**BitSight Security Performance Management for Splunk Add-on Installation Guide**

**Updated 2022-01-12**

**Table of Contents**

[***Introduction 1***](#_gjdgxs)

[***Prerequisites 2***](#_30j0zll)

[***Architecture 2***](#_1fob9te)

[***Installation 3***](#_3znysh7)

[***Use Cases 6***](#_tyjcwt)

[***Upgrade instructions 7***](#_3dy6vkm)

[***Reference Material 7***](#_1t3h5sf)

# Introduction

**BitSight Security Performance Management for Splunk**

BitSight Security Performance Management (SPM) supports evidence-based cyber risk monitoring, enabling security leaders to define the performance standards most appropriate for their organization, and manage the work required to achieve those standards. A fundamental tenet of BitSight’s SPM solution is the ability to contextualize an organization’s cybersecurity performance over time. Leveraging meaningful metrics that are independently verified to correlate to breach risk, this view of “performance over time” ultimately guides the organization in its effort to reduce cyber risk to achieve desired business outcomes. The advanced security performance analytics facilitate a universal understanding of the organization’s cyber risk aiding business leaders and board members delivery of effective cybersecurity program oversight for the organization.

Security leaders and their teams rely on BitSight SPM to:

* + Continuously monitor the effectiveness of security controls
	+ Facilitate uniform performance targets across the organization
	+ Provide in-depth comparisons of the organization’s cybersecurity performance against peers
	+ Streamline program management decisions, including the ongoing remediation of security controls
	+ Communicate program performance to non-technical stakeholders using meaningful context

Bring BitSight Security Ratings findings information into your security program through this add-on for *Splunk Enterprise* and *Splunk Enterprise Security*. The integration automatically maps the BitSight risk vectors to Splunk’s Common Information Model to enable relevant workflows based on the observations from the BitSight data.

This visibility enables you to pinpoint and control the sources of infections in your company infrastructure, seamlessly going from awareness to rapid remediation. The observations forensics reveal source ports, destination ports, malware command-and-control IP addresses, and more to assist your company in connecting the security and IT teams to respond faster and more effectively to threats.

**BitSight Work from Home - Remote Office**

With the significant increase in remote work, *BitSight Work from Home - Remote Office* allows you to query your VPN logs and detect systems, which may be at risk, that are remotely connecting to your network. BitSight Security Performance Management for Splunk allows a user to quickly identify home office IP addresses by leveraging the Network Sessions data model to use available log sources in Splunk like VPNs logs. Those IPs are then used to gather security risk observations from BitSight. These observations can be used to:

* Discover security issues that reside on work from home IPs to help inform existing incident response or insider threat activities.
* Monitor higher risk remote operating environments, such as access to sensitive data or intellectual property (e.g., Exes, software devs).
* Educate employees on potential security issues as part of security training & awareness programs.

# Prerequisites

This add-on and app requires a BitSight Security Ratings *Security Performance Management* subscription for your organization, as well as Splunk Enterprise or Splunk Enterprise Security. It is compatible with both on-premise or SaaS Splunk instances. This application is built using Python, which should be included by default in Splunk.

# Architecture

The BitSight Splunk add-on leverages the BitSight API to retrieve ratings and risk vector level findings information, as well as infections and vulnerabilities. The BitSight data is updated every 24 hours. When the BitSight Security Performance Management for Splunk add-on is run, it will retrieve the following data:

| **Paths** | **Descriptions** |
| --- | --- |
| /diligence/statistics  | Get diligence statistics of an organization |
| /observations  | Retrieve detail information about risk category data of companies in the Company's portfolio |
| /industries/statistics  | Get observation statistics of an organization and industry by risk vector |
| /findings/summary  | Get Findings Present Summary data for a folder |
| /assets/findings  |  Get observations with asset information for company  |
| /observations/statistics | Get observation statistics of an organization  |
| /graph\_data  | Get ratings graph data for a folder  |
| /diligence/historical-statistics  | Get entity diligence findings counts |
| v2/alerts | Get alerts triggered in an organization |

The BitSight findings are mapped to the [Splunk Common Information Model](https://docs.splunk.com/Documentation/CIM/4.15.0/User/Overview), which links the BitSight findings to some default views in Spunk.

*Mapping to Splunk’s Common Information Model*

| **Splunk Model** | **Risk Vector or Risk Type** |
| --- | --- |
| Intrusion Detection / Malware | Compromised Systems |
| Endpoint / Ports | Open Ports / Web Application Headers / Server Software |
| Certificates | SSL Certificates |
| Vulnerabilities | Patching Cadence |
| Web | Potentially Exploited / Insecure Systems |
| Data Loss Prevention | Breach / Exposed Credentials |
| Network Resolutions (DNS) | SPF / DKIM / DNSSEC |

# Installation

The BitSight Security Performance Management for Splunk add-on and app is available for download in the *Splunkbase*. Sign in to *Splunkbase* and download the latest version available.

