ThreatQuotient

A Securonix Company

Google Threat Intelligence Reports Operation

Version 2.0.0

February 24, 2026

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: tq-support@securonix.com
Web: https://ts.securonix.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: tq-support@securonix.com
Support Web: https://ts.securonix.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	2.0.0
Compatible with ThreatQ Versions	>= 5.12.0
Support Tier	ThreatQ Supported

Introduction

The Google Threat Intelligence Reports Operation enables enrichment of supported indicators within ThreatQ by retrieving related intelligence reports and contextual data from Google Threat Intelligence for IP addresses, domains, URLs, and file hashes.

The operation provides the following action:

- **Enrich** - provides enrichment information for the selected indicator.

The operation is compatible with the following indicator types:

- FQDN
- IP Address
- IPv6 Address
- MD5
- SHA-1
- SHA-256
- URL

This integration was previously known as the Mandiant Threat Intelligence Reports Operation.

Prerequisites

The following is required in order to run the operation:

- A Google Threat Intelligence API Key.

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.

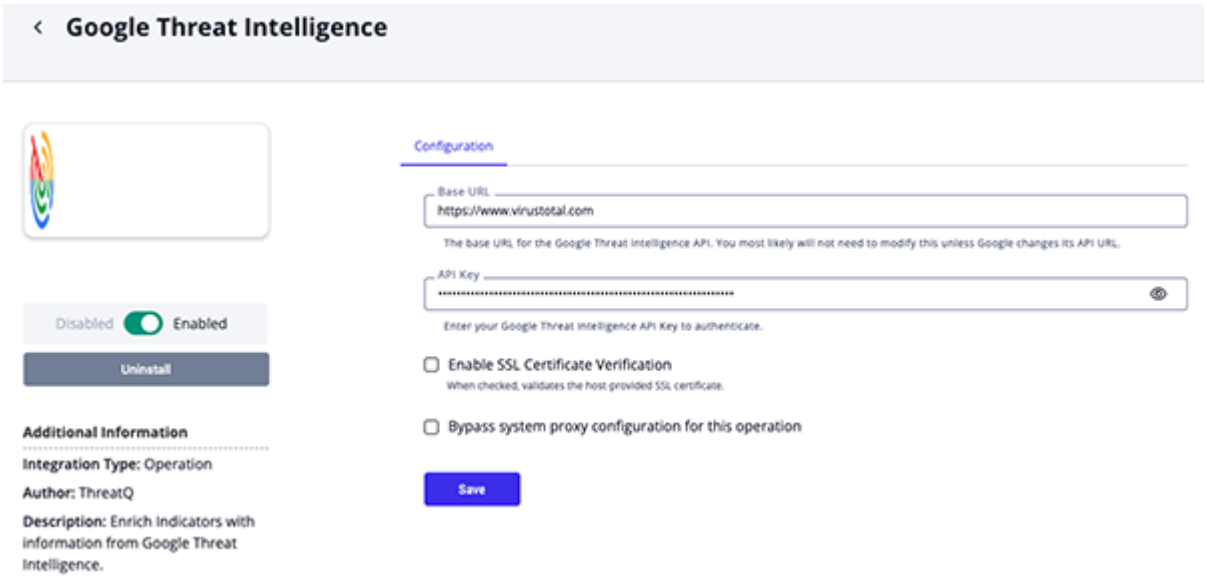
Configuration

> 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	Enter the base URL for the Google Threat Intelligence API. The default is `https://www.virustotal.com`. > You most likely will not need to modify this parameter unless Google changes its API URL.
API Key	Enter your Google Threat Intelligence API Key.
Enable SSL Certificate Verification	Enable this parameter if the operation should validate the host-provided SSL certificate.



