National Cybersecurity API Guide

Publication Date – November 9,, 2021

Table of Contents

Manage National Cybersecurity via API

National Cybersecurity takes advantage of existing endpoints, along with `/sovereign` API endpoint paths to maximize the integration of National Cybersecurity data with risk management systems and solutions.

Endpoints

Companies

Path	Purpose	Description
`/v1/companies/company_guid`	GET: Country Details	Retrieve National Cybersecurity information during the past 1 year.
`/v1/companies/company_guid/observations`	GET: Detailed Company Observations	View detailed observations for a company.

Industries

Path	Purpose	Description
`/v1/industries/countries`	GET: Industry and Country Ratings	Retrieve information about the most recent rating of country/industry combinations in the portfolio. This lists the security ratings of available industries within a country as an array.

Portfolio

Path	Purpose	Description
`/v2/portfolio`	GET: Portfolio Details	Information regarding your National Cybersecurity portfolio.
`/v1/portfolio/countries`	GET: Geographic IP Address Space	Retrieve information about the geographic IP address space of your National Cybersecurity portfolio. This can be used to determine which companies need to comply with data residency requirements.
`/v1/portfolio/filters`	GET: Portfolio Filters	This returns infections, open ports, and vulnerabilities in your portfolio, and also

		statistics on infections and vulnerabilities that are present.
`/v1/portfolio/guids`	GET: Portfolio Unique Identifiers	Returns a simple list of company or country unique identifiers in your portfolio.
`/v1/portfolio/ratings`	GET, POST: Security Rating Details of Countries in Your Portfolio	Get security rating details of the countries in your portfolio, including the unique identifiers of particular countries.
`/v2/portfolio/summaries`	GET: Portfolio Summary	Get a summary of your portfolio. This can be used to get a list of the possible values for querying GET: Portfolio Details.

Sovereign

Sovereign endpoint documentation for managing National Cybersecurity. The sovereign endpoint takes advantage of existing endpoints, along with sovereign-specific endpoints to maximize the integration of National Cybersecurity data with risk management systems and solutions.

Path	Purpose	Description
`/sovereign/network-resources/ips/ip_address`	GET: National Cybersecurity Network Resources	Determine if a specific IP address belongs to the address space of one of your subscribed countries.
`/sovereign/network-resources/ips/ip_address`	GET: National Cybersecurity Network Resources	Determine if a specific IP address belongs to the address space of one of your subscribed countries.
`/sovereign/observations`	GET: National Cybersecurity Observations	Retrieve the most recent 1,000 observations within the primary country of your National Cybersecurity portfolio.
`/sovereign/observations/companies/kpis/`	GET: National Cybersecurity Companies KPI	See observation distinct company counts for each supported filter.
`/sovereign/observations/counts`	GET: National Cybersecurity Observation Counts	Retrieve the total count of all observed findings throughout all risk vectors, that were observed in companies attributed to a country.
`/sovereign/observations/kpis`	GET: KPI for National Cybersecurity Observations	Retrieve top infections, top vulnerabilities, and the most common open ports for companies in your National Cybersecurity portfolio.

Make API responses more readable with JQ

JQ is a command-line processor that can neatly display JSON, and should make troubleshooting and testing API calls easier.

In the cURL examples in this document, some of them end with jq. Visit the JQ website for installation instructions. Put | jq at the end of any cURL request to make the response easier to read.

GET: Country Details

https://api.bitsighttech.com/companies/country_guid

Get 1 year of BitSight data of subscribed companies or countries.

Parameters

*Required.

Parameter	Description	Values
format	Format the response data.	*[String]* json
guid*	Identify the company or country to query.	*[String]* Company or country unique identifier [company_guid or country_guid]. See GET: National Cybersecurity Portfolio Details.

Example Request

```
curl
'https://api.bitsighttech.com/companies/5d04c480-b1e7-48af-9633-82996a8446fc
' -u api_token:
```

Example Response

```
{
  "guid": "5d04c480-b1e7-48af-9633-82996a8446fc",
  "custom_id": null,
  "name": "Florin",
  "description": "",
  "ipv4_count": 0,
  "people_count": 55860330,
  "industry": null,
  "homepage": null,
  "primary_domain": null,
  "type": "COUNTRY",
  "display_url": null,
  "rating_details": {
  […]
  },
  "ratings": [
  […]
```

```
  ],
  "search_count": 0,
  "subscription_type": "Countries",
  "subscription_type_key": "countries",
  "subscription_end_date": null,
  "confidence": "LOW",
  "bulk_email_sender_status": "NONE",
  "service_provider": false,
  "customer_monitoring_count": 3
}
```


Response Attributes

The response is similar to that of the Companies API endpoint for, but some fields will be empty or `null`, as there are differences between the data for National Cybersecurity and Enterprise subscriptions.

Field	Description
`guid` *String* [`company_guid` or `country_guid`]	The queried company or country.
`custom_id` *String*	For internal BitSight use.
`name` *String*	The name of the company or country.
`description` *String*	This is empty for National Cybersecurity.
`ipv4_count` *Integer*	This is `0` for National Cybersecurity.
`people_count` *Integer*	The combined number of employees that are attributed to this company or country.
`industry` *Null*	This is `null` for National Cybersecurity. To get information about industries within a country, see GET: Ratings of Industries Within a Country.
`homepage` *Null*	This is `null` for National Cybersecurity.
`primary_domain` *Null*	This is `null` for National Cybersecurity.
`type` *String*	This is `COUNTRY` for National Cybersecurity.

`display_url` *Null*	This is null for National Cybersecurity.
`rating_details` *Object*	Risk vector grade details.
`ratings` *Array*	Historical rating information.
`search_count` *Integer*	The number of times this company has been listed in search results.
`subscription_type` *String*	This is `Countries` for National Cybersecurity.
`subscription_type_key` *String*	This is `countries` for National Cybersecurity.
`subscription_end_date` *Null*	This is `null` for National Cybersecurity.
`confidence` *String*	For internal BitSight use.
`bulk_email_sender_status` *String*	For internal BitSight use.
`service_provider` *Boolean*	This is `false` for National Cybersecurity.
`customer_monitoring_count` *Integer*	The number of companies that are monitoring this company.

GET: Detailed Company Observations

`https://api.bitsighttech.com/ratings/v1/companies/company_guid/observations`

Retrieve detailed information (observations) about the risk category data of companies in your portfolio.

The information is similar to what is shown on the Forensics view of a security rating report, but includes Compromised Systems, Diligence, and User Behavior. Observations do not all necessarily impact the company's rating.

Events and Observations

The BitSight platform normally displays events in groups so that the relation between individual events is obvious, especially if they span several days. This endpoint shows the individual events that comprise the ones shown in the platform.

> **Example:** An event shown in the platform that spans 8 days may show up as 8 or more separate observations in the API.

Parameters

Observations can be filtered with query parameters to make it easier to pick out relevant items from our data stores. Queries are formatted like so:

```
api.bitsighttech.com/ratings/v1/companies/company_guid/observations?risk_types=botnet_infections&port=21
```

Separate multiple parameters with the "&" (ampersand) marker.

Parameter	Description	Values
`company_guid`	Identify the company to query.	*[String]* Company unique identifier [`company_guid`]. See GET: Portfolio Details.
`cursor`	Navigate through multiple pages of results.	*[String]* See cursor for details.
`domain_name`	The domain name to match. Not all observations are associated with particular domain names.	*[String]* The domain name. **Example:** `www.saperix.com`
`end_date`	Sets the end of the date range (inclusive) that the query will match.	*[String]* `YYYY-MM-DD`

`grades`	Filters by a comma-separated list of record grades.	*[String]* • `GOOD` • `FAIR` • `NEUTRAL` • `WARN` • `BAD`
`ip_address`	The IP address to match. Not all observations are associated with particular IP addresses.	*[String]* Any IPv4 address (e.g, “192.0.2.0”) and any IPv6 address (e.g, “2001:DB8::”). This can be an IPv4 address, in dotted notation, or an IPv6 address.
`limit`	Set the maximum number of results.	*[Integer]* Any number from `1` to `1000`. See limit for details. **Default:** `100`
`port`	For observations on a particular network port, this matches the port given port number (e.g 80).	*[Integer]* Any port number, up to 65535.
`risk_types`	The risk types of the observations. Access to some risk types is dependent on the subscription type.	*[String]* Comma-separated risk types.
`start_date` *[string, query]*	Sets the beginning of the date range (inclusive) that the query will match.	*[String]* `YYYY-MM-DD`

Example Request

Use a company’s unique identifier (GUID) to look up its observations. You may opt to specify one or more risk types to return. See the query parameters or refer to the pagination recommendations.

```
curl
'https://api.bitsighttech.com/ratings/v1/companies/company_guid/observations
?risk_types=risk_type' -u api_token:
```

Example Response

If you specify more than one risk type in the `risk_types` parameter of your request, the server will respond with an array of individual records from all the risk types you requested.


```
{
"data": [{
    "risk_type": "spf",
    "observation_id": "ABCDEFCWq5Bx9K4Q-gAAAAAAzCGfs=",
    "collection_date": "2016-07-02",
    "event_date": "2016-07-02",
    "forensics": {
        "domain_name": "samplecompany.com"
    },
    "details": {
        "occurrences": {
            "first_seen": "2016-07-02 02:32:27",
            "last_seen": "2016-07-02 02:32:28",
            "representative_timestamp": "2016-07-02 02:32:28",
            "count": 1
        },
        "grade": "BAD",
        "issue": "",
        "dns": {
            "query_type": 16,
            "error_code": 0,
            "answer": "[[TXT, v=spf1, mx, ip4:xxx.xxx.24.7,
ip4:xxx.xxx.24.6, ip4:xxx.xxx.24.33, ip4:xxx.xxx.24.99, ip4:xxx.xxx.24.9,
ip4:xxx.xxx.24.74, ip4:xxx.xxx.204.5, ip4:xxx.xxx.168.11, -all]]"
        }
    }
]
}
```


Response Attributes

Observations are sorted by date, with the most recent first.

