Attack Surface Intelligence API

Mark Glinski
2 months ago · Updated

Follow

In this article:

> **Note:** This article supports Version 2.0 of the Attack Surface Intelligence API. We update this article continually. If you do not see information you need, contact your sales engineer or customer success manager; or post a question in our Community.

Use this guidance to integrate the Attack Surface Intelligence (ASI) API into your workflows for threat investigation and attack surface management.

Understand what you can do with this API

ASI provides direct access to SecurityScorecard's data with more than 4.1 billion IP addresses scanned every 10 days across 1500+ ports globally. Using powerful search capabilities, you can find and correlate the latest information on IPs, open ports, and vulnerabilities, threat actors, ransomware group campaigns, and other data points.

> **Note:** Attack Surface Intelligence does not surface potential vulnerabilities. It surfaces Common Vulnerability Enumerations (CVEs) that we confirm as being actual vulnerabilities. SecurityScorecard does, however, flag potential vulnerabilities as an issue type. Learn more.

Query specific facet-related endpoints

You can run queries on specific facets, which represent attributes or fields of the data you can use to filter or group search results:

- Investigate an IP address
- Investigate an open port on an IP address
- Investigate a vulnerability
- Investigate active malware infections
- Investigate a ransomware family
- Investigate a threat actor

Run searches an any facets

Using the */search* endpoint, run queries on any facet to return varieties of data relevant to your investigations.

See all possible expressions for any facet

Using the */facets* endpoint, you can see all possible expressions or values for any facet to help you run searches with better results.

Understand query syntax

SecurityScorecard stores ASI data with Amazon Web Services (AWS), so ASI uses AWS CloudSearch query structures for searching. Learn more about how ASI uses CloudSearch query syntax.

Get started: Create an API token

To get started, create an API token in the SecurityScorecard platform. This token enables you to communicate with all the endpoints documented here.

After you create the token, include it in the header of your requests as in the following example:

```
--header 'Authorization: Bearer (token)' \
```

Investigate an IP address

```
/details/asset/(IP-address)
```

Query on an IP address for its location, attributed ownership, certificate data, open ports and resources running on them, vulnerabilities, threat-related data, and more.

Insert *asset* into the URL path and specify the IP address that you want to investigate:

Example request

```
curl --location --request GET 'https://platform-api.securityscorecard.io/asi/details/asset/123
--header 'Authorization: Bearer (token)' \
--data-raw ''
```

Example response

```
{
    "attribution": [
        {
            "company": "example1",
            "domain": "example1.de",
            "industry": "INFORMATION_SERVICES",
            "score": 3.80000000000000e+01,
            "scorecard": "(ID)"
        },
        {
            "company": "Example2 , Inc.",
            "domain": "example2.net",
            "industry": "TECHNOLOGY",
            "score": 3.90000000000000e+01,
            "scorecard": "(ID)"
        },
        {...}
    ],
    "certs": [
        {
            "domain": "concours.enspd-udo.cm",
            "has_crl_urls": "false",
            "has_subject": "true",
            "hash": "(hash)",
            "is_certificate_chain_valid": "false",
            "issuer_country": "US",
            "last_seen": "2022-09-15 18:06:14.000",
            "md5": "(hash)",
            "pem": "-----BEGIN CERTIFICATE-----\(certificate)\n-----END CERTIFICATE-----",
            "port": 443,
            "service": "https",
            "sha1": "(hash)",
            "sha256": "(hash)",
            "sig_algo": "sha256WithRSAEncryption",
            "status": "Invalid Certificate Chain",
            "verify_string": "certificate has expired"
        }
    ],
    "cves": [
        {
            "cve": "CVE-2016-7048",
            "cvss": 9.3,
            "last_seen": "2022-09-17 10:40:06.000",
            "maturity": "Unknown",
            "port": 5432
        },
        {
            "actor": "APT17",
            "cve": "CVE-2019-9193",
            "cvss": 9,
            "last_seen": "2022-09-17 10:40:06.000",
            "maturity": "High",
            "port": 5432
        },
        {...},
            "cve": "CVE-2016-0766",
            "cvss": 9,
            "last_seen": "2022-09-17 10:40:06.000",
            "maturity": "Unknown",
            "port": 5432
        },
        {
            "cve": "CVE-2015-0244",
            "cvss": 7.5,
            "last_seen": "2022-09-17 10:40:06.000",
            "maturity": "Unknown",
            "port": 5432
        },
//Entries removed for readability
        {
            "cve": "CVE-2021-36368",
            "cvss": 2.6,
            "last_seen": "2022-10-15 10:49:00.000",
            "maturity": "Unknown",
            "port": 22
        }
    ],
    "location": {
        "city_name": "",
        "country_code": "FR",
        "country_name": "France",
        "hostname": "(host1)"
    },
    "ports": [
        {
            "first_seen": "2022-06-13 23:47:09.000",
            "last_seen": "2022-10-15 10:49:00.000",
            "port": 5432,
            "product": "",
            "service": "postgresql",
            "version": ""
        },
        {
            "first_seen": "2022-05-29 09:00:55.000",
            "last_seen": "2022-10-15 10:49:00.000",
            "port": 443,
            "product": "",
            "service": "https",
            "version": ""
        },
        {
            "cpe": [
                "cpe:/a:openbsd:openssh:8.2p1",
                "cpe:/o:linux:linux_kernel"
            ],
            "first_seen": "2022-05-29 09:00:55.000",
            "last_seen": "2022-10-15 10:49:00.000",
            "os_type": "Linux",
            "port": 22,
            "product": "OpenSSH",
            "service": "ssh",
            "version": "8.2p1 Ubuntu 4ubuntu0.5"
        },
        {
            "cpe": [
                "cpe:/a:vsftpd:vsftpd:3.0.3"
            ],
            "first_seen": "2022-06-13 23:47:09.000",
            "last_seen": "2022-10-15 10:49:00.000",
            "os_type": "Unix",
            "port": 21,
            "product": "vsftpd",
            "service": "ftp",
            "version": "3.0.3"
        },
        {
            "cpe": [
                "cpe:/a:igor_sysoev:nginx:1.18.0",
                "cpe:/o:linux:linux_kernel"
            ],
            "first_seen": "2022-05-29 09:00:55.000",
            "last_seen": "2022-10-15 10:49:00.000",
            "os_type": "Linux",
            "port": 80,
            "product": "nginx",
            "service": "http",
            "version": "1.18.0"
        }
    ],
    "threat_actors": [
        {
            "actor": "APT17",
            "attribution_method": "SSC internal Threat Research",
            "last_seen": "2022-10-15 00:00:00.000",
            "link": "CVE-2019-9193",
            "link_type": "cve",
            "origin": "CN"
        },
        {
            "actor": "Cobalt Group",
            "attribution_method": "SSC internal Threat Research",
            "last_seen": "2022-10-15 00:00:00.000",
            "link": "CVE-2019-9193",
            "link_type": "cve"
        }
    ]
}
```

Returned data for */asset/(ip)*

attribution object

Returned data for the *attribution* object, which provides information about the organization to which the IP is attributed to, as well as its Scorecard:

Key	Description
company	The organization that the IP is attributed to

domain	The domain that the IP is attributed to
industry	The industry in which the organization operates.
score	The overall score for the Scorecard for the domain to which the IP attributed. The score appears in scientific notation, for example, a value of *4.700000000000000e+01* equals a score of 47.
scorecard	The identifier for the organization's Scorecard

certs object

Returned data for the *certs* object:

