ThreatQuotient

Mandiant Intelligence Reports Operation Guide

Version 1.1.0

April 11, 2023

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: support@threatq.com
Web: support.threatq.com
Phone: 703.574.9893

Contents

Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Support

This integration is designated as **ThreatQ Supported**.

Support Email: support@threatq.com
Support Web: https://support.threatq.com
Support Phone: 703.574.9893

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.

> ⚠ ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.0
Compatible with ThreatQ Versions	>= 4.0.0
Support Tier	ThreatQ Supported
ThreatQ Marketplace	https://marketplace.threatq.com/details/mandiant-reports-operation

Introduction

The Mandiant Intelligence Reports operation allows users to submit indicators to Mandiant Intelligence and returns related reports and enrichment IOCs.

The operation provides the following actions:

- **Mandiant Report Link** - creates a link in ThreatQ to the Mandiant report.
- **Enrich** - provides enrichment information for the indicator.

The operation is compatible with indicator object types.

Installation

Perform the following steps to install the integration:

> The same steps can be used to upgrade the integration to a new version.

1. Log into https://marketplace.threatq.com/.
2. Locate and download the integration file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration file using one of the following methods:
   - Drag and drop the file into the dialog box
   - Select **Click to Browse** to locate the integration file on your local machine

   > ThreatQ will inform you if the operation already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the operation contains changes to the user configuration. The new user configurations will overwrite the existing ones for the operation and will require user confirmation before proceeding.

The operation is now installed and will be displayed in the ThreatQ UI. You will still need to configure and then enable the operation.

Configuration

> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Operation** option from the *Type* dropdown (optional).
3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Base URL	The Base URL for the Mandiant Intelligence API.
Public API Key	Your API public key provided by Mandiant.
Private API Key	Your API private key provided by Mandiant.

5. Review any additional settings, make any changes if needed, and click on **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.

Actions

The operation provides the following actions:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Mandiant Report Link	Creates a link in ThreatQ to the Mandiant report.	Indicators	IP Address, FQDN, CVE, MD5, SHA-1, SHA-256, URL
Enrich	Provides Enrichment information.	Indicators	IP Address, FQDN, CVE, MD5, SHA-1, SHA-256, URL

Mandiant Report Link

The Mandiant Report Link action ingests in ThreatQ the link(s) to the Mandiant report(s) as attributes of the selected indicator. It uses on of the following endpoints, depending on the indicator type.

ThreatQuotient provides sample response and data mapping based on the indicator object type submitted. Options include:

- CVEs
- All Other Indicator Types

CVE indicators

```
GET http://{base_url}/v4/indicator?value={indicator_value}&include_reports=true
```