The user role with which the add-on will be configured should have Search capabilities. (usually available for admin roles)

**NOTE:** The BitSight for Security Performance Management Add-on is intended for use with BitSight SPM licenses for 1st party visibility into your organization’s security posture. You must have a BitSight SPM license (such as MyOrg) in order to use this Add-on. To learn more, please contact your BitSight representative.

Once you have downloaded the packages, please follow the steps outlined below:

*Install apps and add-ons from within Splunk Enterprise:*

1. Log in to Splunk Enterprise.

2. On the Apps menu, click **Manage Apps**.

3. Click **Install app from file**.

4. In the Upload app window, click **Choose File**.

5. Locate the .tar.gz file you just downloaded, and then click **Open or Choose**.

6. Click **Upload**.

7. Click **Restart Splunk**, and then confirm that you want to restart.

*Install apps and add-ons directly into Splunk Enterprise:*

1. Put the downloaded file in the $SPLUNK\_HOME/etc/apps directory.

2. Untar and unzip your app or add-on, using a tool like tar -xvf (on \*nix) or WinZip (on Windows).

3. Restart Splunk.

4. After you install a Splunk app, you will find it on Splunk Home.

Once the add-on is installed, it can be accessed from the Apps menu on the left.



**How to Configure the Add-on**

Once you open the add-on, you will see the following tabs:

* *Inputs:* Configure your add-on to connect to BitSight.
* *Configuration:*
	+ Proxy: Define proxy settings.
	+ Logging: Define log level
	+ Authentication: Provide BitSight API URL and BitSight API Token
		- BitSight API URL: Provide BitSight API URL
		- BitSight API Token: Please enter your BitSight API token, which is retrieved from the BitSight platform. Best practice is to create an API token specifically for use in the application, as opposed to a specific user token, to ensure the token can be used without breaking existing integrations if certain users' accounts are deactivated. Please create an email alias specifically for the integration and generate a token leveraging this email alias, to ensure that the integration does not depend on a specific user’s email address.

In order to generate an API token, login to your BitSight portal → click on the gear icon at the top right and select Account → scroll to the bottom of the page where you can generate a new 'API token' or use an already created token → Copy the API Token and paste it in the field labeled as such in Splunk. Remember, your API token should be treated as a password. If you think your token may have been compromised, you can always generate a new one from the same page, which will make the old one invalid.



* + Work From Home: Enter the index in which you want to ingest data from wfh custom command. Make sure the index exists.
* *My Company:* View prebuilt dashboard panels with BitSight observations.
* *Search:* Correlate BitSight data with other data in Splunk.
* *Work from Home - Remote Access:* Use Splunk’s search capability in conjunction with BitSight to monitor issues with remote users connected to your network.

In the *Inputs* tab you will need to provide the following information:

Name - The name of this configuration set.

*Interval* - How often the BitSight data should be pulled (measured in seconds). By default, this is 86400 seconds (once per day). Users should leave this setting as is, as the BitSight ratings and ratings data are refreshed once per day.

*Index* - The index where you want to log BitSight data to.

*Start Date* - The date (UTC in "YYYY-MM-DD" format) from when to start collecting the data. The default value taken will be 90 days ago. Earliest allowed date is 400 days before today.

*Companies -* Select the companies for which you want to collect data. It will take a few seconds to populate.



**Configuration**

The Proxy tab includes controls to enable proxy settings required by your organization. Allows you to define the host, port, and credentials for use with your organization’s proxy configuration.

The Logging tab allows you to select the level of activity logging you want to capture for the add-on.

The Authentication tab allows you to configure the BitSight API URL and BitSight API Token.

The Work From Home tab allows you to configure the Custom Command Index in which you want to ingest data from wfh custom command. Make sure the index exists

**BitSight Work from Home - Remote Office**

Use Splunk’s Network Sessions data model to pull residential IPs associated with your remote workforce’s VPN connections. Search results will show any BitSight observations, specifically any Compromised Systems or Open Port findings, associated with those IP observations in the last 30 days.

If you want to specify a customer query instead of using the Network Session data model:

1. Go to **Settings > Searches, Reports, Alerts**:
2. Select the **Work From Home IPs**:

3. Edit the query in the Edit Search window:



Custom search queries should return IP address. The query results must be sent to “src\_ip | wfh” to function correctly. For example:

 \*\*search\_query\*\* | eval src\_ip = source\_ip | table src\_ip | wfh

If you specify your own search, there is a limit of one request every ten minutes to allow for processing potentially very large data sets. The BitSight Work from Home query needs to end in “src-ip”, and the job is picked up every ten minutes. The feature does not support IPV6 addresses.

# Use Cases

*BitSight Security Performance Management for Splunk*

Bring BitSight findings data into Splunk. This visibility enables you to pinpoint and control the sources of infections in your company infrastructure, seamlessly going from awareness to rapid remediation. The integration automatically maps the BitSight observations to Splunk’s Common Information Model to enable relevant workflows based on the BitSight observations data.

