BITSIGHT KNOWLEDGE BASE

Alerts API Endpoint

Publication Date – February 27, 2020

Alerts API Endpoint

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

This provides a list of the most recent alerts generated by the platform and detailed information for single alerts.

Change the conditions for alerts from the Alert Preferences page.

> ℹ This endpoint is paginated using the `limit` and `offset` parameters. It will return the most recent 100 alerts by default.

Paths

Path	Purpose	Description	Method
`/`	Alerts	Get an array that consists of alert objects.	GET
`/latest`	Recent Alerts	Get an array of alerts that were generated on the most recent date.	GET

Version 1 Paths

> ! **Note:** Version 2 is now available.

Path	Purpose	Description	Method
`/`	Alerts [Deprecated]	Get an array that consists of alert objects.	GET
`/latest`	Latest Alerts [Deprecated]	Get an array of alerts that were generated on the most recent date.	GET
`/percent/{alert_guid}/`	Alert Details	Use the “href” URI from any of the alerts returned by the API for details about any of your alerts.	GET
`/vulnerability/{vulnerability_alert_guid}?format=json`	Vulnerability Alert Details	Get the details of a Vulnerability and Infections alert.	GET

GET: Alerts

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

Get a list of your existing alerts and their details.

Example Request

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

URL - Recent Alerts

Use the following path to return an array of alerts that were generated on the most recent date.

```
https://api.bitsighttech.com/ratings/v2/alerts/latest
```

Example Request - Recent Alerts

Refer to the parameters available for this endpoint to filter by date.

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

Example Response

The `results` key is a list (array) of alert objects.

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

"next":"https://api.bitsighttech.com/ratings/v2/alerts/?limit=100&offset=100"
   },
   "count":12345,
   "results":[
[…]
      {
         "guid":12345678,
         "alert_type":"RISK_CATEGORY",
         "alert_date":"2019-07-10",
         "start_date":"2019-07-09",
         "company_name":"Example, Inc.",
         "company_guid":"e8d8503e-beae-4d6a-add4-5666c5491881",
         "company_url":"/company/e8d8503e-beae-4d6a-add4-5666c5491881/",
         "folder_guid":"02fa3d99-dfe5-4695-a26a-fa0a6f1ff98b",
         "folder_name":"Continuous Monitoring",
         "severity":"WARN",
         "trigger":"Insecure Systems"
      }
   ]
}
```

Response Attributes

Key	Description	Data Type
`links`	Contains navigation links for pagination.	Object
`previous`	Navigate to the previous page.	String [URL]
`next`	Navigate to the next page.	String [URL]
`count`	The total number of alerts across all the pages.	Integer
`guid`	The unique identifier of this alert.	String
`alert_type`	The type of condition that triggered the alert. See alert types.	String [Slug]
`alert_date`	The date when the alert is generated.	String [YYYY-MM-DD]
`start_date`	The start date of the alert period.	String [YYYY-MM-DD]
`company_name`	The name of the company that triggered the alert.	String
`company_guid`	The unique identifier of the company that this alert was generated for.	String
`company_url`	The path to this company's overview page in the BitSight Security Ratings Platform.	String [URL]
`folder_guid`	The unique identifier of the folder for which the alert was created. This may be your "All Companies" folder if the company was not in a specific folder.	String
`folder_name`	The name of this folder.	String
`severity`	The level of change that generated this alert. See alert severity.	String
`trigger`	The type of data that generated this alert.	String

GET: Alerts [Deprecated]

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

Get a list of your existing alerts and their details.

> ! Version 2 is now available.

Example Request

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

Example Response

The entire response is an array, consisting of alert objects.

