Compromise Assessment

Why Mandiant

Mandiant has been at the forefront of cybersecurity and cyber threat intelligence since 2004. Our incident responders have been on the frontlines of the most complex breaches worldwide. We have a deep understanding of both existing and emerging threat actors, as well as their rapidly changing tactics, techniques and procedures.

Benefits

- Analysis of your specific environment to find evidence of ongoing or past compromise
- A view into systemic risks and exposures
- Identification of security hygiene issues
- Recommendations to improve your organization's incident response
- Flexibility to deploy on-premises or cloud-hosted technology

A Mandiant Compromise Assessment combines our extensive experience responding to intrusions carried out by advanced threat actors and industry-leading threat intelligence to deliver an assessment that:

- Identifies ongoing or past intrusions within your organization
- Assesses risk by identifying weaknesses in security architecture, vulnerabilities, improper usage or policy violations, and system security misconfigurations
- Increases your organization's ability to respond effectively to future incidents

The need for compromise assessments

High-profile data breaches in the news represent only a fraction of the intrusion activity carried out globally. Knowing whether your organization has been breached and identifying ways to reduce risk is crucial to preventing your organization from becoming the next major data breach headline.

Our approach

We combine our extensive experience responding to global intrusions and unparalleled analysis of industry-leading threat intelligence to deliver an assessment that meets your business objectives with speed, scale, and efficiency. In addition to identifying evidence of past or ongoing attacker activity, the assessment offers:

- **Context derived from threat intelligence**
  Provides insight into attacker attribution and motivation so organizations know if they are being targeted.
- **Identification of risks**
  Identifies security architecture and configuration weaknesses, including missing patches, or security software.
- **Facilitation of future investigations**
  Recommends strategic options that can better prepare your organization's security team to respond to intrusions.

Mandiant consultants search endpoints, monitor network traffic, inspect email, and analyze logs from other security devices for evidence of attacker activity. The consultants also use signatureless data analysis techniques to find previously unseen attacker activity. Customers choose the correct combination of technologies that makes the most sense for their environment.

- **Endpoint inspection.** Mandiant consultants provide real-time detection of attacker activity including malware and other TTPs and investigate Windows, macOS and Linux endpoints—with the flexibility of on-premises and cloud deployments.
- **Network inspection.** Mandiant consultants strategically detect compromise activity such as malware command and control communication, unauthorized remote access, and data theft.
- **Email inspection.** Mandiant consultants inspect inbound and outbound email. Our expert and dynamic inspection of attachments enables the identification of intrusion campaigns.
- **Log inspection.** Mandiant consultants leverage multiple technologies to review logs from applications and infrastructure to identify malicious activity.

Endpoint inspection

- Real-time alerting of ongoing suspicious or malicious activity
- Commodity malware detection
- Cross-platform operating system support
  - Windows
  - macOS
  - Linux
- Identification of anomalies that would indicate the presence of advanced malware

Network inspection

- Full packet capture combined with custom detection signatures
- Automated detection and decoding of attacker command and control traffic

Email inspection

- Detect targeted phishing attacks used by attackers to regain access to the environment after a remediation event
- Analysis of email attachments and URLs against a comprehensive cross-matrix of operating systems, applications and web browsers
- Support analysis against Microsoft Windows and macOS operating system images
- Uncover threats hidden in files including password-protected and encrypted attachments