Sample Response:


```
{
    "id": "vulnerability--96206e18-0e0d-5a4f-b7d7-ffa344fe9a3e",
    "type": "vulnerability",
    "is_publishable": true,
    "risk_rating": "redacted",
    "analysis": "redacted",
    "executive_summary": "<p>A deserialization of untrusted data vulnerability exists within the HTTPServlet
ILServlet.java component in Redhat JBoss Enterprise Application Platform 4.0 and earlier that, when exploited, allows
a remote attacker to execute arbitrary code.",
    "description": "<p>The National Vulnerability Database has provided the following description:</
p>\n<p><em>HTTPServerILServlet.java in JMS over HTTP Invocation Layer of the JbossMQ implementation, which is enabled
by default in Red Hat Jboss Application Server &lt;= Jboss 4.X does not restrict the classes for which it performs
deserialization.</em></p>",
    "exploitation_vectors": [
        "General Network Connectivity"
    ],
    "title": "Redhat JBoss Enterprise Application Platform HTTPServlet ILServlet.java 4.3.0 Deserialization of
Untrusted Data Vulnerability",
    "associated_actors": "redacted",
    "associated_malware": "redacted",
    "associated_reports": [
        {
            "report_id": "22-00018047",
            "report_type": "Event Coverage/Implication",
            "title": "Actor Update for July 25, 2022 – Aug. 1, 2022",
            "published_date": "2022-08-01T17:16:10.988Z",
            "audience": [
                "cyber crime",
                "cyber espionage",
                "fusion",
                "operational"
            ]
```

```
        },
        {
            "report_id": "23-00003477",
            "report_type": "Vulnerability Report",
            "title": "Redhat JBoss Enterprise Application Platform HTTPServlet ILServlet.java 4.3.0 Deserialization
of Untrusted Data Vulnerability",
            "published_date": "2023-02-24T19:40:44.97Z",
            "audience": [
                "vulnerability"
            ]
        }
    ],
    "exploitation_consequence": "Code Execution",
    "cwe": "Deserialization of Untrusted Data",
    "cve_id": "CVE-2017-7504",
    "vulnerable_products": "redacted",
    "exploitation_state": "redacted",
    "vendor_fix_references": "redacted",
    "date_of_disclosure": "2017-05-16T00:00:00.000Z",
    "observed_in_the_wild": "redacted",
    "vulnerable_cpes": "redacted",
    "was_zero_day": "redacted",
    "workarounds": "redacted",
    "publish_date": "2023-02-24T19:40:44.000Z",
    "updated_date": "2023-03-22T21:26:57.000Z",
    "last_modified_date": "2023-03-31T22:25:33.611Z",
    "available_mitigation": [
        "Patch"
    ],
    "sources": [
        {
            "source_name": "National Vulnerability Database",
            "date": "2017-05-19T20:00:00.000Z",
            "url": "https://nvd.nist.gov/vuln/detail/CVE-2017-7504",
            "is_vendor_fix": false
        },
        {
            "source_name": "RedHat Inc",
            "url": "https://access.redhat.com/downloads",
            "title": "Downloads",
            "is_vendor_fix": true
        }
    ],
    "exploits": "redacted",
    "common_vulnerability_scores": {
        "v2.0": {
            "access_complexity": "LOW",
            "access_vector": "NETWORK",
            "authentication": "NONE",
            "availability_impact": "PARTIAL",
            "base_score": 7.5,
            "confidentiality_impact": "PARTIAL",
            "exploitability": "redacted",
            "integrity_impact": "PARTIAL",
            "remediation_level": "redacted",
            "report_confidence": "redacted",
            "temporal_score": 6.2,
            "vector_string": "redacted"
        },
        "v3.0": {
            "attack_complexity": "LOW",
```

```
            "attack_vector": "NETWORK",
            "availability_impact": "HIGH",
            "base_score": 9.8,
            "confidentiality_impact": "HIGH",
            "exploit_code_maturity": "redacted",
            "integrity_impact": "HIGH",
            "privileges_required": "NONE",
            "remediation_level": "redacted",
            "report_confidence": "redacted",
            "scope": "UNCHANGED",
            "temporal_score": 9.8,
            "user_interaction": "NONE",
            "vector_string": "redacted"
        }
    },
    "audience": [
        "intel_vuln"
    ],
    "intel_free": false,
    "affects_ot": false,
    "aliases": [],
    "cisa_known_exploited": null,
    "cpe_ranges": [
        {
            "start_cpe": {
                "uri": "cpe:2.3:a:redhat:jboss_enterprise_application_platform:4.3.0:cp10:*:*:*:*:*:*",
                "vendor": "Red Hat Inc.",
                "product": "Jboss Enterprise Application Platform (EAP) (Application)",
                "version": "4.3.0 CP10"
            },
            "start_rel": "=",
            "end_cpe": null,
            "end_rel": null
        }
    ],
    "cwe_details": {
        "id": "CWE-502",
        "title": "Deserialization of Untrusted Data"
    },
    "days_to_patch": null,
    "epss": {
        "score": 0.33373,
        "percentile": 0.9638
    },
    "mve_id": "MVE-2017-11200",
    "version_history": [
        {
            "date": "2023-03-22T21:44:21.000Z",
            "version_notes": [
                "New source added: (http://www.securityfocus.com/bid/98595)",
                "New source added: (https://bugzilla.redhat.com/show_bug.cgi?id=1451441)"
            ]
        }
    ],
    "workarounds_list": []
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.associated_reports[].report_id	Indicator.Attribute	Mandiant Report	N/A	https://advantage.mandiant.com/reports/22-00015388	N/A

Other Indicator Types

```
GET http://{base_url}/v4/v4/vulnerability/{indicator_value}
```

Sample Response:

```
{
    "indicators": [
        {
            "id": "ipv4--71323d70-6939-5798-90f4-df83938bbd83",
            "mscore": 100,
            "type": "ipv4",
            "value": "118.219.221.72",
            "is_publishable": true,
            "sources": [
                {
                    "first_seen": "2022-09-02T23:34:08.019+0000",
                    "last_seen": "2022-09-02T23:34:08.019+0000",
                    "osint": true,
                    "category": [],
                    "source_name": "blocklist_net_ua"
                },
                {
                    "first_seen": "2022-09-04T18:03:02.030+0000",
                    "last_seen": "2023-03-27T06:51:00.480+0000",
                    "osint": true,
                    "category": [
                        "malware",
                        "download-location"
                    ],
                    "source_name": "urlhaus"
                }
            ],
            "misp": {
                "akamai": false,
                "alexa": false,
                "alexa_1M": false,
                "amazon-aws": false,
                "apple": false,
                "automated-malware-analysis": false,
                "bank-website": false,
                "captive-portals": false,
                "cisco_1M": false,
                "cisco_top1000": false,
                "cisco_top10k": false,
                "cisco_top20k": false,
                "cisco_top5k": false,
```