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 action:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Enrich	Provides enrichment information for the submitted indicator.	Indicator	FQDN, IP Address, IPv6 Address, MD5, SHA-1, SHA-256, URL

Enrich

The Enrich operation action enriches submitted indicators with information from Google Threat Intelligence.

```
GET https://www.virustotal.com/api/v3/{indicator_type}/{indicator_value}
```

Sample Response:


```
{
  "data": {
    "id": "45.154.13.229",
    "type": "ip_address",
    "links": {
      "self": "https://www.virustotal.com/api/v3/ip_addresses/45.154.13.229"
    },
    "attributes": {
      "threat_severity": {
        "version": "I3",
        "threat_severity_level": "SEVERITY_NONE",
        "threat_severity_data": {
          "belongs_to_bad_collection": true
        },
        "last_analysis_date": "1713287964",
        "level_description": "Severity NONE because it has no detections."
      },
      "reputation": 0,
      "mandiant_ic_score": 35,
      "last_https_certificate_date": 1713287964,
      "tags": [],
      "whois": "inetnum: 45.0.0.0 - 45.255.255.255\nnetname: IANA-
NETBLOCK-45\ndescr: This network range is not fully allocated to APNIC.\ndescr:
\ndescr: If your whois search has returned this message, then you have\ndescr:
searched the APNIC whois database for an address that is\ndescr: allocated by
another Regional Internet Registry (RIR).\ndescr:\ndescr: Please search the
other RIRs at whois.arin.net or whois.ripe.net\ndescr: for more information
about that range.\ncountry: AU\nadmin-c: IANA1-AP\ntech-c: IANA1-AP\nabuse-c:
AA1452-AP\nstatus: ALLOCATED PORTABLE\nremarks: For general info on spam
complaints email spam@apnic.net.\nremarks: For general info on hacking  abuse
complaints email abuse@apnic .net.\nmnt-by: APNIC-HM\nmnt-lower: APNIC-HM\nmnt-
irt: IRT-APNIC-AP\nlast-modified: 2021-02-15T05:31:12Z\nsource: APNIC\nirt:
IRT-APNIC-AP\naddress: Brisbane, Australia\ne-mail: helpdesk@apnic.net\nabuse-
mailbox: helpdesk@apnic.net\nadmin-c: HM20-AP\ntech-c: NO4-AP\nauth: #
Filtered\nremarks: APNIC is a Regional Internet Registry.\nremarks: We do not
operate the referring network and\nremarks: are unable to investigate
complaints of network abuse.\nremarks: For information about IRT, see
www.apnic.net/irt\nremarks: helpdesk@apnic.net was validated on
2020-02-03\nmnt-by: APNIC-HM\nlast-modified: 2023-08-18T00:42:38Z\nsource:
APNIC\nrole: ABUSE APNICAP\naddress: Brisbane, Australia\ncountry: ZZ\nphone:
+000000000\ne-mail: helpdesk@apnic.net\nadmin-c: HM20-AP\ntech-c: NO4-AP\nnic-
```

```
hdl: AA1452-AP\nremarks: Generated from irt object IRT-APNIC-AP\nremarks:
helpdesk@apnic.net was validated on 2020-02-03\nabuse-mailbox:
helpdesk@apnic.net\nmnt-by: APNIC-ABUSE\nlast-modified:
2023-08-18T19:08:30Z\nsource: APNIC\nrole: Internet Assigned Numbers
Authority\naddress: see http://www.iana.org.\nadmin-c: IANA1-AP\ntech-c: IANA1-
AP\nnic-hdl: IANA1-AP\nremarks: For more information on IANA services\nremarks:
go to IANA web site at http://www.iana.org.\nmnt-by: MAINT-APNIC-AP\nlast-
modified: 2018-06-22T22:34:30Z\nsource: APNIC\n",
      "first_seen_itw_date": 1616047642,
      "last_analysis_results": {
        "Acronis": {
          "method": "blacklist",
          "engine_name": "Acronis",
          "category": "harmless",
          "result": "clean"
        }
      },
      "network": "45.154.12.0/22",
