



Recorded Future App for Splunk

Recorded Future, Inc

Table of Contents

1. Overview	1
2. Updates in V.2.3 (latest)	5
3. Upgrade App	6
4. Install	7
4.1. Requirements	7
4.2. Instructions	7
4.3. Install on a Search Head Cluster	8
5. Malware Threat Hunts	9
5.1. Threat Hunt Dashboard	9
5.2. Malware Threat Hunt	9
6. Alert Center	12
6.1. Limitation for the number of alerts	13
7. Alerting Rules	14
7.1. Setup	14
7.2. Classic Alerts Dashboard	14
7.3. Playbook Alerts Dashboard	15
8. Correlations	16
8.1. Correlation Types	16
8.2. When a correlation rule is saved	16
8.3. Correlation Dashboards	21
8.4. Technical Information	22
9. Enrichment Dashboards	23
9.1. Technical Information	23
10. Sigma Rules	24
10.1. Setup	24
11. Sigma Detections	26
12. Splunk Enterprise Security Integration	27
12.1. Install	27
12.2. Setup Correlations	27
12.3. Adaptive Response Threat Hunt	32
13. Collective Insights	34
13.1. Limit Detection Sharing for Organisations within a Multi-org Enterprise	34
14. Troubleshoot	36
14.1. Reports	36
14.2. Logs	36
14.3. Report Issue	37
15. Further Help	38
16. Technical documentation	39
17. Server-side dashboard generation	40
18. Customization of savedsearches	41

19. API documentation	42
20. Threat Hunting API	43
20.1. Threat hunt profiles	43
20.2. Threat hunt runs	45

Chapter 1. Overview

Recorded Future has partnered with Splunk to deliver robust intelligence directly into Splunk Enterprise and Enterprise Security. The integrations and their intelligence support correlation against internal telemetry data to detect high-risk IOCs, faster alert triage, and reduce time spent on manual research.

Splunk Enterprise Features

Correlations

Correlations detect malicious events with a low rate of false positives. Dedicated correlation views help shorten the time spent on event triage. All views provide full Context as to why the event is considered malicious - including the source of this information. Correlations Use Cases are available for IPs, domains, hashes, vulnerabilities, and URLs.

