Remediating Your Findings via API

Publication Date – August 23, 2021

Endpoints

Get an understanding of your findings and track your remediation efforts.

Companies

Path	Purpose	Description
`/v1/companies/company_guid/assets/statistics?format=json`	GET: Asset Risk Matrix	Get the counts and the severity of security findings for a given company. This includes findings that were observed within the last 60 days.
`/v1/companies/company_guid/findings`	GET: Finding Details	Get an organization's finding details.
`/v1/companies/company_guid/observations`	GET: Detailed Company 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.

Domain Squatting

Path	Purpose	Description
`/domain-squatting/company_guid/`	GET: Domain Squatting Details	See Domain Squatting activity on your organization's domains.

Remediations

Path	Purpose	Description
`/v1/remediations`	GET: Remediation Tracking	Track your remediation efforts with Issue Tracking for Remediation.
`/v1/remediations`	POST: Track the Remediation of a Finding	Manage your findings for remediation tracking and assign users to remediate.

Users

Path	Purpose	Description
`/v2/users`	GET: Users	Get a list of all the users within your account to assign them to remediate a finding.

GET: Asset Risk Matrix

⇤ Companies

https://api.bitsighttech.com/ratings/v1/companies/company_guid/assets/statistics

This endpoint is the underlying data of the Asset Risk Matrix. It returns counts and the severity of security findings for a given company. This includes findings that were observed within the last 60 days.

Findings are grouped by the importance of the asset that the finds relate to, in a 3x3 (9 findings) or 4x4 matrix (16 findings).

Parameters

*Required.

See query parameters for details on the `format` (value: `json`) parameter.

Parameter	Description	Values
`company_guid`* *[string, path]*	Identify the company to query.	Company unique identifier [`company_guid`]. See GET: Portfolio Details.

Example Request

```
curl
https://api.bitsighttech.com/ratings/v1/companies/company_guid/assets/statis
tics?format=json -u api_token:
```

Example Response

```
{
   "assets": [
      {
         "asset": "foobar.com",
         "importance": 0,
         "importance_category": "low",
         "stats": {
            "grades": {
               "total": 2,
               "good": 1,
               "fair": 0,
               "warn": 0,
               "bad": 0,
               "neutral": 1,
               "na": 0
            }
         },
         "tags": [
         ]
      },
[...]
   ],
   "stats": {
      "critical": {
         "grades": {
            "total": 33,
            "good": 11,
            "fair": 18,
            "warn": 4,
            "bad": 0,
            "neutral": 0,
            "na": 0
         }
      },
[...]
   }
}
```

Response Attributes

Field	Description
`assets` *Object*	The list of assets for the company and a summary of the findings information within those assets.
`asset` *String*	The name of the asset.

	`importance` *Integer*	The numeric importance of the asset to the organization.
	`importance_category` *String*	The importance category of the asset.
	`stats` *Object*	A summary of statistics about the findings in the asset.
	`grades` *String*	The finding grade for which summary statistics will be generated from.
	`total` *Integer*	The number of findings that's related to the asset.
	`good` *Integer*	The number of findings that's related to the asset with the grade, "good."
	`fair` Integer	The number of findings that's related to the asset with the grade, "fair."
	`warn` *Integer*	The number of findings that's related to the asset with the grade, "warn."
	`bad` *Integer*	The number of findings that's related to the asset with the grade, "bad."
	`neutral` *Integer*	The number of findings that's related to the asset with the grade, "neutral."
	`na` *Integer*	The number of findings that's related to the asset with the grade, "N/A."
`stats` *Object*		A summary of findings for each category of asset importance in the company. The number and names of the importance categories depend whether the asset risk matrix is configured to be 3x3 or 4x4.
	Asset Importance Category *String*	The name of the importance category for which the findings summary statistics are calculated. The names of the importance categories depend whether the asset risk matrix is configured to be 3x3 or 4x4.
	`grades` Object	The findings grade for which the summary statistics will be generated from.
	`total` *Integer*	The number of findings for the company that's related to the asset importance category.
	`good` *Integer*	The number of findings for the company that's related to the asset importance category, with the grade, "good."

		`fair` *Integer*	The number of findings for the company that's related to the asset importance category, with the grade, "fair."
		`warn` *Integer*	The number of findings for the company that's related to the asset importance category, with the grade, "warn."
		`bad` *Integer*	The number of findings for the company that's related to the asset importance category, with the grade, "bad."
		`neutral` *Integer*	The number of findings for the company that's related to the asset importance category, with the grade, "neutral."
		`na` *Integer*	The number of findings for the company that's related to the asset importance category, with the grade, "N/A."

Errors and Status Codes

See the common errors and status codes.

```
200
```

GET: Finding Details

⇤ Companies

https://api.bitsighttech.com/ratings/v1/companies/company_guid/findings

Get an organization's finding details.

- This includes the finding details of risk types that affect or will affect security ratings; Compromised Systems, Diligence (except Domain Squatting), and File Sharing.
- This does not include Domain Squatting and Public Disclosures (Security Incidents and Other Disclosures), as they cannot be queried via the API.

The return is limited to 100 results per page by default. Refer to the pagination fields (`links`, `previous`, `next`) to navigate multiple pages of results. Use the `limit` and `offset` parameters to modify this limit. You can also use the `affects_rating` parameter to filter findings that have an impact on the letter grade by setting it to `true` or the opposite by setting it to `false`.

To view all findings, ensure the `affects_rating` parameter is not included.

- Parameters
- Example Request
- Example Response
- Response Attributes

Parameters

*Required.

See query parameters for details on the following parameters:

- `fields`
- `format`
- `limit` (default: `100`)
- `offset` (default: `100`)
- `q`
- `sort`

> Not compatible with the `details` field.

Parameter	Description	Values
`affects_rating` *[boolean, query]*	Filter by findings that have an impact on the letter grade.	A `true` value includes only the findings that have an impact on the letter grade.

`assets.asset` *[string, query]*	Filter by asset.	• Domain • IP Address
`assets.category` *[string, query]*	Filter by asset importance.	Asset importance: • `low` • `medium` • `high` • `critical` • `none`
`assets.combined_importance` *[string, query]*	Filter by combined asset importance.	Comma-separated asset importance: • `low` • `medium` • `high` • `critical` • `none`
`assets.hosted_by` *[string, query]*	Filter by the hosting provider.	Hosting provider's company unique identifier [`company_guid`]. See GET: Portfolio Details.
`details.grade` *[string, query]*	Filter by Diligence finding grade or N/A for Compromised Systems and User Behavior findings. ⚠ Incompatible with `grade_lt` and `grade_gt`.	Finding grades: • `GOOD` • `FAIR` • `WARN` • `BAD` • `NEUTRAL` • `NA` (N/A)
`details.grade_gt` *[string, query]*	Include a range from the selected finding grade to GOOD. ⚠ Incompatible with `grade`.	`NEUTRAL < BAD < WARN < FAIR < GOOD`
`details.grade_lt` *[string, query]*	Include a range from the selected finding grade to BAD. ⚠ Incompatible with `grade`.	`NEUTRAL < BAD < WARN < FAIR < GOOD`
`details.infection.family` *[string, query]*	Filter by infections.	Comma-separated infection names. See Compromised Systems findings.

		Example: `Gamarue`
`details.observed_ips_contains` *[string, query]*	Include findings from a particular IP address.	IP Address
`details.vulnerabilities.severity` *[string, query]*	Filter by vulnerability severity.	The BitSight Severity of vulnerabilities: • `minor` • `moderate` • `material` • `severe`
`evidence_key` *[string, query]*	Filter by the company's asset (domain or IP address) that's attributed to the finding.	• Domain • IP Address
`expand` *[string, query]*	Include issue tracking for remediation information.	`remediation_history`
`first_seen` *[string, query]*	Include findings that were first seen on this date. ⚠ Incompatible with `first_seen_lt` and `first_seen_gt`.	Date [`YYYY-MM-DD`]
`first_seen_gt` *[string, query]*	Include findings that were first seen after this date. ⚠ Incompatible with `first_seen`.	Date [`YYYY-MM-DD`]
`first_seen_gte` *[string, query]*	Include findings that were first seen on and after this date. ⚠ Incompatible with `first_seen`.	Date [`YYYY-MM-DD`]

`first_seen_lt` *[string, query]*	Include findings that were first seen prior to this date. ⚠ Incompatible with `first_seen`.	Date [`YYYY-MM-DD`]
`first_seen_lte` *[string, query]*	Include findings that were first seen on and prior to this date. ⚠ Incompatible with `first_seen`.	Date [`YYYY-MM-DD`]
`guid`* *[string, path]*	The company to query.	Company unique identifier [`company_guid`]. See GET: Portfolio Details.
`last_remediation_status_date` *[string, query]*	Include findings that last had a remediation status change on this date. ⚠ Incompatible with `last_remediation_status_date_lt` and `last_remediation_status_date_gt`.	Date [`YYYY-MM-DD`]
`last_remediation_status_date_gt` [string, query]	Include findings that last had a remediation status change after this date. ⚠ Incompatible with `last_remediation_status_date`.	Date [`YYYY-MM-DD`]
`last_remediation_status_date_gte` *[string, query]*	Include findings that last had a remediation status change on and after this date. ⚠ Incompatible with `last_remediation_status_date`.	Date [`YYYY-MM-DD`]

`last_remediation_status_date_lt` [string, query]	Include findings that last had a remediation status change prior to this date. ⚠ Incompatible with `last_remediation_status_date`.	Date [`YYYY-MM-DD`]
`last_remediation_status_date_lte` *[string, query]*	Include findings that last had a remediation status change prior to and on this date. ⚠ Incompatible with `last_remediation_status_date`.	Date [`YYYY-MM-DD`]
`last_remediation_status_label` *[string, query]*	Filter by the current remediation status of the finding.	The remediation status of the finding: • `No Status` • `Open` • `To Do` • `Work In Progress` • `Resolved` • `Risk Accepted`
`last_seen` *[string, query]*	Include findings that were last seen on this date. ⚠ Incompatible with `last_seen_lt` and `last_seen_gt`.	Date [`YYYY-MM-DD`]
`last_seen_gt` *[string, query]*	Include findings that were last seen after this date. ⚠ Incompatible with `last_seen`.	Date [`YYYY-MM-DD`]
`last_seen_gte` *[string, query]*	Include findings that were last seen on and after this date. ⚠ Incompatible with `last_seen`.	Date [`YYYY-MM-DD`]

`last_seen_lt` *[string, query]*	Include findings that were last seen prior to this date. ⚠ Incompatible with `last_seen`.	Date [`YYYY-MM-DD`]
`last_seen_lte` *[string, query]*	Include findings that were last seen on and prior to this date. ⚠ Incompatible with `last_seen`.	Date [`YYYY-MM-DD`]
`remediation_assignments` *[string, query]*	Filter by users assigned to the findings.	Comma-separated user unique identifier [`user_guid`]. See GET: Users.
`risk_category` *[string, query]*	Filter by particular risk categories.	Comma-separated risk categories: • `Compromised Systems` • `Diligence` • `User Behavior`
`risk_vector` *[string, query]*	Filter by particular risk vectors. ⚠ Does not include Domain Squatting, Security Incidents, and Other Disclosures.	Comma-separated risk vector slug names. See risk types.
`risk_vector_label` *[string, query]*	Filter by particular risk vectors. ⚠ Does not include Domain Squatting, Security Incidents, and Other Disclosures.	Comma-separated risk vector slug names. See risk types.
`severity` *[decimal, query]*	Filter by finding severity.	• `1` to `3.9` = Minor • `4` to `6.9` = Moderate • `7` to `8.9` = Material • `9` to `10` = Severe
`severity_gt` *[decimal, query]*	Include finding severity that are of greater severity.	• `1` to `3.9` = Minor • `4` to `6.9` = Moderate • `7` to `8.9` = Material • `9` to `10` = Severe

`severity_gte` *[decimal, query]*	Include finding severity that are of greater or equal severity.	• `1` to `3.9` = Minor • `4` to `6.9` = Moderate • `7` to `8.9` = Material • `9` to `10` = Severe
`severity_lt` *[decimal, query]*	Include finding severity that are of lesser severity.	• `1` to `3.9` = Minor • `4` to `6.9` = Moderate • `7` to `8.9` = Material • `9` to `10` = Severe
`severity_lte` *[decimal, query]*	Include finding severity that are of lesser or equal severity.	• `1` to `3.9` = Minor • `4` to `6.9` = Moderate • `7` to `8.9` = Material • `9` to `10` = Severe
`severity_category` *[string, query]*	Filter by finding severity.	• `minor` • `moderate` • `material` • `severe`
`tags_contains` *[string, query]*	Filter by infrastructure tags.	Infrastructure tags [My Company ➔ My Company Details ➔ My Infrastructure ➔ Tags].
`vulnerabilities` *[string, query]*	Filter by vulnerability.	Comma-separated vulnerability name. See the Vulnerability Catalog.