      "continent": "AS",
      "as_owner": "MOACK.Co.LTD",
      "country": "KR",
      "asn": 138195,
      "last_analysis_stats": {
        "malicious": 0,
        "suspicious": 0,
        "undetected": 32,
        "harmless": 62,
        "timeout": 0
      },
      "last_seen_itw_date": 1655397785,
      "last_modification_date": 1746637167,
      "total_votes": {
        "harmless": 0,
        "malicious": 0
      },
      "whois_date": 1713222068,
      "jarm": "3fd3fd20d3fd3fd21c42d42d000000937221baefa0b90420c8e8e41903f1d5",
      "regional_internet_registry": "APNIC",
      "last_analysis_date": 1713287954,
      "last_https_certificate": {
        "cert_signature": {
          "signature_algorithm": "sha256RSA",
          "signature":
"df3a652aa0a5b21920b0554d2ccafcd68471e0f8bf445c57877c540c8f29e2a9c1e2e13a455b7e
07dca63330801c9ece9d9d58b44e471a35815241c425489c94bde07c597c5cc21e0aca452d75905
685e52ca591fb27e0fe45227ec5a60ccf0c2819d6eaf52d51f5e04928bc369d3c3c847cbafe3cfe
7ab36f87ea71549f85e9526fbfdb838fb54e221cac594b1c3c3d6a32573e602b210ca77989bb3fc
56f1d51868b5938d27c3d97adb2459613b7b536383161969cdd24448617cbc6b8dc82df246bd6b8
b992d144ca0dc2a55e2c08c3017d576684df46f81dcb628fa3c5363424d94b914f65efaa4c83d40
54e8774ae63a9296546c4cbd2814f87d712bb03"
        },
```

```
        "extensions": {
          "authority_key_identifier": {
            "keyid": "78df91905feedeacf6c575ebd54c5553ef244ab6"
          },
          "subject_key_identifier": "ba370b6e8713bcc5e05fcd61f1406674764039fc",
          "subject_alternative_name": [
            "juoffer.com",
            "www.juoffer.com"
          ],
          "key_usage": [
            "digitalSignature",
            "keyEncipherment"
          ],
          "extended_key_usage": [
            "serverAuth",
            "clientAuth"
          ],
          "certificate_policies": [
            "2.23.140.1.2.1"
          ],
          "ca_information_access": {
            "OCSP": "http://ocsp.digicert.com",
            "CA Issuers": "http://cacerts.digicert.com/
EncryptionEverywhereDVTLSCA-G2.crt"
          },
          "CA": false,
          "1.3.6.1.4.1.11129.2.4.2":
"0482016c016a007700eecdd064d5db1acec55cb79db4cd13a23287467cbcecde"
        },
        "validity": {
          "not_after": "2024-08-20 23:59:59",
          "not_before": "2023-08-20 00:00:00"
        },
        "size": 1538,
        "version": "V3",
        "public_key": {
          "algorithm": "RSA",
          "rsa": {
            "modulus":
"b2f83f6781fa5ed3f32a2385110b2d89c3aff8e67fe06af33132163354ce68a7785f5c6e35f2d6
8797434acd232c716967e891c876c545d3ef6c23d9e6d478ac35471a159101b5b5735de360a8bfc
42bcc51fc0aa3bab6f695fc946dd0e62af61e14f9f5a686a3bfa8cda8f0c5162ee2d77bc4e4039f
4fc1924a0c1e9ad9141306854c13691e607a9b52cc3477f01a9de7316bd0cf1b21dfb4c6cda14bc
d788ff72c0ee99cfc860af365c03a5dd4a0234bb94320354e38370717958d28fef87b9ffb62677d
e78ca394a98af2043345b47b5bf0fc04cbc0e13a1d15af44430315cb391e565c7ecedc59842425c
c908375bd9f3d7f83ca62a8f9f7d88f292e37b1",
            "exponent": "10001",
            "key_size": 2048
          }
        },
```

```
        "thumbprint_sha256":
"595ac1d22ba540a8a92a66436094e54dbb6265f6f9a8227470c56dade415e60a",
        "thumbprint": "db988be0f18edc5db901b82854f1cfd026895623",
        "serial_number": "76b33e3cb51cc417fe6a884dbee617a",
        "issuer": {
          "C": "US",
          "O": "DigiCert Inc",
          "OU": "www.digicert.com",