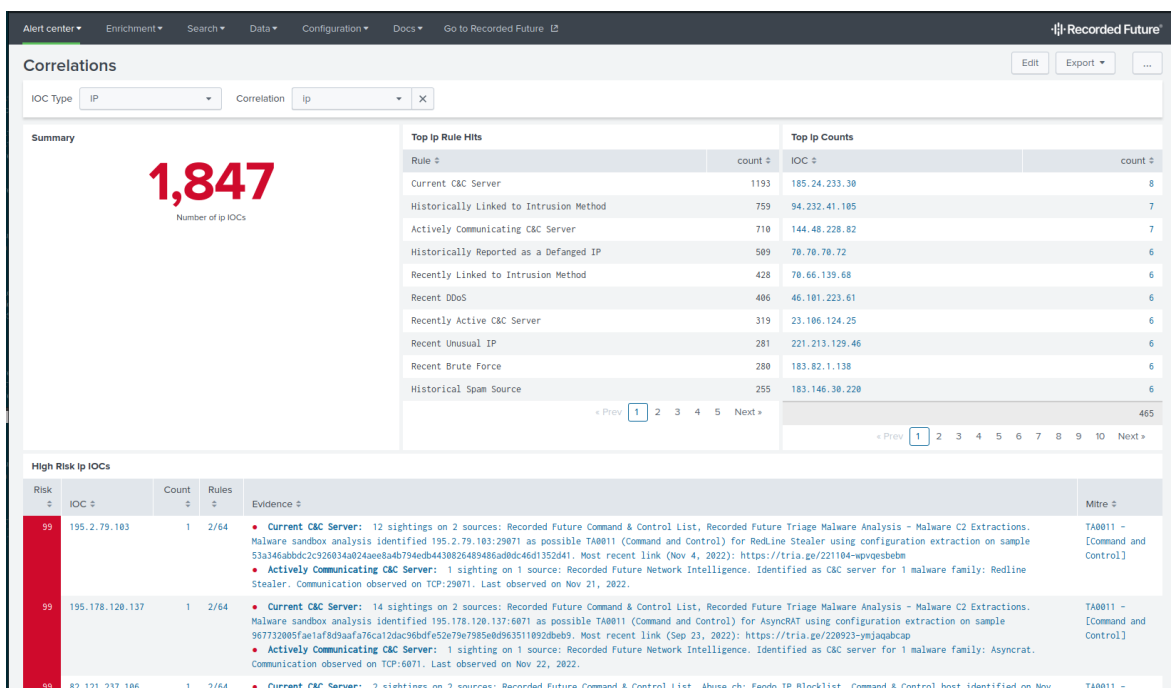


Figure 1. Correlation view

IOC Enrichment

Context (intelligence) for a suspicious IOC is often critical for deciding if an event is malicious. The app has several Enrichment views which present detailed intelligence about an IOC. Intelligence views are available for IPs, domains, hashes, vulnerabilities, URLs, and malware.

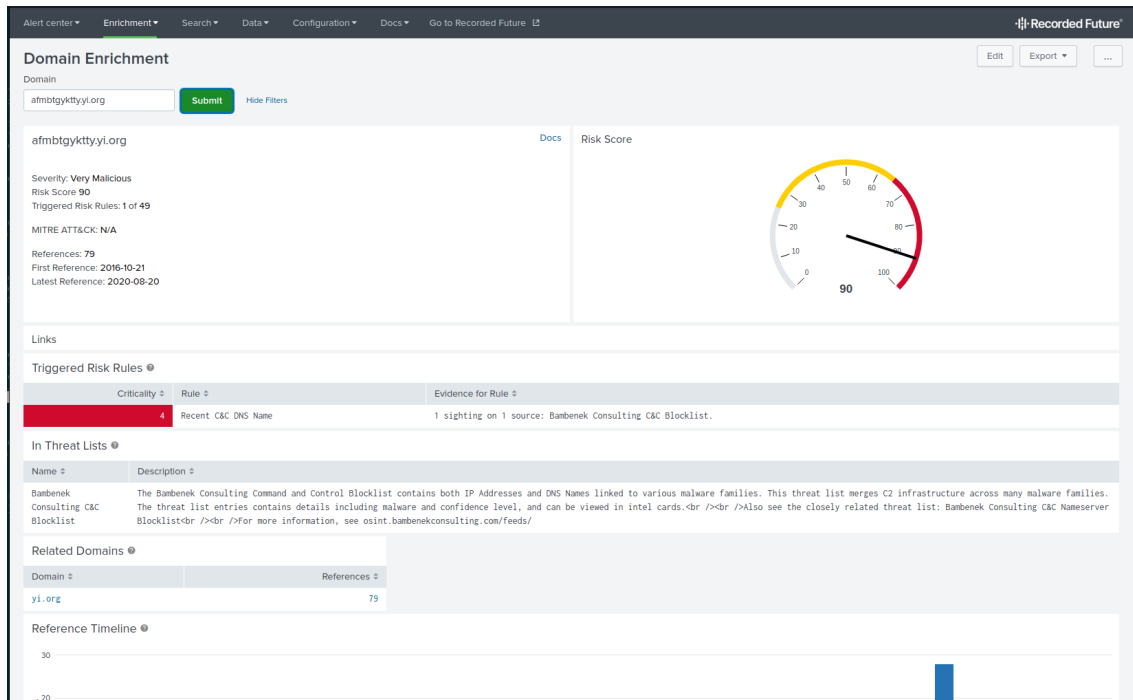


Figure 2. Enrichment view provides ample context for a suspicious IOC

Sigma Rules

With The Recorded Future App for Splunk, Sigma Rule deployment takes a few clicks. Recorded Future’s Insikt group produces Detection Rules (currently in Sigma, Snort, and YARA formats). All rules are converted from YML to saved queries in the Splunk Processing Language (SPL) format to make deployment as easy as possible.