Key	**Description**
domain	Domain of this IP
has_crl_urls	Whether there is a list of revoked public key certificates created and digitally signed by the CA who issues the certificate for this IP
has_subject	Whether the certificate is targeting a subject, such as an IP, for certification

is_certificate_chain_valid	Whether the SSL certificate chain is valid
issuer_country	Country of the SSL certificate issuer for an IP
last_seen	Most recent date and time that our scans detected this certificate
md5	MD5 hash for an SSL certificate (with SNI detection) for this IP
pem	.pem file that contains the concatenated certificate
port	Open port on this IP on which the certificate was detected
service	Service that uses transport layer security (TLS) that was detected on the open port of this IP, such as HTTPS, SSH, or MySQL
sha1	SHA1 hash for an MD5 certificate for this IP
sha256	SHA256 hash for an MD5 certificate for this IP
sig_aglo	SSL certificate signature algorithm used

	for this IP
status	Whether or not the certificate is invalid
verify_string	SSL certificate verification string for this IP

cpe object

Returned data about products running on this IP:

Key	**Description**
cpe	Common product enumeration identifier ID for a product found on this IP, as it appears in NIST's Official CPE dictionary
first_seen	Earliest date and time that our scans detected this product on this IP
last_seen	Most recent date and time that our scans detected this product on this IP
os_type	Operating system for the product running on this IP
port	Port on this IP where the product or service was discovered

product	Name of the product with the CPE identifier, found on this IP
service	Type of service that the product discovered on this IP provides, such as SSH

cves object

Returned data about vulnerabilities discovered on this IP, including whether they have been weaponized by threat actors:

Key	Description
actor	Threat actor groups known to have weaponized the vulnerability
cve	Identifier for this Common Vulnerability Enumeration, as it appears in the National Vulnerability Database
cvss	Common Vulnerability Scoring System Version 2.0 score for a vulnerability
last_seen	Most recent date and time that our scans detected this vulnerability on this IP
maturity	Whether the vulnerability is known to have been weaponized by threat actors for an exploit *Unknown* (also referred to as *proof of concept*) means

	that although a method has been devised to exploit the vulnerability, the CVE is not known to have been been weaponized by a threat actor. *High* means that the vulnerability is known to have been weaponized.
port	Port on the IP, where we detected the vulnerability

location **object**

Returned data about the geographic location of this IP:

Key	**Description**
city_name	City where this IP is located
country_code	International Organization for Standardization (ISO) code for the country where this IP is located
country_name	Name of the country where this IP is located
host_name	Label assigned to the device running at this IP address

ports **object**

Returned data for the *ports* object, which provides information open ports discovered on this IP:

Key	**Description**
first_seen	Earliest date and time that our scans detected this open port on this IP
last_seen	Most recent date and time that our scans detected this open port on this IP
port	Open port number detected on this IP
product	Name of software product running on the open port detected on this IP
service	Name of service running on this open port detected on this IP
version	Version number, if available, of a product running on this open port, detected on this IP

threat_actor **object**

Returned data about threat actors known to have weaponized vulnerabilities that we discovered on this IP:

Key	**Description**

actor	Threat actor group known to have weaponized a vulnerability on this IP. See the MITRE ATT&CK listing of threat actor groups.
attribution_method	How we identified a connection between the threat actor and this IP. Possible sources include: • SecurityScorecard's internal threat research • Published information about a CVE found on the IP • Analysis of malware • Community feeds through our malware information sharing platform (MISP)
last_seen	Most recent date and time that our scans made an observation on the IP, linking to the threat actor
link	Name of the artifact that connects the threat actor to this IP, for example, a CVE ID such as *CVE-2019-9193*
link_type	The type of artifact that links the threat actor to this IP
origin	The nation that the threat actor is associated with, identified by its International Organization for Standardization (ISO) country code

Return to the top of this section.

Investigate an open port on an IP address

```
/details/asset/(IP-address)/port/(port-number)
```

Query on an open port running on an IP to learn about the resources running on that port.

Insert *port* into the URL path and specify the port number that you want to investigate:

Example request

```
curl --location --request GET 'https://platform-api.securityscorecard.io/asi/details/asset/123
--header 'Authorization: Bearer (token)' \
--header 'Content-Type: application/json' \
--data-raw ''
```

Example response

```
{
    "title": "Port 22 - ssh",
    "port": 22,
    "service": "ssh",
    "product": "OpenSSH",
    "version": "8.2p1 Ubuntu 4ubuntu0.5",
    "scripts": "[{\"@id\":\"ssh2-enum-algos\",\"@output\":\"\\n  kex_algorithms: (9)\\n      c
    "firstSeen": "2022-05-29 09:00:55.000",
    "lastSeen": "2022-10-15 10:49:00.000",
    "device": "",
    "os": "Linux",
    "cpe": [
        "cpe:/a:openbsd:openssh:8.2p1",
        "cpe:/o:linux:linux_kernel"
    ]
}
```

Returned data

Field	Description
title	Port number and service running on it
port	Port number
service	Service running on the port
product	Products running on the port
version	Version of product running on the port
scripts	A collection of semi-structured output for all the scripts that were run against that IP. Output typically includes an *@id* property with the name of the script and *@output* with the standard output log. Some scripts may also output a *table* property with more structured information.
firstSeen	First date and time our scans detected the open port

lastSeen	Most recent date and time our scans detected the open port as of this query
device	Type of device running on the port, such as a router or webcam
os	Operating system of the resource running on the port
cpe	Common Platform Enumeration of the resource running on the port

Return to the top of this section.

Investigate a vulnerability

```
/details/cve/(CVE-ID)
```

Learn about a vulnerability, including its severity score, publication date, and any threat actors known to exploit it.

Insert *cve* into the URL path and specify the CVE ID that you want to investigate:

Example request

```
curl --location --request GET 'https://platform-api.securityscorecard/asi/v2/details/cve/CVE-2
--header 'Authorization: Bearer (token)' \
--data-raw ''
```

Example response

```
{
    "title": "CVE-2022-22719",
    "threatActors": [],
    "weaponized": "Unknown",
    "description": "A carefully crafted request body can cause a read to a random memory area
    "cvss3": 5,
    "cwe": "CWE-665",
    "published": "2022-03-14T11:15:00",
    "modified": "2022-10-06T02:41:00"
}
```

We are compiling descriptions for returned data. Check this page for future updates.

Return to the top of this section.

Investigate active malware infections

```
/active-infections/(malware-family)
```

Learn how malware infections may be connected to certain assets, vulnerabilities, or threat actors.

Insert *active-infections* into the URL path and specify the malware family that you want to investigate:

Example request

```
curl --location --request GET 'https://platform-api.securityscorecard.io/asi/details/active-in
--header 'Authorization: Bearer (token)' \
--data-raw ''
```

Example response

We shortened the number of returned records for this article.

```
{
    "domains": [
        {
            "name": "example1.net",
            "quantityOfIps": 34
        },
        {
            "name": "example2.net",
            "quantityOfIps": 43
        },
        {
            "name": "example3.net",
            "quantityOfIps": 47
        },
        {
            "name": "example4.net",
            "quantityOfIps": 80
        },
        {
            "name": "example5.net",
            "quantityOfIps": 199
        },
    "quantityOfRequests": 1251972619,
    "family": "andromeda",
    "title": "andromeda",
    "category": "Malware",
    "observed": "Sun Oct 16 2022"
}
```

We are compiling descriptions for returned data. Check this page for future updates.

Return to the top of this section.

Investigate a ransomware family

```
/ransomware/(ransomware-family)
```

Get information about ransomware families, including the number of victims and global cases.