          "CN": "Encryption Everywhere DV TLS CA - G2"
        },
        "subject": {
          "CN": "juoffer.com"
        }
      },
      "gti_assessment": {
        "threat_score": {
          "value": 1
        },
        "severity": {
          "value": "SEVERITY_NONE"
        },
        "contributing_factors": {
          "mandiant_association_actor": true,
          "mandiant_confidence_score": 35,
          "gti_confidence_score": 59,
          "malicious_sandbox_verdict": false,
          "mandiant_association_report": true,
          "mandiant_association_malware": true,
          "safebrowsing_verdict": "harmless"
        },
        "verdict": {
          "value": "VERDICT_UNDETECTED"
        },
        "description": "This indicator did not match our detection criteria and
there is currently no evidence of malicious activity."
      }
    }
  }
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data.attributes.gti_assessment.contributing_factors.mandiant_confidence_score	Indicator.Attribute	Mandiant Score	N/A	100	N/A
.data.attributes.gti_assessment.contributing_factors.normalised_categories[]	Indicator.Attribute	Category	N/A	N/A	N/A
.data.attributes.gti_assessment.contributing_factors.gti_confidence_score	Indicator.Attribute	Confidence Score	N/A	99	N/A
.data.attributes.gti_assessment.severity.value	Indicator.Attribute	Severity	N/A	High	Title-cased . Severity_ was removed
.data.attributes.gti_assessment.threat_score.value	Indicator.Attribute	Threat Score	N/A	100	N/A
.data.attributes.gti_assessment.threat_score.value	Indicator.Attribute	Normalised Threat Score	N/A	High	Normalized based on user-field mapping.
.data.attributes.gti_assessment.verdict.value	Indicator.Attribute	Verdict	N/A	VERDICT_MALICIOUS	N/A
.data.attributes.gti_assessment.contributing_factors.safebrowsing_verdict	Indicator.Attribute	Safe Browsing Verdict	N/A	Harmless	N/A
.data.attributes.gti_assessment.contributing_factors.pervasive_indicator	Indicator.Attribute	Is Pervasive	N/A	True	Converted to String
.data.attributes.last_analysis_stats.malicious	Indicator.Attribute	Malicious Count	N/A	N/A	N/A
.data.attributes.last_analysis_stats.suspicious	Indicator.Attribute	Suspicious Count	N/A	N/A	N/A
.data.attributes.as_owner	Indicator.Attribute	As Organization	N/A	MOACK.Co.LTD	N/A
.data.attributes.asn	Indicator.Attribute	ASN	N/A	MOACK.Co.LTD	N/A
.data.attributes.regional_internet_registry	Indicator.Attribute	RIR	N/A	APNIC	N/A
.data.attributes.last_http_response_code	Indicator.Attribute	Last HTTP Response Code	N/A	200	N/A
.data.attributes.title	Indicator.Attribute	Site Title	N/A	N/A	N/A
.data.attributes.last_submission_date	Indicator.Attribute	Last Submission Date	N/A	2015-10-29T03:20:53	N/A
.data.attributes.md5	Related Indicator.Value	MD5	N/A	2c397d151a6137a2a9be6455d143d165	N/A
.data.attributes.sha1	Related Indicator.Value	SHA-1	N/A	2cc2ad776a7a4149ddded992	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
				`c05b6c458accb0c6`	
`.data.attributes.sha256`	`Related Indicator.Value`	`SHA-1`	`N/A`	`2cc2ad776a7a4149ddded992c05b6c458accb0c6`	`N/A`
`.data.attributes.meaningful_name`	`Indicator.Attribute`	`Meaningful Name`	`N/A`	`Malicious`	`N/A`
`.data.attributes.continent`	`Indicator.Attribute`	`Continent Code`	`N/A`	`AS`	`N/A`
`.data.attributes.country`	`Indicator.Attribute`	`Country Code`	`N/A`	`RU`	`N/A`

CVE

`GET https://www.virustotal.com/api/v3/collections/vulnerability--{CVE_ID}`

Sample Response:

