Mandiant

THREAT INTELLIGENCE INTEGRATIONS

In addition to a number of integrations supported by our legacy APIs, Mandiant Advantage Threat Intelligence (MATI) can be consumed, analyzed, and operationalized in a number of platforms central to our customers' existing threat intelligence workflows utilizing our **Threat Intelligence API** (https://docs.mandiant.com/home/mati-threat-intelligence-api-v4).

Mandiant integrations

The following integrations were developed and are maintained by Mandiant:

Integration	Developed By	Description	Mandiant API Version	Type	Vendor Links
Cortex XSOAR (Enrichment)	Mandiant	Collects threat intelligence from Mandiant and adds it to the Cortex XSOAR indicator store for use during automated enrichment and investigations	v4	SOAR	**Learn More and Download** (https://docs.mandiant.com/home/mati-palo-alto-cortex-xsoar-integration)
Elastic SIEM	Mandiant	Collects threat intelligence from Mandiant for correlation in Elastic SIEM to help discover potential threats.	v4	SIEM	**Learn More and Download** (https://docs.elastic.co/integrations/ti_mandiant_advantage)
IBM QRadar	Mandiant	Collect indicators and ingest into the QRadar SIEM to drive correlation and alerting	v4	SIEM	**Learn More and Download** (https://docs.mandiant.com/home/mandiant-advantage-for-ibm-qradar)
Maltego	Mandiant	Enriches indicators with intelligence from Mandiant	v4	Analyst Research	**Learn More and Download** (https://www.maltego.com/downloads/)

Integration	Developed By	Description	Mandiant API Version	Type	Vendor Links
Microsoft Sentinel / Defender for Endpoint	Mandiant	An Azure Logic App that collects indicators from Mandiant and adds them to either Microsoft Sentinel or Defender for Endpoint using the Microsoft Graph Security API	v4	SIEM / Endpoint	**Docker version** (https://docs.mandiant.com/home/mati-microsoft-sentinel-and-defender-integrations-docker-setup-guide) **Azure Logic App version** (https://docs.mandiant.com/home/microsoft-sentinel-defender-atp-integration-admin-guide)
MISP	Mandiant	The Mandiant MISP Collector allows users to pull in threat intelligence from Mandiant into MISP's open-source data aggregation and threat sharing platform	v4	TIP	**Learn More and Download** (https://docs.mandiant.com/home/mandiant-misp-collector)
ServiceNow Vuln Response	Mandiant	The Vulnerability Response app, powered by Mandiant, enhances customers' vulnerability prioritization workflows and enable efficient remediation of vulnerabilities.	v4	Vulnerability Response	**Learn More and Download** (https://store.servicenow.com/sn_appstore_store.do#!/store/application/2e6c4e6d876b8e1455bd53d73cbb35f4)

Integration	Developed By	Description	Mandiant API Version	Type	Vendor Links
Splunk SIEM	Mandiant	The Mandiant Advantage App for Splunk allows users to pull in threat intelligence from Mandiant into Splunk's powerful data platform	v4	SIEM	**Learn More and Download** (https://docs.mandiant.com/home/mandiant-advantage-for-splunk)
Splunk SIEM (Cloud)	Mandiant	This Splunk Cloud-focused app is a lightweight app focused on ingesting Indicators of Compromise (IoC) for use in Splunk detections.	v4	SIEM	**Learn More** (https://splunkbase.splunk.com/app/7306)
Splunk SOAR	Mandiant	Pulls Mandiant data into Splunk SOAR for infrastructure orchestration, case management, playbook automation, and integrated threat intelligence	v4	SOAR	**Learn More and Download** (https://docs.mandiant.com/home/mati-splunk-soar-integration)

Google and Mandiant integrations

The following integrations were co-developed by Google and Mandiant as a joint offering for Google Cloud Security customers:

Integration	Developed By	Description	Mandiant API Version	Type	Vendor Links
VirusTotal	VirusTotal	Joint customers can now see Mandiant Threat Intelligence data (IoC reputation, malware toolkit/family attribution, threat actor attribution} in VirusTotal IoC (domain, IP, URL, file) reports.	v4	TIP	**Learn More** (https://developers.virustotal.com/docs/docs-mandiant-connector)

Technical Accelerators

The following technical acceleration (TA) scripts are developed by the Mandiant Intel Services tech team, and are supported as time allows. These TA scripts enable you to interact with the API and are primarily provided for example code and to demonstrate specific use cases where an official integration may not exist.