```
            "cloudflare": false,
            "common-contact-emails": false,
            "common-ioc-false-positive": false,
            "covid": false,
            "covid-19-cyber-threat-coalition-whitelist": false,
            "covid-19-krassi-whitelist": false,
            "crl-hostname": false,
            "crl-ip": false,
            "dax30": false,
            "disposable-email": false,
            "dynamic-dns": false,
            "eicar.com": false,
            "empty-hashes": false,
            "fastly": false,
            "google": false,
            "google-chrome-crux-1million": false,
            "google-gcp": false,
            "google-gmail-sending-ips": false,
            "googlebot": false,
            "ipv6-linklocal": false,
            "majestic_million": false,
            "majestic_million_1M": false,
            "microsoft": false,
            "microsoft-attack-simulator": false,
            "microsoft-azure": false,
            "microsoft-azure-appid": false,
            "microsoft-azure-china": false,
            "microsoft-azure-germany": false,
            "microsoft-azure-us-gov": false,
            "microsoft-office365": false,
            "microsoft-office365-cn": false,
            "microsoft-office365-ip": false,
            "microsoft-win10-connection-endpoints": false,
            "moz-top500": false,
            "mozilla-CA": false,
            "mozilla-IntermediateCA": false,
            "multicast": false,
            "nioc-filehash": false,
            "ovh-cluster": false,
            "parking-domain": false,
            "parking-domain-ns": false,
            "phone_numbers": false,
            "public-dns-hostname": false,
            "public-dns-v4": false,
            "public-dns-v6": false,
            "public-ipfs-gateways": false,
            "rfc1918": false,
            "rfc3849": false,
            "rfc5735": false,
            "rfc6598": false,
            "rfc6761": false,
            "second-level-tlds": false,
            "security-provider-blogpost": false,
            "sinkholes": false,
            "smtp-receiving-ips": false,
            "smtp-sending-ips": false,
            "stackpath": false,
            "tenable-cloud-ipv4": false,
            "tenable-cloud-ipv6": false,
            "ti-falsepositives": false,
            "tlds": false,
```

```
                "tranco": false,
                "tranco10k": false,
                "university_domains": false,
                "url-shortener": false,
                "vpn-ipv4": false,
                "vpn-ipv6": false,
                "whats-my-ip": false,
                "wikimedia": false
            },
            "last_updated": "2023-03-27T11:23:32.402Z",
            "first_seen": "2022-08-06T12:15:00.000Z",
            "last_seen": "2023-03-27T06:51:00.000Z",
            "reports": []
        }
    ]
}
```


ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.indicators[].reports[].report_id	Indicator.Attribute	Mandiant Report	N/A	https://advantage.mandiant.com/reports/22-00015388	N/A

Enrich

The Enich action uses the endpoint from `Mandiant Report Link Action` to retrieve the id of the reports and based on them will load the details of the reports using the following endpoint:

`GET https://api.intelligence.mandiant.com/v4/report/{reportId}`

Sample Response:


```
{
    "id": "report--f1514d66-a695-503a-99e3-70a1ede83496",
    "report_id": "23-00005140",
    "report_type": "TTP Deep Dive",
    "publish_date": "2023-03-23T01:25:02.494Z",
    "title": "Mandiant Blog – UNC961 in the Multiverse of Mandiant: Three Encounters with a Financially Motivated
Threat Actor",
    "audience": [
        "critical infrastructure",
        "cyber crime",
        "cyber espionage",
        "cyber physical",
        "freemium",
        "fusion",
        "hacktivism",
        "operational",
        "standard",
        "strategic",
        "vulnerability"
    ],
    "threat_scape": [
        "Cyber Crime",
        "Cyber Espionage",
        "Cyber Physical",
        "Hacktivism",
        "Standard",
        "Strategic",
        "Vulnerability"
    ],
    "requester_org_id": "Threatquotient, Inc. (Partner)",
    "version_one_publish_date": "2023-03-23T01:25:02.494Z",
    "threat_detail": "<p style=\"margin: 0in; font-size: 10pt; font-family: 'Open Sans'>,...</ul>",
    "tags": {
        "affected_industries": [
            "Aerospace & Defense",
            "Agriculture",
            "Automotive",
            "Chemicals & Materials",
            "Civil Society & Non-profits",
            "Construction & Engineering",
            "Education",
            "Energy & Utilities",
            "Financial Services",
            "Governments",
            "Healthcare",
            "High Tech/Software/Hardware/Services",
            "Hospitality",
```