Example Request

```
curl https://api.bitsighttech.com/ratings/v1/companies/company_guid/findings
-u api_token:
```

Example Response


```
{
   "links":{
      "previous":null,
      "next":null
   },
   "count":1,
   "results":[
      {
         "temporary_id":"A9Jq47BBjea129322347d12e29c54b488752b3b71e",
         "affects_rating":false,
         "assets":[
            {
               "asset":"11.111.111.111",
               "category":"high",
               "importance":0.09,
               "is_ip":true
            }
         ],
         "details":{

⊕ See Finding Details:
Compromised Systems
Diligence
File Sharing

         },
         "evidence_key":"11.111.111.111:23",
         "first_seen":"2019-05-29",
         "last_seen":"2019-12-20",
         "related_findings":[
         ],
         "risk_category":"Diligence",
         "risk_vector":"open_ports",
         "risk_vector_label":"Open Ports",
         "rolledup_observation_id":"_aAAa1AA_a1aAA1A1aaAAa==",
         "severity":10.0,
         "severity_category":"severe",
         "tags":[
            "Remote Office"
         ],
         "remediation_history":{
            "last_requested_refresh_date":null,
            "last_refresh_status_date":null,
            "last_refresh_status_label":null,
            "last_remediation_status_label":"Work In Progress",
            "last_remediation_status_date":"2020-08-18",
            "remediation_assignments":[
               "11111111-aaaa-1111-aaaa-111111111111"
            ],
            "last_remediation_status_updated_by":"Arnold Brown"
```

```
         },
         "asset_overrides":[
            {
               "asset":"11.111.111.111",
               "importance":"high",
               "override_importance":null
            }
         ],
         "duration":null,
         "comments":"User from Actors Films said: \"Look at this finding\"
at 2018-11-29 20:30 UTC;\nArnold Brown said: \"I changed the remediation
status.\" at 2020-08-18 18:38 UTC"
      }
   ]
}
```


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 findings.
`results` *Array*	Findings.
`temporary_id` *String*	A temporary identifier for this finding.
`affects_rating` *Boolean*	Indicates if this finding has an impact on the letter grade.
`assets` *Array*	Asset details.
`asset` *String*	The asset (IP address or domain) associated with this finding.
`category` *String*	The BitSight-calculated asset importance.

	`importance` *Decimal*	For internal BitSight use.
	`is_ip` *Boolean*	A true value indicates this asset is an IP address.
`details` *Object*		Details of this finding. The included keys vary, depending on the risk type. See: • Compromised Systems • Diligence (except Domain Squatting) • File Sharing
`evidence_key` *String*		The company's asset (domain or IP address) that's attributed to the finding. The IP addresses of other companies are masked, in accordance with our responsible disclosure policy. Please review our terms and conditions, and then update your IP Visibility configurations accordingly.
`first_seen` *String* [`YYYY-MM-DD`]		The date of the first observation.
`last_seen` *String* [`YYYY-MM-DD`]		The date of the most recent observation.
`related_findings` *Array*		Details of related findings.
`risk_category` *String*		The risk category associated with this finding.
`risk_vector` `String`		The slug name of the risk vector associated with this finding.
`risk_vector_label` `String`		The name of the risk vector associated with this finding.
`rolledup_observation_id` *String* [`observation_id`]		A unique identifier for this observation.
`severity` *Decimal*		The severity of the finding, which is the measured risk that this finding introduces.
`severity_category` *String*		The slug name of the finding severity.
`tags` *Array*		Infrastructure tags that help identify this asset.

`remediation_history` *Object*	If expand=remediation_history parameter is set, the remediation history of the finding is included.
`last_requested_refresh_date` *String* [`YYYY-MM-DD`]	The date when a finding refresh that included this finding was last requested.
`last_refresh_status_date` *String* [`YYYY-MM-DD`]	The date when a refresh of the remediation status of this finding was last requested.
`last_refresh_status_label` *String*	The current refresh status of this finding.
`last_remediation_status_label` *String*	The current remediation status of this finding.
`last_remediation_status_date` *String* [`YYYY-MM-DD`]	The date when the remediation status of this finding was last changed.
`remediation_assignments` Array [`user_guid`]	The users who are assigned to remediate this finding.
`last_remediation_status_updated_by` *String*	The name of the user who updated the remediation status of this finding.
`asset_overrides` *Array*	User-assigned asset importance details.
`asset` *String*	The domain or IP address.
`importance` *String*	The user-assigned asset importance.
`override_importance` *Null*	For internal BitSight use.
`duration` *Null*	For internal BitSight use.
`comments` *String*	A thread of finding comments.

Compromised Systems Finding Details

⇤ Finding Details

The `details` field for the `/v1/companies/company_guid/findings` path shows the details of findings. The included subkeys vary, depending on the risk vector.

> The IP addresses of other companies are masked, in accordance with our responsible disclosure policy.

Example Response

For keys that are specific to certain risk vectors, refer to the following sections:

- Botnet Infections
- Spam Propagation
- Malware Servers
- Unsolicited Communications
- Potentially Exploited

```
[See Fields That Apply to All Findings]

            "geo_ip_location":"US",
            "infection":{
               "family":"Gamarue",
               "description":"Gamarue is a family of malware that can give
attackers remote access to infected devices. It is distributed through spam
messages and infected removable storage devices.",
               "references":[

"https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-descripti
on?Name=Win32%2fGamarue"
               ],
               "data_exfiltration":true,
               "unauthorized_access":true,
               "implies_other_infections":false,
               "resource_abuse":false,
               "target_platforms":[
                  "Win32"
               ]
            },
            "remediations":[
            ],

[Risk Vector Specific Keys]

            "rollup_end_date":"2019-05-31",
            "rollup_start_date":"2019-05-21",
```

Response Attributes

The following attributes apply to all Compromised Systems findings:

Field	Description
`geo_ip_location` *String*	A 2-letter ISO country code indicating this finding's country of origin.
`infection` *Object*	Contains infection details.
`family` *String*	The malware family of this infection.
`description` *String*	An overview of this infection.
`references` *Array*	A list of URLs as a source of information.
`data_exfiltration` *Boolean*	Indicates if this infection allows any unauthorized transfers of sensitive information.
`unauthorized_access` *Boolean*	Indicates if this infection allows attackers to connect and then log in as a legitimate user.
`implies_other_infections` *Boolean*	Indicates if this infection may lead to other infections.
`resource_abuse` *Boolean*	Indicates if this infection is misusing assets.
`target_platforms` *Array*	A list of platforms that are potentially affected.
`remediations` *Object*	If this is a Diligence finding, this contains information about this finding and instructions to remediate it.
`rollup_end_date` *String* [`YYYY-MM-DD`]	The date of the most recent observation.
`rollup_start_date` *String* [`YYYY-MM-DD`]	The date of the first observation.

Botnet Infections Finding Details

Example Botnet Infections Request

```
curl
https://api.bitsighttech.com/ratings/v1/companies/company_guid/findings?risk
_vector=botnet_infections -u api_token:
```

Example Botnet Infections Response

```
[See Fields That Apply to All Compromised Systems Findings]

            "server_name":"exampledomain.us",
            "user_agent":"Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1;
Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR
3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)",
            "dest_port":443,
            "detection_method":"Sinkhole",
            "src_port":51445
```

Botnet Infections Response Attributes

Field	Description
`server_name` *String*	The domain name of the affected server. **Example:** `exampledomain.us`
`user_agent` *String*	Browser details. **Examples:** • `Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)` • `Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0`
`dest_port` *Integer*	The number of the affected port.
`detection_method` *String*	The method used to detect this observation.
`src_port` *Integer*	The number of the source port.

Spam Propagation Finding Details

Example Spam Propagation Request

```
curl
https://api.bitsighttech.com/ratings/v1/companies/company_guid/findings?risk
_vector=spam_propagation -u api_token:
```

Example Spam Propagation Response

```
[See Fields That Apply to All Compromised Systems Findings]

            "spam_type":"Malformed Email",
            "detection_method":"Mail Server Connection Analysis",
```

Field	Description
`spam_type` *String*	The type of spam. **Example:** `Malformed Email`
`detection_method` *String*	The method used to detect this observation.

Malware Servers Finding Details

Example Malware Servers Request

```
curl
https://api.bitsighttech.com/ratings/v1/companies/company_guid/findings?risk
_vector=malware_servers -u api_token:
```

Example Malware Servers Response

```
[See Fields That Apply to All Compromised Systems Findings]

            "server_name":"exampledomain.us",
            "portal_type":"Malicious",
```

Malware Servers Response Attributes

Field	Description
`server_name` *String*	The domain name of the affected server. **Example:** `exampledomain.us`
`portal_type` *String*	**Values:** • `Malicious` • `Malware`

Unsolicited Communications Finding Details

Example Unsolicited Communications Request

```
curl
https://api.bitsighttech.com/ratings/v1/companies/company_guid/findings?risk
_vector=unsolicited_comm -u api_token:
```

Example Unsolicited Communications Response

```
[See Fields That Apply to All Compromised Systems Findings]

            "dest_port":22,
            "probe_count":141,
```

Unsolicited Communications Response Attributes

Field	Description
`dest_port` *Integer*	The number of the affected port.
`probe_count` *Integer*	The number of scans.

Potentially Exploited Finding Details

Example Potentially Exploited Request

```
curl
https://api.bitsighttech.com/ratings/v1/companies/company_guid/findings?risk
_vector=potentially_exploited -u api_token:
```

Example Potentially Exploited Response

```
[See Fields That Apply to All Compromised Systems Findings]

            "server_name":"exampledomain.us",
            "user_agent":"Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0)
Gecko/20100101 Firefox/64.0",
            "dest_port":80,
            "detection_method":"Sinkhole",
            "src_port":56750
```

Field	Description
`server_name` *String*	The domain name of the affected server. **Example:** `exampledomain.us`
`user_agent` *String*	Browser details. **Examples:** • `Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)` • `Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0`
`dest_port` *Integer*	The number of the affected port.
`detection_method` *String*	The method used to detect this observation.
`src_port` *Integer*	The number of the source port.

Diligence Finding Details

⇤ Finding Details

The `details` field for the `/v1/companies/company_guid/findings` path shows the details of findings. The included subkeys vary, depending on the risk vector.

> The IP addresses of other companies are masked, in accordance with our responsible disclosure policy.

Example Response

For fields that are specific to certain risk vectors, refer to the following sections and use the `risk_types` parameter values:

- SPF Domains
- DKIM Records
- TLS/SSL Certificates
- TLS/SSL Configurations
- Open Ports
- Web Application Headers
- Patching Cadence
- Insecure Systems
- Server Software
- Desktop Software
- Mobile Software
- DNSSEC
- Mobile Application Security
- Domain Squatting – Findings for this risk vector cannot be queried via the API

```
[See Fields That Apply to All Findings]

            "Diligence_annotations":{

[Risk Vector Specific Keys]

},
            "grade":"NEUTRAL",
            "remediations":[
               {
                  "help_text":"This domain is missing a DNSKEY record and
therefore cannot be authenticated using DNSSEC.",
                  "message":"DNSSEC is not configured on this domain",
                  "remediation_tip":"You will need to set up DNSSEC for your
domain, including generating necessary keys and updating DNS zone records
accordingly. See this <a target=\"new\"
href=\"https://www.digitalocean.com/community/tutorials/how-to-setup-dnssec-
on-an-authoritative-bind-dns-server--2\">DigitalOcean guide</a> for
instructions which may be applicable to your server configuration, as well
```

```
as <a target=\"new\"
href=\"http://www.dnssec.net/practical-documents\">dnssec.net</a> for
practical documents related to DNSSEC setup."
                }
            ],
            "rollup_end_date":"2019-01-26",
            "rollup_start_date":"2018-10-06"
        },
        "evidence_key":"example.com",
```

Response Attributes

The following attributes apply to all Diligence findings:

Field	Description
`diligence_annotations` *Object*	Contains Diligence finding details.
`grade` *String*	
`remediations` *Object*	Contains information about the finding and instructions to remediate it, if any.
`help_text` *String*	An overview of this finding.
`message` *String*	Details of this finding.
`remediation_tip` *String*	The recommended remediation instructions.
`rollup_end_date` *String* [`YYYY-MM-DD`]	The date when this finding was last observed.
`rollup_start_date` *String* [`YYYY-MM-DD`]	The date when this finding was first observed.