```
[
    {
        "alert_type": "PERCENT_CHANGE",
        "company_guid": "b940aa61-42c9-33c4-9233-d8194c305db3",
        "href": "https://api.bitsighttech.com/ratings/v1/alerts/percent/1029",
        "company_name": "Saperix, Inc.",
        "alert_date": "2017-02-18",
        "guid": 1029,
        "folder_guid": "cb7ea5c9-e58f-4f85-a45c-6642c11d07ea"
    },
     {
        "alert_type": "RATING_THRESHOLD",
        "company_guid": "e8307b19-2d54-945e-add7-85163c99289a",
        "href":
"https://api.bitsighttech.com/ratings/v1/alerts/threshold/1031",
        "company_name": "Insurance Services, Inc.",
        "alert_date": "2017-03-18",
        "guid": 1031,
        "folder_guid": "cb7ea529-e58f-4f85-a45c-ac42c11d07ea"
    }
]
```

Response Attributes

Key	Description	Data Type
`alert_type`	The type of condition that triggered the alert. See alert types.	String
`company_guid`	The unique identifier of the company that this alert was generated for. > **Portfolio Quality Alerts:** This value will be "`none`."	String
`href`	URI of the alert API resource, which contains additional details about the alert. Make an API call directly to this URI to return detailed information about the alert.	String
`company_name`	The name of the company that triggered the alert. > **Portfolio Quality Alerts:** This value will be "`none`."	String
`alert_date`	The date when the alert was generated.	String [YYYY-MM-DD]
`guid`	The unique identifier of the alert.	Integer
`folder_guid`	The unique identifier of the folder for which the alert was created. This may be your "All Companies" folder if the company was not in a specific folder.	String

GET: Latest Alerts [Deprecated]

`https://api.bitsighttech.com/ratings/v1/alerts/latest`

This endpoint returns an array of alerts that were generated on the most recent date.

> ! Version 2 is now available.

Example Request

Refer to the parameters available for this endpoint to filter by date.

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

Example Response

```
[
    {
        "guid": 1029,
        "alert_date": "2016-07-01",
        "company_name": "Saperix, Inc.",
        "company_guid": "b230aa61-42c9-33c4-9233-d8194c305ef0",
        "href": "https://api.bitsighttech.com/ratings/v1/alerts/percent/1029",
        "alert_type": "PERCENT_CHANGE"
    },
    {
        "guid": 1031,
        "alert_date": "2016-07-01",
        "company_name": "Insurance Services, Inc.",
        "company_guid": "d8306b19-2e11-945e-add7-85163c88289a",
        "href":
"https://api.bitsighttech.com/ratings/v1/alerts/threshold/1031",
        "alert_type": "THRESHOLD"
    }
]
```

Response Attributes

Key	Description	Data Type
`guid`	The unique identifier of the alert.	Integer
`alert_date`	The date when the alert was generated.	String [YYYY-MM-DD]
`company_name`	The name of the company that triggered the alert. **Portfolio Quality Alerts:** This value will be `none`.	String
`company_guid`	The unique identifier of the company that this alert was generated for. **Portfolio Quality Alerts:** This value will be `none`.	String
`href`	The URI of the alert API resource, which contains additional details about the alert. Make an API call directly to this URI to return detailed information about the alert.	String
`alert_type`	The type of condition that triggered the alert. See alert types.	String

GET: Alert Details

https://api.bitsighttech.com/ratings/v1/alerts/percent/alert_guid

Use the “href” URI from any of the alerts returned by the API for details about any of your alerts. Each request will return a single alert object.

Example Request

Refer to the parameters available for this endpoint to filter by date.

```
curl https://api.bitsighttech.com/ratings/v1/alerts/percent/1029 -u api_token:
```

Example Response

