Mandiant

MATI XSOAR ENRICHMENT INTEGRATION

Integration settings

Parameter	Description	Required
API Key	Your API Key from Mandiant Advantage Threat Intelligence	True
Secret Key	Your Secret Key from Mandiant Advantage Threat Intelligence	True
Timeout	API calls timeout	False
Source Reliability	Reliability of the source providing the intelligence data	True
Traffic Light Protocol Color	The Traffic Light Protocol (TLP) designation to apply to indicators enriched	False
Tags	Supports CSV values	False
Map Attack Pattern Relationships to Mitre ATT&CK	When enabled the integration will attempt to map Attack Pattern relationships to Attack Pattern Indicators created by the Mitre ATT&CK Integration	False

Commands

Command-specific information is outlined in the following tabs.

Files

Get information about a file hash from Mandiant.

Base command

```
file
```

Input

Argument	Description	Required
file	List of files	True

Context output

Path	Type	Description
DBotScore.Score	number	The actual score calculated using the Mandiant Threat Score
DBotScore.Vendor	string	The vendor used to calculate the score
DBotScore.Indicator	String	The indicator that was tested
DBotScore.Type	string	The indicator type
DBotScore.Reliability	string	The reliability definition of the vendor used to calculate the score as defined in the integration settings

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

Path	Type	Description
File.SHA1	string	The SHA1 hash of the file
File.SHA256	string	The SHA256 hash of the file
File.MD5	string	The MD5 hash of the file
File.name	string	The name of the indicator
File.Campaign	string	A comma separated list of any campaigns associated with the indicator
File.TrafficLightProtocol	string	The traffic light protocol color associated with the indicator
File.Malicious.description	string	A description of why the file is malicious
File.Malicious.vendor	string	The vendor providing the description
File.MalwareFamily	string	A comma separated list of any Malware Families associated with the indicator
File.Relationships	list	A list of relationship objects associated with the indicator
File.Hashes	list	A list of hash objects associated with the indicator
Mandiant.File.threat_rating.confidence_level	string	The confidence level of the indicator's threat rating
Mandiant.File.threat_rating.confidence_score	number	The confidence score of the indicator's threat rating
Mandiant.File.threat_rating.severity_level	string	The severity level of the indicator
Mandiant.File.threat_rating.severity_reason	list	A list of severity reasons that contribute to the severity level of the indicator
Mandiant.File.threat_rating.threat_score	number	The threat score of the indicator
Mandiant.File.campaigns	list	A list of campaign objects associated with the indicator
Mandiant.File.last_seen	date	The date and time that the indicator was last seen
Mandiant.File.first_seen	date	The date and time that the indicator was first seen
Mandiant.File.mscore	number	The confidence score of the indicator
Mandiant.File.attributed_associations	list	A list of attribution objects (Threat Actors, Malware Families) associated with the indicator
Mandiant.File.value	string	The value of the indicator
Mandiant.File.last_updated	date	The date and time that the indicator was last updated by Mandiant

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

Path	Type	Description
Mandiant.File.associated_hashes	list	A list of file hashes associated with the indicator (MD5, SHA1, SHA256)
Mandiant.File.sources	list	A list of source objects associated with the indicator
Mandiant.File.type	string	The indicator's type
Mandiant.File.id	string	The indicator's Mandiant ID
Mandiant.File.reports	list	A list of Mandiant reports associated with the indicator

IPV4

Get information about an IP address from Mandiant.

Base command

```
ip
```

Input

Argument	Description	Required
ip	List of IPs	True

Context output

Path	Type	Description
DBotScore.Score	number	The actual score calculated using the Mandiant Threat Score
DBotScore.Vendor	string	The vendor used to calculate the score
DBotScore.Indicator	String	The indicator that was tested
DBotScore.Type	string	The indicator type
DBotScore.Reliability	string	The reliability definition of the vendor used to calculate the score as defined in the integration settings
IP.Address	string	The IP address value
IP.Campaign	string	A comma separated list of any campaigns associated with the indicator
IP.TrafficLightProtocol	string	The traffic light protocol color associated with the indicator
IP.MalwareFamily	string	A comma separated list of any Malware Families associated with the indicator
IP.Relationships	list	A list of relationship objects associated with the indicator
IP.STIXID	string	The stix id of the CVE