```
{
  "data": {
    "id": "vulnerability--cve-2004-0210",
    "type": "collection",
    "links": {
      "self": "https://www.virustotal.com/api/v3/collections/vulnerability--
cve-2004-0210"
    },
    "attributes": {
      "risk_factors": [
        "Local Access Required"
      ],
      "cve_id": "CVE-2004-0210",
      "files_count": 1,
      "creation_date": 1646663312,
      "alt_names": [],
      "targeted_regions": [],
      "alt_names_details": [],
      "priority": "P1",
      "source_regions_hierarchy": [],
      "field_sources": [
        {
          "source": {
            "sources": [],
            "field_type": "Ranked",
            "source_name": "Cybersecurity and Infrastructure Security Agency
(CISA)",
            "source_url": ""
          },
          "field": "cvss.cvssv3_x"
```

```
        }
      ],
      "cisa_known_exploited": {
        "ransomware_use": "Unknown",
        "due_date": 1648080000,
        "added_date": 1646265600
      },
      "status": "COMPUTED",
      "collection_type": "vulnerability",
      "workarounds": [],
      "technologies": [],
      "recent_activity_summary": [
        0,
        0
      ],
      "first_seen_details": [],
      "date_of_disclosure": 1089676800,
      "capabilities": [],
      "origin": "Google Threat Intelligence",
      "cvss": {
        "cvssv3_x": {
          "vector": "CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H",
          "base_score": 7.8,
          "temporal_score": 7.8
        },
        "cvssv2_0": {
          "vector": "AV:L/AC:L/Au:N/C:C/I:C/A:C/E:F/RL:OF/RC:C",
          "base_score": 7.2,
          "temporal_score": 6.0
        }
      },
      "available_mitigation": [
        "Patch"
      ],
      "affected_systems": [],
      "top_icon_md5": [],
      "tags": [
        "has_exploits",
        "observed_in_the_wild"
      ],
      "sources": [
        {
          "url": "https://exchange.xforce.ibmcloud.com/vulnerabilities/16590",
          "title": "Microsoft Windows POSIX buffer overflow allows local
attacker to gain privileges",
          "cvss": {
            "cvssv3_x": null,
            "cvssv2_0": null,
            "cvssv3_x_translated": null,
            "cvssv4_x": null
```

```
          },
          "md5": null,
          "unique_id": null,
          "published_date": 1089748800,
          "name": "IBM Corp.",
          "source_description": null
        }
      ],
      "targeted_industries_tree": [],
      "urls_count": 0,
      "last_seen_details": [],
      "references_count": 0,
      "malware_roles": [],
      "subscribers_count": 0,
      "tags_details": [
        {
          "first_seen": null,
          "description": null,
          "last_seen": null,
          "value": "observed_in_the_wild",
          "confidence": "possible"
        }
      ],
      "private": true,
      "epss": {
        "percentile": 0.9259,
        "score": 0.10564
      },
      "executive_summary": "\n\n* A Buffer Overflow vulnerability exists that,
when exploited, allows a local, privileged attacker to bypass certain security
mechanisms.\n* This vulnerability has been confirmed to be exploited in the
wild. Unverified exploit code is available.\n* Google Threat Intelligence Group
(GTIG) considers this a Medium-risk vulnerability due to the potential for
bypassing certain security mechanisms, offset by local access requirements.\n*
Mitigation options include a patch.\n",
      "motivations": [],
      "version_history": [
        {
          "date": 1743734117,
          "version_notes": [
            "exploitation_vectors: Added ['Unspecified Local Vector'] to
existing exploitation_vectors. "
          ]
        }
      ],
      "vulnerable_products": "",
      "last_modification_date": 1743734117,
      "cpes": [
        {
          "end_rel": null,
```