Integration	Developed By	Description	Mandiant API Version	Type	Vendor Links
Mandiant MAVE (v1.22)	Mandiant	Enriches a given list of vulnerabilities with intelligence from Mandiant	v4	App	**Learn More and Download (https://docs.mandiant.com/home/mati-mandiant-mave-integration)**
Mandiant Threat Intel Client for Python	Mandiant	Library that enables developers/customers to easily access the Mandiant Advantage Threat Intelligence data and use it in their own scripts and systems.	v4	Library	**Learn More and Download (https://github.com/google/mandiant-ti-client)**
MicroFocus ArcSIght	Mandiant	Collects indicators from Mandiant and adds them to an ArcSight index to drive correlation searches for alerting and threat hunting	v4	SIEM	Pending

Third-party integrations

The following integrations were developed and are maintained by the third-party vendors listed:

Integration	Developed By	Description	Mandiant API Version	Type	Vendor Links
Analyst1	Analyst1	Access and organize Mandiant intelligence reports using the Analyst1 platform	v4	TIP	**Learn More (https://analyst1.com/partners/)**
Anomali ThreatStream	Anomali	The Anomali integration with Mandiant provides access to contextually rich threat intelligence from Mandiant including indicators of compromise, threat actors, malware families, and finished intelligence reports.	v4	TIP	**Learn More and Download (https://ui.threatstream.com/store?q=mandiant)**

Integration	Developed By	Description	Mandiant API Version	Type	Vendor Links
Cyware	Cyware Situational Awareness Platform	Collects intelligence from Mandiant and makes it available in the Cyware security operations platform	v4	TIP	**Learn More and Download (https://cyware.com/)**
EclecticIQ	EclecticIQ	Collects intelligence from Mandiant and makes it available in the EclecticIQ security operations platform	v4	TIP	**Learn More and Download (https://www.eclecticiq.com/partners)**
Netskope	Netskope	Collects intelligence from Mandiant and makes it available in the Netskope security operations platform	v4	SIEM / UEBA	Pending
Nucleus	Nucleus	Collects intelligence from Mandiant and makes it available in the Nucleus vulnerability management platform	v4	Vulnerability Intelligence	**Learn More and Download (https://nucleussec.com/threat-intelligence/)**
OpenCTI	OpenCTI	The Open CTI integration collects intelligence from Mandiant, including, indicators, threat actors, malware families, and vulnerabilities; and makes the data available in the Open CTI platform	v4	TIP	**Learn More and Download (https://github.com/OpenCTI-Platform/connectors/tree/master/external-import/mandiant)**
Polarity	Polarity	Collects intelligence from Mandiant and makes it available in the Polarity security operations platform	v3 and v4	TIP	**Learn More and Download (https://polarity.io/integrations/mandiant/)**

Integration	Developed By	Description	Mandiant API Version	Type	Vendor Links
Recorded Future	Recorded Future	Collects intelligence from Mandiant and makes it available into Intelligence Cards within Recorded Future	v4	TIP	**Learn More and Download (https://www.recordedfuture.com/intelligence-card-extension)**
Securonix	Securonix	Collects intelligence from Mandiant and makes it available in the Securonix Unified Defense SIEM platform	v4	SIEM	**Learn More and Download (https://documentation.securonix.com/bundle/securonix-cloud-user-guide/page/content/active-deployment-guides/google-mandiant-third-party-intelligence.htm)**
					Learn More and Download (https://assets.sentinelone.com/mandiantsb/automatically-enrich-detection-sb?lb-mode=overlay&gclid=Cj0KCQjw2eilBhCCARIsAG0Pf8s0LfLcWREVT-6NSELnjs6