If the system returns a “Detail not found” message, please try using query parameters. No results matched the specified query parameters. Double check to make sure the specified parameters are spelled correctly or see the full list of parameters.

Observations will be returned as JSON and cannot be returned as XML. A JSON object is returned by the API with a data array field. Separate objects of individual observations are within the data array, with the following attributes:

Field	Description
`risk_type` *String*	The slug name of the risk type.

`observation_id` *String*	A unique identifier for the observation.
`collection_date` *String* [`YYYY-MM-DD`]	The date when the observation was collected from the data source.
`event_date` *String* [`YYYY-MM-DD`]	The date when the event was observed.
`forensics` *Object*	Contains data for conducting network forensics based on the provided information.
`host_ip` *String*	An IP address associated with the event if it's related to the risk type. The IP address will be masked, unless the organization's subscription does not include IP addresses. If your organization has the Forensics package, you will see this field for your own organization and the extra details.
`host_port` *String*	A network port associated with the event.
`domain_name` *String*	The domain name associated with the IP address of the observation.
`details` *Object*	Contains details about occurrences.
`occurrences` *Object*	
`first_seen` *String* [`YYYY-MM-DD HH:MM:SS`]	The date when the observation started.
`last_seen` *String* [`YYYY-MM-DD HH:MM:SS`]	The date when the observation ended.
`representative_timestamp` *String* [`YYYY-MM-DD HH:MM:SS`]	The representative timestamp.
`count` *Integer*	The number of times the observation was counted (typically 1).
`grade` *String*	The record grade that's associated with the observation.
`issue` *Array*	Contains associated issue messages (strings) that are related to the observation.
`grade` *String*	The grade assigned to this record.

	`issue` *String*	A description of the issue found with the record, if any.
	`dns` *Object*	
	`query_type` *Integer*	The type of DNS query issued to retrieve this record. See DNS query types.
	`error_code` *Integer*	The DNS response code received after issuing the query. See DNS response codes.
	`answer` *String*	The contents of the returned record from the DNS.

GET: Ratings of Industries Within a Country

https://api.bitsighttech.com/ratings/v1/industries/countries

Get information about the most recent rating of country/industry combinations in your portfolio. This lists the BitSight Security Ratings of available industries within a country.

Parameters

Parameter	Description	Values
`countries`	Filter industries by countries.	*[String]* Comma-separated 2-letter country codes.

Example Request

```
https://api.bitsighttech.com/ratings/v1/industries/countries/?format=json -u api_token:
```

Example Response


```
[
   {
      "country_name":"Demo Country 1",
      "rating":790,
      "guid":"c930a384-a32f-40af-bc0d-e656a1cc6458",
      "industry_name":"Aerospace/Defense",
      "country_code":"A1"
   },
   {
      "country_name":"Demo Country 1",
      "rating":790,
      "guid":"277407fb-4a45-4c07-93d6-9ab92a3621e2",
      "industry_name":"Business Services",
      "country_code":"A1"
   }
]
```

Response Attributes

Field	Description
`country_name` *String*	The name of this country.
`rating` *Integer*	The aggregate BitSight Security Rating of this industry within this country.
`guid` *String* [`industry_guid`]	The unique identifier of this industry.
`industry_name` *String*	The name of this industry.
`country_code` *String*	The 2-letter country-code of this country.

GET: Portfolio Details

`https://api.bitsighttech.com/ratings/v2/portfolio`

Get information about the companies in your portfolio.

Parameters

See query parameters for details on the following parameters:

- `fields`
- `format`
- `limit` (Default 100)
- `offset`
- `q`
- `sort`

Parameter	Description	Values
`exclude_subscription_type.slug`	Exclude one or more subscription types.	*[Array]* Subscription slug names. See the `subscription_types` field in GET: Portfolio Summary.
`filter_group`	Group filters and modify the way the filters intersect with each other.	*[String]* **Example to show all the companies with an A in Botnet Infections:** `?filter_group=risk_vectors&risk_vectors.slug=botnet_infections&risk_vectors.grade=A`
`risk_vectors.grade`	Filter companies with certain risk vector letter grades. Does not include N/A letter grades. • On its own, this includes companies that have any of the specified grades in any risk vector. • This can be intersected with the `risk_vectors.slug` parameter.	*[String]* • Risk vector letter grades. • Use `filter_group=risk_vectors` to filter by specific grades in specific risk vectors.

`risk_vectors.slug`	Filter companies with graded risk vectors. • On its own, this includes companies with a grade in any of the specified risk vectors. • This can be intersected with the `risk_vectors.grade` parameter.	*[String]* • Risk vector slug names. See risk types. • Use `filter_group=risk_vectors` to filter by specific grades in specific risk vectors.
`software.category`	Filter companies by the supported statuses of their software. • On its own, this includes companies that have at least one software of any of the specified categories. • This can be intersected with the `software.name` parameter.	*[String]* • The supported status: ◦ `Supported` ◦ `Unsupported` ◦ `Unknown` • Use `filter_group=software` to filter by specific software in specific categories.
`software.name`	Filter companies with certain software detected on their network. • On its own, this includes companies that have any of the specified software, across all software categories. • This can be intersected with the `software.category` parameter.	*[String]* • Software name. • Use `filter_group=software` to filter by specific software in specific categories.
`folder`	Filter companies by folder.	*[Array]* • Folder unique identifiers [`folder_guid`]. See GET: Folder Details. • `null` to include companies that are not in a folder.
`industry.name`	Filter companies by their industry.	*[Array]* Industry names. See the `industries` field in GET: Portfolio Summary.
`industry.slug` *[array, query]*	Filter companies by their industry.	*[Array]* Industry slug names. See: `"industry":{"slug":"industry_slug_name"}`

`infections`	Filter companies that have certain infections.	*[Array]* Infection names. See the `infections` key in GET: Portfolio Summary.
`open_ports`	Filter companies by open ports.	*[Array]* Service names and port numbers. See: • Detected Services • Typical Services • Potentially Vulnerable **Example:** `'SIP,Port 8081'`
`products`	Filter by companies that use certain service provider products.	*[Array]* Product names. See the `products` field in GET: Portfolio Summary.
`product_types`	Filter by companies that use certain service provider product types.	*[Array]* Product types. See the `product_types` field in GET: Portfolio Summary.
`providers`	Filter companies that rely on certain service providers.	*[String]* The name of the service provider. See the `providers` field in GET: Portfolio Summary.
`rating`	Filter companies by their rating.	*[Integer]* A 10-point incremental number between 250 and 900.
`rating_gt`	Filter companies that have a rating greater than the given value.	*[Integer]* A 10-point incremental number between 250 and 900.
`rating_gte`	Filter companies that have a rating greater than or equal to the given value.	*[Integer]* A 10-point incremental number between 250 and 900.
`rating_lt`	Filter companies that have a rating less than the given value.	*[Integer]* A 10-point incremental number between 250 and 900.
`rating_lte`	Filter companies that have a rating less than or equal to the given value.	*[Integer]* A 10-point incremental number between 250 and 900.
`security_incident_categories`	Filter companies (including their subsidiaries) that have been affected by a Public Disclosures event in the past year.	*[Array]* Public Disclosure risk vector slug names. • `data_breaches` • `other`
`subscription_type.slug`	Filter companies by subscription type.	*[Array]* `countries`

`tier`	Filter companies by their tier.	*[Array]* • Tier unique identifiers [`tier_guid`]. See GET: Tiers. • `null` to include companies that are not in a tier.
`type`	Filter companies by how their rating was curated.	*[String]* • `CURATED` = This report was curated by BitSight. • `SELF_PUBLISHED` = This report was published by this company, as a way to communicate the differences in their services and their associated security ratings. • `PRIVATE` = This report is available only to their own organization. The organization does not appear in searches from other BitSight customers.
`vulnerabilities`	Filter companies that have certain vulnerabilities.	*[Array]* Vulnerability names. See the `vulnerabilities` field in GET: Portfolio Summary.