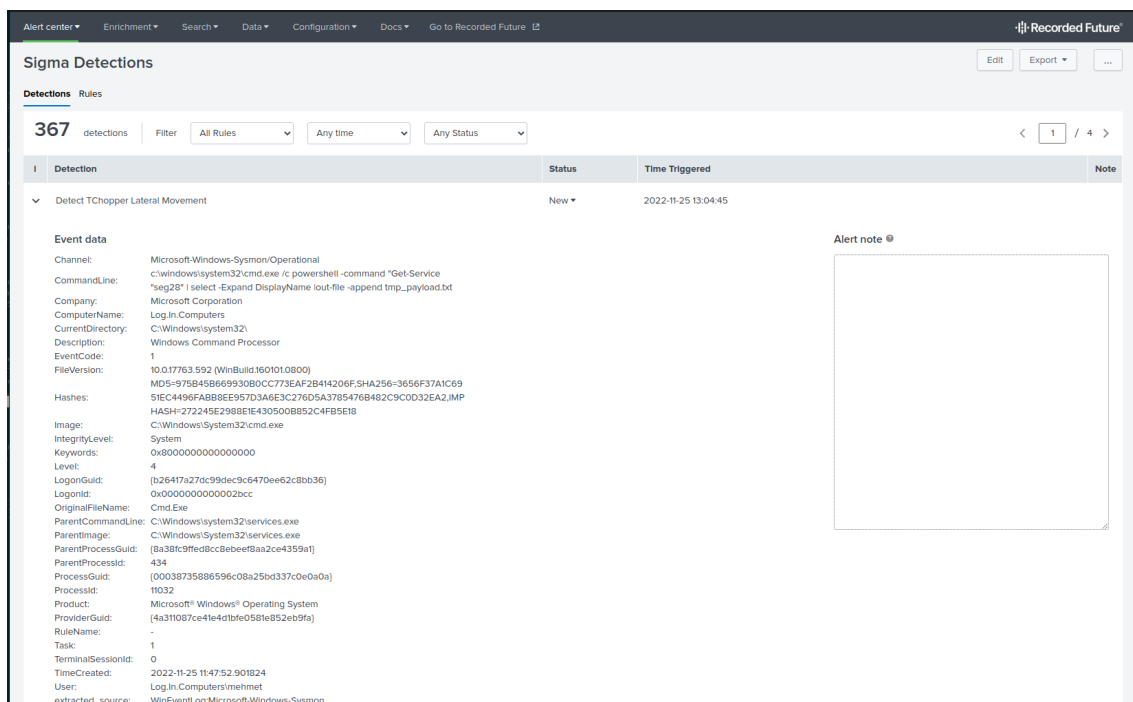


Figure 3. Sigma Detection Rules

Recorded Future Alerts

Recorded Future’s platform offers a wide range of Classical Alerts and Playbook alerts.

These alerts can be monitored and handled from within the app.

Alert	Time Triggered	Alert Type	Status	Note
> ● 70 Default IP risklist - 172.247.104.122	2022-11-25 12:08:06	Correlation	New ▾	
> ● 95 Default IP risklist - 103.242.0.140	2022-11-25 12:07:04	Correlation	In Progress ▾	
> ● 98 Default IP risklist - 82.157.61.211	2022-11-25 12:07:04	Correlation	In Progress ▾	📄
> ● 91 Default IP risklist - 102.157.237.191	2022-11-25 12:06:02	Correlation	New ▾	
> ● 95 Default IP risklist - 211.193.125.214	2022-11-25 12:05:00	Correlation	In Progress ▾	
> ● 78 Default IP risklist - 125.163.160.229	2022-11-25 12:05:00	Correlation	New ▾	
> Detect TChopper Lateral Movement	2022-11-25 12:04:00	Sigma Detection	In Progress ▾	📄
> Detect TChopper Lateral Movement	2022-11-25 12:02:58	Sigma Detection	New ▾	
> ● 96 Default IP risklist - 137.184.177.241	2022-11-25 12:02:56	Correlation	New ▾	
> ● 70 Default IP risklist - 114.34.171.53	2022-11-25 12:02:56	Correlation	New ▾	
> Detect TChopper Lateral Movement	2022-11-25 12:01:56	Sigma Detection	New ▾	

Figure 4. Recorded Future Alert

Splunk Enterprise Security Features

If the Splunk system has Splunk Enterprise Security installed, additional Threat detection options are available:

IOC Enrichment

Adaptive Response Action

An Adaptive response action makes it possible to provide Context to Notable events automatically. It's also possible to run the action ad-hoc.