Integration	Developed By	Description	Mandiant API Version	Type	Vendor Links
SentinelOne	SentinelOne	Collects intelligence from Mandiant and makes it available in the Sentinel One XDR platform	v4	XDR	1CRjl149-95VDG2uWCJ4OH8NFOa75EzkaAgUDEALw_wcB&utm_medium=paid-search&utm_source=google-paid&utm_campaign=seur-bau-trademark&utm_term=Sentinelone&utm_medium=paid-search&utm_source=google-paid&utm_campaign=seur-bau-trademark&utm_term=Sentinelone&gclid=Cj0KCQjw2eilBhCCARIsAG0Pf8s0LfLcWREVT-6NSELnjs61CRjl149-95VDG2uWCJ4OH8NFOa75EzkaAgUDEALw_wcB)
Siemplify	Siemplify	Collects intelligence from Mandiant and makes it available in the Siemplify security operations platform	v4	SOAR	Learn More and Download (https://www.siemplify.co/marketplace/search/?search=mandiant)

Integration	Developed By	Description	Mandiant API Version	Type	Vendor Links
Silobreaker	Silobreaker	Collects intelligence from Mandiant and makes it available in the Splunk Threat Intelligence platform	v4	TIP	**Learn More and Download (https://www.silobreaker.com/partners/integration-partners/mandiant/)**
Splunk Threat Intelligence	Splunk	Collects intelligence from Mandiant and makes it available in the ThreatConnect security operations platform	v4	TIP	**Learn More and Download (https://docs.splunk.com/Documentation/SIM/current/User/Threatintelsources)**
Sumo Logic SOAR	Sumo	Collects intelligence from Mandiant and makes it available in the Sumo security operations platform	v4	SOAR	**Learn More (https://help.sumologic.com/docs/platform-services/automation-service/app-central/integrations/mandiant-advantage-threat-intelligence/#mandiant-threat-intelligence-configuration)**

Integration	Developed By	Description	Mandiant API Version	Type	Vendor Links
Swimlane	Swimlane	The Mandiant Threat Intelligence plugin integrates with Swimlane to express cyber threats and provide observable information.	v4	SOAR	**Learn More and Download** (https://aphub.swimlane.com/swimbundles/swimlane/sw_mandiant_threat_intelligence_v4)
Synapse	Vertex	Collects intelligence from Mandiant and makes it available in the Synapse security operations platform	v4	TIP	**Learn More and Download** (https://synapse.docs.vertex.link/projects/rapid-powerups/en/latest/storm-packages/synapse-mandiant/index.html)
Threat Command	Rapid7	Collects intelligence from Mandiant and makes it available in the Rapid7 Threat Command platform	v4	TIP	**Learn More and Download** (https://docs.rapid7.com/threat-command/tip-sources/)
ThreatConnect	ThreatConnect	Collects intelligence from Mandiant and makes it available in the ThreatQuotient platform	v4	TIP	**Learn More and Download** (https://threatconnect.com/marketplace/mandiant/)

Integration	Developed By	Description	Mandiant API Version	Type	Vendor Links
ThreatQuotient	ThreatQuotient	Collects intelligence from Mandiant and makes it available in the ThreatQuotient platform	v4	TIP	**Learn More and Download (https://marketplace.threatq.com/details/mandiant-threat-intelligence-cdf)**
Vulcan	Vulcan Platform	Mandiant adds another layer of intelligence to the CVE severity based on extensive vulnerabilities research.	v4	Vulnerability Intelligence	**Learn More and Download (https://help.vulcancyber.com/en/articles/5834793-mandiant-connector)**