
- In most cases Mandiant can determine exactly what data is being accessed or stolen

**Mandiant’s Intelligence**

What’s so special about Mandiant Intelligence? First, we keep our intelligence under extremely close guard. The fact that we don’t make it available to the public means the attackers don’t have it either so it maintains its effectiveness over time. We also constantly update the intelligence based on the latest attacks seen by our incident response team and our staff of network analysts.

**CASE STUDY**

**What Happened?** Things were quiet until suddenly Mandiant identified a known command and control channel using a certificate known to be used by an advanced threat actor.

**What Action Was Taken?** Mandiant analysts observed and analyzed the traffic to confirm the malicious nature of the communication and notified the customer within an hour of the traffic starting.

**What Was the Result?** The customer investigated and discovered that the machine was a laptop belonging to a contractor whose machine was never authorized to be connected to their network. Once identified, the customer was able to remove the machine from their network before it was able to do any damage.

Mandiant’s products and services protect the world’s most valuable data every day from targeted attacks. Our unique combination of intelligence, experience and technology equip organizations to detect, respond and contain attackers before they reach their objective.