```
          "end_cpe": null,
          "start_rel": "=",
          "start_cpe": {
            "version": "",
            "product": "Windows 2000",
            "uri":
"cpe:2.3:o:microsoft:windows_2000:-:sp3:*:*:advanced_server:*:*:*",
            "vendor": "Microsoft"
          }
        }
      ],
      "summary_stats": {
        "first_submission_date": {
          "min": 1639345444.0,
          "max": 1639345444.0,
          "avg": 1639345444.0
        },
        "last_submission_date": {
          "min": 1639390624.0,
          "max": 1639390624.0,
          "avg": 1639390624.0
        },
        "files_detections": {
          "min": 0.0,
          "max": 0.0,
          "avg": 0.0
        }
      },
      "exploitation_vectors": [
        "Local Access",
        "Unspecified Local Vector"
      ],
      "analysis": "\n\nAn attacker could exploit this vulnerability to gain
elevated privileges. An attacker would need to specially craft a malicious
application and run it on the vulnerable system. A failed attempt at
exploitation could potentially cause a crash of the application, resulting in a
denial-of-service condition.\n\nThis vulnerability has been exploited by the
Tsar Team since at least 2007 in a variety of campaigns. For more information,
please refer to the report, \"[Overview of Tsar Team Espionage Activity]
(https://advantage.mandiant.com/reports/16-00014614).\"\n\nIn January 2014, a
campaign of targeted spam messages began with the intent of installing Gameover
Zeus on victim systems. For more information, please refer to the report,
\"[Gameover Zeus Resumes Operations with Altered Malware and Increased Use of
Fluxxy and KOL Fast-Flux Infrastructure Hosting](https://
advantage.mandiant.com/reports/Intel-1167778).\"\n\nCISA added this
vulnerability to its Known Exploited Vulnerabilities Catalog on March 3, 2022,
with a required remediation date of March 24, 2022.\n\n  \nMandiant Threat
Intelligence considers this a Medium-risk vulnerability due to the potential
for escalation of privileges, offset by the local access required.\n\n",
      "ip_addresses_count": 0,
```

```
      "risk_rating": "MEDIUM",
      "days_to_report": 6446,
      "exploitation_consequence": "Security Bypass",
      "intended_effects": [],
      "mati_genids_dict": {
        "cve_id": "vulnerability--e35ba016-5a4d-55e1-a812-ee56477a6df6",
        "report_id": "report--c81eb59b-89fe-5c73-8659-5cd10d51e2b3",
        "mve_id": "vulnerability--23e4110d-ee84-5250-8ce3-ef5e84cad030"
      },
      "name": "CVE-2004-0210",
      "exploitation_state": "Confirmed",
      "predicted_risk_rating": "",
      "targeted_industries": [],
      "exploitation": {
        "first_exploitation": 1474761600,
        "tech_details_release_date": null,
        "exploit_release_date": 1089936000
      },
      "domains_count": 0,
      "counters": {
        "files": 1,
        "domains": 0,
        "ip_addresses": 0,
        "urls": 0,
        "iocs": 1,
        "subscribers": 0,
        "attack_techniques": 0
      },
      "autogenerated_tags": [],
      "targeted_informations": [],
      "merged_actors": [],
      "detection_names": [],
      "operating_systems": [],
      "mitigations": [],
      "threat_scape": [],
      "exploit_availability": "Unverified",
      "cwe": {
        "title": "Buffer Overflow",
        "id": "CWE-120"
      },
      "mve_id": "MVE-2004-88",
      "vendor_fix_references": [
        {
          "url": "http://www.kb.cert.org/vuls/id/647436",
          "title": "Microsoft Windows contains a buffer overflow in the POSIX
subsystem",
          "cvss": null,
          "md5": null,
          "unique_id": "VU#647436",
          "published_date": 1089835200,
```

```
          "name": "CERT/CC",
          "source_description": null
        }
      ],
      "collection_links": [],
      "targeted_regions_hierarchy": [],
      "description": "\n\nThe National Vulnerability Database (NVD) has
provided the following description:\n\n*The POSIX component of Microsoft
Windows NT and Windows 2000 allows local users to execute arbitrary code via
certain parameters, possibly by modifying message length values and causing a
buffer overflow.*\n\n",
      "is_content_translated": false,
      "aggregations": {
        "files": {
          "tags": [
            {
              "value": "javascript",
              "count": 1
            }
          ],
          "vhash": [
            {
              "value": "3101773ac42964b4fd3c05b2c4d8e433",
              "count": 1,
              "total_related": 36356,
              "prevalence": 2.750577621300473e-5
            }
          ],
          "tlshhash": [
            {
              "value":
"T12632B6D94839693321BB861947072A5DFA5D401B53A8E719FC8C874C9FB21A0C6E8F98",
              "count": 1,
              "total_related": 1,
              "prevalence": 1.0
            }
          ],
          "embedded_domains": [
            {
              "value": "www.securityfocus.com",
              "count": 1,
              "total_related": 44620,
              "prevalence": 2.2411474675033616e-5
            }
          ],
          "embedded_urls": [
            {
              "value": "https://www.securityfocus.com/bid/10710/info",
              "count": 1,
              "total_related": 1,
```