```
{
    "guid": 1029,
    "alert_date": "2015-02-01",
    "company_name": "Saperix, Inc.",
    "company_guid": "b940aa61-42c9-33c4-9233-d8194c305db3",
    "start_date": "2017-01-30",
    "start_rating": 710,
    "end_rating": 650,
    "folder_guid": "cb7ea5c9-e58f-4f85-a45c-6642c11d07ea",
    "company_url": "/company/15379",
    "rating_change_pct": -5,
    "alert_severity": "WARN",
    "alert_type": "PERCENT_CHANGE"
}
```

Response Attributes

Key	Description	Data Type
`guid`	The unique identifier of the alert.	Integer
`alert_date`	The date when the alert was generated.	String [YYYY-MM-DD]
`company_name`	The name of the company that triggered the alert.	String
`company_guid`	The unique identifier of the company that this alert was generated for. **Portfolio Quality Alerts:** This value will be `none`.	String
`info_category`	The corresponding risk category for this alert, e.g. "Exposed Credentials." **Informational Alerts only.**	String
`message`	Additional details about this alert. **Informational alerts only.**	String
`start_date`	The date when the rating was observed before the change.	String [YYYY-MM-DD]
`start_rating`	The company's security rating during the start date. **Percent Change and Threshold alerts only.**	Integer
`end_rating`	The company's security rating when the alert was generated. **Percent Change and Threshold alerts only.**	Integer
`folder_guid`	The unique identifier of the folder where the alert was created. This may be your "All Companies" folder if the company was not in a specific folder.	String
`company_url`	Append this to "bitsight.com" to visit the company's security rating overview page directly.	String
`rating_change_pct`	A positive or negative number indicating the percentage change in rating, from the start date to the end date. **Percent Change alerts only.**	Integer

`alert_severity`	Indicators used for all types of alerts. For a Decrease and Critical Decrease rating level, an alert is generated when the ratings reach or cross below the level. For Increase thresholds, the alert is generated when the ratings reach or cross above the level. See alert severity.	String
`rating_threshold`	The rating that the alert preference threshold was set to. **Rating Threshold alerts only.**	String
`risk_category`	The corresponding risk type for this alert. See risk types. Risk Vector Grade alerts only.	String
`start_grade`	The starting grade for the alert. **Risk Vector and NIST CSF (grade change) alerts only.**	Integer
`end_grade`	The ending grade for the alert. **Risk Vector and NIST CSF (grade change) alerts only.**	Integer
`nist_category`	The corresponding NIST CSF category code for this alert, e.g. PR.PT. **NIST CSF alerts only.**	String
`nist_category_name`	The human-readable subcategory name, e.g. Proactive Technology. **NIST CSF alerts only.**	String
`grade_threshold`	The letter grade threshold that was crossed when the alert was generated. **NIST CSF alerts only.**	String
`alert_type`	The type of condition that triggered the alert. See alert types.	String

GET: Vulnerability Alert Details

https://api.bitsighttech.com/ratings/v1/alerts/vulnerability/vulnerability_alert_guid?format=json

Use this path to get the details of a vulnerability and infections alert. The Vulnerabilities and Infections alert type allows you to filter and get alerts on infections and vulnerabilities that affect companies in your portfolio.

- Only available if the Vulnerability and Infection alert is enabled.
- Not available for Alerts Only, Countries, and Applicants subscription types.

Example Response