Example Request

```
curl https://api.bitsighttech.com/ratings/v2/portfolio -u api_token:
```

Example Response


```
{
   "links":{
      "previous":null,
      "next":"null"
   },
   "count":4,
   "summaries":{
      "my-company":"a940bb61-33c4-42c9-9231-c8194c305db3"
   },
   "results":[
      {
         […]
         "guid":"1b3d260c-9e23-4e19-b3a5-a0bcf67d74d9",
         "custom_id":null,
         "name":"Actors Films",
```

```
         "shortname":"Actors Films",
         "network_size_v4":512,
         "rating":750,
         "rating_date":"2020-09-20",
         "added_date":"2018-01-22",
         "industry":{
            "name":"Media/Entertainment",
            "slug":"mediaentertainment"
         },
         "sub_industry":{
            "name":"Motion Pictures and Film",
            "slug":"motion_pictures_and_film"
         },
         "type":[
            "CURATED",
            "PRIVATE"
         ],

"logo":"https://api.bitsighttech.com/ratings/v1/companies/1b3d260c-9e23-4e19
-b3a5-a0bcf67d74d9/logo-image",

"sparkline":"https://api.bitsighttech.com/ratings/v1/companies/1b3d260c-9e23
-4e19-b3a5-a0bcf67d74d9/sparkline?size=small",
         "subscription_type":{
            "name":"Alerts Only",
            "slug":"alerts-only"
         },
         "primary_domain":"actorsfilms.us",

"display_url":"https://service.bitsighttech.com/app/company/1b3d260c-9e23-4e
19-b3a5-a0bcf67d74d9/overview/",
         "tier":"e325bd1d-b5ee-4fa5-a1ee-8e87518b0746",
         "life_cycle":{
            "name":"Onboarding",
            "slug":"onboarding"
         },
         "relationship":{
            "name":"Subsidiary",
            "slug":"subsidiary"
         }
      }
   ]
}
```

Response Attributes

Field	Description
`links` *Object*	Navigation for multiple pages of results. See pagination.
`previous` *String*	The URL to navigate to the previous page of results.
`next` *String*	The URL to navigate to the next page of results.
`count` *Integer*	The number of companies in your portfolio.
`summaries` *Object*	Your My Company.
`my-company` *String* [`company_guid`]	The unique identifier of your My Company.
`results` *Array*	Companies in your portfolio.
`guid` *String* [`company_guid`]	The unique identifier of this company in your portfolio.
`custom_id` *String*	An identifier for this company, as defined by your organization.
`name` *String*	The name of this company.
`shortname` *String*	The abbreviated name of this company.
`network_size_v4` *Integer*	The number of unique IP addresses that belong to this company.
`rating` *Integer*	The current BitSight Security Rating of this company.
`rating_date` *String* [`YYYY-MM-DD`]	The date when this rating was generated.
`added_date` *String* [`YYYY-MM-DD`]	The date when this company was added to the portfolio.
`industry` *Object*	The industry of this company.

`name` *String*	The name of this industry.
`slug` *String*	The slug name of this industry.
`sub_industry` *Object*	The sub-industry of this company.
`name` *String*	The name of this sub-industry.
`slug` *String*	The slug name of this sub-industry.
`type` *Array*	How this company's rating was curated.
`logo` *String*	The URL where this company's logo image file is stored in the BitSight platform.
`sparkline` *String*	The URL path to the 1-year trend line of this company's ratings.
`subscription_type` *Object*	The subscription used by your organization to subscribe to this company.
`name` *String*	The name of this subscription type.
`slug` *String*	The slug name of this subscription type.
`primary_domain` *String*	The main domain that belongs to this company.
`display_url` *String*	The URL path to this company's overview page in the BitSight platform.
`tier` *String* [`tier_guid`]	The unique identifier of this company's tier.
`life_cycle` *Object*	Not applicable to National Cybersecurity.
`name` *String*	The name of this Life Cycle stage.
`slug` *String*	The slug name of this Life Cycle stage.

`relationship` *String*		Not applicable to National Cybersecurity.
	`name` *String*	The name of this company relationship.
	`slug` *String*	The slug name of this company relationship.

GET: Portfolio Summary

`https://api.bitsighttech.com/ratings/v2/portfolio/summaries`

Get a summary of your portfolio. This can be used to get a list of the possible values for querying GET: Portfolio Details.

Parameters

See query parameters for details on the `fields` (default: all fields) parameter.

Parameter	Description	Values
`folder`	Include only companies in the given folder.	*[String]* Folder unique identifier [`folder_guid`]. See GET: Folder Details.
`tier`	Include only companies in the given tier.	*[String]* Tier unique identifier [`tier_guid`]. See GET: Tiers.

Example Request

```
curl https://api.bitsighttech.com/ratings/v2/portfolio/summaries -u
api_token:
```

Example Response


```
{
   "subscription_types":[
      "continuous_monitoring"
   ],
   "industries":[
      "Technology"
   ],
   "types":[
      "CURATED"
   ],
   "countries":[
      "US"
   ],
   "infections":[
      "GigaClicks"
   ],
```

```
   "vulnerabilities":[
      "CVE-2016-10712",
      "Ticketbleed"
   ],
   "open_ports":[
      "AMQP",
      "Port 1010"
   ],
   "software":[
      "WordPress"
   ],
   "providers":[
      "Black Hills Technologies"
   ],
   "products":[
      "Black Hills POS"
   ],
   "product_types":[
      "Order Management"
   ]
}
```

Response Attributes

Field	Description
`subscription_types` *Array*	Available subscription types.
`industries` *Array*	The industries of companies in your portfolio.
`types` *Array*	How the rating of companies in your portfolio were curated.
`countries` *Array*	The locations of companies in your portfolio.
`infections` *Array*	Infections that are present in your portfolio.
`vulnerabilities` *Array*	Vulnerabilities that are present in your portfolio.
`open_ports` *Array*	Ports that are open in your portfolio.
`software` *Array*	Software programs used in your portfolio.
`providers` *Array*	Service providers that companies in your portfolio rely on.
`products` *Array*	Service provider products used in your portfolio.
`product_types` *Array*	The types of service provider products used in your portfolio.

GET: Geographic IP Address Space

https://api.bitsighttech.com/ratings/v1/portfolio/countries

Get an understanding of the geographic IP address space of your portfolio. This can be used to determine which vendors need to comply with data residency requirements.

Example Request

```
curl https://api.bitsighttech.com/ratings/v1/portfolio/countries -u
api_token:
```

Example Response

```
{
  "companies": {
      "a940bb61-33c4-42c9-9231-c8194c305db3":{
         "ipv4":{
[…]
            "A1":1
         }
      },
   "initial_counts":{
[…]
      "Demo Country 1":1
   },
   "countries":{
      "A1":{
         "name":"Demo Country 1"
      }
}
```

Response Attributes

The data is returned as a dictionary (field/value pairs).

Field	Description
`companies` *Object*	IPv4 details of companies in your portfolio.
GUID *String* [`company_guid`]	The unique identifier of this company.
`ipv4` *Object*	IPv4 totals by country code.
2-letter Country Code *Integer*	The total number of IP addresses this company has in that country.
`initial_counts` *Object*	The number of this country's IP addresses.
Country Name *Integer*	The number of IP addresses in this country of companies in your portfolio.
`countries` *Object*	Country details of your portfolio.
2-letter Country Code *Object*	Details of this country.
`name` *String*	The name of this country.

GET: Portfolio Filters

https://api.bitsighttech.com/ratings/v1/portfolio/filters

This is a powerful system that returns infections, open ports, and vulnerabilities affecting each company in your portfolio, as well as statistics for all infections and vulnerabilities present.

This API does not currently have the capability to return companies that are affected by a specific botnet or vulnerability.

Example Request (No Parameters - Default)

This will return all data: vulnerabilities, botnets, and open ports affecting your portfolio.

```
curl https://api.bitsighttech.com/ratings/v1/portfolio/filters -u api_token:
```

Example Request 2

Botnet Infections information for a single folder:

```
curl
https://api.bitsighttech.com/ratings/v1/portfolio/filters?fields=infections&
folder=folder_guid -u api_token:
```

Example Request 3

To get open ports and vulnerabilities (but not infections) for all companies in the portfolio:

```
curl
https://api.bitsighttech.com/ratings/v1/portfolio/filters?fields=vulnerabili
ties,open_ports -u api_token:
```

Parameters

Combine query parameters with the `/portfolio/filter` path to return some or all data:

Parameter	Description	Values
`fields`	Include specific organization fields.	*[String]* Comma-delimited: • `vulnerabilities` • `open_ports` • `botlist`
`folder`	Show only companies in the specified folder.	*[String]* Folder unique identifier [`folder_guid`]. See GET: Folder Details.
`format`	Format of response data.	*[String]*
`quarters_back`	Get ratings from the last day of the quarter, set back by a selected number of quarters from today.	*[Integer]* # = Number of Quarters
`rating_date`	The most recent rating date.	*[String]* `YYYY-MM-DD`
`show_event_evidence`	Filter companies with enhanced event evidence.	*[Boolean]* `true` = Show only organizations that have enhanced event evidence enabled.
`show_ips`	Filter organizations with visible IP addresses.	*[Boolean]* `true` = Show only organizations with visible IP addresses.