Insert *ransomware* into the URL path and specify the ransomware family that you want to investigate:

Example request

```
curl --location --request GET 'https://platform-api.securityscorecard.io/asi/details/ransomwar
--header 'Authorization: Bearer (token)' \
--data-raw ''
```

Example response

```
{
    "victims": "(victim-domains)",
    "victimsNumber": 785,
    "globalCases": 798,
    "lastSeen": "2022-09-25 00:00:00.000",
    "title": "CONTI"
}
```

We are compiling descriptions for returned data. Check this page for future updates.

Return to the top of this section.

Investigate a threat actor

```
/details/threat-actor/(threat-actor-group)
```

Get details about a threat actor and how they might be connected to certain assets or vulnerabilities that they have been known to exploit.

Insert *threat-actor* into the URL path and specify the threat actor group that you want to investigate:

Example request

```
curl --location --request GET 'https://platform-api.securityscorecard.io/asi/details/threat-ac
--header 'Authorization: Bearer (token)' \
--data-raw ''
```

Example response

```
{
    "title": "Lazarus Group",
    "origin": "KP",
    "description": "Since 2009, HIDDEN COBRA actors have leveraged their capabilities to targe
    "aka": [
        "Bureau 121",
        "NICKEL GLADSTONE",
        "Group 77",
        "ATK3",
        "APT 38",
//Entries removed for readability
    ],
    "insights": [
        "https://www.theregister.co.uk/2019/04/10/lazarus_group_malware/",
        "https://blogs.jpcert.or.jp/en/2021/01/Lazarus_tools.html",
        "https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/a-lo
        "https://www.bleepingcomputer.com/news/security/lazarus-group-deploys-its-first-mac-ma
        "https://blog.trendmicro.com/trendlabs-security-intelligence/what-we-can-learn-from-th
//Entries removed for readability
        "https://dragos.com/adversaries.html"
    ],
    "industries": [
        "Government",
        "Private sector",
        "Private sector",
        "Government"
    ],
    "entities": [
        "Bangladesh Bank",
        "Australia",
        "India",
        "France",
//Entries removed for readability
    ],
    "iocs": [
        {
            "description": "c67b03c0a91eaefffd2f2c79b5c26a2648b8d3c19a22cadf35453455ff08ead0",
            "type": "Hash",
            "source": "http://blog.talosintelligence.com/2022/10/threat-source-newsletter-oct-
            "lastUpdate": "2022-10-06"
        },
        {
            "description": "Tenforums.com",
            "type": "Domain",
            "source": "https://fp.tools/home/forums/threads/Z08_v4o8XPSTRWDj_4yVFA?id=P8z7pL1R
            "lastUpdate": "2022-10-06"
        },
        {
            "description": "e4973db44081591e9bff5117946defbef6041397e56164f485cf8ec57b1d8934",
            "type": "Hash",
            "source": "http://blog.talosintelligence.com/2022/10/threat-source-newsletter-oct-
            "lastUpdate": "2022-10-06"
        }
 ///Entries removed for readabilty
    ]
}
```

We are compiling descriptions for returned data. Check this page for future updates.

Return to the top of this section.

Run queries on any facets

```
/search
```

Run a queries on any ASI facets to access a wide variety of available information about assets and threats. Learn more about available facets in ASI.

- Select pagination settings based on size of result set
- Example request with page parameter
- Example response when page parameter is used in request
- Example request with cursor parameter
- Example response when cursor parameter is used in request

Request parameters

Parameter	Description
query	The facet that you want to search on and the expression, or value, for that facet, separated by a colon. Examples: *has_infection:1* *ssl_verify_string:'certificate has expired'* *threat_actor:'Packrat'*
sort	The field you want to sort results by. Possible values in the *IPV4* index: *scan_date*

ax_cvss_score

min_scorecard_grade

_score

avd_grade

city

cloud_provider

cloud_region

country_name

has_cve

has_cve_been_exploited

has_infection

has_malhash

has_malrep

has_ransomware

has_scorecard

has_screenshot

has_ssl_cert

has_threatactor

hostname

max_cvss_score

min_scorecard_grade

postal

scan_time (default)

ssl_is_certificate_chain_valid

state

Possible values for the *leakedCreds* index:

_score (default),

has_ransomware

sortDir	Whether you want to sort results in ascending or descending order. Possible values: *asc (ascending)* *desc (descending)*
page	The page number for paginated results. Your query typically generates more results than what a single "page" can display. You run the query with the page parameter set at *1*, *2*, or more to see consecutive pages of and view remaining results. To query for more than 10,000 results, use the *cursor* parameter instead of page. Learn more about pagination settings.
index	The set of structured data examined by a search engine looking for information relevant to your query. Possible values: *IPV4* *leakedCreds*

parser	Compiler for the search query. Possible options are: *simple* *structured* *lucene* *dismax* Learn more about these parsers.
size	Number of results to return.
cursor	Parameter for paginating more than 10,000 results in a search.

Select pagination settings based on size of result set

Use different pagination parameters depending on the number of returned results and how you want to view them.

If your search returns a large number of results, such as more than 10,000, and you want only to see the first few pages, use the *page* and *size* parameters.

If your search returns more than 10,000 results, and you want to download all of them, use the *cursor* and *size* parameters:

- Specify *cursor=initial* in your initial search request and include the *size* parameter to specify how many hits you want to get.
- Amazon CloudSearch returns a cursor value in the response that you use to get the next set of hits.
- Cursors are intended to page through a result set within a reasonable amount of time of the initial request. Using a stale cursor can return stale results.

Learn more about paginating results in Amazon CloudSearch.

Example request with *page* parameter

```
curl --location --request POST 'https://platform-api.securityscorecard.io/asi/search' \
--header 'Authorization: Bearer (token)' \
--header 'Content-Type: application/json' \
--data-raw '{
  "query": "has_infection:1",
  "sort": "country_name",
  "sortDir": "asc",
  "page": 3,
  "index": "ipv4",
  "parser": "structured",
  "size": 10
}'
```