```
{
   "guid":1,
   "alert_date":"1980-03-28",
   "company_name":"Example Company",
   "company_guid":"dd231077-fb19-46ba-9dd0-0884c8d48624",
   "start_date":"1981-06-09",
   "folder_guid":"a1c5a0d5-6226-45c4-897d-e9c9144bff98",
   "company_url":"/company/dd231077-fb19-46ba-9dd0-0884c8d48624/",
   "alert_type":"VULNERABILITY",
   "alert_severity":null,
   "message":"test message"
}
```

Response Attributes

Key	Description	Data Type
guid	The unique identifier of this alert.	String
alert_date	The date when the alert is generated.	String [YYYY-MM-DD]
company_name	The name of the company that triggered the alert.	String
company_guid	The unique identifier of the company that this alert was generated for.	String
start_date	The start date of the alert period.	String [YYYY-MM-DD]
folder_guid	The unique identifier of the folder for which the alert was created. This may be your "All Companies" folder if the company was not in a specific folder.	String
company_url	The path to this company's overview page in the BitSight Security Ratings Platform.	String [URL]
alert_type	The type of condition that triggered the alert. This path always has the value, "VULNERABILITY." See all alert types.	String
alert_severity	The level of change that generated this alert. The "VULNERABILITY" alert type is always "INFORMATIONAL." See alert severity.	String
message	Describes the vulnerability or infection that triggered this alert.	String

Parameters

Path Parameters

`company_guid`

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

`folder_guid`

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

Query Parameters

Parameter	Description	Value
`alert_date` *[string, query]*	Filter alerts by the specified alert date.	`YYYY-MM-DD`
`alert_date_gt` *[string, query]*	Filter alerts after the requested date. ! This parameter is incompatible with `alert_date`.	`YYYY-MM-DD`
`alert_date_gte` *[string, query]*	Filter alerts after or on the requested date. ! This parameter is incompatible with `alert_date`.	`YYYY-MM-DD`
`alert_date_lt` *[string, query]*	Filter alerts prior to the requested date. ! This parameter is incompatible with `alert_date`.	`YYYY-MM-DD`
`alert_date_lte` *[string, query]*	Filter alerts prior to or on the requested date. ! This parameter is incompatible with `alert_date`.	`YYYY-MM-DD`
`alert_type` *[string, query]*	Filter alerts by the specified alert type.	See alert types.
`company_guid` *[string, query]*	Filter alerts by the specified company unique identifier.	See GET: Portfolio Details.
`expand` *[string, query]*	If `expand=details` is set, the return will include additional alert details.	See alert details.

`folder_guid` *[string, query]*	Filter alerts by the specified folder unique identifier.	See GET: Folder Details.
`limit` *[integer, query]*	Set the maximum number of records to return in a response.	**Default:** 100
`offset` *[integer, query]*	Set the page to start returning records from.	A `0` (zero) or no value will cause the results to start with the first record of the result set.
`q` *[string, query]*	Full-text search for matching records.	Company name.
`severity` *[string, query]*	Filter alerts by the specified severity level.	See alert severity.
`sort` *[string, query]*	Sort the alerts by the specified parameters, separated by a comma. Alerts are sorted by `alert_date`, by default.	• `guid` • `alert_date` • `alert_type` • `company_name` • `folder_name` • `trigger` • `severity`

Alert Details

When `expand=details` is set, you will see the following fields:

Percent Change

- `rating_change_pct` = Percent rating change.
- `start_rating` = The security rating on the `start_date`.
- `end_rating` = The security rating on the `alert_date`.

Rating Threshold

- `rating_threshold` = The rating threshold that was crossed to generate the alert.
- `start_rating` = The security rating on the `start_date`.
- `end_rating` = The security rating on the `alert_date`.

Risk Category/Risk Vector

- `risk_vector` = The risk vector that triggered the alert.
- `start_grade` = The risk vector letter grade on the `start_date`.
- `end_grade` = The risk vector letter grade on the `alert_date`.
- `threshold_grade` = The grade that was reached or crossed to generate the alert.

NIST Category

- `nist_category` = The NIST category that triggered the alert.
- `nist_category_display_name` = The display name of the NIST category.
- `start_grade` = The NIST category letter grade on the `start_date`.
- `end_grade` = The NIST category letter grade on the `alert_date`.
- `threshold_grade` = The grade that was reached or crossed to generate the alert.

Informational

- `category` = The informational category of alert. This currently includes only Exposed Credentials.

`message` = Detailed information on why the informational alert was triggered.

Alert Severity

These indicate the level of change that generates an alert.

Key	Description
`INFORMATIONAL`	
`INCREASE`	⌃ Increase - Indicates the company's cybersecurity risk is decreasing and their posture is improving.
`WARN`	⌄ Decrease - Indicates when a company is starting to have trouble responding to security issues. Their security rating slightly decreased, so their risk started to increase.
`CRITICAL`	︾ Critical Decrease - Indicates the company needs to significantly improve their response times to new issues or has a history of delayed risk preparedness.

Alert Types

Each of the alert types help your organization better monitor the security performance of your portfolio.

ⓘ These are case-sensitive and are all in uppercase letters.

Value	Type	Description
`INFORMATIONAL`	Informational Risk Vectors	Receive alerts when new information is available for informational risk vectors. This is currently used for only Exposed Credentials.
`NIST_CATEGORY`	NIST CSF Grade Change	Receive alerts when National Institute of Standards and Technology CyberSecurity Framework (NIST CSF) grades cross or reach a set threshold.
`PERCENT_CHANGE`	Percent Change	Receive alerts when security ratings change by a set percentage.
`RATING_THRESHOLD`	Rating Threshold	Receive alerts when security ratings cross or reach a set threshold.
`RISK_CATEGORY`	Risk Vector Letter Grade Change	Receive alerts when risk vector letter grades cross or reach a set threshold.
`VULNERABILITY`	Vulnerabilities and Infections	Filter and get alerts on vulnerabilities and infections that affect companies in your portfolio.