Example Response


```
{
  "data": {
    "vulnerabilities": {
      "06111982-d568-42c7-ad87-d2075e1c494a": ["Logjam", "POODLE"],
      "3c87e467-7474-42da-8369-c4c2573851d8": ["Logjam", "POODLE"]
    },
    "botlist": {
      "06111982-d568-42c7-ad87-d2075e1c494a": ["Conficker", "Zeus", "Zusy",
],
      "12345678-c3b0-a2d2-bb80-d5df44c3a2e5": ["Conficker", "Genieo",
"RevMob", "SniperSpy"],
    },
    "open_ports": {
      "06111982-d568-42c7-ad87-d2075e1c494a": ["NetBIOS", "HTTP", "AMQP",
"XMPP"],
      "12345678-c3b0-a2d2-bb80-d5df44c3a2e5": ["HTTP", "HTTPS"],
```

```
    }
  },
  "initial_counts": {
    "vulnerabilities": {
      "Logjam": 2,
      "POODLE": 2
    },
    "botlist": {
      "Conficker": 2,
      "Zeus": 1,
      "Zusy": 1,
      "Genieo": 1,
      "RevMob": 1,
      "SniperSpy": 1
    },
    "open_ports": {
      "HTTP": 2,
      "HTTPS": 1,
      "NetBIOS": 1,
      "AMQP": 1,
      "XMPP": 1
    }
  }
}
```


Response Attributes

Field	Description
`data` *Object*	Top-level object for information about organizations in your portfolio.
`vulnerabilities` *Object*	Organizations with Patching Cadence vulnerabilities.
GUID *Array*	A list of the Patching Cadence vulnerabilities in this organization (GUID). **Example:** `["Logjam", "DROWN", "POODLE"]`
`botlist` *Object*	Organizations with Botnet Infections.
GUID *Array*	A list of the Botnet Infections in this organization (GUID). **Example:**

	`["ZeroAccess", "Genieo", "Conficker", "Bedep", "Gozi"]`
`open_ports` *Object*	Organizations with open ports.
GUID *Array*	A list of the open ports in this organization. **Example:** `["HTTP", "MS RDP", "SMTP with STARTTLS", "HTTPS"]`
`initial_counts` *Object*	Statistical information about vulnerabilities, Botnet Infections, and Open Ports across your portfolio.
`vulnerabilities` *Object*	A list of the type and number of Patching Cadence vulnerabilities across your portfolio.
Vulnerability Name *Integer*	The name of the vulnerability (string) and the number of organizations in your portfolio that are affected by it (integer). **Example:** `"Logjam": 1995,`
`botlist` *Object*	A list of the type and number of Botnet Infections across your portfolio.
Botnet Name *Integer*	The name of the botnet (string) and the number of organizations in your portfolio that are affected by it (integer). **Example:** "Port Scanner": 282,
`open_ports` *Object*	A list of the type and number of Open Ports across your portfolio.
Open Port Name *Integer*	The name of the open port (string) and the number of organizations in your portfolio that have the port open. **Example:** `"Distributed Hash Table": 135,`

GET: Portfolio Unique Identifiers

https://api.bitsighttech.com/ratings/v1/portfolio/guids

Returns a simple list of company or country unique identifiers in your portfolio.

Example Response

```
[
  "06111982-d568-42c7-ad87-d2075e1c494a",
  "12345678-c3b0-a2d2-bb80-d5df44c3a2e5"
]
```

Example Request

```
curl https://api.bitsighttech.com/ratings/v1/portfolio/guids -u api_token:
```

Response Attributes

The server returns an array of country unique identifier text strings [`country_guid`].

GET, POST: Security Rating Details of Countries in Your Portfolio

https://api.bitsighttech.com/ratings/v1/portfolio/ratings

Get security rating details of the countries in your portfolio, including the unique identifiers of particular countries.

Parameters

Parameter	Description	Values
`expand`	Show the letter grades of each risk vector. This parameter might result in a large amount of data. See error 413 for details.	*[String]* `rating_details`
`period`	Specify a time interval to filter the ratings data.	*[String]* • `daily` • `monthly` • `latest` **Example:** `?period=monthly`
`start_date`	Filter the ratings data by starting date.	*[String]* `YYYY-MM-DD`
`end_date`	Filter the ratings data by the end date.	*[String]* `YYYY-MM-DD`

Example GET Request

Use a GET request to retrieve data for your entire portfolio.

```
curl -X GET
'https://api.bitsighttech.com/ratings/v1/portfolio/ratings?expand=rating_det
ails&start_date=YYYY-MM-DD&end_date=YYYY-MM-DD&period=time_interval' -u
api_token:
```

Example POST Request

Use a POST to customize the JSON body for the request, i.e. select a subset of countries instead of your entire portfolio.

```
curl -X POST
https://api_token@service.bitsighttech.com/ratings/v1/portfolio/ratings -d
'{"companies":["country_a_guid","country_b_guid"],"start_date":"YYYY-MM-DD",
"end_date":"YYYY-MM-DD","expand":"rating_details","period":"time_interval'
```

Example Response


```
[
   {
      "ratings":[
         {
            "date":"2019-10-19",
            "rating":600,
            "percentile":20
         }
      ],
      "guid":"5d04c480-b1e7-48af-9633-82996a8446fc",
      "name":"Demo Country 1"
   }
]
```

Response Attributes

The following table describes the attributes of a country's rating details object.

Field	Description
`ratings` *Array*	A list of objects containing security rating details of a country.
`date` *String* [`YYYY-MM-DD`]	The date when this rating details object was retrieved.
`rating` *Integer*	The headline security rating of this country on the specified date.
`percentile` *Integer*	
`guid` *String* [`country_guid`]	The unique identifier of this country.
`name` *String*	The name of this country.

Errors and Status Codes

Code	Description
413	The amount of data being computed is too high. We recommend making the response smaller either by setting the period parameter value to latest (?period=latest) or by not including the expand parameter.

GET: National Cybersecurity Network Resources

https://api.bitsighttech.com/sovereign/network-resources/ips/ip_address

Determine if a specific IP address belongs to the address space of one of your subscribed countries.

Parameters

*Required.

Parameter	Description	Values
`ip_address`* *Path*	Identify the IP address to query.	*[String]* IP address.

Example Request

```
curl
'https://api.bitsighttech.com/sovereign/network-resources/ips/12.345.67.890'
-u api_token:
```

Response Codes

Code	Description
`200 - OK`	The address belongs to your subscribed country.
`403 - Unauthorized`	The address does not belong to any of your subscribed countries.

GET: National Cybersecurity Observations

`https://api.bitsighttech.com/sovereign/observations`

Use this endpoint to retrieve 1,000 of the most recent observations within your primary country.

Parameters

See query parameters for details on the `cursor` parameter.

Scope Filtering

Parameter	Description	Values
`country_codes`	Filter by multiple countries.	*[Array]* Comma-separated 2-letter country codes.
Date	Filter by dates. To get historical data between two dates, ensure the `history` parameter is set to `true` (`history=true`).	
`end_date`	Filter by end date.	*[String]* `YYYY-MM-DD`
`start_date`	Filter by start date.	*[String]* `YYYY-MM-DD`
`date_interval`	Filter by date interval.	*[String]* • `7d` (Default) • `30d`
`industries`	Filter by multiple industries.	*[Array]* Comma-separated industry names. See the `industries` field in GET: Portfolio Summary.
`industry`	Filter by industry.	*[String]* Industry name. See the `industries` field in GET: Portfolio Summary.
`ip`	Filter by IP address.	*[String]*

	Not all observations will necessarily be associated with an IP address.	• IPv4 Address (Dotted Notation) • IPv6 Address
`ips`	Filter by multiple IP addresses.	*[Array]* Comma-separated IP addresses. • IPv4 Address (Dotted Notation) • IPv6 Address
`limit`	Set the maximum number of results.	*[Integer]* A number greater than `0` (zero). **Default:** `1000`

Data Filtering

Parameter	Description	Values
`categories`	Filter by file sharing category (User Behavior).	*[Array]* Comma-separated File Sharing category names.
`infections`	Filter by infections.	*[Array]* Comma-separated infection names. See `infections` in GET: National Cybersecurity Observation Details by Risk Type.
`open_ports`	Filter by network services.	*[Array]* Comma-separated port numbers or service names. See `service` in GET: National Cybersecurity Observation Details by Risk Type. This is case-sensitive.
`risk_types`	Filter by risk types.	*[Array]* Comma-separated risk type slug names. See risk types.
`vulnerabilities`	Filter by vulnerabilities.	*[String]* Comma-separated vulnerability names or CVE ID. See `vulnerability` details in GET: National Cybersecurity Observation Details by Risk Type.
`vulnerability_classification`	Filter by vulnerability confidence level.	*[String]* • `Potential` = Low confidence/potential vulnerabilities.