Example response when *page* parameter is used in request

We shortened the number of returned records in this sample for readability.

```
{
    "facets": {
        "countries": [
            {
                "name": "Germany",
                "value": 3509266
            },
            {
                "name": "United States",
                "value": 3173609
            },
            {
                "name": "Russia",
                "value": 3170365
            },
            {
                "name": "China",
                "value": 3161915
            },
            {
                "name": "Brazil",
                "value": 2883384
            },
            {
                "name": "South Korea",
                "value": 1347922
            },
            {
                "name": "United Kingdom",
                "value": 1207672
            },
///More countries (removed for readability)
        ],
        "threatActors": [
            {
                "name": "Packrat",
                "value": 1660788
            },
            {
                "name": "APT37",
                "value": 1042654
            },
            {
                "name": "Cobalt Group",
                "value": 575548
            },
            {
                "name": "Sandworm Team",
                "value": 571020
            },
///More threat actors (removed for readability)
        ],
        "cves": [
            {
                "name": "CVE-2017-9765",
                "value": 2010600
            },
            {
                "name": "CVE-2019-7659",
                "value": 2010600
            },
            {
                "name": "CVE-2020-14145",
                "value": 656076
            },
            {
                "name": "CVE-2021-41617",
                "value": 653705
            },
            {
                "name": "CVE-2018-20685",
                "value": 371722
            },
///More CVEs (removed for readability)
        ],
        "ports": [
            {
                "name": "7547",
                "value": 9516468
            },
            {
                "name": "80",
                "value": 3490036
            },
            {
                "name": "5060",
                "value": 3302791
            },
            {
                "name": "443",
                "value": 2742752
            },
            {
                "name": "53",
                "value": 2587287
            },
            {
                "name": "22",
                "value": 1685618
            },
            {
                "name": "8089",
                "value": 1299776
            },
            {
                "name": "2000",
                "value": 1229530
            },
            {
                "name": "4567",
                "value": 1176088
            },
            {
                "name": "21",
                "value": 1138268
            }
        ],
        "products": [
            {
                "name": "Unknown cwmp",
                "value": 3204554
            },
            {
                "name": "Unknown tcpwrapped",
                "value": 1941685
            },
            {
                "name": "AVM FRITZ!OS SIP",
                "value": 1476124
            },
            {
                "name": "gSOAP",
                "value": 1285984
            },
///More products (removed for readability)
        ],
        "orgs": [
            {
                "name": " Example1",
                "value": 3228443
            },
            {
                "name": "Example2",
                "value": 3228443
            },
            {
                "name": "Example3",
                "value": 1636074
            },
            {
                "name": "Example4",
                "value": 1577117
            },
            {
                "name": "Example5",
                "value": 1493940
            },
            {
                "name": "Example6",
                "value": 1333114
            },
///More orgs (removed for readability)
        ]
    },
    "hits": [
        {
            "detectedLibraries": [
                "core-js"
            ],
            "time": "2022-05-08T18:35:37Z",
            "cloud": "",
            "cloudRegion": "",
            "hasMalrep": false,
            "maliciousReputation": [],
            "hasCVE": false,
            "cves": [],
            "cvss": [],
            "deviceType": [],
            "hasRansomware": false,
            "ransomwareVictims": [],
            "ransomwareGroups": [],
            "hasSSLCert": false,
            "ports": [
                "49152"
            ],
            "services": [
                "upnp"
            ],
            "minGrade": "1.0",
            "hostnames": [
                "example11.com"
            ],
            "hasScorecard": true,
            "products": [],
            "country": " and Saba\"",
            "organizations": [
                "Example11"
            ],
            "hasCVEExploited": false,
            "ips": [
                "123.4.56.789"
            ],
            "sslValid": false,
            "hasThreatActor": false,
            "threatActors": [],
            "hasInfection": true,
            "infections": [
                "pva.torrent.openinternet",
                "pva.torrent.openinternet"
            ],
            "countryCode": "BQ",
            "industries": [
                "UNKNOWN"
            ],
            "cpe": "",
            "dnsRecords": [],
            "grade": "",
            "mainAttribution": [
                "1",
                "telbo.net",
                "Telbo",
                "UNKNOWN",
                1
            ],
            "detectedLibraryVersion": "core-js-pure@2.6.11",
            "domains": [],
            "osTypes": [],
            "id": "(ID)"
        },
        {
            "detectedLibraries": [
                "core-js"
            ],
            "time": "2022-07-17T03:28:12Z",
            "cloud": "",
            "cloudRegion": "",
            "hasMalrep": false,
            "maliciousReputation": [],
            "hasCVE": false,
            "cves": [],
            "cvss": [],
            "deviceType": [],
            "hasRansomware": false,
            "ransomwareVictims": [],
            "ransomwareGroups": [],
            "hasSSLCert": false,
            "ports": [
                "21"
        ],
        "services": [
            "ftp"
        ],
        "minGrade": "1.0",
        "hostnames": [],
        "hasScorecard": true,
        "products": [
            "Unknown ftp"
        ],
        "country": " and Saba\"",
        "organizations": [
            "Telbo"
        ],
        "hasCVEExploited": false,
        "ips": [
            "190.4.75.252"
        ],
        "sslValid": false,
        "hasThreatActor": false,
        "threatActors": [],
        "hasInfection": true,
        "infections": [
            "adware.android.imp",
            "adware.android.imp"
        ],
        "countryCode": "BQ",
        "industries": [
            "UNKNOWN"
        ],
            "cpe": "",
            "dnsRecords": [],
            "grade": "",
            "mainAttribution": [
                "1",
                "telbo.net",
                "Telbo",
                "UNKNOWN",
                1
            ],
            "detectedLibraryVersion": "core-js-pure@2.6.11",
            "domains": [],
            "osTypes": [],
            "id": "190.4.75.252"
        },
        {
            "detectedLibraries": [
                "core-js"
            ],
            "time": "2022-04-28T21:00:32Z",
            "cloud": "",
            "cloudRegion": "",
            "hasMalrep": false,
            "maliciousReputation": [],
            "hasCVE": false,
            "cves": [],
            "cvss": [],
            "deviceType": [],
            "hasRansomware": false,
            "ransomwareVictims": [],
            "ransomwareGroups": [],
            "hasSSLCert": false,
            "ports": [
                "21"
            ],
            "services": [
                "tcpwrapped"
            ],
            "minGrade": "1.0",
            "hostnames": [
                "telbo-200-6-150-23.cust.telbo.net"
            ],
            "hasScorecard": true,
            "products": [
                "Unknown tcpwrapped"
            ],
            "country": " and Saba\"",
            "organizations": [
                "Example12"
            ],
            "hasCVEExploited": false,
            "ips": [
                "223.4.56.789"
            ],
            "sslValid": false,
            "hasThreatActor": false,
            "threatActors": [],
            "hasInfection": true,
            "infections": [
                "pva.torrent.openinternet"
            ],
            "countryCode": "BQ",
            "industries": [
                "UNKNOWN"
            ],
            "cpe": "",
            "dnsRecords": [],
            "grade": "",
            "mainAttribution": [
                "1",
                "example1.com",
                "Example1",
                "UNKNOWN",
                1
            ],
            "detectedLibraryVersion": "core-js-pure@2.6.11",
            "domains": [],
            "osTypes": [],
            "id": "200.6.150.23"
        },
        {
            "detectedLibraries": [
                "WordPress",
                "core-js"
            ],
            "time": "2022-04-19T14:59:24Z",
            "cloud": "",
            "cloudRegion": "",
            "hasMalrep": false,
            "maliciousReputation": [],
            "hasCVE": false,
            "cves": [],
            "cvss": [],
            "deviceType": [],
            "hasRansomware": false,
            "ransomwareVictims": [],
            "ransomwareGroups": [],
            "hasSSLCert": false,
            "ports": [
                "21"
            ],
            "services": [
                "tcpwrapped"
            ],
            "minGrade": "0.0",
            "hostnames": [
                "node-ba09f69e0.cust.telbo.net"
            ],
            "hasScorecard": true,
            "products": [
                "Unknown tcpwrapped"
            ],
            "country": " and Saba\"",
            "organizations": [
                " Banco do Brasil",
                "Banco do Brasil",
                "Telbo"
            ],
            "hasCVEExploited": false,
            "ips": [
                "186.159.105.224"
            ],
            "sslValid": false,
            "hasThreatActor": false,
            "threatActors": [],
            "hasInfection": true,
            "infections": [
                "pva.torrent.openinternet",
                "pva.torrent.openinternet",
                "pua.android.cheetah"
            ],
            "countryCode": "BQ",
            "industries": [
                "FINANCIAL_SERVICES",
                "UNKNOWN"
            ],
            "cpe": "",
            "dnsRecords": [],
            "grade": "",
            "mainAttribution": [
                "0",
                "example114.net",
                " Example14",
                "FINANCIAL_SERVICES",
                3
            ],
            "detectedLibraryVersion": "core-js-pure@2.6.11",
            "domains": [],
            "osTypes": [],
            "id": "(ID)"
```

```
        },
        {
            "detectedLibraries": [
                "WordPress",
                "core-js"
            ],
            "time": "2022-07-12T15:58:39Z",
            "cloud": "",
            "cloudRegion": "",
            "hasMalrep": false,