```
              "prevalence": 1.0
            }
          ]
        }
      }
    },
    "context_attributes": {
      "shared_with_me": false,
      "role": "viewer"
    }
  }
}
```

ThreatQuotient provides the following default mapping for this action:

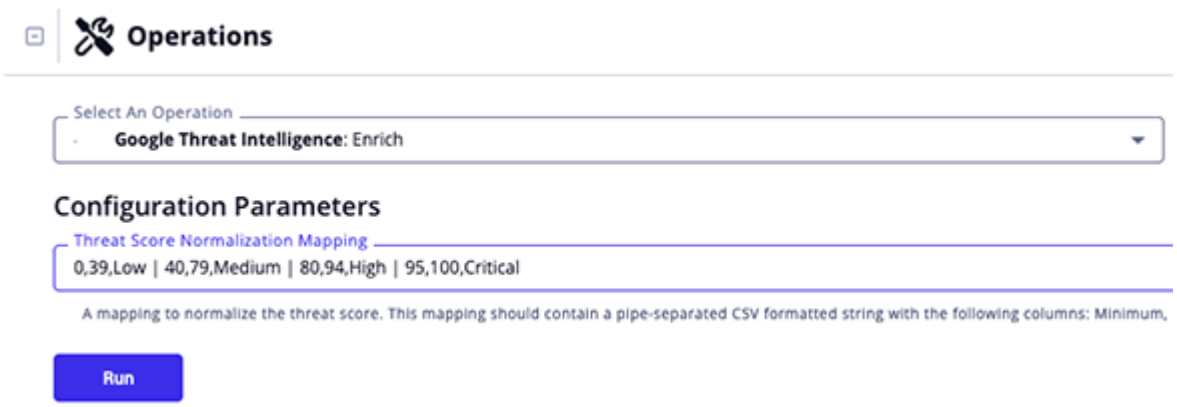
FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data.attributes.description	Indicator.Description	N/A	N/A	The National Vulnerability Database (NVD) has provided.....	N/A
.data.attributes.analysis	Indicator.Description	N/A	N/A	An attacker could expl	N/A
.data.attributes.cvss.cvssv2_0.vector	Indicator.Attribute	CVSS v2 Vector	N/A	AV:L/AC:L/Au:N/C:C/I:C/A:C/E:F/RL:OF/RC:C	N/A
.data.attributes.cvss.cvssv2_0.base_score	Indicator.Attribute	CVSS v2 Base Score	N/A	7.2	N/A
.data.attributes.cvss.cvssv2_0.temporal_score	Indicator.Attribute	CVSS v2 Temporal Score	N/A	6.0	N/A
.data.attributes.cvss.cvssv3_x.vector	Indicator.Attribute	CVSS v3 Vector	N/A	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	N/A
.data.attributes.cvss.cvssv3_x.base_score	Indicator.Attribute	CVSS v3 Base Score	N/A	7.8	N/A
.data.attributes.cvss.cvssv3_x.temporal_score	Indicator.Attribute	CVSS v3 Temporal Score	N/A	7.8	N/A
.data.attributes.exploitation_vectors[]	Indicator.Attribute	Exploitation Vector	N/A	Local Access	N/A
.data.attributes.epss.score	Indicator.Attribute	EPSS Score	N/A	0.10564	N/A

Run Configuration Options

> These configuration options are set after selecting the action to run against an object and are not set from the operation's configuration screen.

The following configuration option is available after selecting the action:

RUN OPTION	DESCRIPTION
Threat Score Normalization Mapping	Enter mapping to normalize the threat score. This mapping should contain a pipe-separated CSV formatted string with the following columns: Minimum, Maximum, Normalized Value. **Default:** `0,39,Low | 40,79,Medium | 80,94,High | 95,100,Critical`



Change Log

- **Version 2.0.0**
  - Updated the operation to use the Google API.
  - Removed the **Mandiant Report Link** operation action.
  - Updated the minimum ThreatQ version to 5.12.0.
  - Updated the operation name from **Mandiant Intelligence Reports Operation** to **Google Threat Intelligence Reports Operation**.
- **Version 1.0.0**
  - Initial release