	Only applicable with the `vulnerabilities` parameter.	• `Confirmed` = High confidence or confirmed vulnerabilities. • `All` (Default) = All vulnerabilities, regardless of confidence level.

Example Request

```
curl 'https://api.bitsighttech.com/sovereign/observations' -u api_token:
```

Example Response


```
{
    "has_more_observations": true,
    "links": {
        "next":
"https://api.bitsighttech.com/sovereign/observations/?cursor=TkVYVCwxNjEwMjM
2ODAwMDAwLDE2MTAzMTk3NzgwMDAsQUFBQUZYV0p0bkhsR0NxQkFBQUFBQmRqTnRKUWFIQkdhVzV
uWlhKd2NtbHVkRFV1TlM0ek9BPT0%3D"
    },
    "included_observations": 1000,
    "observations": [
        {
            "risk_type": "insecure_systems",
            "observation_id":
"AAAAFD5oh6zNVnIYAAAAABerK6tUb3JyZW50VHJhY2tlcjp0b3JyZW50X3RyYWNrZXJfZXhwaXJ
lZA==",
            "collection_date": "2021-06-26",
            "event_date": "2021-06-26",
            "occurrences": {
                "event_date": "2021-06-26",
                "representative_timestamp": "2021-06-26 23:54:56",
                "last_seen": "2021-06-26 23:54:56",
                "first_seen": "2021-06-26 00:18:11",
                "count": 108
            },
            "forensics": {
                "host_ip": "83.38.12.221"
                "host_port": 8443
            },
            "country": {
                "name": "Valencia (Spain)",
                "code": "ES-VC"
            },
            "entities": [
                {
                    "name": "Anon Telecomm, Inc.",
                    "guid": "12345678-abcd-efgh-1234-abcdefghijkl",
```

```
                    "industry_sector": "Telecommunications",
                    "in_portfolio": false,
                    "has_parent": true,
                    "is_service_provider": true,
                    "sub_industry": "Telecommunications"
                }
            ],
            "details": {
            ⊕ See Details by Risk Type
            }
        }
    ],
    "cursors": {
        "next":
"TkVYVCwxNjEwMjM2ODAwMDAwLDE2MTAzMTk3NzgwMDAsQUFBQUZYV0p0bkhsR0NxQkFBQUFBQmR
qTnRKUWFIQkdhVzVuWlhKd2NtbHVkRFV1TlM0ek9BPT0="
    },
    "scope": {
        "date_interval": "7d",
        "type": "country",
        "end_date": "2021-01-10",
        "value": "US"
    }
}
```


Response Attributes

Field	Description
`scope` *Object*	Details of this request.
`type` *String*	For internal BitSight use.
`value` *String*	The two-letter country code.
`date_interval` *String*	The date interval in the number of days.
`end_date` *String* [`YYYY-MM-DD`]	The end date of the date interval.
`included_observations` *Integer*	The number of observations included in the results.
`has_more_observations` *Boolean*	A true value indicates additional observations are available.

`cursors` *Object*	Navigation for multiple pages of results. See pagination.
`next` *String*	The URL to navigate to the next page of results.
`observations` *Array*	Observation details.
Object	A unique observation.
`risk_type` *String*	The slug name of the associated risk vector.
`observation_id` *String*	An identifier for this observation.
`collection_date` *String* [`YYYY-MM-DD`]	The date when findings were observed.
`event_date` *String* [`YYYY-MM-DD`]	The date when the observations rolled up into a finding.
`occurrences` *Object*	Unique occurrences.
`event_date` *String* [`YYYY-MM-DD`]	The date of this occurrence.
`representative_timestamp` *String* [`YYYY-MM-DD HH:MM:SS`]	The date and time of this occurrence.
`last_seen` *String* [`YYYY-MM-DD HH:MM:SS`]	The most recent date and time when this observation occurred.
`first_seen` *String* [`YYYY-MM-DD HH:MM:SS`]	The first date and time when this observation occurred.
`count` *Integer*	The total count of this unique occurrence.
`forensics` *Object*	Forensic details.
`host_ip` *String*	The host IP address.
`host_port` *Integer*	The host port number.
`country`	The country of origin.

Object	
`name` *String*	The name of this country.
`code` *String*	The country code.
`entities` *Array*	Companies in the BitSight inventory.
Object	A company.
`name` *String*	The name of this company.
`guid` *String* [`company_guid`]	The unique identifier of this company.
`industry_sector` *String*	The industry of this company.
`in_portfolio` *Boolean*	A `true` value indicates this company is in your portfolio.
`has_parent` *Boolean*	A `true` value indicates this company is a child subsidiary of another company within the organization.
`is_service_provider` *Boolean*	A `true` value indicates this company is a service provider.
`sub_industry` *String*	The sub-industry of this company.
`details` *Object*	Observation details. The details vary, depending on the risk type [`risk_type`].
`links` *Object*	Navigation for multiple pages of results. See pagination.
`next` *String*	The URL to navigate to the next page of results.

GET: National Cybersecurity Observation Details by Risk Type

`https://api.bitsighttech.com/sovereign/observations`

The observations field that's included with GET: National Cybersecurity Observations (`/sovereign/observations`) shows the details of observations. The details vary, depending on the risk type [`risk_type`].

- Botnet Infections
- Spam Propagation
- Malware Servers
- Potentially Exploited
- TLS/SSL Certificates
- TLS/SSL Configurations
- Open Ports
- Web Application Headers
- Insecure Systems
- Server Software
- File Sharing
- Vulnerability

All other risk types are not compatible with this endpoint.

Botnet Infections

Slug Name: `botnet_infections`

Example Response


```
"infection": "RootSTV",
 "infection_id": 123,
 "source_port": 54264,
 "dest_port": 80,
 "cc_ip": "XXX.4.56.78",
 "detection_method": "Sinkhole",
 "request_method": "POST"
```

Response Attributes

Field	Description
`infection` *String*	The name of the infection.
`infection_id` *Integer*	An identifier for the infection.
`source_port` *Integer*	The source port number.
`dest_port` *Integer*	The destination port number.
`cc_ip` *String*	The IP address of the malware's command and control server (C&C or C2 Server).
`detection_method` *String*	The method used to detect this observation.
`request_method` *String*	The method used to communicate with the malware.

⇧ Back to Directory

Spam Propagation

Slug Name: `spam_propagation`

Example Response

```
"email_from_address": "<richard.kuga@saperix.com>",
 "email_sender_address": "<richard.kuga@saperix.com>",
 "email_subject": "Payment from your account.",
 "detection_method": "spam-trap",
 "infection": "Spam Bot"
```

Response Attributes

Field	Description
`email_from_address` *String*	The "From" email address.
`email_sender_address` *String*	The "From" email address.

`email_subject` *String*	The Subject of the email.
`detection_method` *String*	The method used to detect this observation.
`infection` *String*	The infection type.

⇧ Back to Directory

Malware Servers

Slug Name: `malware_servers`

Example Response

```
                "type": "Malware"
```

Response Attributes

Field	Description
`type` *String*	**Values:** • `Malicious` • `Malware`

⇧ Back to Directory

Potentially Exploited

Slug Name: `potentially_exploited`

Example Response

```
                "infection": "AMCleaner",
                 "infection_id": 123,
                 "source_port": 59186,
                 "dest_port": 80,
                 "cc_ip": "XXX.45.67.89",
                 "request_method": "GET",
                 "user_agent": "msphlpr/1.9 CFNetwork/811.11 Darwin/16.7.0
(x86_64)"
```

Response Attributes

Field	Description
`infection` *String*	The name of the potentially unwanted application (PUA) or potentially unwanted program (PUP).
`infection_id` *Integer*	An identifier for the infection.
`source_port` *Integer*	The source port number.
`dest_port` *Integer*	The destination port number.
`cc_ip` *String*	The IP address of the malware's command and control server (C&C or C2 Server).
`detection_method` *String*	The method used to detect this observation.
`request_method` *String*	The method used to communicate with the malware.