            "maliciousReputation": [],
            "hasCVE": false,
            "cves": [],
            "cvss": [],
            "deviceType": [],
            "hasRansomware": false,
            "ransomwareVictims": [],
            "ransomwareGroups": [],
            "hasSSLCert": false,
            "ports": [
                "21"
            ],
            "services": [
                "tcpwrapped"
            ],
            "minGrade": "0.0",
            "hostnames": [
                "node-ba09f6a79.cust.telbo.net"
            ],
            "hasScorecard": true,
            "products": [
                "Unknown tcpwrapped"
            ],
            "country": " and Saba\"",
            "organizations": [
                " Example15",
                "Example16",
                "Example"
            ],
            "hasCVEExploited": false,
            "ips": [
                "323.4.56.789"
            ],
            "sslValid": false,
            "hasThreatActor": false,
            "threatActors": [],
            "hasInfection": true,
            "infections": [
                "pva.torrent.openinternet"
            ],
            "countryCode": "BQ",
            "industries": [
                "FINANCIAL_SERVICES",
                "UNKNOWN"
            ],
            "cpe": "",
            "dnsRecords": [],
            "grade": "",
            "mainAttribution": [
                "0",
                "example15.com",
                " Example15",
                "FINANCIAL_SERVICES",
                3
            ],
            "detectedLibraryVersion": "core-js-pure@2.6.11",
            "domains": [],
            "osTypes": [],
            "id": "(ID)"
        },
        {
            "detectedLibraries": [
                "WordPress"
            ],
            "time": "2022-10-16T13:52:22Z",
            "cloud": "",
            "cloudRegion": "",
            "hasMalrep": false,
            "maliciousReputation": [],
            "hasCVE": false,
            "cves": [],
            "cvss": [],
            "deviceType": [],
            "hasRansomware": false,
            "ransomwareVictims": [],
            "ransomwareGroups": [],
            "hasSSLCert": false,
            "ports": [
                "10443"
            ],
            "services": [
                "cirrossp"
            ],
            "minGrade": "1.0",
            "hostnames": [],
            "hasScorecard": true,
            "products": [],
            "country": " and Saba\"",
            "organizations": [
                "Example16"
            ],
            "hasCVEExploited": false,
            "ips": [
                "423.45.67.899"
            ],
            "sslValid": false,
            "hasThreatActor": false,
            "threatActors": [],
            "hasInfection": true,
            "infections": [
                "pva.torrent.openinternet",
                "pva.torrent.openinternet",
                "pva.torrent.openinternet",
                "pva.torrent.openinternet",
                "pva.torrent.openinternet",
                "pva.torrent.openinternet",
                "pva.torrent.openinternet",
                "pva.torrent.openinternet",
                "pva.torrent.openinternet",
                "pva.torrent.openinternet",
                "pva.torrent.openinternet",
                "pva.torrent.openinternet",
                "pva.torrent.openinternet"
            ],
            "countryCode": "BQ",
            "industries": [
                "UNKNOWN"
            ],
            "cpe": "",
            "dnsRecords": [],
            "grade": "",
            "mainAttribution": [
                "1",
                "example17.net",
                "Example17",
                "UNKNOWN",
                1
            ],
            "detectedLibraryVersion": "",
            "domains": [],
            "osTypes": [],
            "id": "(ID)"
        },
        {
            "detectedLibraries": [
                "WordPress"
            ],
            "time": "2022-10-14T15:37:53Z",
            "cloud": "",
            "cloudRegion": "",
            "hasMalrep": false,
            "maliciousReputation": [],
            "hasCVE": false,
            "cves": [],
            "cvss": [],
            "deviceType": [],
            "hasRansomware": false,
            "ransomwareVictims": [],
            "ransomwareGroups": [],
            "hasSSLCert": false,
            "ports": [
                "80"
            ],
            "services": [
                "http"
            ],
            "minGrade": "0.0",
            "hostnames": [],
            "hasScorecard": true,
            "products": [
                "micro_httpd"
            ],
            "country": " and Saba\"",
            "organizations": [
                " Example18",
                "Example19"
            ],
            "hasCVEExploited": false,
            "ips": [
                "190.97.115.5"
            ],
            "sslValid": false,
            "hasThreatActor": false,
            "threatActors": [],
            "hasInfection": true,
            "infections": [
                "adware.android.imp",
                "adware.android.imp",
                "adware.android.imp",
                "adware.android.imp"
            ],
            "countryCode": "BQ",
            "industries": [
                "FINANCIAL_SERVICES"
            ],
            "cpe": "cpe:/a:acme:micro_httpd,cpe:/o:acme:micro_httpd",
            "dnsRecords": [],
            "grade": "",
            "mainAttribution": [
                "0",
                "example20.net",
                " Example20",
                "FINANCIAL_SERVICES",
                2
            ],
            "detectedLibraryVersion": "",
            "domains": [],
            "osTypes": [],
            "id": "(ID)"
        },
        {
            "detectedLibraries": [
                "WordPress",
                "core-js"
            ],
            "time": "2022-10-14T04:19:59Z",
            "cloud": "",
            "cloudRegion": "",
            "hasMalrep": false,
            "maliciousReputation": [],
            "hasCVE": false,
            "cves": [],
            "cvss": [],
            "deviceType": [],
            "hasRansomware": false,
            "ransomwareVictims": [],
            "ransomwareGroups": [],
            "hasSSLCert": false,
            "ports": [
                "21"
            ],
            "services": [
                "tcpwrapped"
            ],
            "minGrade": "0.0",
            "hostnames": [
                "example21.net"
            ],
            "hasScorecard": true,
            "products": [],
            "country": " and Saba\"",
            "organizations": [
                "Example22",
                " Example22",
                "Example23"
            ],
            "hasCVEExploited": false,
            "ips": [
                "186.159.109.98"
            ],
            "sslValid": false,
            "hasThreatActor": false,
            "threatActors": [],
            "hasInfection": true,
            "infections": [
                "pua.android.cheetah",
                "pua.android.cheetah",
                "pua.android.cheetah",
                "pua.android.cheetah",
                "pua.android.cheetah",
                "pua.android.cheetah",
                "pua.android.cheetah",
                "pua.android.cheetah",
                "pua.android.cheetah"
            ],
            "countryCode": "BQ",
            "industries": [
                "UNKNOWN",
                "FINANCIAL_SERVICES"
            ],
            "cpe": "",
            "dnsRecords": [],
            "grade": "",
            "mainAttribution": [
                "0",
                "example24.net",
                " Example24",
                "FINANCIAL_SERVICES",
                3
            ],
            "detectedLibraryVersion": "core-js-pure@2.6.11",
            "domains": [],
            "osTypes": [],
            "id": "(ID)"
        },
        {
            "detectedLibraries": [
                "WordPress",
                "core-js"
            ],
            "time": "2022-08-21T04:15:35Z",
            "cloud": "",
            "cloudRegion": "",
            "hasMalrep": false,
            "maliciousReputation": [],
            "hasCVE": false,
            "cves": [],
            "cvss": [],
            "deviceType": [],
            "hasRansomware": false,
            "ransomwareVictims": [],
            "ransomwareGroups": [],
            "hasSSLCert": false,
            "ports": [
                "21"
            ],
            "services": [
                "tcpwrapped"
            ],
            "minGrade": "0.0",
            "hostnames": [
                "example26.net"
            ],
            "hasScorecard": true,
            "products": [
                "Unknown tcpwrapped"
            ],
            "country": " and Saba\"",
            "organizations": [
                "Example26",
                " Example26",
                "Example27"
            ],
            "hasCVEExploited": false,
            "ips": [
                "123.45.67.890"
            ],
            "sslValid": false,
            "hasThreatActor": false,
            "threatActors": [],
            "hasInfection": true,
            "infections": [
                "pva.torrent.openinternet",
                "pva.torrent.openinternet",
                "pva.torrent.openinternet",
                "pva.torrent.openinternet",
                "pva.torrent.openinternet"
            ],
            "countryCode": "BQ",
            "industries": [
                "UNKNOWN",
                "FINANCIAL_SERVICES"
            ],
            "cpe": "",
            "dnsRecords": [],
            "grade": "",
            "mainAttribution": [
                "0",
                "example28.com",
                " Example28",
                "FINANCIAL_SERVICES",
                3
            ],
            "detectedLibraryVersion": "core-js-pure@2.6.11",
            "domains": [],
            "osTypes": [],
            "id": "(ID)"
        },
        {
            "detectedLibraries": [],
            "time": "2022-05-29T09:24:36Z",
            "cloud": "",
            "cloudRegion": "",
            "hasMalrep": false,
            "maliciousReputation": [],
            "hasCVE": false,
            "cves": [],
            "cvss": [],
            "deviceType": [],
            "hasRansomware": false,
            "ransomwareVictims": [],
            "ransomwareGroups": [],
            "hasSSLCert": false,
            "ports": [
                "7547"
            ],
            "services": [
                "tcpwrapped"
            ],
            "minGrade": "",
            "hostnames": [],
            "hasScorecard": false,
            "products": [],
            "country": " and Saba\"",
            "organizations": [],
            "hasCVEExploited": false,
            "ips": [
                "204.157.85.74"
            ],
            "sslValid": false,
            "hasThreatActor": false,
            "threatActors": [],
            "hasInfection": true,
            "infections": [
                "pua.android.cheetah"
            ],
            "countryCode": "BQ",
            "industries": [],
            "cpe": "",
            "dnsRecords": [],
            "grade": "",
            "mainAttribution": [],
            "detectedLibraryVersion": "",
            "domains": [],
            "osTypes": [],
            "id": "204.157.85.74"
        }
    ],
    "found": 36508440,
    "isError": false,
    "errorType": "",
    "errorCode": 0
}
```