SPF Domains Finding Details

Example SPF Domains Request

```
curl
https://api.bitsighttech.com/ratings/v1/companies/company_guid/findings?risk
_vector=spf -u api_token:
```

Example SPF Domains Response

```
[See Fields That Apply to All Diligence Findings]

               "domain.com":{
                  "message":"Effective",
                  "score":"good",
                  "mech_tags":{
                    "multiple_records":"true",
                    "?all":"spf-ineffective"
                  },
                  "spf_record":[
                     "v=spf1 include:_spf.domain.com ~all"
                  ]
               },
               "_spf.domain.com":{
                  "message":"Effective",
                  "score":"good",
                  "mech_tags":{
                  },
                  "spf_record":[
                     "v=spf1 include:_netblocks.domain.com
include:_netblocks2.domain.com include:_netblocks3.domain.com ~all"
                  ]
               },
               "total":{
                  "message":"Effective",
                  "score":"good",
                  "mech_tags":{
                  },
                  "spf_record":[
                  ]
               },
               "_netblocks.domain.com":{
                  "message":"Effective",
                  "score":"good",
                  "mech_tags":{
                  },
                  "spf_record":[
                     "v=spf1 ip4:12.345.678.9/24 ip4:11.222.333.4/19
ip4:12.123.1.1/20 ip4:23.234.23.2/20 ip4:34.34.345.3/18 ip4:45.456.4.4/16
ip4:567.567.5.5/21 ip4:678.678.6.6/16 ip4:789.78.789.7/17
ip4:890.890.890.8/19 ip4:098.098.09.0/19 ~all"
                  ]
               }
```

SPF Domains Response Attributes

Field	Description
`domain` *Object*	
`message` *String*	Indicates if this SPF record is effective. **Examples:** • `Effective` • `No SPF record for subdomain`
`score` *String*	
`mech_tags` *Object*	
`multiple_records` *Boolean*	
`?all` *String*	
`spf_record` *String*	The SPF record version, followed by the mechanism that defines the IP addresses that are allowed to send mail from the domain.
`total` *Object*	

DKIM Records Finding Details

Example DKIM Records Request

```
curl
https://api.bitsighttech.com/ratings/v1/companies/company_guid/findings?risk
_vector=dkim -u api_token:
```

Example DKIM Records Response

```
[See Fields That Apply to All Diligence Findings]

                "answer":[
                   {
                      "record":[
```

```
                        "TXT",
                        "k=rsa;
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwXNZF1j8sJPDleRjf9SPBNem0ik58k
F1ilC1nUgKAttl9v7FX9hXJXPmLNhVtSKVZ8yruaeOZLeIxtgtk1s81zzIE5Mj0AiGn2wlFt4kYf
qlDfYe95YLQHjynu4i7vj1Tjksf62btcCbL+3XhbK+oD5PlqYhXHWuzoKoEp5L4lCihgkONvU/oy
7NNeE6quqfF/y0YSLwF2WVA2Kd8L6R0Ar2dYT/3wZCFknI7xhvPqh9HNcIWBELGPwtXcsHbX1wvB
lCgNQAUcdJrf2YWzAwqmZ564/1ipL1IMk1nafPJk75ktumVNz6ORuIn3jbZWp9rRpnaeI9cu/8Kf
SKH2EY9QIDAQAB"
                    ],
                    "keylen":2048,
                    "algorithm":"rsa"
                }
```


DKIM Records Response Attributes

Field	Description
`answer` *Object*	DKIM finding details.
`record` *Array*	The DKIM record.
`keylen` *Integer*	The bit strength of this key. See key length recommendations.
`algorithm` *String*	The algorithm used to encrypt and decrypt messages.

TLS/SSL Certificates Finding Details

Example TLS/SSL Certificates Request

```
curl
https://api.bitsighttech.com/ratings/v1/companies/company_guid/findings?risk
_vector=ssl_certificates -u api_token:
```

Example TLS/SSL Certificates Response

```
[See Fields That Apply to All Diligence Findings]

                "sampleName":"11.222.33.44:443",
                "certchain":[
                    {
                        "startDate":"2001-01-01",
                        "endDate":"2050-01-02",
```

```
                      "serialNumber":"1234567890",
                      "keyLength":2048,

"subjectName":"C=US,CN=subdomain.organization.com,O=Organization",
                      "dnsName":[
                         "subdomain.organization.com",
                         "othersubdomain1.organization.com",
                         "othersubdomain.organization.com"
                      ],
                      "keyAlgorithm":"RSA",
                      "issuerName":"C=US,CN=Organization Common Name
Certificate Authority,O=Organization",
                      "signatureAlgorithm":"SHA1WITHRSA"
                   }
                ]
             },
             "observed_ips":[
                "xxx.xxx.33.44:443"
             ],
             "dest_port":0,
```


TLS/SSL Certificates Response Attributes

Field	Description
`certchain` *Object*	Contains certificate chain details.
`startDate` *String* [`YYYY-MM-DD`]	The date when this certificate started.
`endDate` *String* [`YYYY-MM-DD`]	The date when this certificate expires.
`serialNumber` *Integer*	The serial number of the certificate within this chain.
`keyLength` *Integer*	The bit strength of this key.
`subjectName` *String*	The distinguished name of the owner of the certificate, made up of attribute assertion values. **Values:** • `OU` = Country or Region • `C` = 2-letter ISO Country Code • `O` = Organization Name • `CN` = Common Name

		`dnsName` *Array*	A list of domain names within this chain. **Example**: `organization.com`
		`keyAlgorithm` *String*	The algorithm used to encrypt and decrypt messages.
		`issuerName` *String*	The distinguished name of the certificate issuer, made up of attribute assertion values. **Values:** • `C` = 2-letter ISO Country Code • `ST` = State/Province • `L` = Locality • `O` = Organization Name • `OU` = Country or Region • `CN` = Common Name
		`signatureAlgorithm` *String*	The signing algorithm used in this certificate.
	`sample_name` *String*		IP address.
`observed_ips` *Array*			A list of observed IP addresses.
`dest_port` *Integer*			The destination port number.

TLS/SSL Configurations Finding Details

Example TLS/SSL Configurations Request

```
curl
https://api.bitsighttech.com/ratings/v1/companies/company_guid/findings?risk
_vector=ssl_configurations -u api_token:
```

Example TLS/SSL Configurations Response

```
[See Fields That Apply to All Diligence Findings]

                "dhLength":1024,
                "certchain":[
                    {
```

```
                      "startDate":"2018-07-17",
                      "endDate":"2028-07-15",
                      "serialNumber":"12345678901234567890",
                      "keyLength":4096,

"subjectName":"C=IT,ST=Italy,L=Udine,O=Organization,OU=IT
department,CN=subdomain.organization.com",
                      "dnsName":[
                         "subdomain.organization.com"
                      ],
                      "keyAlgorithm":"RSA",

"issuerName":"C=IT,ST=Italy,L=Udine,O=Organization,OU=IT
department,CN=subdomain.organization.com",
                      "signatureAlgorithm":"SHA256WITHRSA"
                   }
                ],
                "dhPrime":"44444444{240 digits}b11bb1bb"
             },
             "geo_ip_location":"US",
             "dest_port":993,
```


TLS/SSL Configurations Response Attributes

Field	Description
`dhLength` *Integer*	The configured key length.
`certchain` *Object*	Contains certificate chain details.
`startDate` *String* [`YYYY-MM-DD`]	The date when this certificate started.
`endDate` *String* [`YYYY-MM-DD`]	The date when this certificate expires.
`serialNumber` *Integer*	The serial number of the certificate within this chain.
`keyLength` *Integer*	The bit strength of this key.

		`subjectName` *String*	The distinguished name of the owner of the certificate, made up of attribute assertion values. **Values:** • `OU` = Country or Region • `C` = 2-letter ISO Country Code • `O` = Organization Name • `CN` = Common Name
		`dnsName` *Array*	A list of domain names within this chain. **Example:** `subdomain.organization.com`
		`keyAlgorithm` *String*	The algorithm used to encrypt and decrypt messages.
		`issuerName` *String*	The distinguished name of the certificate issuer, made up of attribute assertion values. **Values:** • `C` = 2-letter ISO Country Code • `ST` = State/Province • `L` = Locality • `O` = Organization Name • `OU` = Country or Region • `CN` = Common Name
		`signatureAlgorithm` *String*	The signing algorithm used in this certificate.
	`dhPrime` *String*		The Diffie-Hellman prime.
`geo_ip_location` *String*			A 2-letter ISO country code indicating this finding's country of origin.
`dest_port` *Integer*			The destination port number.

Open Ports Finding Details

Example Open Ports Request

```
curl
https://api.bitsighttech.com/ratings/v1/companies/company_guid/findings?risk
_vector=open_ports -u api_token:
```

Example Open Ports Response

```
[See Fields That Apply to All Diligence Findings]

               "status":"HTTP/1.1 200 OK",
               "product":"Apache httpd",
               "title":"Example Home Page",
               "CPE":[
                  "a:php:php:5.3.10-1ubuntu3.26",
                  "a:apache:http_server:2.2.22"
               ],
               "server":"Apache/2.2.22 (Ubuntu)",
               "version":"2.2.22",
               "transport":"tcp"
            },
```

Open Ports Response Attributes

Field	Description
`status` *String*	The status code that's an indication that the server was able to process the request sent by the client.
`product` *String*	The web server.
`title` *String*	The title of the page.
`CPE` *Array*	A list of Common Platform Enumeration (CPE) names.
`server` *String*	The web server and software version.
`version` *String*	The server software version.
`transport` *String*	The transmission protocol used in the connection.

Web Application Headers Finding Details

Example Web Application Headers Request

```
curl
https://api.bitsighttech.com/ratings/v1/companies/company_guid/findings?risk
_vector=application_security -u api_token:
```

Example Web Application Headers Response

```
[See Fields That Apply to All Diligence Findings]

               "record":"HTTP/1.1 200 OK\r\nContent-Type: text/html;
charset=utf-8\r\nX-Frame-Options: SAMEORIGIN\r\nX-Robots-Tag:
noarchive\r\nLast-Modified: Wed, 25 Jul 2018 07:33:34 GMT\r\nExpires: Sat,
04 Aug 2018 12:06:13 GMT\r\nDate: Sat, 04 Aug 2018 12:06:13
GMT\r\nCache-Control: private, max-age=5\r\nX-Content-Type-Options:
nosniff\r\nX-XSS-Protection: 1; mode=block\r\nServer: GSE\r\nAccept-Ranges:
none\r\nVary: Accept-Encoding\r\nTransfer-Encoding: chunked",
               "title":"Saperix, Inc.",
               "html":[
               ],
               "required":[
                  {
                     "name":"Set-Cookie",
                     "is_missing":true,
                     "value":"",
                     "components":[
                     ],
                     "annotations":[
                        {
                           "help_text":"For HTTP connections, no headers are
graded unless Set-Cookie is defined.",
                           "message":"No Set-Cookie found",
                           "remediation_tip":"Please review all <a
target=\"new\"
href=\"https://help.bitsighttech.com/hc/en-us/articles/360008632054\">header
requirements</a>. Define your set-cookie header to be graded as “GOOD” and
enable grading for all other headers."
                        }
                     ]
                  }
               ],
               "optional":[
                  {
                     "name":"X-XSS-Protection",
                     "is_missing":false,
                     "value":"1; mode=block",
                     "components":[
```

```
                    ],
                    "annotations":[
                    ]
                }
            ]
        },
        "observed_ips":[
            "www.saperix.com[2222:a2a2:2222:222:2:2:2:2013]:80"
        ],
        "dest_port":80,
```


Web Application Headers Response Attributes

Field	Description
`record` *Array*	
`title` *String*	The title of the page.
`html` *Array*	
`required` *Object*	Contains required header details.
`name` *String*	The name of this required header type.
`is_missing` *Boolean*	A `true` value indicates this header is missing.
`value` *String*	
`components` *Object*	
`annotations` *Object*	The description of this finding and recommended remediation instructions.
`help_text` *String*	A description of this finding.
`message` *String*	An overview of this finding.
`remediation_tip` *String*	The recommended remediation instructions.

	`optional` *Object*			Contains optional header details.
		`name` *String*		The name of this optional header type.
		`is_missing` *Boolean*		A `true` value indicates this header is missing.
		`value` *String*		
		`components` *Object*		
		`annotations` *Object*		The description of this finding and recommended remediation instructions.
			`help_text` *String*	A description of this finding.
			`message` *String*	An overview of this finding.
			`remediation_tip` *String*	The recommended remediation instructions.
`observed_ips` *Array*				A list of observed IP addresses.
`dest_port` *Integer*				The number of the affected port.