⇧ Back to Directory

TLS/SSL Certificates

Slug Name: `ssl_certificates`

Example Response


```
                "grade": {
                     "grade": "GOOD"
                 },
                 "cert_chain": [
                     {
                         "startDate": "2016-11-10",
                         "endDate": "2041-11-11",
                         "issuerName": "C=US,O=DigiCert
Inc,OU=www.digicert.com,CN=DigiCert High Assurance EV Root CA",
                         "startsubjectName": "C=US,O=DigiCert
Inc,OU=www.digicert.com,CN=DigiCert High Assurance EV Root CA",
                         "startkeyAlgorithm": "RSA",
                         "startsignatureAlgorithm": "SHA1WITHRSA",
                         "keyLength": 2048,
                         "serialNumber":
"111222333444555111222333444555123456 7",
                         "dnsName": [
                             "*.example.com"
                         ]
                     }
                 ],
                 "observed_ips": [
                     "123.123.12.12",
                     "98.7.65.432"
                 ]
```


Response Attributes

Field	Description
`grade` *Object*	Finding grade details.
`grade` *String*	The finding grade.
`cert_chain` *Array*	Certificate chain details.
Object	The details of a certificate in the chain.
`startDate`	The date when this certificate started.

String [YYYY-MM-DD]	
endDate *String* [YYYY-MM-DD]	The expiration date of this certificate.
issuerName *String*	The distinguished name of the certificate issuer, made up of attribute assertion values.
startsubjectNam *String*	The distinguished name of the owner of the certificate, made up of attribute assertion values.
startkeyAlgorithm *String*	The algorithm used to encrypt and decrypt messages.
startsignatureAlgorithm *String*	The signing algorithm used in this certificate.
keyLength *Integer*	The bit strength of this key.
serialNumber *Integer*	The serial number of the certificate within this chain.
dnsName *Array*	The name of the Domain Name Server (DNS).
observed_ips *Array*	Observed IP addresses.

⇧ Back to Directory

TLS/SSL Configurations

Slug Name: ssl_configuration

Example Response


```
                "message": [
                     "Allows insecure protocol: TLSv1.0",
                     "Allows insecure protocol: TLSv1.1"
                 ],
                 "grade": {
                     "grade": "BAD"
                 },
                 "dh_length": 2048,
                 "dh_prime": "ffffffffffffffffc90fdaa2{464
digits}8aacaa68ffffffffffffffff",
                 "observed_ips": [
                     "123.456.789.000"
                 ]
```

Response Attributes

Field	Description
`message` *Array*	A description of the finding.
`grade` *Object*	Finding grade details.
`grade` *String*	The finding grade.
`dh_length` *Integer*	The configured key length.
`dh_prime` *String*	The Diffie-Hellman prime.
`observed_ips` *Array*	Observed IP addresses.

⇧ Back to Directory

Open Ports

Slug Name: `open_ports`

Example Response


```
               "grade": {
                    "grade": "GOOD"
                },
                "response": "HTTP/1.1 403 Forbidden\r\nDate: Sun, 27 Jun
2021 23:41:08 GMT\r\nServer: Apache/2.4.7 (Ubuntu)\r\nContent-Length:
280\r\nContent-Type: text/html; charset=iso-8859-1",
                "service": "HTTPS",
                "message": [
                    "Detected service: HTTPS"
                ],
                "low_vulnerabilities": [
                    "CVE-2017-7679",
                    "CVE-2016-8743"
                ]
```

Response Attributes

Field	Description
`grade` *Object*	Finding grade details.
Object	A finding grade.
`grade` *String*	The finding grade.
`response` *String*	The response code that indicates if the server was able to process the request sent by the client.
`service` *String*	The service that's running on this port.
`message` *Array*	The type of service running on this port.
`low_vulnerabilities` *Array*	Potential vulnerabilities for this finding, identified by its Common Vulnerabilities and Exposures ID (CVE ID).
`high_vulnerabilities` *Array*	Confirmed vulnerabilities for this finding, identified by its Common Vulnerabilities and Exposures ID (CVE ID).

⇧ Back to Directory

Web Application Headers

Slug Name: `application_security`

Example Response


```
"message": [
     "hh_moved"
 ],
 "grade": {
     "grade": "NEUTRAL"
 },
 "headers": [
     "HTTP/1.1 301 Moved Permanently",
     "Date: Sun, 27 Jun 2021 21:43:21 GMT",
     "Server: Apache",
     "Cache-Control: no-cache",
     "Location: https://www.saperix.com",
     "X-Powered-By: Apache2",
     "MS-Author-Via: DAV",
     "Vary: Accept-Encoding",
```

```
                    "Content-Length: 0",
                    "Content-Type: text/html; charset=utf-8"
                ],
                "http_issues": {
                    "general_issues": [
                        "hh_moved"
                    ]
                }
```


Response Attributes

Field	Description
`message` *Array*	Descriptions of the finding.
`grade` *Object*	Finding grade details.
`grade` *String*	The finding grade.
`headers` *Array*	Web application headers.
`http_issues` *Object*	HTTP issue details.
`general_issues` *Array*	General HTTP issues.

⇧ Back to Directory

Insecure Systems

Slug Name: `insecure_systems`

Example Response


```
                "grade": {
                     "grade": "WARN"
                 },
                 "message": [
                     "File sharing: Tracker"
                 ],
                 "category": "TorrentTracker",
                 "sub_category": "torrent_tracker_expired",
                 "source_port": "58107",
                "path_info": "/announce.php",
                 "user_agent": "uTorrent/355(111915940)(45988)"
```


Response Attributes

Field	Description
`grade` *Object*	Finding grade details.
`grade` *String*	The finding grade.
`message` *Array*	A description of the finding.
`category` *String*	
`sub_category` *String*	
`source_port` *Integer*	The source port number.
`path_info` *String*	The file path information.
`user_agent` *String*	The user's form of communication with the malware.

⇧ Back to Directory

Server Software

Slug Name: `server_software`

Example Responses

Apache


```
                "grade": {
                    "grade": "NEUTRAL"
                },
                "typeColumnText": "Apache",
                "detailsColumnText": "Software version is incomplete",
                "modalData": {
                    "type": "incomplete-version"
                },
                "modalTags": {
                    "Type": "Apache",
                    "OS family": "Unknown",
                    "Upstream version": "",
                    "HTTP Server header": "Apache"
                }
```


NGINX


```
                "grade": {
                    "grade": "NEUTRAL"
                },
                "typeColumnText": "nginx",
                "versionColumnText": "1.12.1",
                "detailsColumnText": "OS-specific software version is
unknown",
                "modalData": {
                    "type": "possible-backports"
                },
                "modalTags": {
                    "Type": "nginx",
                    "Version": "1.12.1"
```


OpenSSH


```
                "grade": {
                    "grade": "BAD"
                },
                "typeColumnText": "OpenSSH",
                "versionColumnText": "7.2p2",
                "detailsColumnText": "OS-specific software version is
```

```
unsupported",
                "modalData": {
                    "name": "openssh-server",
                    "osRelease": {
                        "name": "Ubuntu 16.04 LTS",
                        "familyName": "Ubuntu",
                        "version": "16.04 LTS",
                        "url":
"https://wiki.ubuntu.com/XenialXerus/ReleaseNotes"
                    },
                    "obsoletedOn": "2018-01-22",
                    "version": "1:7.2p2-4ubuntu2.2",
                    "latestPackageVersion": "1:7.2p2-4ubuntu2.8",
                    "type": "obsolete-package"
                },
                "modalTags": {
                    "Type": "OpenSSH",
                    "Banner": "SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.2",
                    "Upstream version": "7.2p2"
                }
```


PHP


```
               "grade": {
                    "grade": "NEUTRAL"
                },
                "typeColumnText": "PHP",
                "versionColumnText": "7.1.18",
                "detailsColumnText": "Support status is unknown",
                "modalData": {
                    "type": "unknown"
                },
                "modalTags": {
                    "Type": "PHP",
                    "Upstream version": "7.1.18",
                    "HTTP Server header": "Apache/2.4.6 (CentOS)
OpenSSL/1.0.2k-fips PHP/7.1.18",
                    "HTTP X-Powered-By header": "PHP/7.1.18"
```

Response Attributes

Field	Description
`grade` *Object*	Finding grade details.
`grade` *String*	The finding grade.
`typeColumnText` *String*	The type of server software package.
`versionColumnText` *String*	The software version.
`detailsColumnText` *String*	Software support details.
`modalData` *Object*	Software type details.
`name` *String*	The name of the server.
`osRelease` *Object*	Released OS details.
`name` *String*	The full name of the server type.
`familyName` *String*	The server type.
`version` *String*	The latest software version.
`url` *String*	The release notes URL.
`obsoletedOn` *String* [`YYYY-MM-DD`]	The date when the software became obsolete.
`version` *String*	The current software version.
`latestPackageVersion` *String*	The latest package version.

	`type` *String*	The software status.
`modalTags` *Object*		Server software details.
	`Type` *String*	The type of server software package.
	`Banner` *String*	The software and package name.
	`OS family` *String*	The operating system family.
	`Upstream version` *String*	The upstream software version.
	`HTTP Server header` *String*	The HTTP server header.
	`HTTP X-Powered-By header` *String*	The HTTP X-Powered-By header.
	`Version` *String*	The software version.