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

Path	Type	Description
IP.Publications	list	A list of report objects associated with the indicator
Mandiant.IP.threat_rating.confidence_level	string	The confidence level of the indicator's threat rating
Mandiant.IP.threat_rating.confidence_score	number	The confidence score of the indicator's threat rating
Mandiant.IP.threat_rating.severity_level	string	The severity level of the indicator
Mandiant.IP.threat_rating.severity_reason	list	A list of severity reasons that contribute to the severity level of the indicator
Mandiant.IP.threat_rating.threat_score	number	The threat score of the indicator
Mandiant.IP.campaigns	list	A list of campaign objects associated with the indicator
Mandiant.IP.last_seen	date	The date and time that the indicator was last seen
Mandiant.IP.first_seen	date	The date and time that the indicator was first seen
Mandiant.IP.mscore	number	The confidence score of the indicator
Mandiant.IP.attributed_associations	list	A list of attribution objects (Threat Actors, Malware Families) associated with the indicator
Mandiant.IP.value	string	The value of the indicator
Mandiant.IP.last_updated	date	The date and time that the indicator was last updated by Mandiant
Mandiant.IP.sources	list	A list of source objects associated with the indicator
Mandiant.IP.type	string	The indicator's type
Mandiant.IP.id	string	The indicator's Mandiant ID
Mandiant.IP.reports	list	A list of Mandiant reports associated with the indicator

URL

Get information about a URL from Mandiant.

Base command

```
url
```

Input

Argument	Description	Required
url	List of URLs	True

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

Context output

Path	Type	Description
DBotScore.Score	number	The actual score calculated using the Mandiant Threat Score
DBotScore.Vendor	string	The vendor used to calculate the score
DBotScore.Indicator	String	The indicator that was tested
DBotScore.Type	string	The indicator type
DBotScore.Reliability	string	The reliability definition of the vendor used to calculate the score as defined in the integration settings
URL.Data	string	The URL value
URL.Campaign	string	A comma separated list of any campaigns associated with the indicator
URL.TrafficLightProtocol	string	The traffic light protocol color associated with the indicator
URL.MalwareFamily	string	A comma separated list of any Malware Families associated with the indicator
URL.Relationships	list	A list of relationship objects associated with the indicator
URL.STIXID	string	The stix id of the CVE
Mandiant.URL.threat_rating.confidence_level	string	The confidence level of the indicator's threat rating
Mandiant.URL.threat_rating.confidence_score	number	The confidence score of the indicator's threat rating
Mandiant.URL.threat_rating.severity_level	string	The severity level of the indicator
Mandiant.URL.threat_rating.severity_reason	list	A list of severity reasons that contribute to the severity level of the indicator
Mandiant.URL.threat_rating.threat_score	number	The threat score of the indicator
Mandiant.URL.campaigns	list	A list of campaign objects associated with the indicator
Mandiant.URL.last_seen	date	The date and time that the indicator was last seen
Mandiant.URL.first_seen	date	The date and time that the indicator was first seen
Mandiant.URL.mscore	number	The confidence score of the indicator
Mandiant.URL.attributed_associations	list	A list of attribution objects (Threat Actors, Malware Families) associated with the indicator
Mandiant.URL.value	string	The value of the indicator

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

Path	Type	Description
Mandiant.URL.last_updated	date	The date and time that the indicator was last updated by Mandiant
Mandiant.URL.sources	list	A list of source objects associated with the indicator
Mandiant.URL.type	string	The indicator's type
Mandiant.URL.id	string	The indicator's Mandiant ID
Mandiant.URL.reports	list	A list of Mandiant reports associated with the indicator

Domains

Get information about a domain from Mandiant.

Base command

```
domain
```

Input

Argument	Description	Required
domain	List of domains	True

Context output

Path	Type	Description
DBotScore.Score	number	The actual score calculated using the Mandiant Threat Score
DBotScore.Vendor	string	The vendor used to calculate the score
DBotScore.Indicator	String	The indicator that was tested
DBotScore.Type	string	The indicator type
DBotScore.Reliability	string	The reliability definition of the vendor used to calculate the score as defined in the integration settings
Domain.name	string	The domain name
Domain.Campaign	string	A comma separated list of any campaigns associated with the indicator
Domain.TrafficLightProtocol	string	The traffic light protocol color associated with the indicator
Domain.MalwareFamily	string	A comma separated list of any Malware Families associated with the indicator
Domain.Relationships	list	A list of relationship objects associated with the indicator
Domain.STIXID	string	The stix id of the CVE