```
            "Insurance",
            "Legal & Professional Services",
            "Manufacturing",
            "Media & Entertainment",
            "Oil & Gas",
            "Pharmaceuticals",
            "Retail",
            "Technology",
            "Telecommunications",
            "Transportation"
        ],
        "intended_effects": [
            "IP or Confidential Business Information Theft",
            "Credential Theft/Account Takeover",
            "Financial Theft",
            "Disruption",
            "Degradation",
            "Denial and Deception",
            "Embarrassment/Exposure/Brand Damage"
        ],
        "motivations": [
            "Financial or Economic",
            "Opportunistic"
        ],
        "ttps": [
            "Enabling Infrastructures",
            "Malware Propagation and Deployment",
            "Network Reconnaissance",
            "Ransomware",
            "Web Application Attacks"
        ],
        "target_geographies": [
            "Global"
        ],
        "targeted_informations": [
            "Financial Data",
            "Intellectual Property",
            "Credentials",
            "IT Information",
            "Legal Documents",
            "Government Information",
            "Sales_Marketing Data",
            "Authentication Cookies",
            "Customer Data",
            "Corporate Employee Info"
        ]
    },
    "relations": {},
    "cve_ids": [
        "CVE-2021-44228,CVE-2021-26084,CVE-2019-19781,CVE-2020-14750,CVE-2021-22205,CVE-2017-7504"
    ],
    "cve_ids_array": [
        "CVE-2021-44228",
        "CVE-2021-26084",
        "CVE-2019-19781",
        "CVE-2020-14750",
        "CVE-2021-22205",
        "CVE-2017-7504"
    ],
    "cvss_base_score": "0",
    "cvss_temporal_score": "0",
```

```
    "zero_day": false,
    "in_the_wild": false,
    "report_confidence": "ND",
    "version": 1,
    "previous_versions": [
        {
            "report_id": "23-00005140",
            "title": "Mandiant Blog – UNC961 in the Multiverse of Mandiant: Three Encounters with a Financially
Motivated Threat Actor",
            "publish_date": "2023-03-23T01:25:02.494Z",
            "version_number": 1
        }
    ]
}
```


ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.title	Indicator.Attribute	N/A	N/A	APT42: Crooked Charms, Cons, and Compromises	N/A
.tags.affected_industries[]	Indicator.Attribute	Affected Industry	N/A	Civil Society & Non-profits	For non-CVE indicators
.tags.source_geographies[]	Indicator.Attribute	Source Geography	N/A	Iran	For non-CVE indicators
.tags.target_geographies[]	Indicator.Attribute	Target Geography	N/A	Australia	For non-CVE indicators
.tags.ttps[]	Indicator.Attribute	TTP	N/A	Social Engineering	For non-CVE indicators
.tags.actors[].name	Indicator.Attribute	Actor Name	N/A	APT42	For non-CVE indicators
.tags.malware_families[].name	Indicator.Attribute	Malware Family	N/A	TABBYCAT	For non-CVE indicators
.networks[].domain	Indicator.Value	N/A	N/A	flashplayer.exe	For non-CVE indicators
.networks[].url	Indicator.Value	N/A	N/A	https://access.redhat.com/downloads	For non-CVE indicators
.networks[].ip	Indicator.Value	N/A	N/A	185.163.46.131	For non-CVE indicators
.files[].md5	Indicator.Value	N/A	N/A	9d0e761f3803889dc83c180901dc7b22	For non-CVE indicators
.files[].sha1	Indicator.Value	N/A	N/A	ecf9b7283fda023fa37ad7fdb15be4eadded4e06	For non-CVE indicators
.files[].sha256	Indicator.Value	N/A	N/A	d4375a22c0f3fb36ab788c0a9d6e0479bd19f48349f6e192b10d83047a74c9d7	For non-CVE indicators
.files[].malwareFamily	Indicator.Attribute	Malware Family	N/A	MAGICDROP	For non-CVE indicators
.files[].actor	Indicator.Attribute	Actor	N/A	APT42	For non-CVE indicators

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.technologies[].cpe	Indicator.Attribute	CPE	N/A	N/A	For CVE indicators
.source[].title	Indicator.Attribute	Source Title	N/A	National Vulnerability Database	For CVE indicators
.vulnerable_products	Indicator.Attribute	Vulnerable Products	N/A	Microsoft reports that the following products...	For CVE indicators
.mitigations[]	Indicator.Attribute	Mitigation	N/A	Patch	For CVE indicators
.vulnerability_types[]	Indicator.Attribute	Vulnerability Type	N/A	Unknown	For CVE indicators
.vendor_fix_text	Indicator.Attribute	Vendor Fix	N/A	icrosoft released fixes...	For CVE indicators
.cvss_base_score	Indicator.Attribute	CVSS Base Score	N/A	0	For CVE indicators
.risk_rating	Indicator.Attribute	Risk Rating	N/A	LOW	For CVE indicators
.exploit_rating	Indicator.Attribute	Exploit Rating	N/A	Confirmed	For CVE indicators

Change Log

- **Version 1.0.0**
  - Initial release