Patching Cadence Finding Details

Example Patching Cadence Request

```
curl
https://api.bitsighttech.com/ratings/v1/companies/company_guid/findings?risk
_vector=patching_cadence -u api_token:
```

Example Patching Cadence Response

```
[See Fields That Apply to All Diligence Findings]

                "remediation_dates":[
                   {
                      "last":"2019-03-31 04:36:36",
```

```
                "first":"2019-03-10 02:55:19"
            }
        ],
        "is_remediated":true
    },
    "vulnerability_name":"cve-2014-3566",
```

Patching Cadence Response Attributes

Field	Description
`remediation_dates` *Object*	Contains a log of remediation history details.
`last` *String* [`YYYY-MM-DD HH-MM-SS`]	The date and time of the most recent observation.
`first` *String* [`YYYY-MM-DD HH-MM-SS`]	The date and time of the first observation.
`is_remediated` *Boolean*	Indicates if this record has been remediated.
`vulnerability_name` *String*	The vulnerability name, as logged in the National Vulnerability Database (NVD).

Insecure Systems Finding Details

Example Insecure Systems Request

```
curl
https://api.bitsighttech.com/ratings/v1/companies/company_guid/findings?risk
_vector=insecure_systems -u api_token:
```

Example Insecure Systems Response

```
[See Fields That Apply to All Diligence Findings]

                "risks":[
                    "Remote command execution"
                ],
                "references":[
```

```
                "http://domain.com/path/filename.pdf",
                "https://domain2.com/path2/",
                "https://subdomain.domain3.com/path.html"
            ],
            "source_ip":"00.00.000.00",
            "path_info":"/store/products"
        },
        "sample_count":1,
        "sample_values":"",
        "server_name":"domain4.com",
        "user_agent":"",
        "dest_port":80,
        "src_port":39994
```


Insecure Systems Response Attributes

Field	Description
`risks` *Array*	A description of the risks involved with this system.
`references` *Array*	A list of URLs as a source of information.
`source_ip` *String*	The IP address of this insecure system.
`path_info` *String*	The URL path.
`sample_count` *Integer*	
`sample_values` *String*	
`server_name` *String*	The domain name of the affected server.
`user_agent` *String*	Browser details.
`dest_port` *Integer*	The number of the affected port.
`src_port` *Integer*	The number of the source port.

Server Software Finding Details

Example Server Software Request

```
curl
https://api.bitsighttech.com/ratings/v1/companies/company_guid/findings?risk
_vector=server_software -u api_token:
```

Example Server Software Response


```
[See Fields That Apply to All Diligence Findings]

               "modal_data":{

"url":"https://wiki.ubuntu.com/PrecisePangolin/ReleaseNotes",
                  "type":"obsolete-os-release",
                  "name":"Ubuntu 12.04 LTS",
                  "supportEndedOn":"2017-04-28",
                  "supportedReleases":[
                     {

"url":"https://wiki.ubuntu.com/DiscoDingo/ReleaseNotes",
                        "familyName":"Ubuntu",
                        "name":"Ubuntu 19.04",
                        "version":"19.04"
                     }
                  ]
               },
               "modal_tags":{
                  "Upstream version":"5.3.10",
                  "Type":"PHP",
                  "HTTP Server header":"",
                  "HTTP X-Powered-By header":"PHP/5.3.10-1ubuntu3.26"
                  "OS family":"CentOS"
               },
               "server":"PHP",
               "version":"5.3.10"
            },
            "geo_ip_location":"TH",
            "observed_ips":[
               "55.555.555.55"
            ],
            "port_list":[
               81
            ],
            "dest_port":81,
```

Server Software Response Attributes

Field	Description
`modal_data` *Object*	Contains server details.
`url` *String*	The release notes from the developer.
`type` *String*	Indicates the status of this server software.
`name` *String*	The name and version of the operating system.
`supportEndedOn` *String* [`YYYY-MM-DD`]	The date when this server software version was no longer supported.
`supportedReleases` *Array*	A list of supported operating systems and their details.
`url` *String*	The release notes for this supported operating system from the developer.
`familyName` *String*	The product line of this supported operating system.
`name` *String*	The name of this supported operating system.
`version` *String*	The version of this supported operating system.
`modal_tags` *Object*	Contains server software package details.
`Upstream version` *String*	
`Type` *String*	The type of server software package.
`HTTP Server header` *String*	
`HTTP X-Powered-By header` *String*	

		`OS family` *String*	
	`server` *String*		
	`version` *String*		The current server software package.
`geo_ip_location` *String*			A 2-letter ISO country code indicating this finding's country of origin.
`observed_ips` *Array*			A list of observed IP addresses.
`port_list` *Array*			A list of associated ports.
`dest_port` *Integer*			The number of the affected port.

Desktop Software Finding Details

Example Desktop Software Request

```
curl
https://api.bitsighttech.com/ratings/v1/companies/company_guid/findings?risk
_vector=desktop_software -u api_token:
```

Example Desktop Software Response

```
[See Fields That Apply to All Diligence Findings]

            "estimation_of_users":"1",
               "count_ips":1,
               "operating_system_rule":{
                  "is":"match",
                  "version":"10895.56",
                  "eol":"2018-11-02",
                  "launch":"2018-09-18"
               },
               "sample_ips":[
                  "55.5.555.555"
               ]
            },
            "geo_ip_location":"US",
            "operating_system_family":"Chrome OS",
            "operating_system_grade":"WARN",
```

```
            "operating_system_support_status":"UNSUPPORTED",
            "operating_system_version":"10895.78.0",
            "user_agent_family":"Chrome",
            "user_agent_grade":"WARN",
            "user_agent_support_status":"UNSUPPORTED",
            "user_agent_version":"69.0.3497",
```

Desktop Software Response Attributes

Field	Description
`estimation_of_users` *Integer*	The estimated number of affected users, which is based on the number of distinct cookies with a unique pair of browser and operating system versions.
`count_ips` *Integer*	The number of IP addresses that are attributed to this finding.
`operating_system_rule` *Object*	Contains details of the logic for determining the supported status of the operating system.
`is` *String*	
`version` *String*	The version of the operating system.
`eol` *String* [`YYYY-MM-DD`]	The end-of-life date for this operating system.
`launch` *String* [`YYYY-MM-DD`]	The launch date of this operating system version.
`sample_ips` *Array*	A sampled list of attributed IP addresses.
`geo_ip_location` *String*	A 2-letter ISO country code indicating this finding's country of origin.
`operating_system_family` *String*	The operating system type.
`operating_system_grade` *String*	An assessment of this operating system. **Values:** `GOOD`, `FAIR`, `NEUTRAL`, `WARN`, `BAD`
`operating_system_support_status` *String*	Indicates if this operating system is supported.

`operating_system_version` *String*	The current version of this operating system.
`user_agent_family` *String*	The browser type.
`user_agent_grade` *String*	An assessment of this browser. **Values:** `GOOD, FAIR, NEUTRAL, WARN, BAD`
`user_agent_support_status` *String*	Indicates if this browser is supported.
`user_agent_version` *String*	The current version of this browser.

Mobile Software Finding Details

Example Mobile Software Request

```
curl
https://api.bitsighttech.com/ratings/v1/companies/company_guid/findings?risk
_vector=mobile_software -u api_token:
```

Example Mobile Software Response

```
[See Fields That Apply to All Diligence Findings]

            "estimation_of_users":"1",
               "count_ips":1,
               "operating_system_rule":{
                  "is":"match",
                  "version":"8",
                  "eol":"9999-01-01",
                  "launch":"2017-08-21"
               },
               "sample_ips":[
                  "55.5.555.55"
               ]
            },
            "geo_ip_location":"US",
            "operating_system_family":"Android",
            "operating_system_grade":"GOOD",
            "operating_system_support_status":"SUPPORTED",
            "operating_system_version":"8.0.0",
            "user_agent_family":"Chrome Mobile",
            "user_agent_grade":"GOOD",
```

```
            "user_agent_support_status":"SUPPORTED",
            "user_agent_version":"71.0.3578",
```

Mobile Software Response Attributes

Field	Description
`estimation_of_users` *Integer*	The estimated number of affected users.
`count_ips` *Integer*	The number of IP addresses that are attributed to this finding.
`operating_system_rule` *Object*	Contains details of the logic for determining the supported status of the operating system.
`is` *String*	
`version` *String*	The version of the operating system.
`eol` *String* [`YYYY-MM-DD`]	The end-of-life date for this operating system.
`launch` *String* [`YYYY-MM-DD`]	The launch date of this version.
`sample_ips` *Array*	A sampled list of attributed IP addresses.
`geo_ip_location` *String*	A 2-letter ISO country code indicating this finding's country of origin.
`operating_system_family` *String*	The operating system type.
`operating_system_grade` *String*	An assessment of this operating system. **Values** • `GOOD` • `FAIR` • `NEUTRAL` • `WARN` • `BAD`
`operating_system_support_status` *String*	Indicates if this operating system is supported.

`operating_system_version` *String*	The current version of this operating system.
`user_agent_family` *String*	The browser type.
`user_agent_grade` *String*	An assessment of this browser. **Values** • `GOOD` • `FAIR` • `NEUTRAL` • `WARN` • `BAD`
`user_agent_support_status` *String*	Indicates if this browser is supported.
`user_agent_version` *String*	The current version of the browser.

DNSSEC Finding Details

Example DNSSEC Request

```
curl
https://api.bitsighttech.com/ratings/v1/companies/company_guid/findings?risk
_vector=dnssec -u api_token:
```

Example DNSSEC Response

```
[See Fields That Apply to All Diligence Findings]

                "dnskeys":[
                   {
                      "protocol":3,
                      "sepFlag":false,
                      "algorithm":"RSASHA1",
                      "keyLength":1104,
                      "zoneKeyFlag":true,

"publicKey":"TUlHZk1BMEdDU3FHU0liM0RRRUJBUVVBQTRHTkFEQ0JpUUtCZ1FEWmdod1lZb01
0RG9mYW15d1l6N2lqTmRaSTBwZzM1QytJSGUzekhLdmZrYk5CUllQT3hJMmNpdE5kbFpvM1JhYXF
yTkRYS1J1ZG5QQm1Rb2NrbkJkSk0xOUE2YXc4NlRucVZRYjV6TE9SUzc4ckVXK2dTWjYvaWxTS1V
LWEhVdkZYYmkvSmRqaFNvSy8wcVU3cVBIbUxQTUFxV25iK3krZnJwR3RVb2xyb3pRSURBUUFC"
                   }
                ],
```

```
                "rrsigs":[
                ],
                "security outcome":"Provably Insecure",
                "nsecs":[
                   {
                      "recordHash":"1tpjk84ghl5ehmqoutn58emum81uroel",
                      "recordType":"NSEC3",
                      "algorithm":"SHA1",
                      "flags":"Opt-out",
                      "iterations":0,
                      "nextHash":"1tpl435in5dsmhstd5mo6r6hi5oj3gg9",
                      "prevHash":"1TPI9B2TDBBG8L0JGJ4CS6KTTTTL9M2F",
                      "salt":"-",
                      "types":"NS DS RRSIG"
                   }
                ],
                "reason":"{{saperix.com./DNSKEY}} does not have a validated
chain of trust",
                "dses":[
                ]
```


DNSSEC Response Attributes

Field	Description
`dnskeys` *Object*	Domain Name Service (DNS) record details.
`protocol` *Integer*	
`sepFlag` *Boolean*	
`algorithm` *String*	The algorithm used for this record.
`keyLength` *Integer*	The bit strength of this key. Keys shorter than 2048 bits may be insecure.
`zoneKeyFlag` *Boolean*	
`publicKey` *String*	The public portion of the Zone Signing Key pair.
`rrsigs` *String*	The private portion of a Zone Signing Key is used to generate a digital signature, known as a Resource Record Signature (RRSIG).

