MANDIANT
NOW PART OF Google Cloud

AUTOMATED DEFENSE DATASHEET

Breach Analytics for Chronicle

Highlights

- Discover who is targeting your organization and what they are after
- Get an early knowledge advantage from Mandiant Threat Intelligence
- Find qualified IOCs fast
- Save time for the security analyst

Mitigate the risk of a headline breach with an early knowledge advantage

Cyber security breaches have increased over the last decade, with more aggressive threat actors and more targeted attacks. When another breach makes headlines, many CISOs and security professionals wonder, "Could we have been compromised by that same attack?"

Mandiant Breach Analytics for Chronicle uses findings from Mandiant Incident Response and deep threat intelligence research to systematically reduce an organization's threat exposure. Automation delivers continuous, proactive detection of new adversary presence and behavior at a fraction of the cost of today's manual efforts.

Real-time threat insights

Reliance on traditional rule-based or signature technologies, and open-source repositories, is simply not enough. The lag between threat discovery and SIEM rule writing and deployment, and the fact that open sources are visible to adversaries, can result in missed indicators of compromise (IOC). Breach Analytics can help minimize this lag and facilitate better security decision-making.

Powered by the Mandiant Intel Grid™, which contains a trove of information that may not all be widely known or categorized, Breach Analytics takes the latest indicators of compromise from Mandiant Incident Response engagements, insight from our threat intelligence analysts and frontline learnings from Mandiant Managed Defense clients. It continuously compares them to your current and historical cyber security data to create your early knowledge advantage.

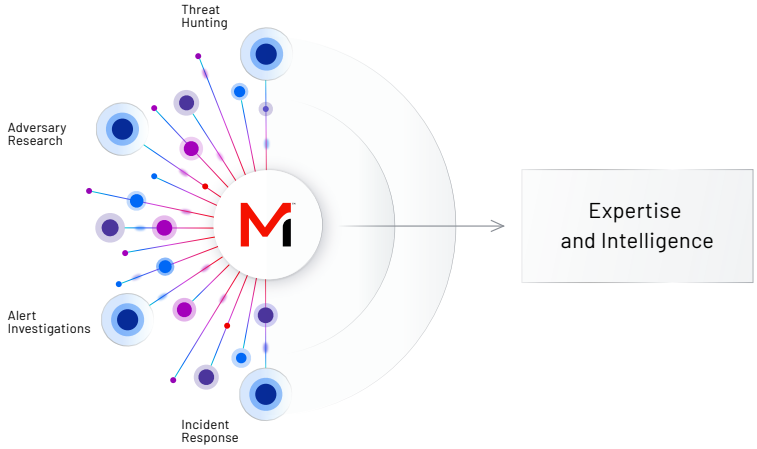

FIGURE 1. Mandiant Intel Grid.™

Rapid prioritization of meaningful IOCs

IOC matches are also prioritized against alert-based contextual information and the Mandiant IC-Score, a data science-based "maliciousness" scoring algorithm that filters out benign indicators and helps teams focus on relevant, high-priority IOCs.

Systems considered to be "clean" can be presented with new threats as adversaries and their motivations keep evolving with their attacks sophistication and techniques. Pointing out geography and industry prevalence and indications of active incident response operations significantly reduce the discoverability time and increase available time to investigate.

Fast time-to-value

Organizations using the Google Cloud Chronicle SIEM can quickly deploy and easily start Breach Analytics via the Mandiant Advantage SaaS platform. Once operational, teams gain actionable 24x7 access to Mandiant Threat Intelligence and can analyze system and network logs throughout their IT environments—endpoint, network, on premise and the cloud—to detect underlying IOCs. They can then identify, review and take actions on them to reduce the impact of targeted attacks. Dramatic reduction of false positives decreases mean-time-to-detect—how long an attacker "dwells" in a network before being detected.

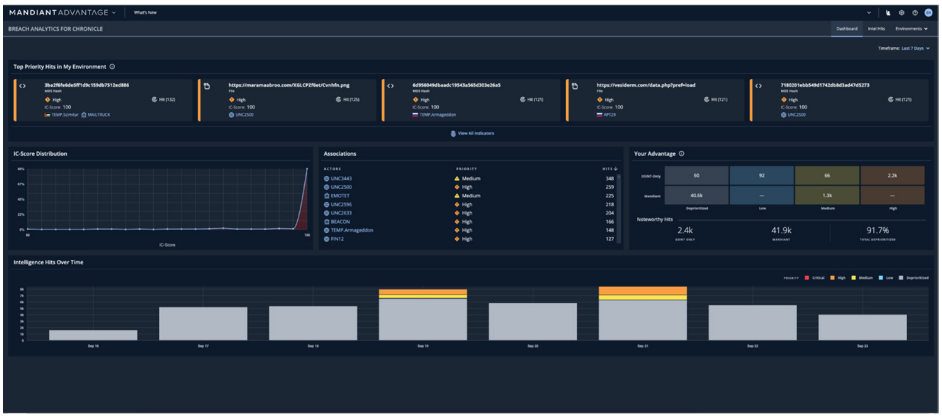

FIGURE 2. Critical IOCs are prioritized based on two decisions: time and relevancy. Customers can click-to-contact Mandiant for rapid response.

Source and Indicators

Mandiant Breach Analytics includes various indicator data.

- Indicator sources
  - OSINT
  - Mandiant Indicator List
- Indicator Types
  - Domains
  - IP Address
  - Hash (SHA1, SHA256, SHA512, MD5)
  - URLs

Why Mandiant

- 200K+ hours responding to attacks per year
- 3K+ threat actors tracked at any time
- 600+ consultants in over 25 countries
- 300+ security researchers and intelligence analysts
- 70+ third-party security controls supported

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

Mandiant
11951 Freedom Dr, 6th Fl, Reston, VA 20190
(703) 935-1700
833.3MANDIANT (362.6342)
info@mandiant.com

About Mandiant
Since 2004, Mandiant® has been a trusted partner to security-conscious organizations. Today, industry-leading Mandiant threat intelligence and expertise drive dynamic solutions that help organizations develop more effective programs and instill confidence in their cyber readiness.

MANDIANT
NOW PART OF Google Cloud