Example initial request with *cursor* parameter

```
curl --request POST \
--url https://api.securityscorecard.io/asi/search \
--header 'Authorization: Token (token)' \
--header 'accept: */*' \
--header 'content-type: application/json' \
--data '
{
"page": 0,
"index": "ipv4",
"parser": "structured",
"size": 10,000
"query": "has_infection:1",
"cursor": "initial",
"sort": "country_name"
}
'
```

Example response when *cursor* parameter is used in request

We shortened the results for display purposes.

See the *cursor* value at the bottom of the result set. You would use this value to specify the next set of hits.

```
{
  "facets": {
    "countries": [
      {
        "name": "Germany",
        "value": 4548845
      },
      {
        "name": "Russian Federation",
        "value": 3867762
      },
      {
        "name": "United States",
        "value": 3846666
      },
//We removed other returned countries to make the example more readable.
    ],
    "threatActors": [
      {
        "name": "Packrat",
        "value": 1849277
      },
      {...},
      {
        "name": "21",
        "value": 1477702
      }
    ],
    "products": [
      {
        "name": "Unknown cwmp",
        "value": 3624393
      },
      {
        "name": "AVM FRITZ!OS SIP",
        "value": 2048443
      },
      {...},
      {
        "name": "OpenSSH",
        "value": 921965
      }
    ],
    "attributedDomains": [
      {
        "name": "example4.com.br",
        "value": 3885557
      },
      {...},
      {
        "name": "example9.com",
        "value": 2112667
      }
    ],
    "orgs": [
      {
        "name": "Example",
        "value": 3885557
      },
      {
        "name": "Example",
        "value": 3885557
      },
      {...},
      {
        "name": "Example",
        "value": 1778897
      }
    ]
  },
  "hits": [
    {
      "detectedLibraries": [],
      "time": "2022-11-20T10:15:16Z",
      "cloud": "",
      "cloudRegion": "",
      "hasMalrep": false,
      "maliciousReputation": [],
      "hasCVE": false,
      "cves": [],
      "cvss": [],
      "deviceType": [],
      "hasRansomware": false,
      "ransomwareVictims": [],
      "ransomwareGroups": [],
      "hasSSLCert": false,
      "ports": [
        "443"
      ],
      "services": [
        "https"
      ],
      "minGrade": "",
      "hostnames": [
        "hst147.tidningen.aland.fi"
      ],
      "hasScorecard": false,
      "products": [],
      "country": "Åland Islands",
      "organizations": [],
      "hasCVEExploited": false,
      "ips": [
        "123.456.789.1"
      ],
      "sslValid": false,
      "hasThreatActor": false,
      "threatActors": [],
      "hasInfection": true,
      "infections": [
        "adware.android.imp"
      ],
      "countryCode": "AX",
      "industries": [],
      "cpe": "",
      "dnsRecords": [],
      "grade": "",
      "mainAttribution": [],
      "detectedLibraryVersion": "",
      "domains": [],
      "osTypes": [],
      "id": "194.110.186.147"
    },
    {
      "detectedLibraries": [
        "Drupal"
      ],
      "time": "2022-11-18T23:48:38Z",
      "cloud": "",
      "cloudRegion": "",
      "hasMalrep": false,
      "maliciousReputation": [],
      "hasCVE": true,
      "cves": [
        "CVE-2022-23943",
        "...",
        "CVE-2021-44224"
      ],
      "cvss": [],
      "deviceType": [],
      "hasRansomware": false,
      "ransomwareVictims": [],
      "ransomwareGroups": [],
      "hasSSLCert": true,
      "ports": [
        "80",
        "443"
      ],
      "services": [
        "https",
        "http"
      ],
      "minGrade": "",
      "hostnames": [
        "ls-dial-dyn100.ls.aland.fi"
      ],
      "hasScorecard": true,
      "products": [],
      "country": "Åland Islands",
      "organizations": [
        "Example1"
      ],
      "hasCVEExploited": false,
      "ips": [
        "123.456.789.2"
      ],
      "sslValid": false,
      "hasThreatActor": true,
      "threatActors": [
        "Gamaredon Group"
      ],
      "hasInfection": true,
      "infections": [
        "pva.newsdaily",
        "...",
        "pva.newsdaily"
      ],
      "countryCode": "AX",
      "industries": [
        "FINANCIAL_SERVICES"
      ],
      "cpe": "",
      "dnsRecords": [],
      "grade": "",
      "mainAttribution": [
        "3",
        "example",
        "Example",
        "FINANCIAL_SERVICES",
        1
      ],
      "detectedLibraryVersion": "7",
      "domains": [],
      "osTypes": [],
      "id": "123.456.789.10"
    },
    {
      "detectedLibraries": [],
      "time": "2022-11-06T11:43:29Z",
      "cloud": "",
      "cloudRegion": "",
      "hasMalrep": false,
      "maliciousReputation": [],
      "hasCVE": false,
      "cves": [],
      "cvss": [],
      "deviceType": [],
      "hasRansomware": false,
      "ransomwareVictims": [],
      "ransomwareGroups": [],
      "hasSSLCert": true,
      "ports": [
        "443",
        "80"
      ],
      "services": [
        "http"
      ],
      "minGrade": "",
      "hostnames": [
        "smtp.rabe.ax"
        ],
        "hasScorecard": false,
        "products": [
          "Microsoft IIS httpd"
        ],
        "country": "Åland Islands",
        "organizations": [],
        "hasCVEExploited": false,
        "ips": [
          "123.456.789.3"
        ],
        "sslValid": false,
        "hasThreatActor": false,
        "threatActors": [],
        "hasInfection": true,
        "infections": [
          "adware.android.imp",
          "adware.android.imp",
          "...",
          "pua.android.cheetah"
        ],
        "countryCode": "AX",
        "industries": [],
        "cpe": "cpe:/a:microsoft:internet_information_services:10.0,cpe:/o:microsoft:windows",
        "dnsRecords": [],
        "grade": "",
        "mainAttribution": [],
        "detectedLibraryVersion": "",
        "domains": [],
        "osTypes": [
          "Windows"
        ],
        "id":"123.456.789.0"
      },
      {
        "detectedLibraries": [],
        "time": "2022-11-13T15:00:49Z",
        "cloud": "",
        "cloudRegion": "",
        "hasMalrep": false,
        "maliciousReputation": [],
        "hasCVE": false,
        "cves": [],
        "cvss": [],
        "deviceType": [],
        "hasRansomware": false,
        "ransomwareVictims": [],
        "ransomwareGroups": [],
        "hasSSLCert": false,
        "ports": [
          "3389",
          "5985"
        ],
        "services": [
          "ms-wbt-server",
          "http"
        ],
        "minGrade": "",
        "hostnames": [],
        "hasScorecard": false,
        "products": [
          "Microsoft HTTPAPI httpd"
        ],
        "country": "Åland Islands",
        "organizations": [],
        "hasCVEExploited": false,
        "ips": [
          "123.456.789.1"
        ],
        "sslValid": false,
        "hasThreatActor": false,
        "threatActors": [],
        "hasInfection": true,
        "infections": [
          "generic_malware"
        ],
        "countryCode": "AX",
        "industries": [],
        "cpe": "cpe:/o:microsoft:windows",
        "dnsRecords": [],
        "grade": "",
        "mainAttribution": [],
        "detectedLibraryVersion": "",
        "domains": [],
        "osTypes": [
          "Windows"
        ],
        "195.133.20.247"
      },
      {
```

```
    "detectedLibraries": [],
    "time": "2022-12-19T13:37:45Z",
    "cloud": "",
    "cloudRegion": "",
    "hasMalrep": true,
    "maliciousReputation": [
      "IPsum (aggregation of all feeds) - level 1 - lot of false positives feed"
    ],
    "hasCVE": false,
    "cves": [],
    "cvss": [],
    "deviceType": [],
    "hasRansomware": false,
    "ransomwareVictims": [],
    "ransomwareGroups": [],
    "hasSSLCert": false,
    "ports": [
      "139",
      "5985",
      "3389",
      "135",
      "445",
      "1029",
      "1026",
      "1025",
      "1027"
    ],
    "services": [
      "microsoft-ds",
      "http",
      "netbios-ssn",
      "msrpc",
      "ms-wbt-server"
    ],
    "minGrade": "",
    "hostnames": [],
    "hasScorecard": false,
    "products": [
      "Microsoft Windows RPC",
      "Microsoft HTTPAPI httpd",