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

Path	Type	Description
Mandiant.Domain.threat_rating.confidence_level	string	The confidence level of the indicator's threat rating
Mandiant.Domain.threat_rating.confidence_score	number	The confidence score of the indicator's threat rating
Mandiant.Domain.threat_rating.severity_level	string	The severity level of the indicator
Mandiant.Domain.threat_rating.severity_reason	list	A list of severity reasons that contribute to the severity level of the indicator
Mandiant.Domain.threat_rating.threat_score	number	The threat score of the indicator
Mandiant.Domain.campaigns	list	A list of campaign objects associated with the indicator
Mandiant.Domain.last_seen	date	The date and time that the indicator was last seen
Mandiant.Domain.first_seen	date	The date and time that the indicator was first seen
Mandiant.Domain.mscore	number	The confidence score of the indicator
Mandiant.Domain.attributed_associations	list	A list of attribution objects (Threat Actors, Malware Families) associated with the indicator
Mandiant.Domain.value	string	The value of the indicator
Mandiant.Domain.last_updated	date	The date and time that the indicator was last updated by Mandiant
Mandiant.Domain.sources	list	A list of source objects associated with the indicator
Mandiant.Domain.type	string	The indicator's type
Mandiant.Domain.id	string	The indicator's Mandiant ID
Mandiant.Domain.reports	list	A list of Mandiant reports associated with the indicator

Vulnerabilities

Get information about a CVE from Mandiant.

Base command

```
cve
```

Input

Argument	Description	Required
cve	List of CVEs	True

Context output

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

Path	Type	Description
CVE.VulnerableConfigurations	list	A list of CPE objects
CVE.Publications	list	A list of reports associated with the CVE
CVE.Modified	date	The date that the CVE was last modified
CVE.STIXID	string	The stix id of the CVE
CVE.VulnerableProducts	list	A list of CPE objects
CVE.Published	date	The date that the CVE was last published
CVE.TrafficLightProtocol	string	The traffic light protocol color associated with the CVE
CVE.CVSS.score	number	The CVSS score of the CVE
CVE.CVSS.Vector	string	The CVSS Vector of the CVE
CVE.CVSS.Version	number	The CVSS version of the CVE
CVE.ID	string	The CVE ID
CVE.Description	string	A description of the CVE
DBotScore.Score	number	The actual score calculated using the CVSS score
DBotScore.Vendor	string	The vendor used to calculate the score
DBotScore.Indicator	String	The indicator that was tested
DBotScore.Type	string	The indicator type
DBotScore.Reliability	string	The reliability definition of the vendor used to calculate the score as defined in the integration settings
Mandiant.CVE.is_predicted	bool	If the risk rating was predicted (True) or set by an analyst (False)
Mandiant.CVE.date_of_disclosure	date	The date and time that the CVE was disclosed
Mandiant.CVE.associated_reports	list	A list of reports associated with the CVE
Mandiant.CVE.exploits	list	A list of exploits associated with the CVE
Mandiant.CVE.cve_id	string	The CVE ID of the CVE
Mandiant.CVE.workarounds_list	list	A list of workarounds associated with the CVE
Mandiant.CVE.vendor_fix_references	list	A list of vendor fix references associated with the CVE
Mandiant.CVE.version_history	list	A list of history objects containing links to detail about each version of the CVE

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

Path	Type	Description
Mandiant.CVE.risk_rating	list	The risk rating associated with the CVE
Mandiant.CVE.first_publish_date	date	The date and time that the CVE was fist published
Mandiant.CVE.exploitation_consequence	string	The exploitation consequence associated with the CVE
Mandiant.CVE.vulnerable_cpes	list	A list of vulnerable cpe objects associated with the CVE
Mandiant.CVE.updated_date	date	The date and time that the CVE was last updated
Mandiant.CVE.workarounds	string	A summary of any workarounds associated with the CVE
Mandiant.CVE.available_mitigation	list	A list of mitigations associated with the CVE
Mandiant.CVE.associated_actors	list	A list of Threat Actor objects associated with the CVE
Mandiant.CVE.title	string	The title of the CVE
Mandiant.CVE.common_vulnerability_scores	object	An object coontaining common vulnerability score objects associated with the CVE
Mandiant.CVE.sources	list	A list of sources associated with the CVE
Mandiant.CVE.type	string	The type of indicator
Mandiant.CVE.vulnerable_products	list	A summary of any vulnerable products associated with the CVE
Mandiant.CVE.exploitation_vectors	list	A list of exploitation vectors associated with the CVE
Mandiant.CVE.id	string	The Mandiant ID of the CVE
Mandiant.CVE.last_modified_date	date	The date and time that the CVE was last modified
Mandiant.CVE.observed_in_the_wild	bool	If the CVE was observed in the wild (True) of not (False)
Mandiant.CVE.was_zero_day	bool	If the CVE was determined to be a zero day exploit (True) of not (False)
Mandiant.CVE.exploitation_state	string	The current exploitation state of the CVE
Mandiant.CVE.associated_malware	list	A list of Malware Family objects associated with the CVE
Mandiant.CVE.description	string	A description of the CVE
Mandiant.CVE.cpe_ranges	list	A list of CPE objects objects associated with the CVE