Risk Based Alerting support

The app integrates with Splunk's Risk Based Alerting framework. Correlation searches that create Notable Events (which are handled in Splunk Enterprise's Incident review dashboard) can be set up for many Use cases. Each Notable Event contains a large amount of context for the detected IOC, including MITRE ATT&CK tags. However, correlations also produce Risk Events which over time helps tie together different suspicious events; and only surface what really matters as a Notable Event.

Incident Review

Search... Show Charts Hide Filters

Saved filters: Select... Add tags...
 Urgency: Select...
 Status: Select...
 Owner: Select...
 Security Domain: Select...
 Type: Select...
 Search Type: Correlation S... Select...
 Time or Associations: Time Last 24 ho...

Save new filters Update Clear all Submit
 Time Range: Last 24 hours

3334 Notables Unselect all Edit Selected Edit All Matching Events (3334) 1 Add Selected to Investigation
< Prev 1 2 3 4 5 ... Next >
20 per page Refresh

<input type="checkbox"/>	<input type="checkbox"/>	Title	Risk Object	Risk Score	Risk Events	Type	Time	Disposition	Security Domain	Urgency	Status	Owner	Actions
<input type="checkbox"/>	<input type="checkbox"/>	Default IP risklist	101.89.74	95	-	Risk Notable	Today, 1:50 PM	Undetermined	Threat	Critical	New	unassigned	

Description:
IOC detected by correlation with the Recorded Future Risk List: The default risk list for IP

Additional Value

Fields

Destination	103.229.64.132	GO	
Name	103.229.64.132		▼
Original	threatmatch/dest		▼
Splunk Source			▼
RF Triggered	2/64		▼
Rules			▼
RF Very Malicious Evidence	[Actively Communicating C&C Server]: 1 sighting on 1 source: Recorded Future Network Intelligence. Identified as C&C server for 1 malware family: Plugx. Communication observed on TOP-443, TCP-8080, TCP-53. Last observed on Nov 23, 2022. [Current C&C Server]: 1 sighting on 1 source: Recorded Future Command & Control List. Command & Control host identified on Nov 3, 2022.		
Risk Object	101.89.74		▼
Risk Object Type	system		▼
Risk Score	95		▼
Severity	critical		▼
Source	101.89.74	GO	▼
Source User	unknown	B82195.0	▼
Threat	ip		▼
Category			▼
Threat	ip_intel		▼
Collection			▼
Threat	p_default_ip_risklist:103.229.64.132		▼
Collection Key			▼

Related Investigations:
Currently not investigated.

Correlation Search:
[Recorded Future Correlation:ip](#)

History:
[View all review activity for this Notable Event](#)

Contributing Events:
[Show all risk events involving 101.89.74](#)

Adaptive Responses:

Response	Mode	Time	User	Status
Notable	saved	2022-11-25T13:50:09+0000	splunk-system-user	✓ success
Risk Analysis	saved	2022-11-25T13:50:09+0000	splunk-system-user	✓ success

[View Adaptive Response Invocations](#)

Next Steps:

1 No next steps defined.

Figure 5. Risk Based Alerting: Notable event created with additional Context and Risk assessment.

Chapter 2. Updates in V.2.3 (latest)

Malware Threat Map

Added Recorded Future Malware Threat Map to Splunk Enterprise

This release contains a new dashboard housing the Malware Threat Map, displaying relevant malware threats to your Organization.

- New dashboard with Malware Threat Map
 - Possibility for multiorg clients to select map for any given org.

Threat Hunt on Malware

Added support for Threat Hunts in Splunk Enterprise

Carry out threat hunts in your environment based on Recorded Future's collection of linked indicators. Utilise the Malware Threat Map to make informed decisions on what malware is relevant to hunt for and let the app do the rest.

- New results dashboard in the Alert Center
 - Create threat hunt profiles to define the parameters of threat hunts
 - Run threat hunt profile to identify relevant indicators in your environment.
-

Chapter 3. Upgrade App

Upgrading to Recorded Future for Splunk 2.0 can be done by installing the new version. Some configuration adjustments may be done, see below.