      "Microsoft Windows netbios-ssn",
      "Microsoft Windows Server 2008 R2 - 2012 microsoft-ds"
    ],
    "country": "Åland Islands",
    "organizations": [],
    "hasCVEExploited": false,
    "ips": [
      "123.456.789.4"
    ],
    "sslValid": false,
    "hasThreatActor": false,
    "threatActors": [],
    "hasInfection": true,
    "infections": [
      "generic_malware",
      "...",
      "generic_malware"
    ],
    "countryCode": "AX",
    "industries": [],
    "cpe": "cpe:/o:microsoft:windows",
    "dnsRecords": [],
    "grade": "",
    "mainAttribution": [],
    "detectedLibraryVersion": "",
    "domains": [],
    "osTypes": [
      "Windows Server 2008 R2 - 2012",
      "Windows"
    ],
    "id": "124.456.789.0"
  },
  {
    "detectedLibraries": [
      "Drupal",
      "core-js"
    ],
    "time": "2022-12-18T06:09:51Z",
    "cloud": "",
    "cloudRegion": "",
    "hasMalrep": false,
    "maliciousReputation": [],
    "hasCVE": false,
    "cves": [],
    "cvss": [],
    "deviceType": [],
    "hasRansomware": false,
    "ransomwareVictims": [],
    "ransomwareGroups": [],
    "hasSSLCert": false,
    "ports": [
      "22",
      "8291",
      "80",
      "2000"
    ],
    "services": [
      "tcpwrapped",
      "bandwidth-test"
    ],
    "minGrade": "",
    "hostnames": [
      "213-204-33-50.aland.net"
    ],
    "hasScorecard": true,
    "products": [
      "MikroTik bandwidth-test server"
    ],
    "country": "Åland Islands",
    "organizations": [
      "Example2",
      "Example3",
      "Example4",
      "Example5"
    ],
    "hasCVEExploited": false,
    "ips": [
      "123.456.789.7"
    ],
    "sslValid": false,
    "hasThreatActor": false,
    "threatActors": [],
    "hasInfection": true,
    "infections": [
      "pva.torrent.openinternet",
      "pva.newsdaily",
      "adware.android.imp",
      "...",
      "adware.android.imp"
    ],
    "countryCode": "AX",
    "industries": [
      "MANUFACTURING",
      "TELECOMMUNICATIONS",
      "UNKNOWN"
    ],
    "cpe": "",
    "dnsRecords": [],
    "grade": "",
    "mainAttribution": [
      "1",
      "example1.com",
      "example1",
      "MANUFACTURING",
      5
    ],
    "detectedLibraryVersion": "7,core-js-global@3.24.1",
    "domains": [],
    "osTypes": [],
    "id": "124.456.789.0"
```

```
    },
    {
      "detectedLibraries": [
        "Drupal"
      ],
      "time": "2022-12-16T09:24:10Z",
      "cloud": "",
      "cloudRegion": "",
      "hasMalrep": false,
      "maliciousReputation": [],
      "hasCVE": false,
      "cves": [],
      "cvss": [],
      "deviceType": [],
      "hasRansomware": false,
      "ransomwareVictims": [],
      "ransomwareGroups": [],
      "hasSSLCert": false,
      "ports": [
        "8433"
      ],
      "services": [],
      "minGrade": "",
      "hostnames": [],
      "hasScorecard": false,
      "products": [],
      "country": "Åland Islands",
      "organizations": [],
      "hasCVEExploited": false,
      "ips": [
        "123.456.789.8"
      ],
      "sslValid": false,
      "hasThreatActor": false,
      "threatActors": [],
      "hasInfection": true,
      "infections": [
        "adware.android.imp"
      ],
      "countryCode": "AX",
      "industries": [],
      "cpe": "",
      "dnsRecords": [],
      "grade": "",
      "mainAttribution": [],
      "detectedLibraryVersion": "7",
      "domains": [],
      "osTypes": [],
      "id": "124.456.789.0"
    },
    {
      "detectedLibraries": [
        "Drupal",
        "core-js"
      ],
      "time": "2022-12-18T20:41:45Z",
      "cloud": "",
      "cloudRegion": "",
      "hasMalrep": false,
      "maliciousReputation": [],
      "hasCVE": false,
      "cves": [],
      "cvss": [],
      "deviceType": [],
      "hasRansomware": false,
      "ransomwareVictims": [],
      "ransomwareGroups": [],
      "hasSSLCert": true,
      "ports": [
        "443"
      ],
      "services": [
        "https"
      ],
      "minGrade": "",
      "hostnames": [],
      "hasScorecard": true,
      "products": [],
      "country": "Åland Islands",
      "organizations": [
        "Example6",
        "Example7",
        "Example8",
        "Example9"
      ],
      "hasCVEExploited": false,
      "ips": [
        "123.456.789.9"
      ],
      "sslValid": false,
      "hasThreatActor": false,
      "threatActors": [],
      "hasInfection": true,
      "infections": [
        "android.digitime.fota"
      ],
      "countryCode": "AX",
      "industries": [
        "TELECOMMUNICATIONS",
        "UNKNOWN",
        "MANUFACTURING"
      ],
      "cpe": "",
      "dnsRecords": [],
      "grade": "",
      "mainAttribution": [
        "1",
        "example2.com",
        "Example2",
        "UNKNOWN",
        4
      ],
      "detectedLibraryVersion": "7,core-js-global@3.24.1",
      "domains": [],
      "osTypes": [],
      "id": "124.456.789.0"
    },
    {
      "detectedLibraries": [],
      "time": "2022-11-20T02:10:19Z",
      "cloud": "",
      "cloudRegion": "",
      "hasMalrep": false,
      "maliciousReputation": [],
      "hasCVE": false,
      "cves": [],
      "cvss": [],
      "deviceType": [],
      "hasRansomware": false,
      "ransomwareVictims": [],
      "ransomwareGroups": [],
      "hasSSLCert": true,
      "ports": [
        "80",
        "443"
      ],
      "services": [
        "http",
        "https"
      ],
      "minGrade": "",
      "hostnames": [
        "mail.vatten.ax"
      ],
      "hasScorecard": false,
      "products": [
        "Microsoft IIS httpd",
        "Microsoft-IIS/10.0"
      ],
      "country": "Åland Islands",
        "organizations": [],
        "hasCVEExploited": false,
        "ips": [
          "123.456.789.10"
        ],
        "sslValid": false,
        "hasThreatActor": false,
        "threatActors": [],
        "hasInfection": true,
        "infections": [
          "pua.android.cheetah",
          "...",
          "pua.android.cheetah"
        ],
        "countryCode": "AX",
        "industries": [],
        "cpe": "cpe:/a:microsoft:internet_information_services:10.0,cpe:/o:microsoft:windows,cpe
        "dnsRecords": [],
        "grade": "",
        "mainAttribution": [],
        "detectedLibraryVersion": "",
        "domains": [],
        "osTypes": [
          "Windows"
        ],
        "id": "124.456.789.0"
      },
      {
        "detectedLibraries": [
          "Drupal",
        "core-js"
      ],
      "time": "2022-10-27T05:13:43Z",
      "cloud": "",
      "cloudRegion": "",
      "hasMalrep": false,
      "maliciousReputation": [],
      "hasCVE": false,
      "cves": [],
      "cvss": [],
      "deviceType": [
        "firewall"
      ],
      "hasRansomware": false,
      "ransomwareVictims": [],
      "ransomwareGroups": [],
      "hasSSLCert": true,
      "ports": [
        "80",
        "443"
      ],
      "services": [
        "http"
      ],
      "minGrade": "",
      "hostnames": [
        "213-204-46-50.bredband.aland.net"
      ],
      "hasScorecard": true,
      "products": [
          "SonicWALL firewall http config"
        ],
        "country": "Åland Islands",
        "organizations": [
          "Example10",
          "Example11",
          "Example12",
          "Example13"
        ],
        "hasCVEExploited": false,
        "ips": [
          "123.456.789.11"
        ],
        "sslValid": false,
        "hasThreatActor": false,
        "threatActors": [],
        "hasInfection": true,
        "infections": [
          "adware.android.imp"
        ],
        "countryCode": "AX",
        "industries": [
          "UNKNOWN",
          "MANUFACTURING",
          "TELECOMMUNICATIONS"
        ],
        "cpe": "",
        "dnsRecords": [],
        "grade": "",
        "mainAttribution": [
          "1",
          "example3.com",
          "Example3",
          "MANUFACTURING",
          5
        ],
        "detectedLibraryVersion": "7,core-js-global@3.24.1",
        "domains": [],
        "osTypes": [],
        "id": "124.456.789.0"
      }
    ],
    "found": 44718583,
    "isError": false,
    "errorType": "",
    "errorCode": 0,
    "cursor": "VVU0b1UsQW9JdXc0VnNZVzVrSUVsemJHRnVaSE10TWpFekxqSXdOQzQwTmk0MU1BPT0K"
}
```