* Enriching the security data you already have with BitSight’s external view of compromised systems.
* Leverage Splunk’s workflows to prioritize and assign BitSight discovered incidents for faster response and track remediation efforts.
* Link security incident to related systems, users, and business services within your organization for faster remediation and identification of process failure cause.
* Track in real-time and report post-incident to holistically understand security posture and demonstrate the efficacy of your security programs.

*BitSight Work from Home - Remote Office*

BitSight Work from Home - Remote Office helps security teams identify vulnerabilities and infections on IP addresses known to be associated with remote operating environments. BitSight Security Performance Management for Splunk allows a user to quickly identify home office IP addresses using available log sources in Splunk like VPNs logs, email server logs and other enterprise application logs. Those IPs are then used to gather security risk observations from BitSight. These observations can be used to:

* Discover security issues that reside on work from home IPs to help inform existing incident response or insider threat activities.
* Monitor higher risk remote operating environments such as access to sensitive data or intellectual property (e. Exes, software devs)
* Educate employees on potential security issues as part of security training & awareness programs

Use Splunk’s native search capabilities to collect lists of IP addresses from VPN logs, compare IPs to BitSight WFH findings, and populate existing dashboards with WFH findings in Splunk Enterprise or Splunk Enterprise Security.

# Upgrade instructions

This is the first version of the BitSight Security Performance Management for Splunk add-on. Updates will be documented here as they are made, as well as instructions for upgrade where relevant.

# Reference Material

**Can I run the add-on on demand or manually?**

You can run the add-on on demand or manually by disabling and then enabling a defined input. If an input is disabled and then enabled, the add-on will run immediately with the defined settings.



**How can I access the pre-built BitSight panels and alerts?**

The BitSight add-on comes with prebuilt panels as follows:

* Security Rating
* Count of Observations by Risk Vector
* Compromised Systems
* Infections
* Count of Diligence Observations
* Vulnerabilities

To access these panels, click **Settings** from the BitSight add-on, go to User Interfaces, and then click on **Prebuilt panels**.

**How can I stop the installation of the add-on from timing out?**

If you are experiencing timeout issues while installing the add-on in Splunk Web, please increase your timeout settings as per Splunk's suggestion:

https://docs.splunk.com/Documentation/AddOns/released/Overview/Troubleshootadd-ons#Increase\_timeout\_settings

**Prebuilt Alerts are as follows:**

To view prebuilt alerts, click **Settings** from the BitSight add-on and then go to *Searches, Reports, and Alerts*. The pre-built alerts are:

• Bad Open Ports discovered

• Compromised System

• Patching Cadence

• Vulnerabilities & Infections

**Example**: To see all Bad Open Ports Discovered by BitSight

**SPL query:**

index="Your\_Index" sourcetype="bitsight" | head 1 | spath "findings{}" output=Results

|stats count by Results

|eval \_raw=Results

|spath "id" output=id | spath "results{}" output=res

|stats count by id res | where id="open\_ports"

|eval \_raw=res | spath "risk\_category" output="Risk\_Category" | spath "risk\_vector\_label" output="Risk\_Vector" | spath details{}.grade output="Grade"| where Grade= "BAD" | spath details{}.diligence\_annotations.message output="Message" |spath "evidence\_key" output="Evidence Key" | spath "first\_seen" output="First\_Seen" | sort -"First Seen" | spath "severity" output="Severity"

|eval epochdate=strptime(First\_Seen, "%Y-%m-%d") |eval now=now()

|eval deltaDays = (now - epochdate)/86400 | where deltaDays < 4

|table "Risk\_Category", "Risk\_Vector", "Grade","Severity", "Evidence Key", "First\_Seen", "Message"

This will query all *Bad open ports* discovered in the last 4 days (e.g, replace the number 4 with 10 to see results for the last 10 days). From here, you can correlate this to any other logs indexed in your Splunk instance.

**How do I search for data?**

Splunk allows users to search for data by leveraging Search Processing Language (SPL). If you are not familiar with SPL, please refer to Splunk’s [documentation](https://www.splunk.com/en_us/resources/search-processing-language.html).

Once the BitSight add-on starts logging data to your Splunk instance, you can leverage SPL to query for the data. Below are a couple of examples to help you get started.

**Example #1:** Query for all data logged by BitSight.

To query for all data logged by BitSight, you can simply type in index= sourcetype=bitsight into the search bar. This query will return all observations logged by the BitSight add-on.

**Example #2:** Correlating BitSight data with data enrichment tools.

**NSlookup:**

For investigating an IP address using NSlookup, use the following correlation search:

Correlation query:

index= sourcetype="bitsight" |head 1| spath "observations.data{}" output=Results

| stats count by Results

| eval \_raw=Results

| spath forensics.host\_ip output=HostIP

| stats count by HostIP | where HostIP="XXX.XXX.XXX.XXX"

| nslookup host\_field=HostIP

**Virustotal:**

Correlation query:

index= sourcetype="bitsight" |head 1| spath "observations.data{}" output=Results

| stats count by Results

| eval \_raw=Results

| spath forensics.host\_ip output=HostIP

| stats count by HostIP | **where** HostIP=" XXX.XXX.XXX.XXX "

| **virustotal** ip=HostIP