MANDIANT®

DATA SHEET

Threat Intelligence Application Programming Interface (API)

Integrate industry-leading Mandiant Threat Intelligence into your security systems

FEATURES

To help you integrate and customize our threat intelligence, the API offers:

- **Structured Threat Information Expression (STIX) 2.1 Support:** Uses a data format structure (represented in JSON) that makes it easier to contribute to and ingest cyber threat intelligence while preserving relationships between data objects.
- **Rapid Delivery:** Decouples indicators from reports and delivers them at near-real-time in some cases to increase actionability and usability.
- **Confidence Scoring:** Scores indicators according to confidence on a scale of 0-100.
- **Digital Threat Monitoring:** Provides customers with the ability to receive and filter (based on user options) large volumes of data related to Mandiant Digital Threat Monitoring.
- **Enhanced Metadata:** Includes metadata fields for indicator revocation and external references to reports.
- **Flexible Intelligence Reporting:** Delivers intelligence reports that can be consumed in both machine- (STIX 2.1) and human-readable (PDF, HTML) formats.
- **Intelligent Search:** Provides pattern- and relationship-based searches to quickly find the right intelligence and receive relevant results.

Mandiant customers can quickly and easily incorporate expert threat analysis into their daily security decisions with the Application Programming Interface (API) for Mandiant Threat Intelligence.

With the Mandiant Threat Intelligence API, you can integrate industry-leading Mandiant Threat Intelligence into your protection, detection, investigation and response processes, and fuse it with your security infrastructure and compliance management technologies. The API links your security technologies to the Mandiant Threat Intelligence cloud, which houses more than a decade of the most comprehensive, global cyber threat intelligence available today.

Simple and Flexible Integration Options

The Mandiant Threat Intelligence API provides machine-to-machine-integration with the most contextually rich threat intelligence data available on the market today. The API provides automated access to indicators of compromise (IOCs)—IP addresses, domain names, URLs used by threat actors—as well as information on the adversary, to further enrich integrations. The API supports Python, Java, PHP, C++, and C# programming languages. For more information, read the full **Mandiant Threat Intelligence API documentation online**.

Table 1. Mandiant Threat Intelligence API v.3 features.

Indicators	Report-less indicators and Reports with indicators (Indicators from reports AND Indicators without reports)
Reports	Supported formats: • HTML • PDF • STIX 2.1 JSON
Actors / Malware	Actors, malware families and relationships available in both indicators and reports
Search	Relationship and pattern-based searches
Pivot	Relationship-based searches

Applications

Immediate access to Mandiant Threat Intelligence can influence your most critical decisions, processes and priorities, and help move your organization from a reactive to a proactive security posture. You can put the API to use in several aspects of your security program, including:

- **Security Operations:** Match IOCs with events in your SIEM or security analytics platforms, cut through the noise and automate the prioritization of events that warrant scrutiny.
- **Incident Response:** Gain deep situational awareness with direct access to rich intelligence within the IR, analytics and forensics systems you use daily.
- **Vulnerability and Patch Management:** Access Vulnerability and Exploitation data, which provides rapid access to critical information– often before it appears in the National Vulnerability Database or acquires an assigned CVE number.
- **Network Operations:** Access highly validated IOCs to block attacks with confidence.

For more information on how Mandiant Threat Intelligence can help you stay aware and ahead of cyber threats, visit: **www.FireEye.com/intel**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About Mandiant Solutions

Mandiant Solutions brings together the world's leading threat intelligence and frontline expertise with continuous security validation to arm organizations with the tools needed to increase security effectiveness and reduce business risk.

MANDIANT®