The second request with the *cursor* parameter

The second request uses the cursor value returned with the initial request:

```
curl --request POST \
     --url https://api.securityscorecard.io/asi/search \
     --header 'Authorization: Token (token)' \
     --header 'accept: */*' \
     --header 'content-type: application/json' \
     --data '
```

```
{
     "page": 0,
     "index": "ipv4",
     "parser": "structured",
     "size": 10,
     "query": "has_infection:1",
     "cursor": "VVU0b1UsQW9JdXc0VnNZVzVrSUVsemJHRnVaSE10TWpFekxqSXdOQzQwTmk0MU1BPT0K",
     "sort": "country_name"
}
'
```

We are compiling descriptions for returned data. Check this page for future updates.

Return to the top of this section.

See expressions for facets

You may not know the possible values for a particular facet until you query for it. With the facets endpoint, you can see all possible expressions or values for any facet that you can query for in Attack Surface Intelligence.

> **Tip:** See descriptions for the facets available in ASI searches.

In the following example, you can post all possible values for the facet *threat_actor*. You can then search for information on any of the returned values, such as *Sandworm Team*.

```
{
"names": [
"threat_actor","country_name"
],
"index": "ipv4",
"size": 50
}
```

When querying the facets endpoint, you can specify the number of data points you want to see associated with that value.

The following request returns 30 countries and 30 threat actors, each with more data point in the data set:

```
{
        "names": ["country_name", "threat_actor"],
        "size": 30
}
```

Example request

```
curl --location --request POST 'https://platform-api.securityscorecard.io/asi/facets' \
--header 'Authorization: Bearer (token)' \
--header 'Content-Type: application/json' \
--data-raw '{
  "names": [
    "threat_actor","country_name"
  ],
  "index": "ipv4",
  "size": 5
}'
```

Request parameters

Field	Description

names	The facets that you want to see expressions for. In this example, the facets are *threat_actor* and *country_name*. See all available facets in ASI. **Tip:** Some ASI facets return binary expressions (1=*yes*; 0=*no*). Those facet names begin with *has_*. Disregard those for the purposes of using this query.
index	The set of structured data examined by a search engine looking for information relevant to your query. Possible values: *IPV4* *leakedCreds*
size	Number of returned names

Example response

> **Tip:** In addition to the facet expressions, the query also returns the amount of data entries for each expression. For example, as seen in the following response, the *value* field shows that there are 25,158,731 entries for the threat actor *APT37*.

```
{
    "facets": {
        "threat_actor": [
            {
                "name": "APT37",
                "value": 25158731
            },
            {
                "name": "APT28",
                "value": 16731181
            },
            {
                "name": "Cobalt Group",
                "value": 16708322
            },
            {
                "name": "Sandworm Team",
                "value": 16668504
            },
            {
                "name": "Packrat",
                "value": 16319474
            }
        ],
        "country_name": [
            {
                "name": "United States",
                "value": 73883056
            },
            {
                "name": "Germany",
                "value": 30672952
            },
            {
                "name": "South Korea",
                "value": 25148877
            },
            {
                "name": "China",
                "value": 22446555
            },
            {
                "name": "United Kingdom",
                "value": 16687397
            }
        ]
    }
}
```

We are compiling descriptions for returned data. Check this page for future updates.

Return to the top of this section.

Was this article helpful?

Yes No

0 out of 0 found this helpful

Help Center

Have more questions? Submit a request

Return to top

Recently viewed articles

SecurityScorecard glossary

Prepare for a scoring recalibration

Manage users and permissions in SecurityScorecard

SAML is not enabled after you set up SSO

Attack detected

Related articles

Create your own queries in Attack Surface Intelligence

Ratings API

Analyze comprehensive threat data with Attack Surface Intelligence

Create API tokens for the SecurityScorecard platform

Use example queries or visual filters to find data in Attack Surface Intelligence