You’ve seen the headlines. Today’s threat actors are savvy, sophisticated, and relentless. They target human vulnerabilities to slip through your preventive defenses. When they do, Mandiant Intelligent Response (MIR®) is the weapon that gives your team a decisive advantage over the adversary, revealing their every move and penetrating their attempts to stay hidden.

When attackers get through, Mandiant Intelligent Response® equips you to respond immediately and thoroughly to stop them before they complete their mission.

Product Overview

Are you compromised? How did the attacker get in? What systems are involved? Mandiant Intelligent Response lets you answer these questions so you can respond immediately and keep advanced attackers from achieving their objective in your systems.

- **Sweep Endpoints for Evidence of Compromise**
  Sweeps all of your endpoints for evidence of compromise including malware, general malware behaviors and non-malware attacker tactics.

- **Remotely Investigate Any Endpoint**
  Gets the data needed for investigation securely over the network, without having to wait for access to be granted or exposing administrative credentials to an attacker in control of a system. Collect images and full live response or ask for only the exact data you need.

- **Access Mandiant’s Intel & Create Your Own**
  Utilizes Mandiant’s latest Indicators of Compromise (IOC) library based on our experience on the front lines; you can create your own IOCs as well.

- **Triage Alerts With Automated Host Interrogation**
  Automatically collect info and analyze suspicious systems based on alerts generated by your SIEM, ticketing system or other applications.

HIGHLIGHTS

Unlike other host-based tools, Mandiant was specifically designed to detect and respond to advanced attacker activity.

- **Speed & Scale**
  Designed to rapidly sweep thousands of endpoints at once while other tools are optimized to deep dive one machine at a time.

- **Finds More Than Malware**
  Identifies attacker behavior in addition to malware so you can uncover what attackers are doing – not just their tools.

- **OpenIOC Support**
  Supports the XML-based OpenIOC standard so you can create, edit and share your own Indicators of Compromise.

- **Agent-Based Data Collection**
  Lightweight, non-intrusive agent enables remote data collection without impacting end user functionality.

- **Memory Forensics**
  Analyze live memory without downloading memory images to uncover malware that hides from normal tools.
As soon as you detect a compromise, MIR® allows your team to scale and rapidly investigate thousands of endpoints to determine what systems are compromised and what the attackers are after.

PRODUCT CAPABILITIES
The Mandiant Intelligent Response appliance finds evidence of compromise and forensic artifacts on your endpoints left behind by attacker activity. With MIR you can rapidly sweep tens of thousands of endpoints using Mandiant’s latest intelligence about advanced attacker activity.

OpenIOC Support
- Investigate with your own custom indicators or with those shared by others using the OpenIOC standard.
- Access Mandiant’s proprietary library of Indicators of Compromise (IOC) and develop your own custom indicators using the OpenIOC format.

Response-Focused Forensics
- Hybrid disk / memory forensics perform analysis impossible with conventional tools.

Targeted Data Acquisition at Scale
- Intelligent filtering capabilities in the agent return only the data you need.
- Find answers to forensic questions on thousands of hosts at a time.

Rapid Live Response
- Pre-deployed agents provide immediate, full remote forensic access to any system.
- On-host analysis enables full investigation over slow WAN links without waiting for memory or disk image downloads.

Integration With Other Products
- Works with Mandiant Redline™ to point users to the best-hidden malicious processes.
- Integrates with other detection systems to automate triage of hosts with suspicious activity.

HOW IT WORKS
MIR’s “secret sauce” is the unique combination of Mandiant-based intelligence (gathered from all of our incident response consulting work done worldwide) and your own intelligence working together to search for evidence of compromise.

MIR agents are first deployed to all of your endpoints and are controlled via the Mandiant Console.

The MIR controller is armed initially with Mandiant Indicators of Compromise (IOCs) to do the initial sweep of every host in your environment.

Suspicious hosts are flagged for investigation and you are able to add your own IOCs and continue to sweep your entire environment in order to confirm the scope of the attack, identify all compromised hosts, and move quickly and effectively towards containment and remediation.

CASE STUDY

Thwarts a Bank Heist

Event: A mid-size bank with over $1 billion in assets received two alerts of a potential problem on their network. The first alert was from a Federal law enforcement agency which had received a tip that the bank was targeted. The second alert came from customers who noticed irregular activity in their accounts.

Action: MIR was deployed, collecting data from over 550 systems in their enterprise within three hours.

Remediation: The bank was able to quickly determine which systems had been compromised, what data had been stolen, and even identify dormant malware left behind by the attackers. The information enabled the bank to ensure that the attackers were extricated from their enterprise and normal operations could resume.