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

Path	Type	Description
Mandiant.CVE.mve_id	string	The Mandiant Vulnerability ID of the CVE
Mandiant.CVE.publish_date	date	The date and time that the CVE was published
Mandiant.CVE.aliases	list	A list of alias objects associated with the CVE

Threat Actors

Get information about a Threat Actor from Mandiant.

Base command

```
mati-get-actor
```

Input

Argument	Description	Required
actor_name	Name of the actor to look up	True

Context output

Path	Type	Description
Mandiant.Actor.associated_uncs	list	UNC Threat Actors associated with the fetched Threat Actor
Mandiant.Actor.counts.aliases	number	The number of alternate names the fetched Threat Actor is known as
Mandiant.Actor.counts.associated_uncs	number	The number of UNC Threat Actors associated with the fetched Threat Actor
Mandiant.Actor.counts.attack_patterns	number	The number of Attack Patterns associated with the fetched Threat Actor
Mandiant.Actor.counts.cve	number	The number of vulnerabilities associated with the fetched Threat Actor
Mandiant.Actor.counts.industries	number	The number of industries targeted by the fetched Threat Actor
Mandiant.Actor.counts.malware	number	The number of Malware Families associated with the fetched Threat Actor
Mandiant.Actor.counts.reports	number	The number of finished intelligence reports associated with the fetched Threat Actor
Mandiant.Actor.audience	list	A list of audience objects describing who can read the Threat Actor information
Mandiant.Actor.observed	list	A list of observed objects describing when the Threat Actor was first and last seen
Mandiant.Actor.name	string	The name of the Threat Actor

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

Path	Type	Description
Mandiant.Actor.value	string	The name of the Threat Actor
Mandiant.Actor.last_updated	date	The date and time that the Threat Actor object was last updated by Mandiant
Mandiant.Actor.cve	list	A list of vulnerability objects associated with the Threat Actor
Mandiant.Actor.last_activity_time	date	The date and time that the Threat Actor object was last active
Mandiant.Actor.malware	list	A list of Malware Family objects associated with the Threat Actor
Mandiant.Actor.suspected_attribution	list	A list of Intel objects suspected to be associated with the Threat Actor
Mandiant.Actor.type	string	The Type of XSOAR indicator
Mandiant.Actor.id	string	The Mandiant ID of the Threat Actor
Mandiant.Actor.tools	list	A list of tool objects associated with the Threat Actor
Mandiant.Actor.industries	list	A list of industry objects associated with the Threat Actor
Mandiant.Actor.description	string	A description of the Threat Actor
Mandiant.Actor.motivations	list	A list of motivation objects associated with the Threat Actor
Mandiant.Actor.aliases	list	A list of alias objects describing alternate names associated with the Threat Actor
Mandiant.Actor.locations.source	list	A list of source location objects describing the country that the Threat Actor originates from
Mandiant.Actor.locations.target	list	A list of target country objects describing the countries that the Threat Actor targets
Mandiant.Actor.locations.target_region	list	A list of target region objects describing the regions that the Threat Actor targets
Mandiant.Actor.locations.target_sub_region	list	A list of target sub-region objects describing the sub-regions that the Threat Actor targets

Malware

Get information about a Malware Family from Mandiant.

