Incident Response Service

Case Study: Mandiant IR at work

A multinational professional services firm, with tens of thousands of computers deployed around the world, engaged Mandiant to respond to a potential data breach of critical client data. All work was conducted remotely.

Day 1 - Mandiant consultants began to deploy cloud-based endpoint technology within four hours of notification to 18,000 systems.

- The investigation started that same day.
- Confirmed evidence of compromise was identified within hours of the investigation.

Day 6 - The majority of investigative work completed. Analysis performed on over 18,000 endpoints with in-depth live response analysis of 80 systems.

Day 7 -Containment performed with no disruption to business. Mandiant experts continued to monitor the network to ensure no re-attempts of compromise from the threat actor.

Day 11 - Client was back to business as usual.

Investigate, contain, and remediate critical security incidents with speed, scale, and efficiency

Mandiant incident responders have been on the frontlines of the most complex breaches worldwide since 2004. Unparalleled access to dedicated Mandiant threat intelligence teams provide our incident responders with the very latest attacker tactics, techniques, and procedures (TTPs).

Mandiant's work on the largest and most publicized cyber attacks uniquely qualifies our experts to assist clients with all aspects of an incident response—from technical response to crisis management. We help clients investigate and remediate faster and more efficiently, so they can get back to business.

Overview

The use of cloud and on-premise solutions allow investigations to begin immediately, while managing client data privacy concerns. Within hours, Mandiant incident responders can begin analyzing network traffic and information from thousands of endpoints.

Mandiant experts understand that comprehensive incident and breach response extends beyond the technical investigation, containment, and recovery phases. Therefore, we also assist with executive communication and crisis management—including legal, regulatory, and public relations considerations. Crisis management is critical for controlling reputational damage and legal liabilities.

TABLE 1. Types of incidents we typically manage.

Intellectual property theft	Theft of trade secrets or other sensitive information.
Financial crime	Payment card data theft, illicit ACH/EFT cash transfers, extortion, and ransomware.
Personally identifiable information (PII)	Exposure of information used to uniquely identify individuals.
Protected Health Information (PHI)	Exposure of protected health care information.
Insider threats	Inappropriate or unlawful activity performed by employees, vendors, and other insiders.
Destructive attacks	Attacks solely intended to cause the victim organization hardship by making information or systems unrecoverable.

- **Investigative experience.** Mandiant investigators have honed their skills by conducting and remediating the world's largest and most complex investigations.
- **Threat intelligence.** Industry-leading intelligence assembled from the frontlines of incident response engagements, extensive attacker tradecraft discovery and research through third-party data sources, and Dynamic Threat Intelligence collected by Mandiant threat analyst teams.
- **Crisis management.** Incident responders have years of experience advising clients on incident-related communications—including executive communications, public relations, and disclosure requirements.
- **Malware analysis.** Mandiant reverse engineers analyze malware and write custom decoders and parsers to provide insight into the capabilities and TTPs used by today's attackers.
- **24/7 coverage.** Around the clock attacker activity analysis during investigation and remediation provided by Mandiant Managed Defense.

Our approach

Mandiant investigations include host-, network- and event-based analyses for a comprehensive, holistic assessment of the environment. Our response actions are tailored to help clients respond to and recover from an incident, while managing regulatory requirements and reputational damage. During investigations, Mandiant consultants typically identify:

- Affected applications, networks, systems, and user accounts
- Malicious software and exploited vulnerabilities
- Information accessed or stolen

Incident analysis

1. **Technology deployment and investigation of initial leads:** Deploy the technology most appropriate for a fast and comprehensive incident response. We simultaneously investigate initial client-provided leads to start building Indicators of Compromise (IOCs) that will identify attacker activity, while sweeping the environment for all indicators of malicious activity.
2. **Crisis management planning:** Work with executives, legal teams, business leaders, and senior security personnel to develop a crisis management plan.
3. **Incident scoping:** Monitor real-time attacker activity and search for forensic evidence of past attacker activity to determine the scope of the incident.
4. **In-depth analysis:** Analyze actions taken by the attacker to determine the initial attack vector, establish timeline of activity, and identify extent of the compromise.

   This can include:

   - Live response analysis
   - Forensic analysis
   - Network traffic analysis
   - Log analysis
   - Malware analysis
5. **Damage assessment:** Identify impacted systems, facilities, applications, and information exposure.
6. **Remediation:** Develop a custom containment and remediation strategy based on the actions of the attacker and tailored to the needs of the business. This will eliminate the attacker's access and improve the security posture of the environment to help prevent or limit the damage from future attacks.

Deliverables

Executive, investigative, and remediation reports that withstand third party scrutiny.

- **Executive summary:** High-level summary explaining the timing and investigative process, major findings, and containment activities.
- **Investigative report:** Details on the attack timeline and critical path (how the attacker operated in the environment). Reports include a list of affected computers, locations, user accounts, and information that was stolen or at risk.
- **Remediation report:** Details of containment measures taken, including strategic recommendations to enhance the organization's security posture.