⇧ Back to Directory

File Sharing

Slug Name: `file_sharing`

Example Response

```
                "category": "Movies",
                 "node": "88.88.88.888"
```

Response Attributes

Field	Description
`category` *String*	The BitSight category for the type of torrent. See File Sharing categories.
`node` *String*	The IP address of the endpoint device.

⇧ Back to Directory

Vulnerability

Slug Name: `vulnerability`

Example Response

```
"vulnerabilities": [
     "CVE-2019-17059"
 ],
 "status": "vulnerable",
 "annotation": [],
 "high_vulnerabilities": [
     "CVE-2019-17059"
 ]
```

Response Attributes

Field	Description
`vulnerabilities` *Array*	Confirmed vulnerabilities for this finding, identified by its Common Vulnerabilities and Exposures ID (CVE ID).
`status` *String*	The status of the vulnerability.
`annotation` *Array*	
`high_vulnerabilities` *Array*	Confirmed vulnerabilities for this finding, identified by its Common Vulnerabilities and Exposures ID (CVE ID).

⇧ Back to Directory

GET: National Cybersecurity Companies KPI

`https://api.bitsighttech.com/sovereign/observations/companies/kpis/`

See observation distinct company counts for each supported filter.

Parameters

Scope Filtering

If no scope is set, your country is used as scope. An IP or a country-industry can be alternatively used, but not both (country & IP or country & country-industry) simultaneously.

Parameter	Description	Values
`country_codes`	Filter by multiple countries.	*[Array]* Comma-separated 2-letter country codes.
Date	Filter by dates. To get historical data between two dates, ensure the `history` parameter is set to `true` (`history=true`).	
`end_date`	Filter by end date.	*[String]* `YYYY-MM-DD`
`start_date`	Filter by start date.	*[String]* `industries`
`date_interval`	Filter by date interval.	*[String]* • `7d` (Default) • `30d`
`industries`	Filter by multiple industries.	*[Array]* Comma-separated industry names. See the `industries` field in GET: Portfolio Summary.
`ips`	Filter by multiple IPV4 or IPV6 addresses.	*[Array]* Comma-separated IP addresses. • IPv4 Address (Dotted Notation)

		• IPv6 Address
`limit`	Set the maximum number of results.	*[Integer]* A number greater than `0` (zero).

Data Filtering

Parameter	Description	Values
`categories`	Filter by file sharing category (User Behavior).	*[Array]* Comma-separated File Sharing category names.
`infections`	Filter by infections.	*[Array]* Comma-separated infection names. See `infections` in GET: National Cybersecurity Observation Details by Risk Type.
`open_ports`	Filter by network services.	*[Array]* Comma-separated port numbers or service names. See `service` in GET: National Cybersecurity Observation Details by Risk Type. This is case-sensitive.
`risk_types`	Filter by risk types.	*[Array]* Comma-separated risk type slug names. See risk types.
`vulnerabilities`	Filter by vulnerabilities.	*[String]* Comma-separated vulnerability names or CVE ID. See `vulnerability` details in GET: National Cybersecurity Observation Details by Risk Type.
`vulnerability_classification`	Filter by vulnerability confidence level. Only applicable with the `vulnerabilities` parameter.	*[String]* • `Potential` = Low confidence/potential vulnerabilities. • `Confirmed` = High confidence or confirmed vulnerabilities. • `All` (Default) = All vulnerabilities, regardless of confidence level.

Example Request

```
curl 'https://api.bitsighttech.com/sovereign/observations/companies/kpis/'
-u api_token:
```

Example Response


```
{
   "scope":{
      "type":"country",
      "value":"A1",
      "date_interval":"7d",
      "end_date":"2021-10-20"
   },
   "included_companies":3,
   "total_companies":3,
   "companies":[
      {
         "company":{
            "name":"Saperix, Inc.",
            "guid":"a940bb61-33c4-42c9-9231-c8194c305db3",
            "industry_sector":"Telecommunications",
            "in_portfolio":false,
            "sub_industry":"Telecommunications"
         },
         "count":12345
      }
   ]
}
```


Response Attributes

Field	Description
`scope` *Object*	Company KPI details of the requested country.
`type` *String*	For internal BitSight use.
`value` *String*	The 2-letter country code of the requested country.
`date_interval` *String*	The date interval.
`end_date` *String* [`YYYY-MM-DD`]	The ending date of the interval.
`included_companies` *Integer*	The number of queried companies.

`total_companies` *Integer*	The total number of companies in the country.
`companies` *Array*	Company KPI details.
Object	A company.
`company` *Object*	Details of this company.
`name` *String*	The name of this company.
`guid` *String* [`company_guid`]	The unique identifier of this company.
`industry_sector` *String*	The industry of this company.
`in_portfolio` *Boolean*	A `true` value indicates you are subscribed to this company and it's in your portfolio.
`sub_industry` *String*	The sub-industry of this company.
`count` *Integer*	The total number of results.

GET: National Cybersecurity Observation Counts

`https://api.bitsighttech.com/sovereign/observations/counts`

Retrieve the total count of all observed findings throughout all risk vectors that were observed in companies attributed to a country.

This includes observation details on the following data sets:

- Infections
- Open Ports
- User Behavior
- Compromised Systems
- Diligence
- File Sharing
- Vulnerabilities

Sections:

Parameters

Scope Filtering

Parameter	Description	Values
`country_code`	Filter by country.	*[String]* 2-letter country code.
`country_codes`	Filter by multiple country codes.	*[Array]* Comma-separated 2-letter country codes.
Date	Filter by dates. To get historical data between two dates, ensure the `history` parameter is set to `true` (`history=true`).	

`end_date`	Filter by end date.	*[String]* `YYYY-MM-DD`
`start_date`	Filter by start date.	*[String]* `YYYY-MM-DD`
`history`	Allow the retrieval of historical data between two dates (`start_date` & `end_date`).	*[Boolean]* `true` = Allow date parameters.
`date_interval`	Filter by date interval.	*[String]* • `7d` (Default) • `30d`
`industries`	Filter by multiple industries.	*[String]* Comma-separated industry names. See the `industries` field in GET: Portfolio Summary.
`industry`	Filter by industry.	*[String]* Comma-separated industry name. See the `industries` field in GET: Portfolio Summary.
`ip`	Filter by IPV4 or IPV6 address.	*[String]* • IPv4 Address (Dotted Notation) • IPv6 Address
`ips`	Filter by multiple IPV4 or IPV6 addresses.	*[Array]* Comma-separated IP addresses. • IPv4 Address (Dotted Notation) • IPv6 Address
`period`	Filter by time period.	*[String]* • `daily` (Default) • `monthly`

Output Options

Parameter	Description	Values
`normalize_counts`	Normalize based on 100K habitants.	*[Boolean]* `true` = Normalize

Data Filtering

Parameter	Description	Values
`categories`	Filter by file sharing category (User Behavior).	*[Array]* Comma-separated File Sharing category names.
`infections`	Filter by infections.	*[Array]* Comma-separated infection names. See `infections` in GET: National Cybersecurity Observation Details by Risk Type.
`open_ports`	Filter by network services.	*[Array]* Comma-separated port numbers or service names. See `service` in GET: National Cybersecurity Observation Details by Risk Type. This is case-sensitive.
`risk_types`	Filter by risk types.	*[Array]* Comma-separated risk type slug names. See risk types.
`vulnerabilities`	Filter by vulnerabilities.	*[String]* Comma-separated vulnerability names or CVE ID. See `vulnerability` details in GET: National Cybersecurity Observation Details by Risk Type.
`vulnerability_classification`	Filter by vulnerability confidence level. Only applicable with the `vulnerabilities` parameter.	*[String]* • `Potential` = Low confidence/potential vulnerabilities. • `Confirmed` = High confidence or confirmed vulnerabilities. • `All` (Default) = All vulnerabilities, regardless of confidence level.

Aggregating Results

Parameter	Description	Values
`agg`	Contain aggregated values for a particular category. Categories: • `risk_types` • `infections` • `categories` • `vulnerabilities` • `open_ports`	*[String]* **Example:** `open_ports=agg`

Results by Category

Parameter	Description	Values
`all`	Retrieves all values of a particular category. Categories: • `risk_types` • `infections` • `categories` • `vulnerabilities` • `open_ports`	*[String]* **Example:** `risk_types=all` **Default:** All categories.