`security outcome` *String*		
`nsecs` *Object*		Next Secure (NSEC) record details.
	`recordHash` *String*	The cryptographic hash, which is the scrambled alphanumeric input going in a unilateral, 1-way direction.
	`recordType` *String*	The DNS record types that exist for this NSEC record.
	`algorithm` *String*	The algorithm used for this record.
	`flags` *String*	
	`iterations` *Integer*	The number of different hash versions within this NSEC record.
	`nextHash` *String*	The next record name in the zone (DNSSEC sorting order).
	`prevHash` *String*	The previous record name in the zone (DNSSEC sorting order).
	`salt` *String*	Random text, that's publicly appended to the domain name and before the application of the hash function, to prevent re-use.
	`types` *String*	
`reason` *String*		Describes the cause of this finding.
`dses` *Array*		

Mobile Application Security Finding Details

Example Mobile Application Security Request

```
curl
https://api.bitsighttech.com/ratings/v1/companies/company_guid/findings?risk
_vector=mobile_application_security -u api_token:
```

Example Mobile Application Security Response

[See Fields That Apply to All Diligence Findings]


```
               "app_rate":4.7,
               "app_name":"Raindrops Roses Kittens",
               "app_id":"1212121212",
               "_tests":[
                  "dynamic:afnetworking=false",
                  "dynamic:cookie_without_httponly_flag=0.1",
                  "dynamic:cookie_without_secure_flag=0.1",
                  "dynamic:ipa_broken_ssl=false",
                  "dynamic:ipa_sensitive_data_cert_validation=false",
                  "dynamic:ipa_sensitive_data_flow=0.540425532",
                  "static:address_reference_counting_check=false",
                  "static:address_space_layout_rand_check=false",
                  "static:change_cipher_spec_check=false",
                  "static:heartbleed_check=false",
                  "static:local_auth_check=false",
                  "static:stack_smashing_protection_check=false"
               ],
               "domain":"yay.things.com",
               "test_mask_hex":"0a0a0a0a0a",
               "failed_tests":3,
               "test_bits_bits":"1000110000000000000000000000000000000000",
               "app_release_notes":"Ultimate things\n•Count all the
raindrops\n•Smell all the roses•Pet all the kittens\n\nBug fixes and
usability improvements",
               "store_link":"https://itunes.apple.com/app/id1111111111",
               "test_mask_bits":"1011111000000000000000000000000001111011",
               "platform":"iOS",
               "has_static":true,
               "app_package":"com.things.paperpackage",
               "app_version":"3.2.1",
               "publisher_id":"123456789",

"publisher_link":"https://itunes.apple.com/developer/id123456789",

"app_icon":"https://is1-ssl.mzstatic.com/image/thumb/Things123/v1/11/a1/1a/f
3c13ea2-df7d-4253-aab2-97de6164eb50/source/175x175bb.png",
               "test_bits_hex":"1111111111",
               "app_raw_version":"1.2.3",
               "has_dynamic":true,
               "_weight":0.7404255,
               "app_description":"Raindrops on roses and whiskers on
kittens.\n\nSome of your favorite things!\n\n•\tSee raindrops on roses
\n•\tPet kittens \n•\tGet packages with strings\n\nHave a favorite? Visit
https://yay.things.com to share or contact our team.",
               "_eks":"[domain_name=yay.things.com]",
               "_ekt":"1",
               "vendor_name":"Maria’s Favorite Things",
               "vendor_url":"http://yay.things.com"
            },
```

```
            "operating_system_family":"iOS",
            "user_agent_family":"1212121212",
            "user_agent_name":"Raindrops Roses Kittens",
            "user_agent_version":"3.2.1",
```

Mobile Application Security Response Attributes

Field	Description
`app_rate` *Decimal*	The current rating of this app within the app store.
`app_name` *String*	The name of this app.
`app_id` *Integer*	The identification number of this app, as listed in the app store.
`_tests` *Array*	A list of tests that have been conducted to determine the integrity of this app.
`domain` *String*	The domain of this app developer.
`test_mask_hex` *String*	
`failed_tests` *Integer*	The number of tests that could not be run or were partial assessments.
`test_bits_bits` *Integer*	
`app_release_notes` *String*	Release notes from this app developer.
`store_link` *String*	The listing for this app in the app store.
`test_mask_bits` *Integer*	
`platform` *String*	The platform this app is available in.
`has_static` *Boolean*	
`app_package` *String*	The file for distributing and installing this app.

`app_version` *String*	The current version of this app.
`publisher_id` *String*	The identification number of the app developer, as listed in the app store.
`publisher_link` *String*	The listing URL for the developer in the app store.
`app_icon` *String*	The URL of the image file for this app's icon.
`test_bits_hex` *Integer*	
`app_raw_version` *String*	The initial version of this app.
`has_dynamic` *Boolean*	
`_weight` *Decimal*	
`app_description` *String*	An overview of this app, as described by the app developer.
`_eks` *String*	
`_ekt` *Integer*	
`vendor_name` *String*	The name of the app developer.
`vendor_url` *String*	The URL of the app developer's main website.
`operating_system_family` *String*	The operating system this app is available for.
`user_agent_family` *String*	
`user_agent_name` *String*	
`user_agent_version` *String*	

User Behavior (File Sharing) Finding Details

⇤ Finding Details

The `details` field for the `/v1/companies/company_guid/findings` path shows the details of findings. The included subkeys vary, depending on the risk vector.

File Sharing - Example Request

```
curl
https://api.bitsighttech.com/ratings/v1/companies/company_guid/findings?risk
_vector=file_sharing -u api_token:
```

File Sharing - Example Response

```
[See Fields That Apply to All Findings]

            "geo_ip_location":"US",
            "remediations":[
            ],
            "rollup_end_date":"2019-05-04",
            "rollup_start_date":"2019-05-04",
            "src_port":62348
```

File Sharing - Response Attributes

Field	Description
`geo_ip_location` *String*	A 2-letter ISO country code indicating this finding's country of origin.
`remediations` *Object*	Contains information about the finding and instructions to remediate it, if any.
`rollup_end_date` *String* [`YYYY-MM-DD`]	The date of the most recent observation.
`rollup_start_date` *String* [`YYYY-MM-DD`]	The date of the first observation.
`src_port` *Integer*	The number of the source port.

GET: Detailed Company Observations

⇤ Companies

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.

*Required.

Parameter	Description	Values
`company_guid`* *[string, path]*	Identify the company to query.	Company unique identifier [`company_guid`]. See GET: Portfolio Details.
`domain_name` *[string, query]*	Filter by domain name. Not all observations are associated with a domain.	Domain name. **Example:** `www.example.com`
`end_date` *[string, query]*	Filter by the observation's end date.	`YYYY-MM-DD`
`grades` *[string, query]*	Filter by finding grades.	Comma-separated finding grades.

`ip_address` *[string, query]*	Filter by IP address. Not all observations are associated with an IP address.	Any IPv4 address in dotted notation or an IPv6 address. **Examples:** IPv4 address = 192.0.2.0 IPv6 address = 2001:DB8::
`limit` *[integer, query]*	Set the maximum number of results. The results will include fewer results (even zero), but not more.	Any number from 1 to 1000. **Default:** `100`
`port` *[integer, query]*	Filter observations on a particular network port.	The port number, up to 65535.
`risk_types` *[string, query]*	Filter by observation risk type. Access to some risk types is dependent on the subscription type.	Comma-separated risk types.
`start_date` *[string, query]*	Filter by the observation's starting date.	`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 specified 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":"botnet_infections",
         "observation_id":"AAAAA1CH3qvE2t7jAAAAAHBXFvY=",
         "collection_date":"2020-08-05",
         "event_date":"2020-08-05",
         "forensics":{

⊕ See Event Forensic Details
```

```
            },
            "details":{

⊕ See Event Forensic Details

                }
            }
        }
    ],
    "cursors":{
        "next":"AAAAAAAAAGQKl0_OUZg4Yw==",

"next_url":"https://api.bitsighttech.com/ratings/v1/companies/a940bb61-33c4-
42c9-9231-c8194c305db3/observations?cursor=AAAAAAAAAGQKl0_OUZg4Yw%3D%3D"
    }
}
```


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
`data` *Array*	Observations for the queried company.
`risk_type` *String*	The slug name of this observation's risk type.
`observation_id` *String*	The unique identifier of this 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 this observation was considered as an event.
`forensics` *Object*	Fields for conducting network forensics.
`domain_name` *String*	The host domain.

`host_ip` *String*	The host IP address.
`host_port` *Integer*	The host port number.
`details` *Object*	Observation details.
The included details vary depending on the risk vector. See observation details by [risk type]().	
`occurrences` *Object*	Occurrence details.
`first_seen` *String* [`YYYY-MM-DD HH:MM:SS`]	The starting date and time of this occurrence's duration.
`last_seen` *String* [`YYYY-MM-DD HH:MM:SS`]	The ending date and time of this occurrence's duration.
`representative_timestamp` *String* [`YYYY-MM-DD HH:MM:SS`]	The representative date and time of this occurrence.
`count` *Integer*	The number of times this observation was counted.
`cursors` *Object*	An opaque base64-encoded string that allows you to get the next or previous page of results, which is included with select endpoints with large datasets. If a query matches very few observations and the response contains a cursor but no data, the cursor can then be used to ask the server to continue searching.
`next` *String*	The unique identifier of the next observation.
`next_url` *String*	The URL to navigate to the next page of results.

Event Forensic Details

Event Details

These fields are common to all types of Compromised Systems events:

Field	Description
IP Address	Compromised system activity from this observed IP address (IPV4).
Date Seen	The UTC calendar date for the event.
Location	Country where the IP address of this compromise system resides.
First Seen	The first time the event was seen in a 24-hour period starting at midnight UTC.
Last Seen	The last time the event was seen in a 24-hour period, ending at midnight UTC.
Representative Event Timestamp	When the event was observed, in UTC time.

Observation Details

The `details` field that's included with GET: Detailed Company Observations (`/v1/companies/company_guid/observations`) shows the details of observations. Observation details vary, depending on the risk type [`risk_types`].

- Botnet Infections
- Potentially Exploited
- SPF Domains
- TLS/SSL Certificates
- TLS/SSL Configurations
- Open Ports
- Patching Cadence
- Insecure Systems
- Server Software
- DNSSEC
- File Sharing
- Vulnerability

Botnet Infections

Slug Name: `botnet_infections`

Example Response


```
            "source_port":54710,
             "dest_port":80,
             "server_name":"example.server.com",
             "cc_ip":"XXX.111.222.33",
             "request_method":"POST",
             "detection_mechanism":"Sinkhole",
             "infection":"RootSTV",
```

Response Attributes

Field	Description
`source_port` *Integer*	The source port number.
`dest_port` *Integer*	The destination port number.
`server_name` *String*	The name of the server associated with this observation.
`cc_ip` *String*	The IP address of the malware's Command and Control Server (C&C or C2 Server).
`request_method` *String*	The request method used to communicate with the malware.
`detection_mechanism` *String*	The method used to detect this observation.
`infection` *String*	The name of the infection.

Potentially Exploited

Slug Name: `potentially_exploited`

Example Response

```
            "source_port":56273,
             "dest_port":80,
             "server_name":"example.server.com",
             "cc_ip":"XXX.111.222.33",
             "request_method":"POST",
             "user_agent":"Apache-HttpClient/UNAVAILABLE (java 1.4)",
             "infection":"MobiDash",
```

Response Attributes

Field	Description
`source_port` *Integer*	The source port number.
`dest_port` *Integer*	The destination port number.
`server_name` *String*	The name of the server associated with this observation.
`cc_ip` *String*	The IP address of the malware's Command and Control Server (C&C or C2 Server).
`request_method` *String*	The request method used to communicate with the malware.
`user_agent` *String*	The user's form of communication with the malware.
`infection` *String*	The name of the potential infection.

SPF Domains

Slug Name: `spf`

Example Response


```
            "occurrences":{
                "first_seen":"2020-08-05 03:42:12",
                "last_seen":"2020-08-05 03:42:12",
                "representative_timestamp":"2020-08-05 03:42:12",
                "count":1
             },
             "grade":"GOOD",
             "issue":"Effective",
             "dns":{
                "query_type":16,
                "error_code":0,
                "answer":"[[TXT, v=spf1
include:spf.efwd.registrar-servers.com ~all]]"
             },
             "spf_records":[
                {
                   "domain":"actorsfilms.us",
                   "record":[
                      "v=spf1 include:spf.efwd.registrar-servers.com ~all"
                   ],
                   "grade":"GOOD",
                   "issue":"Effective"
                }
             ]
```


Response Attributes

Field	Description
`occurrences` *Object*	Occurrence details.
`first_seen` *String* [`YYYY-MM-DD HH:MM:SS`]	The starting date and time of this occurrence's duration.
`last_seen` *String* [`YYYY-MM-DD HH:MM:SS`]	The ending date and time of this occurrence's duration.
`representative_timestamp` *String* [`YYYY-MM-DD HH:MM:SS`]	The representative date and time of this occurrence.
`count`	The number of times this observation was counted.

Integer	
`grade` *String*	The finding grade for this observation.
`issue` *String*	A description of this observation.
`dns` *Object*	Domain Name System (DNS) details.
`query_type` *Integer*	For internal BitSight use.
`error_code` *Integer*	For internal BitSight use.
`answer` *String*	The contents of the returned record from the DNS.
`spf_records` *Array*	SPF record details.
`domain` *String*	The domain name.
`record` *Array*	Record details.
`grade` *String*	The finding grade for this observation.
`issue` *String*	A description of this observation.

TLS/SSL Certificates

Slug Name: `ssl_certificates`

Example Response