Base command

```
mati-get-malware
```

Input

Argument	Description	Required
malware_name	Name of the malware family to look up	True

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

Mandiant

Context output

Path	Type	Description
Mandiant.Malware.counts.detections	number	The number of detections associated with the Malware Family
Mandiant.Malware.counts.cve	number	The number of vulnerabilities associated with the Malware Family
Mandiant.Malware.counts.malware	number	The number of Malware Families associated with the Malware Family
Mandiant.Malware.counts.capabilities	number	The number of capabilities associated with the Malware Family
Mandiant.Malware.counts.attack_patterns	number	The number of Attack Patterns associated with the Malware Family
Mandiant.Malware.counts.industries	number	The number of industries targeted by the Malware Family
Mandiant.Malware.counts.actors	number	The number of Threat Actors associated with the Malware Family
Mandiant.Malware.counts.aliases	number	The number of alternate names associated with the Malware Family
Mandiant.Malware.counts.reports	number	The number of finished intelligence reports associated with the Malware Family
Mandiant.Malware.audience	list	A list of audience objects describing who can read the Malware Family information
Mandiant.Malware.operating_systems	list	A list of operating systems that the Malware Family is known to impact
Mandiant.Malware.name	string	The name of the Malware Family
Mandiant.Malware.detections	list	A list of detections associated with the Malware Family
Mandiant.Malware.value	string	The name of the Malware Family
Mandiant.Malware.last_updated	date	The date and time that the Malware Family object was last updated by Mandiant
Mandiant.Malware.cve	list	A list of vulnerability objects associated with the Malware Family
Mandiant.Malware.last_activity_time	date	The date and time that the Malware Family object was last active
Mandiant.Malware.malware	list	A list of Malware Family objects associated with the Malware Family
Mandiant.Malware.capabilities	list	A list of capability objects associated with the Malware Family
Mandiant.Malware.yara	list	A list of yara rule objects associated with the Malware Family

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

Path	Type	Description
Mandiant.Malware.industries	list	A list of industry objects targeted by the Malware Family
Mandiant.Malware.roles	list	A list of roles associated with the Malware Family
Mandiant.Malware.actors	list	A list of Threat Actor objects associated with the Malware Family
Mandiant.Malware.aliases	list	A list of alias objects describing alternate names associated with the Malware Family
Mandiant.Malware.inherently_malicious	number	If 1, the object should be considered a Malware Family, if 0 the object is a Tool

Campaigns

Retrieve information about a Campaign from Mandiant.

Base command

```
mati-get-campaign
```

Input

Argument	Description	Required
campaign_id	ID of the campaign to lookup	True

Context output

Path	Type	Description
Mandiant.Campaign.counts.timeline	number	The number of events in the Campaign timeline
Mandiant.Campaign.counts.campaigns	number	The number of other Campaigns associated with the Campaign
Mandiant.Campaign.counts.malware	number	The number of Malware Families associated with the Campaign
Mandiant.Campaign.counts.actor_collaborations	number	The number of Threat Actor Collaborations associated with the Campaign
Mandiant.Campaign.counts.vulnerabilities	number	The number of Vulnerabilities associated with the Campaign
Mandiant.Campaign.counts.tools	number	The number of Tools associated with the Campaign
Mandiant.Campaign.counts.industries	number	The number of target industries associated with the Campaign
Mandiant.Campaign.counts.actors	number	The number of Threat Actors associated with the Campaign

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

Path	Type	Description
Mandiant.Campaign.counts.reports	number	The number of finished intelligence reports associated with the Campaign
Mandiant.Campaign.profile_update	date	The date and time that the profile of the Campaign was last updated
Mandiant.Campaign.campaign_type	string	The type of the Campaign
Mandiant.Campaign.name	string	The name of the Campaign
Mandiant.Campaign.short_name	string	The short name / ID of the Campaign
Mandiant.Campaign.target_locations.countries	list	A list of country objects that the Campaign targets
Mandiant.Campaign.target_locations.regions	list	A list of region objects that the Campaign targets
Mandiant.Campaign.target_locations.sub_regions	list	A list of sub-region objects that the Campaign targets
Mandiant.Campaign.value	string	The short name / ID of the Campaign
Mandiant.Campaign.last_activity_time	date	The date and time that the Campaign was last known to be active
Mandiant.Campaign.malware	list	A list of Malware Family objects associated with the Campaign
Mandiant.Campaign.actor_collaborations	list	A list of Actor Collaboration objects associated with the Campaign
Mandiant.Campaign.vulnerabilities	list	A list of Vulnerability objects associated with the Campaign
Mandiant.Campaign.type	string	The indicator type
Mandiant.Campaign.tools	list	A list of tool objects associated with the Campaign
Mandiant.Campaign.industries	list	A list of target industry objects associated with the Campaign
Mandiant.Campaign.actors	list	A list of Threat Actor objects associated with the Campaign
Mandiant.Campaign.aliases	list	A list of alias objects associated with the Campaign

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.