MANDIANT

DATASHEET

COMPROMISE ASSESSMENT

Identify ongoing or past attacker activity in your environment

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 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

- Comprehensive analysis of your specific environment focused on finding evidence of ongoing or past compromise
- Provides a view into systemic risks and exposures
- Identifies security hygiene issues
- Provides recommendations for furthering your organization's ability to effectively respond to future incidents
- 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, industry-leading threat intelligence and FireEye technology 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 intrusions and industry-leading threat intelligence with a modular stack of FireEye technology to deliver an assessment that meets your business objectives with speed, scale, and efficiency. In addition to identifying evidence of past or ongoing attack 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 use FireEye technologies to 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.** FireEye Endpoint Security agents are used to provide real-time detection of attacker activity, including malware and other tactics, techniques and procedures, and investigate Windows, macOS and Linux endpoints. Mandiant experts provide the flexibility of on-premises and cloud deployments.
- **Network inspection.** FireEye Network Security sensors are deployed in strategic monitoring locations in your enterprise to detect compromise activity such as malware command and control communication, unauthorized remote access, and data theft.
- **Email inspection.** FireEye Email Security monitoring is conducted on premises or from the cloud and can be configured to passively inspect inbound and outbound email. Dynamic inspection of attachments allows Mandiant experts to identify intrusion campaigns before other signature-based products.
- **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 using the FireEye agent's built-in antivirus engine
- 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

- Detects targeted phishing attacks used by attackers to regain access to the environment after a remediation event
- Leverages the signatureless Multi-Vector Virtual Execution™ (MVX) engine to analyze email attachments and URLs against a comprehensive cross-matrix of operating systems, applications and web browsers
- Supports analysis against Microsoft Windows and macOS operating system images
- Analyzes threats hidden in files including password-protected and encrypted attachments

Learn more at **www.mandiant.com/consulting**

Mandiant
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300
833.3MANDIANT (362.6342)
info@mandiant.com

About Mandiant
Since 2004, Mandiant has been a trusted security leader to organizations that can't afford to fail. Today Mandiant delivers decades of frontline insights at scale through easy-to-deploy and consume SaaS solutions for provable and transformative cyber defense.

MANDIANT