Navigate to **Configuration** > **Troubleshooting** post-upgrade and inspect the output in the panel "Validate App Deployment" in order to verify successful upgrade.



Upgrading from v1.X

Apps running v1.X must first upgrade to v2.0, before they upgrade to the latest release.

Risklist names are changed as part of the v2.0 release, therefore please update any custom solutions to the new risklist name format.

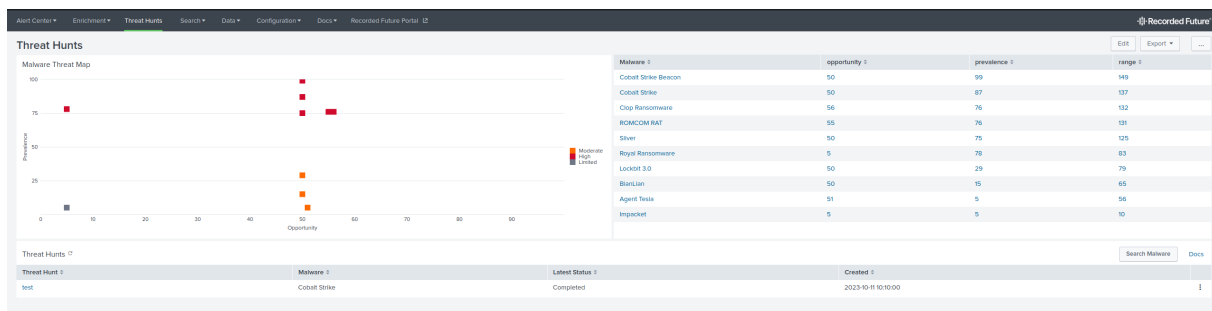
Set Up New Features in 2.3

Splunk Enterprise (App)

Threat hunt

- In order to configure and run a threat hunt
 1. Navigate to the **Threat Hunts** dashboard.
 2. Select a malware in the graph or in the table by clicking on it, or "Search Malware" for malware that isn't displayed.
 3. On the new page, select "Threat Hunt" in the top right.
 4. Configure your threat hunt and click "Start Hunt".

Created profiles are managed in the "..." menu in the **Threat Hunts** dashboard.



Chapter 4. Install

4.1. Requirements

- **Splunk Role**

- The app is designed to run on a Splunk system with the **Search Head** role.

- **Splunk Cloud**

- The application supports Splunk Cloud systems.

- **Splunk Search Head Clusters**

- Splunk Search Head clusters are supported. Once deployed, connect to any node in the cluster to configure and use.

- **Splunk Index Clusters**

- Splunk Index clusters do not affect the application.

- **Operating system**

- Any operating system where Splunk Enterprise can run is supported.

Incompatible apps

Splunk systems that had the old (separate) Recorded Future for Splunk app installed at some point must remove the following apps from the system before installing the app:

- Recorded Future app for Splunk Enterprise (TA_recordedfuture-cyber)
- Recorded Future add-on for Splunk ES (TA-recorded_future)
- Recorded Future App for Splunk v1.* (TA-recordedfuture). Upgrading from v1.* requires an upgrade to v2.0. From v2.0 it's possible to upgrade to this version.

Network

The Splunk server must be able to reach Recorded Future's API (api.recordedfuture.com) on port 443.

Outbound proxies are supported, the details can be configured during initial setup of the app.

4.2. Instructions

The app is available at [SplunkBase](#). It can either be installed directly from SplunkBase or downloaded and installed manually.



The 2.0 release requires a new API key/token. It's not possible to re-use the API key from version 1.x. If you are a current Recorded Future for Splunk user, please reach out to Recorded Future support to request a new API token for Recorded Future for Splunk v2.0.

Once the app has been installed on the Splunk server, it must be configured. The configuration

menu is located at **Configuration > App Settings**.

1. Verify that the application is connected with Recorded Future's API. "Status: Verified" will show when the connection is successful.
2. If the Status is not Verified, the connection can require a proxy. Check "Connect via proxy server" to activate a connection via proxy.
3. Enter the required fields. If the proxy server requires authentication, enter a valid username and password, otherwise leave these fields blank.
4. Connect by clicking [**Verify API URL**]. The Status should be Verified, if it doesn't, review the proxy settings.
 - Only change the API URL or disable SSL verification if asked by your Recorded Future point of contact.
5. Enter the API Token. Contact Recorded Future to receive one.
6. Click [**Verify API Token**].