```
            "grade":"WARN",
             "cert_chain":[
                {
                   "startDate":"2020-06-29",
                   "endDate":"2030-06-28",

"issuerName":"CN=vpn.blakemanpropane.com,unstructuredName=vpn.blakemanpropan
e.com",

"subjectName":"CN=vpn.blakemanpropane.com,unstructuredName=vpn.blakemanpropa
ne.com",
                   "keyAlgorithm":"RSA",
                   "signatureAlgorithm":"SHA256WITHRSA",
                   "keyLength":2048,
                   "serialNumber":"934606686",
                   "dnsName":[
                      "vpn.blakemanpropane.com"
                   ],
                   "serialNumberHex":"37B4F75E"
                }
             ],
             "certificate_serial":"934606686",
             "certificate_serial_hex":"37B4F75E",
             "issues":[
                "Self-signed certificate"
             ],
             "observed_ips":[
                "75.127.18.14:443"
             ],
             "hostnames":[
                "vpn.blakemanpropane.com"
             ]
```


Response Attributes

Field	Description
`grade` *String*	The finding grade for this observation.
`cert_chain` *Array*	Certificate chain details.
`startDate` *String* [`YYYY-MM-DD`]	The date when this certificate started.

`endDate` *String* [`YYYY-MM-DD`]	The date when this certificate expired or expires.
`issuerName` *String*	The distinguished name of the certificate issuer, made up of attribute assertion values. **Values:** • `C` = 2-letter ISO Country Code • `ST` = State/Province • `L` = Locality • `O` = Organization Name • `OU` = Country or Region • `CN` = Common Name
`subjectName` *String*	The distinguished name of the owner of the certificate, made up of attribute assertion values. **Values:** • `OU` = Country or Region • `C` = 2-letter ISO Country Code • `O` = Organization Name • `CN` = Common Name
`keyAlgorithm` *String*	The algorithm used to encrypt and decrypt messages.
`signatureAlgorithm` *String*	The signing algorithm used in this certificate.
`keyLength` *Integer*	The bit strength of this key. See the recommended TLS key length.
`serialNumber` *Integer*	The serial number of the certificate within this chain.
`dnsName` *Array*	A list of domain names within this chain.
`serialNumberHex` *String*	The hex serial number of the certificate within this chain.
`certificate_serial` *Integer*	The serial number of the certificate within this chain.
`certificate_serial_hex` *String*	The hex serial number of the certificate within this chain.
`issues`	Descriptions of any observations.

Array	
`observed_ips` *Array*	Observed IP addresses.
`hostnames` *Array*	Observed hostnames.

TLS/SSL Configurations

Slug Name: `ssl_configuration`

Example Response

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

Response Attributes

Field	Description
`grade` *String*	The finding grade for this observation.
`issues` *Array*	TLS/SSL Configuration observations.
`dh_prime` *String*	The Diffie-Hellman prime.
`dh_length` *Integer*	The configured key length. See the recommended TLS key length.

Open Ports

Slug Name: `open_ports`

Example Response

```
            "grade":"NEUTRAL",
             "response":"HTTP/1.0 400 Bad Request\r\nServer:
AkamaiGHost\r\nMime-Version: 1.0\r\nContent-Type:
text/html\r\nContent-Length: 209\r\nExpires: Wed, 05 Aug 2020 03:27:03
GMT\r\nDate: Wed, 05 Aug 2020 03:27:03 GMT\r\nConnection: close",
             "message":"Detected service: HTTP"
```

Response Attributes

Field	Description
`grade` *String*	The finding grade for this observation.
`response` *String*	The response code that indicates if the server was able to process the request sent by the client.
`message` *String*	The type of service running on this port.

Patching Cadence

Slug Name: `patching_cadence`

Example Response

```
            "vulnerability":"cve-2016-7103",
             "is_remediated":false
```

Response Attributes

Field	Description
`vulnerability` *String*	The Common Vulnerabilities and Exposures (CVE) ID.
`is_remediated` *Boolean*	A `true` value indicates this vulnerability has been patched.

Insecure Systems

Slug Name: `insecure_systems`

Example Response

```
            "grade":"WARN",
             "description":"Endpoint is using abandoned Samsung Media Hub
platform",
             "category":"AbandonedIPTv",
             "subcategory":"abandoned_media_hub",
             "user_agent":"SAMSUNG-Android"
```

Response Attributes

Field	Description
`grade` *String*	The finding grade for this observation.
`description` *String*	A description of this observation.
`category` *String*	The system's category.
`subcategory` *String*	The slug name of the system's subcategory.
`user_agent` *String*	The user's form of communication with the malware.

Server Software

Slug Name: `server_software`

Example Response

```
            "grade":"NEUTRAL",
             "grade_explanation":{
                "type":"possible-backports"
             },
             "tags":{
                "Type":"nginx",
                "Version":"1.14.0"
             }
```

Response Attributes

Field	Description
`grade` *String*	The finding grade for this observation.
`grade_explanation` *Object*	The reason for the finding grade.
`type` *String*	The type of software status.
`name` *String*	The name of the version of the software.
`url` *String*	The URL to the software developer's release notes.
`supportEndedOn` *String* [`YYYY-MM-DD`]	The date when this software was no longer supported.
`supportedReleases` *Array*	Supported software.
`name` *String*	The name of this software and its version.
`familyName` *String*	The name of this software.
`version` *String*	The version of this software.
`url`	The URL to the software developer's release notes.

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

DNSSEC

Slug Name: `dnssec`

Example Response

```
            "grade":"NEUTRAL",
             "issue":"DNSSEC is not configured on this domain",
             "dns":{
                "query_type":48,
                "error_code":0,
                "answer":"[[NSEC3, R3110FQIESVOLC2M36DSAG652FSLGGVE.com.
86400 IN NSEC3 1 1 0 - r31272c70r2p5loina902eut1lvapvmt NS DS RRSIG]]"
```

Response Attributes

Field	Description
`grade` *String*	The finding grade for this observation.
`issue` *String*	A description of this observation.
`dns` *Object*	Domain Name Service (DNS) record details.
`query_type` *Integer*	
`error_code` *Integer*	
`answer` *String*	

File Sharing

Slug Name: `file_sharing`

Example Response

```
            "category":"MOVIES",
             "source_port":6881,
             "node":"111.222.33.44"
```

Response Attributes

Field	Description
`category` *String*	The BitSight category for the type of torrent.
`source_port` *Integer*	The source port number.
`node` *String*	

Vulnerability

Slug Name: `vulnerability`

Example Response

```
            "vulnerability":"CVE-2016-7103",
             "status":"vulnerable",
             "evidence":""
```

Response Attributes

Field	Description
`vulnerability` *String*	The Common Vulnerabilities and Exposures ID (CVE ID).
`status` *String*	The status of the vulnerability. **Values:** • `vulnerable` = A test was performed and the software or device is vulnerable to the vulnerability. • `not-vulnerable` = A test was performed and the software or device is not vulnerable to the vulnerability. • `unknown` = The vulnerability status cannot be determined (e.g., the software or device is unresponsive). • `not-applicable` = The software or device does not match the criteria for testing.
`evidence` *Null*	For internal BitSight use.

GET: Domain Squatting Details

https://api.bitsighttech.com/domain-squatting/company_guid/

See Domain Squatting activity on your organization's domains.

Available for your My Company or SPM Subsidiary subscriptions.

Parameters

*Required.

Parameter	Description	Values
`company_guid`* *[string, path]*	Identify the company to query.	Your organization's (My Company or SPM Subsidiary) company unique identifier [`company_guid`]. See GET: Portfolio Details.

Example Request

Ensure the final slash (/) is included in the path.

```
curl https://api.bitsighttech.com/domain-squatting/company_guid/ -u
api_token:
```

Example Response

```
[
  {
    "domain": "goliathinvest.com",
    "permutations": [
      {
        "name": "goliathinvest.com",
        "state": "Registered to company",
        "type": "Original*"
      },
    ],
    "timestamp": "2020-07-08 12:48:19.297428"
  }
]
```

Response Attributes

Field	Description
`domain` *String*	A domain (asset) that's authentically owned by your organization.
`permutations` *Array*	Variations of the domain.
`name` *String*	A variation of the domain name.
`state` *String*	The current state of the variation. **Values:** • `Registered to company` • `Unregistered`
`type` *String*	Domain squatting can take on various forms that are categorized into typographical errors, spear phishing, and bitsquatting errors (Bit-flip). See Domain Squatting categories.
`timestamp` *String* [`YYYY-MM-DD HH:MM:SS`]	The date and time when this data set was last updated.

GET: Remediation Tracking

⇤ Remediations

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

Track your remediation efforts with Issue Tracking for Remediation.

Parameters

Parameter	Description	Values
`company_guid` *[string, query]*	The company to track remediation.	Company unique identifier [`company_guid`]. See GET: Portfolio Details.
`created_time_gte` *[string, query]*	Filter findings by when they were tracked for remediation starting on and after the specified datetime.	The datetime [`YYYY-MM-DDTHH:MM:SSZ`].
`created_time_lte` *[string, query]*	Filter findings by when they were tracked for remediation starting on and prior to the specified datetime.	The datetime [`YYYY-MM-DDTHH:MM:SSZ`].
`creator` *[string, query]*	Filter by the user assigned to the finding.	User unique identifier [`user_guid`]. See GET: Users.
`evidence_key` *[string, query]*	Filter by the company's asset (domain or IP address) that's attributed to the finding.	• Domain • IP Address
`risk_vector` *[string, query]*	Filter by risk vector.	Comma-separated risk vector slug names. See risk types.
`rolledup_observation_id` *[string, query]*	Filter by observation.	Observation identifier [`observation_id`]. See GET: Finding Details.
`status` *[string, query]*	Filter by remediation status.	Remediation status: • `OPEN` • `TODO` • `WORK_IN_PROGRESS` • `RESOLVED` • `RISK_ACCEPTED`

Example Request

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

Example Response


```
{
   "links":{
      "previous":null,
      "next":null
   },
   "count":1,
   "results":[
      {
         "company_guid":"1b3d260c-9e23-4e19-b3a5-a0bcf67d74d9",
         "risk_vector":"open_ports",
         "evidence_key":"11.111.111.111:23",
         "rolledup_observation_id":"_aAAa1AA_a1aAA1A1aaAAa==",
         "status":{
            "public":false,
            "value":"Open"
         },
         "comment":{
            "public":false,
            "value":null
         },
         "assignments":[
            {
               "guid":"11111111-aaaa-1111-aaaa-111111111111",
               "friendly_name":"Arnold Brown",
               "formal_name":"Arnold Brown",
               "email":"arnold@actorsfilms.us",
               "phone_number":"",
               "is_active":true,
               "last_login_date":"2020-08-18T19:29:46.955518Z",
               "joined_date":"2020-02-02T20:20:20Z",
               "status":"Activated"
            }
         ],
         "created_time":"2020-08-18T18:28:28.986465Z",
         "creator":{
            "guid":"11111111-aaaa-1111-aaaa-111111111111",
            "friendly_name":"Arnold Brown",
            "formal_name":"Arnold Brown",
            "email":"arnold@actorsfilms.us",
            "phone_number":"",
            "is_active":true,
            "last_login_date":"2020-08-18T19:29:46.955518Z",
            "joined_date":"2020-02-02T20:20:20Z",
```