Example Request

```
curl
'https://api.bitsighttech.com/sovereign/observations/counts?country_code=AA'
-u api_token:
```

Example Response

```
{
    "scope": {
        "date_interval": "7d",
        "type": "country",
        "end_date": "2020-07-09",
        "value": "AA"
    },
    "counts": {
        "infections": [
            […]
            {
                "count": 1,
```

```
            "country_name": "Example Country",
            "name": "Locky",
            "country_code": "AA"
        }
    ],
    "open_ports": [
        […]
        {
            "count": 1,
            "country_name": "Example Country",
            "name": "Port 8112",
            "country_code": "AA"
        }
    ],
    "risk_vectors": {
        "user_behavior": [
            {
                "count": 123,
                "country_name": "Example Country",
                "name": "file_sharing",
                "country_code": "AA"
            }
        ],
        "compromised_systems": [
        […]
            {
                "count": 123,
                "country_name": "Example Country",
                "name": "malware_servers",
                "country_code": "AA"
            }
        ],
        "diligence": [
        […]
            {
                "count": 123,
                "country_name": "Example Country",
                "name": "application_security",
                "country_code": "AA"
            }
        ]
    },
    "categories": [
        […]
        {
            "count": 123,
            "country_name": "Example Country",
            "name": "Other",
            "country_code": "AA"
        }
    ],
    "vulnerabilities": [
        […]
```

```
            {
                "count": 123,
                "country_name": "Example Country",
                "name": "CVE-2018-11766",
                "country_code": "AA"
            }
        ]
    }
}
```


Response Attributes

Field	Description
`scope` *Object*	Observation details of the requested country.
`type` *String*	For internal BitSight use.
`value` *String*	The 2-letter country code of the requested country.
`date_interval` *String*	The date interval (7 days or 30 days).
`end_date` *String* [`YYYY-MM-DD`]	The ending date of the interval.
`period` *String*	The time period.
`counts` *Object*	Details of the requested country grouped by data set.
Data Sets	• `risk_vectors` ○ Compromised Systems ○ Diligence ○ User Behavior • `infections` = Infections • `categories` = File Sharing • `vulnerabilities` = Vulnerabilities • `open_ports` = Open Ports
`risk_vectors` *Object*	Risk type details of the requested country.
Risk Category Slug Name *Array*	Risk category details of this country. • `compromised_systems` • `diligence`

	• `user_behavior`
`infections` *Array*	Infection details of the requested country.
`categories` *Array*	File Sharing category details of the requested country.
`vulnerabilities` *Array*	Vulnerability details of the requested country.
`open_ports` *Array*	Open port details of the requested country.
Details	Details for each data set object.
Object	A data set and its details.
`name` *String*	• Risk Category Slug Name = The slug name of the risk vector. • `infections` = The name of the infection family. • `categories` = The name of the file sharing category. • `vulnerabilities` = The name or CVE ID of the vulnerability.
`count` *Integer*	• Risk Category Slug Name = The amount of findings for the risk vector present in the country. • `infections` = The amount of infections present in the country. • `categories` = The number of files shared in the country. • `vulnerabilities` = The amount of vulnerabilities present in the country.
`country_code` *String*	The country code.
`country_name` *String*	The name of the country.
`industry_guid` *String* [`industry_guid`]	If either the industry or industries parameter is used, this industry unique identifier is displayed within the details.
`industry_sector` *String*	If either the `industry` or `industries` parameter is used, this industry name is displayed within the details.
`type` *String*	For internal BitSight use. • `COUNTRY` • `COUNTRY-INDUSTRY`

GET: KPI for National Cybersecurity Observations

`https://api.bitsighttech.com/sovereign/observations/kpis`

Use this to retrieve top infections, top vulnerabilities, and most common open ports for subscribed countries.

Parameters

Parameter	Description	Values
`date_interval`	Limit included observations by date interval.	*[String]* • `7d` (Default) • `30d`
`industry`	Filter observations by industry..	*[String]* Industry name.
`limit`	Limits the number of results.	*[Integer]* **Default:** All values.
`order`	Sort results in ascending or descending order.	*[String]* • `asc` • `desc` **Default:** `desc`

Example Request

```
curl
https://api.bitsighttech.com/sovereign/observations/kpis/?country=country_guid -u api_token: | jq
```

Example Response


```
{
  "scope": {
     "type": "country",
    "value": "FO"
  },
  "kpis": {
    "vulnerabilities": [
      {
            "ipPercentageKpi": 30.365662,
            "name": "Logjam"
      },
      {
            "ipPercentageKpi": 15.580286,
            "name": "POODLE"
      }
    ],
    "infections": [
      {
            "ipPercentageKpi": 37.79707,
            "name": "Ztorg"
      },
      {
            "ipPercentageKpi": 32.92116,
            "name": "Uupay"
      }
    ],
    "open_ports": [
      {
            "ipPercentageKpi": 35.038002,
            "name": "Telnet"
      },
      {
            "ipPercentageKpi": 0.009383503,
            "name": "Port 3389"
      },
      {
            "ipPercentageKpi": 0.009383503,
            "name": "IRC"
      }
    ]
  }
}
```

Response Attributes

Field	Description
`scope` *Object*	
`type` *String*	For internal BitSight use.
`value` *String*	The two-letter country code of the company's country.
`kpis` *Object*	KPI details.
`vulnerabilities` *Array*	Vulnerability details of this country.
`ipPercentageKpi` *Decimal*	The percentage of all observed vulnerabilities in the country that are made up of this vulnerability.
`name` *String*	The name of the vulnerability (CVE or named vulnerability).
`infections` *Array*	Infection details of this country.
`ipPercentageKpi` *Decimal*	The percentage of all observed infections in the country that are made up of this vulnerability.
`name` *String*	The name of the infection.
`open_ports` *Array*	Open port details of this country.
`ipPercentageKpi` *Decimal*	The percentage of all observed ports in the country that are open.
`name` *String*	The name of the service associated with the port or port number.

API Fields: File Sharing Categories

Torrents for the File Sharing risk vector have a content category and sub-category stored in the metadata of the torrent, set by the torrent uploader upon creation.

Application events are considered to be more high-risk than all other File Sharing categories (non-application events).

These categories are mapped in the following manner:

Torrent Category	BitSight Category
applications, applications - mac, applications - windows, software	Applications
books, books - academic, books - audio books, books - comics, books - ebooks, books - fiction, books - magazines, books - non-fiction, books - textbooks	Books
games, games - pc	Games
adult, anime - english-translated, movies, movies - dubbed movies, movies - highres movies	Movies
music, music - lossless, music - mp3, music - transcode	Music
anime, series & tv, television, tv	TV
other	Other

Pagination

The BitSight API might return a large number of results for a given query and will be paginated. Paginated results include the `next` (or `next_url`), `previous`, and `count` fields.

Field	Description
`count` *Integer*	The number of results.
`next` *String*	The URL to navigate to the next page of the results.
`next_url` *String*	Navigate to the next page of the results.
`previous` *String*	The URL to navigate to the previous page of the results.

For select endpoints with large datasets, the `cursor` parameter is included. See query parameters for more information.

Recommendations

We recommend using the following parameters, if available, to modify the response and improve the performance of the API:

- Define a `start_date` and `end_date`.
- The maximum number of records per query is controlled by the `limit` parameter; a request might return fewer records than this (even zero), but not more.

Parameters

Use the following parameters to navigate the BitSight API.

The fields are pre-selected by the object type of the return. Refer to each individual endpoint to get a list of the pre-selected fields for ordering, sorting, and filtering.

Path Parameters

Uses a part of the URL as a parameter.

Path parameters are often unique identifiers (GUID) of a particular data set.

GET: Folder Details

This returns each folder as separate objects and shared folders that are owned by you or are associated with you.

`https://api.bitsighttech.com/ratings/v1/folders`

GET: Tiers

`https://api.bitsighttech.com/ratings/v1/tiers`

Query Parameters

Access field/value pairs for filtering or sorting.

Append a question mark (?) to the URL to indicate the start of a query parameter. Additional query parameters are indicated with an ampersand (&), and if present, the URL should be wrapped with double quotes (").

Example:

```
curl "https://example.com/endpoint?field1=value1&field2=value2"
```

Parameter	Description	Values
`cursor`	For select endpoints with large datasets, this parameter is included. A cursor is an opaque base64-encoded string that allows you to get the next or previous page of results. If a query matches few observations and the response contains a `cursor` but no data, the `cursor` can then be used to ask the server to continue searching.	*[String]*
Date	For large requests, defining a date range may improve the performance of the API.	
`start_date`	The starting date for the date range.	*[String]* `YYYY-MM-DD`
`end_date`	The ending date for the date range.	*[String]* `YYYY-MM-DD`
`fields`	Filter by fields (keys).	*[Array]* Comma-separated field names. Field names are the names of the fields in the response object. The order of the specific fields might not be reflected in the response.
`format`	The format of the response data.	*[String]* **Example:** `json`

`limit`	Set the maximum number of results. The results might include fewer records (even zero), but not more.	*[Integer]* If not set, the default number of results can vary depending on the endpoint.
`next_url`	Navigate to the next page of the results.	*[String]* URL
`offset`	Set the starting point of the return.	*[Integer]* A `0` (zero) value starts the results from the first record in the result set.
`q`	Perform a full-text search for matching records on all searchable fields.	*[String]*
`sort`	Sort the response objects in ascending order (A to Z).	*[Array]* Comma-separated field names. Field names are the names of the fields in the response object. To sort in descending order, place a minus sign (-) immediately before the field name. **Example:** `'field_1,-field_2'` first sorts by ascending `field_1`, and then by descending `field_2`.