```
            "status":"Activated"
        }
    }
  ]
}
```

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 tracked findings for remediation.
`results` *Array*	Tracked findings for remediation.
`company_guid` *String* [`company_guid`]	The queried company.
`risk_vector` *String*	The slug name of the risk vector associated with this finding. See risk types.
`evidence_key` *String*	The company's asset (domain or IP address) that's attributed to the finding.
`rolledup_observation_id` *String* [`observation_id`]	A unique identifier for this observation.
`status` *Object*	Remediation status details.
`public` *Boolean*	This value is always `false`.
`value` *String*	The current remediation status of this finding.
`comment` *Object*	Finding comment details.

	`public` *Boolean*	A `true` value indicates comments on this finding are public.
	`value` *String*	For internal BitSight use. This value is always null.
`assignments` *Array*		User details of those who are assigned to remediate this finding.
	`guid` *String* [`user_guid`]	The assigned user's unique identifier.
	`friendly_name` *String*	The assigned user's full name.
	`formal_name` *String*	The assigned user's full name.
	`email` *String*	The assigned user's email address.
	`phone_number` *String*	The assigned user's phone number.
	`is_active` *Boolean*	A `true` value indicates the assigned user has access to the BitSight platform.
	`last_login_date` *String* [`YYYY-MM-DDTHH:MM:SSZ`]	The datetime when the user last logged in to the BitSight platform.
	`joined_date` *String* [`YYYY-MM-DDTHH:MM:SSZ`]	The datetime when the assigned user's account was created in the BitSight platform.
	`status` *String*	The status of the user's account.
`created_time` *String* [`YYYY-MM-DDTHH:MM:SSZ`]		The datetime when remediation tracking began for this finding.
`creator` *Object*		User details of who started tracking the remediation of this finding.
	`guid` *String* [`user_guid`]	The remediation creator's unique identifier.
	`friendly_name` *String*	The remediation creator's full name.

		`formal_name` *String*	The remediation creator's full name.
		`email` *String*	The remediation creator's email address.
		`phone_number` *String*	The remediation creator's phone number.
		`is_active` *Boolean*	A true value indicates the remediation creator has access to the BitSight platform.
		`last_login_date` *String* [`YYYY-MM-DDTHH:MM:SSZ`]	The datetime when the remediation creator last logged in to the BitSight platform.
		`joined_date` *String* [`YYYY-MM-DDTHH:MM:SSZ`]	The datetime when the remediation creator's account was created in the BitSight platform.
		`status` *String*	The status of the remediation creator's account.

POST: Track the Remediation of a Finding

⇤ Remediations

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

Manage your findings for remediation tracking and assign users to remediate.

Parameters

*Required.

Parameter	Description	Values
`company_guid`* *[string, data]*	Identify your company.	Your company's unique identifier [`company_guid`]. See GET: Portfolio Details.
`evidence_key`* *[string, data]*	Identify the asset (domain or IP address) associated with the finding to remediate.	The asset [`evidence_key`]. See GET: Remediation Tracking.
`risk_vector`* *[string, data]*	Identify a risk vector to remediate.	The risk vector slug name. See risk types.
`rolledup_observation_id`* *[string, data]*	Identify a finding to remediate.	Observation identifier [`observation_id`]. See GET: Remediation Tracking.
`status` *[object, data]*	Edit the finding to remediate. *Requires value and public.	`{"value":"value","public":false}`
`value` *[string, data]*	Change the remediation status of the finding. *Required if status is included.	Remediation status: • `Open` • `To Do` • `Work In Progress` • `Resolved` • `Risk Accepted`
`public` *[boolean, data]*	For internal BitSight use. *Required if status is included.	`false`

`assignments` *[array, data]*	Assign a user to remediate the specified findings.	Comma-separated user unique identifiers [`user_guid`]. See GET: Users.

Example Requests

To assign a user to remediate a finding:

```
curl -X POST --data-ascii '{
   "company_guid":"1b3d260c-9e23-4e19-b3a5-a0bcf67d74d9",
   "rolledup_observation_id":"_aAAa1AA_a1aAA1A1aaAAa==",
   "evidence_key":"11.1.111.11:80",
   "risk_vector":"open_ports",
   "assignments":[
      "11111111-aaaa-1111-aaaa-111111111111"
   ]
}' https://api.bitsighttech.com/ratings/v1/remediations -u api_token:
--header "Content-Type:application/json"
```

To change the remediation status of a finding:

```
curl -X POST --data-ascii '{
   "company_guid":"1b3d260c-9e23-4e19-b3a5-a0bcf67d74d9",
   "rolledup_observation_id":"_aAAa1AA_a1aAA1A1aaAAa==",
   "evidence_key":"11.1.111.11:80",
   "risk_vector":"open_ports",
   "status":{"value":"Risk Accepted","public":false}}'
https://api.bitsighttech.com/ratings/v1/remediations -u api_token: --header
"Content-Type:application/json"
```

GET: Users

⇤ Users

https://api.bitsighttech.com/ratings/v2/users

Get a list of all the users within your account.

Parameters

See query parameters for details on the following parameters:

- `limit` (default: `100`)
- `offset` (default: `100`)
- `q`
- `sort`

Parameter	Description	Values
`email` *[string, query]*	Filter by the user's email address.	
`email_q` *[string, query]*	Search by the user's email address.	
`formal_name_q` *[string, query]*	Search by the user's full name.	
`group.guid` *[array, query]*	Filter the Access Control Group of the user.	Comma-separated group unique identifiers [`group_guid`]. See GET: Access Control Groups.
`guid` *[string, query]*	Filter by a specific user.	User unique identifier [`user_guid`].
`is_available_for_contact` *[boolean, query]*	Filter by Admin, Group Admin, or Portfolio Admin users that have been assigned as a point-of-contact when other users request to add companies to the portfolio.	A `true` value includes users that have been assigned as a point-of-contact for subscription requests.
`is_company_api_token` *[boolean, query]*	Filter by actual users or user accounts for the company API token.	A `true` value includes user accounts that are company API tokens.
`roles.slug` *[array, query]*	Filter by user role.	Comma-separated user role slug name. See user roles.

`status` *[array, query]*	Filter by user account status.	Comma-separated user account status: • `Activated` • `Created` • `Deactivated`

Example Request

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

Example Response


```
{
   "links":{
      "previous":null,

"next":"https://api.bitsighttech.com/ratings/v2/users?limit=100&offset=100"
   },
   "count":1,
   "results":[
      {
         "guid":"11111111-aaaa-1111-aaaa-111111111111",
         "friendly_name":"Arnold",
         "formal_name":"Arnold Brown",
         "email":"arnold@actorsfilms.us",
         "group":{
            "guid":"aaaaaaaa-1111-aaaa-1111-aaaaaaaaaaaa",
            "name":"Analytics Team"
         },
         "status":"Activated",
         "last_login_time":"2020-05-18T15:26:41.038420Z",
         "joined_time":"2020-02-02T20:20:20Z",
         "roles":[
            {
               "name":"Group Admin",
               "slug":"customer_group_admin"
            }
         ],
         "is_available_for_contact":false,
         "is_company_api_token":false,
         "features":[
            {
               "slug":"wfh-ro",
               "value":true,
               "can_update":false
            }
         ]
      }
```

```
    ]
}
```

Response Attributes

Field	Description
`links` *Object*	Navigation for multiple pages of results. See pagination.
`previous` *String*	The URL for navigating to the previous page of results.
`next` *String*	The URL for navigating to the next page of results.
`count` *Integer*	The number of results.
`results` *Object*	User details.
`guid` *String* [`user_guid`]	The unique identifier of this user.
`friendly_name` *String*	The preferred name of this user.
`formal_name` *String*	The full name of this user.
`email` *String*	The email address of this user.
`group` *Object*	The Access Control Group of this user.
`guid` *String* [`group_guid`]	The unique identifier of this group.
`name` *String*	The name of this group.
`status` *String*	The account status of this user.
`last_login_time` *String* [`YYYY-MM-DDTHH:MM:SSZ`]	The date and time when this user last logged in to the BitSight platform.

`joined_time` *String* [`YYYY-MM-DDTHH:MM:SSZ`]	The date and time when this user was added to the BitSight platform.
`roles` *Array*	The role of this user.
`name` *String*	The name of this user's role.
`slug` *String*	The slug name of this user's role.
`is_available_for_contact` *Boolean*	A `true` value indicates this user is an Admin, Group Admin, or Portfolio Manager who has been assigned as a point-of-contact when other users request to add companies to the portfolio.
`is_company_api_token` *Boolean*	A `true` value indicates this user account is a company API token and is not an actual user.
`features` *Array*	User-managed feature details of this user.
`slug` *String*	The slug name of this feature.
`value` *Boolean*	A `true` value indicates this feature is enabled for this user.
`can_update` *Boolean*	A `true` value indicates this user can manage settings for this feature.

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 results per query is controlled by the `limit` parameter; a request might return fewer results than this (even zero), but not more.

Parameters

Path Parameters

Uses a part of the URL as a parameter.

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

GET: Access Control Groups

Get a list of your organization's Access Control Groups and see your organization's default group.

https://api.bitsighttech.com/ratings/v1/access-groups

GET: Portfolio Details

Get information about the companies in your portfolio.

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

Query Parameters

Access key/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?key1=value1&key2=value2"`

Parameter	Description	Values
`cursor` *[string]*	For select endpoints with large datasets, the cursor parameter is included, which is an opaque base64-encoded string that enables navigation to 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.	
Date	For large requests, defining a date range may improve the performance of the API.	
`start_date`	The starting date for the date range.	`YYYY-MM-DD`

[string]		
`end_date` *[string]*	The ending date for the date range.	`YYYY-MM-DD`
`fields` *[string]*	Filter by fields (keys).	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` *[string]*	Set the format of the response data.	**Example:** `json`
`limit` *[integer]*	Set the maximum number of results. The results might include fewer records (even zero), but not more.	If not set, the default number of results can vary depending on the endpoint.
`next_url` *[string]*	Navigate to the next page of the results.	URL
`offset` *[integer]*	Set the starting point of the return.	A `0` (zero) value starts the results from the first result in the result set.
`q` *[string]*	Perform a full-text search for matching records on all searchable fields.	
`sort` *[string]*	Sort the response objects in ascending order (A to Z).	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:** `'key_1,-key_2'` first sorts by ascending `key_1`, and then by descending `key_2`.

Errors and Status Codes

We use standard HTTP response codes to indicate success or failure of an API request. Typically, codes in the 2xx range indicate success, codes in the 4xx range indicate an error that resulted from the provided information (e.g. a required parameter was missing), and codes in the 5xx range indicate an error with our servers.

Code	Status	Description
200	Okay	Everything worked as expected.
400	Bad Request	Often missing a parameter.
401	Unauthorized	No valid API token provided with the request.
402	Request Failed	Parameters were valid but the request failed.
404	Not found	The requested item or resource doesn't exist.
405	Method not allowed	An unsupported request type was attempted.
500, 502, 503, 504	Server errors	Something went wrong on the BitSight end.

API Fields: Risk Types

Not all risk types are returned by the BitSight API. Access is controlled on a per-organization level (i.e., an organization must have the right subscriptions) and depends on the endpoint.

BitSight risk types are grouped in the following manner:

- Compromised Systems
  - Botnet Infections
  - Spam Propagation
  - Malware Servers
  - Unsolicited Communications
  - Potentially Exploited
- Diligence
  - SPF Domains
  - DKIM Records
  - TLS/SSL Certificates
  - TLS/SSL Configurations
  - Open Ports
  - Web Application Headers
  - Patching Cadence
  - Insecure Systems
  - Server Software
  - Desktop Software
  - Mobile Software
  - DNSSEC
  - Mobile Application Security
  - Domain Squatting
- User Behavior
  - File Sharing
  - Exposed Credentials
- Public Disclosures
  - Security Incidents
  - Other Disclosures

Compromised Systems

The Compromised Systems risk category indicates the presence of malware or unwanted software, which is evidence of security controls failing to prevent malicious or unwanted software from running within an organization.

Botnet Infections

The Botnet Infections risk vector indicates that devices on a company's network are participating in a botnet (combination of "robot" and "network"), either as bots or as a command and control (C&C or C2) server.

Paths	Purposes	Fields	Values
`/v1/companies/company_guid/observations`	GET: Detailed Company Observations	`risk_type`	`botnet_infections`
`/v1/companies/company_guid/findings`	GET: Finding Details	`risk_vector`	`botnet_infections`

⇧ Back to Directory

Spam Propagation

The Spam Propagation risk vector is composed of spambots, where a device on a company's network is unsolicitedly sending commercial or bulk email (spam). If spam originates from email addresses or devices within a company's network, this is an indication of an infection.

Paths	Purposes	Fields	Values
`/v1/companies/company_guid/observations`	GET: Detailed Company Observations	`risk_type`	`spam_propagation`
`/v1/companies/company_guid/findings`	GET: Finding Details	`risk_vector`	`spam_propagation`

⇧ Back to Directory

Malware Servers

The Malware Servers risk vector is an indication that a system is engaging in malicious activity, such as phishing, fraud, or scams. A company's network is hosting malware that is meant to lure visitors to a website or send a file that injects malicious code or viruses.

Paths	Purposes	Fields	Values
/v1/companies/company_guid/observations	GET: Detailed Company Observations	risk_type	malware_servers
/v1/companies/company_guid/findings	GET: Finding Details	risk_vector	malware_servers

⇧ Back to Directory

Unsolicited Communications

The Unsolicited Communications risk vector indicates a host is trying to contact a service on another host. It might be attempting to communicate with a server that is not providing or advertising any useful services, the attempt may be unexpected, or the service is unsupported. This also accounts for hosts that might be scanning darknets.

Paths	Purposes	Fields	Values
/v1/companies/company_guid/observations	GET: Detailed Company Observations	risk_type	unsolicited_comm
/v1/companies/company_guid/findings	GET: Finding Details	risk_vector	unsolicited_comm

⇧ Back to Directory

Potentially Exploited

The Potentially Exploited risk vector indicates that a device on a company's network is running a potentially unwanted program (PUP) or potentially unwanted application (PUA).

Paths	Purposes	Fields	Values
/v1/companies/company_guid/observations	GET: Detailed Company Observations	risk_type	potentially_exploited
/v1/companies/company_guid/findings	GET: Finding Details	risk_vector	potentially_exploited

⇧ Back to Directory

Diligence

The Diligence risk category assesses the steps a company has taken to prevent attacks, their best practice implementation, and risk mitigation (e.g., server configurations) to determine if the security practices of an organization are on par with industry-wide best practices.

SPF Domains

The SPF Domains risk vector assesses the effectiveness of Sender Policy Framework (SPF) records, which are DNS records that identify mail servers permitted to send email on behalf of a domain. Properly configured SPF records ensure that only authorized hosts can send email on behalf of a company by providing receiving mail servers the information they need to reject mail sent by unauthorized hosts.

Paths	Purposes	Fields	Values
`/v1/companies/company_guid/observations`	GET: Detailed Company Observations	`risk_type`	`spf`
`/v1/companies/company_guid/findings`	GET: Finding Details	`risk_vector`	`spf`

⇧ Back to Directory

DKIM Records

The DKIM Records risk vector assesses the effectiveness of DomainKeys Identified Mail (DKIM) records, which is a countermeasure against adversaries that are attempting to send fake email by using a company's email domain. Properly configured DKIM records can ensure that only authorized hosts can send email on behalf of a company.

Paths	Purposes	Fields	Values
`/v1/companies/company_guid/observations`	GET: Detailed Company Observations	`risk_type`	`dkim`
`/v1/companies/company_guid/findings`	GET: Finding Details	`risk_vector`	`dkim`

⇧ Back to Directory

TLS/SSL Certificates

The TLS/SSL Certificates risk vector evaluates the strength and effectiveness of the cryptographic keys within TLS and SSL certificates, which are used to encrypt internet traffic. Certificates are responsible for verifying the authenticity of company servers to associates, clients, and guests, and also serves as the basis for establishing cryptographic trust.

Paths	Purposes	Fields	Values
/v1/companies/company_guid/observations	GET: Detailed Company Observations	risk_type	ssl_certificates
/v1/companies/company_guid/findings	GET: Finding Details	risk_vector	ssl_certificates

⇧ Back to Directory

TLS/SSL Configurations

The TLS/SSL Configurations risk vector determines if the used security protocol libraries support strong encryption standards when making connections to other machines. TLS/SSL is a widely used method of securing communications over the Internet.

Paths	Purposes	Fields	Values
/v1/companies/company_guid/observations	GET: Detailed Company Observations	risk_type	ssl_configuration
/v1/companies/company_guid/findings	GET: Finding Details	risk_vector	ssl_configurations

⇧ Back to Directory

Open Ports

The Open Ports risk vector observes ports that are exposed to the Internet, known as “open ports.” While certain ports must be open to support normal business functions and few companies will actually have no ports open, the fewer ports that are exposed to the Internet, the fewer openings there are for attack.

Path	Purpose	Field	Values
/v1/companies/company_guid/observations	GET: Detailed Company Observations	risk_type	open_ports
/v1/companies/company_guid/findings	GET: Finding Details	risk_vector	open_ports

⇧ Back to Directory

Web Application Headers

The Web Application Headers risk vector analyzes security-related fields in the header section of communications between users and an application. They contain information about the messages, determine how to receive messages, and how recipients should respond to a message.

Path	Purpose	Field	Values
/v1/companies/company_guid/observations	GET: Detailed Company Observations	risk_type	application_security
/v1/companies/company_guid/findings	GET: Finding Details	risk_vector	application_security

⇧ Back to Directory

Patching Cadence

The Patching Cadence risk vector evaluates systems that are affected by software vulnerabilities (holes or bugs in software, hardware, or encryption methods that can be used by attackers to gain unauthorized access to systems and their data) and how quickly any issues are fixed.

Path	Purpose	Field	Values
/v1/companies/company_guid/observations	GET: Detailed Company Observations	risk_type	patching_cadence
/v1/companies/company_guid/findings	GET: Finding Details	risk_vector	patching_cadence

⇧ Back to Directory

Insecure Systems

The Insecure Systems risk vector assesses endpoints (which can be any computer, server, device, system, or appliance with internet access) that are communicating with an unintended destination. The software of these endpoints may be outdated, tampered, or misconfigured. A system is classified as “insecure” when these endpoints try to communicate with a web domain that doesn’t yet exist or isn’t registered to anyone.

Path	Purpose	Field	Values
/v1/companies/company_guid/observations	GET: Detailed Company Observations	risk_type	insecure_systems
/v1/companies/company_guid/findings	GET: Finding Details	risk_vector	insecure_systems

⇧ Back to Directory

Server Software

The Server Software risk vector helps track security problems introduced by server software that is no longer supported. Supported software versions receive attention from the software development team and vendor when bugs or vulnerabilities are discovered.

Path	Purpose	Field	Values
/v1/companies/company_guid/observations	GET: Detailed Company Observations	risk_type	server_software
/v1/companies/company_guid/findings	GET: Finding Details	risk_vector	server_software

⇧ Back to Directory

Desktop Software

The Desktop Software risk vector compares the version information of laptop and desktop software with the latest and currently available software versions to determine if the device software is supported or out-of-date.

Path	Purpose	Field	Values
/v1/companies/company_guid/observations	GET: Detailed Company Observations	risk_type	endpoint_pc
/v1/companies/company_guid/findings	GET: Finding Details	risk_vector	desktop_software

⇧ Back to Directory

Mobile Software

The Mobile Software risk vector compares the version information of mobile device operating systems and browsers with the latest and currently available software versions to determine if the device software is supported or out-of-date.

Path	Purpose	Field	Values
/v1/companies/company_guid/observations	GET: Detailed Company Observations	risk_type	endpoint_mobile
/v1/companies/company_guid/findings	GET: Finding Details	risk_vector	mobile_software

⇧ Back to Directory

DNSSEC

The DNSSEC risk vector determines if a company is using the DNSSEC protocol, which is a public key encryption that authenticates DNS servers, and then assesses the effectiveness of its configuration. The DNSSEC protocol protects against DNS spoofing, which involves diverting traffic to an attacker's computer, creating an opportunity for loss of confidentiality, data theft, etc.

Path	Purpose	Field	Values
`/v1/companies/company_guid/observations`	GET: Detailed Company Observations	`risk_type`	`dnssec`
`/v1/companies/company_guid/findings`	GET: Finding Details	`risk_vector`	`dnssec`

⇧ Back to Directory

Mobile Application Security

The Mobile Application Security risk vector analyzes the security aspects of an organization's mobile application offerings that are publicly available in official marketplaces, such as the Apple App Store and Google Play.

Path	Purpose	Field	Values
`/v1/companies/company_guid/observations`	GET: Detailed Company Observations	`risk_type`	`mobile_application_security`
`/v1/companies/company_guid/findings`	GET: Finding Details	`risk_vector`	`mobile_application_security`

⇧ Back to Directory

Domain Squatting

The Domain Squatting risk vector detects the presence of domains named similarly to those that are owned and trademarked by an organization. Detection for these types of domains is based on information provided by DNS queries.

User Behavior

The User Behavior risk category assesses employee activity, such as file sharing and password re-use.

File Sharing

The File Sharing risk vector tracks the sharing of files, such as books, music, movies, TV shows, and applications. This includes files shared over the BitTorrent protocol or when observed on company infrastructure.

Exposed Credentials

The Exposed Credentials risk vector indicates if a company's employees have had their information disclosed as a result of a successful cyber attack on external third parties and also helps identify breached sites and the types of information that were exposed.

Public Disclosures

The Public Disclosures risk category provides information related to possible incidents of undesirable access to a company's data, including breaches, general security incidents, and other disclosures. Information is collected from verifiable news sources, both domestic and international, and by filing Freedom of Information Act (FOIA) requests.

Security Incidents

The Security Incidents risk vector involves a broad range of events related to the undesirable access of a company's data or resources, including personal health information, personally identifiable information, trade secrets, and intellectual property. They're grouped into Breach Security Incidents and General Security Incidents.

Other Disclosures

The Other Disclosures risk vector includes other kinds of publicly disclosed events. It's considered to be the least severe among the Public Disclosures risk vectors.

API Fields: Finding Grades

Diligence findings are graded as GOOD, FAIR, WARN, BAD, or NEUTRAL based on its inherent risk and how best practices can be improved upon. These finding grades contribute towards the letter grade of the risk vector.

Finding grades are not applicable (N/A) to Compromised Systems and User Behavior.

Slug Name	Description
`good`	Low risk, aligned with best practices. These have a significantly positive impact on the letter grade.
`fair`	Light risk and some opportunity to achieve best practices. These have a minor negative impact or no impact on the letter grade depending on the risk vector.
`warn`	Moderate risk and departure from best practices. These have a moderately negative impact on the letter grade.
`bad`	Significant risk and departure from best practices. These have a significantly negative impact on the letter grade.
`neutral`	Observed data with neither positive nor negative risk. This does not positively or negatively impact the letter grade.
`na`	Finding grades are not applicable (N/A) to Compromised Systems and User Behavior.

API Fields: Subscription Types

Unused credits expire at the end of the subscription term.

Subscription Type	Description	Slug Name
Risk Monitoring	Provides a broad range of coverage with your third parties, while still showing visibility into their security ratings and the ability to take action when it matters most. The continuously updated rating provides the current picture of a third party's security posture so you can be confident about when to dig in deeper based on the alert thresholds that are set.	`alerts-only`
Applicants	60-day subscription for Cyber Insurance.	`applicants`
Total Risk Monitoring	Provides robust, continuous monitoring capabilities, giving you the highest level of visibility for monitoring third parties.	`continuous_monitoring`
National Cybersecurity	BitSight Security Ratings for countries.	`countries`
Rapid Underwriting Assessments	Quickly get rating details for any mapped or unmapped company within 1 minute. This is a "pay-per-use" service that goes through a standard invoicing process for each API request, including multiple requests for the same rating report.	
Risk Assessor	Provides flexibility when onboarding third parties and allows periodic assessments without taking away from your larger pool of subscriptions that are used to continuously monitor existing third parties.	
My Company	Continuously monitor your own organization with IP address visibility. Includes Forensics.	
SPM Subsidiary	Provides Total Risk Monitoring for companies in your Ratings Tree.	`my_subsidiary`
My Company Lite	Provides continuous monitoring for your own organization with IP address visibility.	

One-Time	5-day subscription to a selected organization. Reports must be used within 1 year of purchase.	`one-time`
Time-Limited	• Get information about companies you are monitoring. • Get security rating reports for a limited amount of time.	
Vendor Selection	30-day subscription to the security rating of a selected organization. Continuously monitor each organization that is added as a third party. • Expires at the end of the subscription term. • For multi-year subscriptions, the pack is annually replaced with a new one before the end of the term. • Unused subscriptions expire at the end of the subscription term.	`vendor-selection`

API Fields: User Roles

A user can have multiple roles. Permissions are based on the following user roles:

Role	Description	Slug Name
Admin	Full administrative access to the BitSight account, including having insight into product usage of various users and the ability to delegate the management of portfolios to division leaders and other departments. Admins can create groups, modify groups, add users to any group, change the company limit for each group, change distribution list settings, and add companies to any group.	`customer_admin`
Group Admin	This user is associated with an Access Control Group. Companies can put multiple Group Admin in place, each of whom would be responsible for a business unit, department, or country division, without needing to provide the full administrative privileges of an Admin. Group Admin do not see that they are in a group. Group Admin can modify other users and companies for their group; including add or remove companies to the group, add or remove users to the group, and add other Group Admins to their group. They cannot modify an account's distribution list settings, add additional groups, change group limits, modify users who are not part of the group, or promote users to an Admin.	`customer_group_admin`
Portfolio Manager	This user is associated with an Access Control Group. Companies can put multiple Portfolio Managers in place, each of whom would be responsible for a business unit, department, or country division, without needing to provide the full administrative privileges of an Admin. Portfolio Managers can add companies to their group. They cannot modify an account's distribution list settings, add additional groups, change group limits, or create and manage users for their group.	`customer_portfolio_manager`
User	This is a "read-only" role that cannot make any significant changes to the organization's settings or subscriptions. This basic access role has full access to the BitSight Security Ratings Platform and all add-ons the organization has purchased. Users can view companies in the portfolio, create and share folders, submit support tickets, examine events, download/export documents (PDF and CSV).	`customer_user`