4.3. Install on a Search Head Cluster



This section only applies when installing the app on a Search Head Cluster.

The app detects if it is running in a Search Head Cluster and automatically ensures that only the captain node retrieves the Risk Lists and the alerts.

1. Download the package into `$SPLUNK_HOME/etc/shcluster/apps` on the deployer of the Search Head Cluster.
2. Unpack the package, ex:
`tar zxvfp recorded-future-app-for-splunk_231.tgz`
3. Remove the package file:
`rm recorded-future-app-for-splunk_231.tgz`
4. Push the new app to the Cluster nodes:
`splunk apply shcluster-bundle...`
5. Connect to any Search Head Cluster node and follow the normal initial configuration procedure. The app will propagate the configuration to all nodes in the cluster.

Chapter 5. Malware Threat Hunts

5.1. Threat Hunt Dashboard

To start a Threat Hunt you have to initiate it on the malware enrichment page. A button **Threat Hunt** will exist to the right. Clicking on the button will take you to a modal where you can set the parameters of your Threat Hunt.

At the modal you will need to decide a name for your hunt and then select what kind of indicators of compromise (IOC) you want to look for in your Threat Hunt.

Once you have selected index, source types and event fields you are now ready to start your hunt.

This creates a new job in splunk that may take some time to complete depending on the size of your index and how many source types and event fields your are looking at.

The RecordedFuture application will keep track of the status of that job and change the status to "Completed" once the job is done.

The dashboard for Threat Hunts will show you a threat map of relevant to your organization and a list of threat hunts you have initiated. At the right of each line item for a threat hunt there is a menu that allows you to do the following.

5.1.1. Run

It will run the threat hunt again with the same parameters.

5.1.2. Edit

You can amend the threat hunt to use different parameters than used originally.

5.1.3. Duplicate

This will open up the modal for you to change any parameters you might want to change in the original threat hunt and once you click "Start Hunt" it will create a completely new hunt separate from the original hunt.

5.1.4. Delete Hunt

This will delete the entry of the Hunt on the Threat Hunt dashboard. It will not delete any previously initialized threat hunt runs. :experimental: :icons: font :img_location: ../img :last-update-label!:

5.2. Malware Threat Hunt

Malware Threat Hunts enable you to detect IOCs related to a malware family in Splunk events. Hunts use Recorded Future's Technical Links data to make precise detections.



Recorded Future Technical Links

Technical Links are lists of IOCs that are linked to an entity, like a malware families. Recorded Future identifies these links through methods such as malware sandbox analysis, infrastructure analysis, network traffic analysis. An entity's Technical Links are available on its IOC Enrichment Page and in its Portal Intelligence Cards.

5.2.1. Configure a Malware Threat Hunt

To start a Threat Hunt, follow the steps below:

1. Open the Recorded Future App for Splunk, and go to **IOC Enrichment › Malware Enrichment**
2. Enter the malware family to hunt for
3. On the malware's enrichment page, click the **Threat Hunt** button
4. Configure the hunt:
 - Name the hunt
 - Select IOC types to search for
 - Select Splunk Events to search in
5. Click **Start Hunt**
6. Done.

What's Next

- View hunt progress and any IOC detections in **Alert Center › Threat Hunts**.
- Threat Hunt configurations are available in **IOC Enrichment › Threat Hunts**. Editing a configuration will not affect past runs.



Cancel Ongoing Hunts

To stop a hunt that's currently running, go to **Alert Center › Threat Hunts** and click 'cancel' in the table row of the hunt to end.

5.2.2. Manage Threat Hunt impact on search performance

Threat hunts with large amount of events and IOCs can have a significant impact Splunk search performance. To reduce the impact, consider the following:

- **Run the search during off-Hours:** run these hunts over the weekend or when the system isn't busy.
- **Limit search criteria:** If running in off-hours isn't possible, try to limit your search criteria to decrease the load.

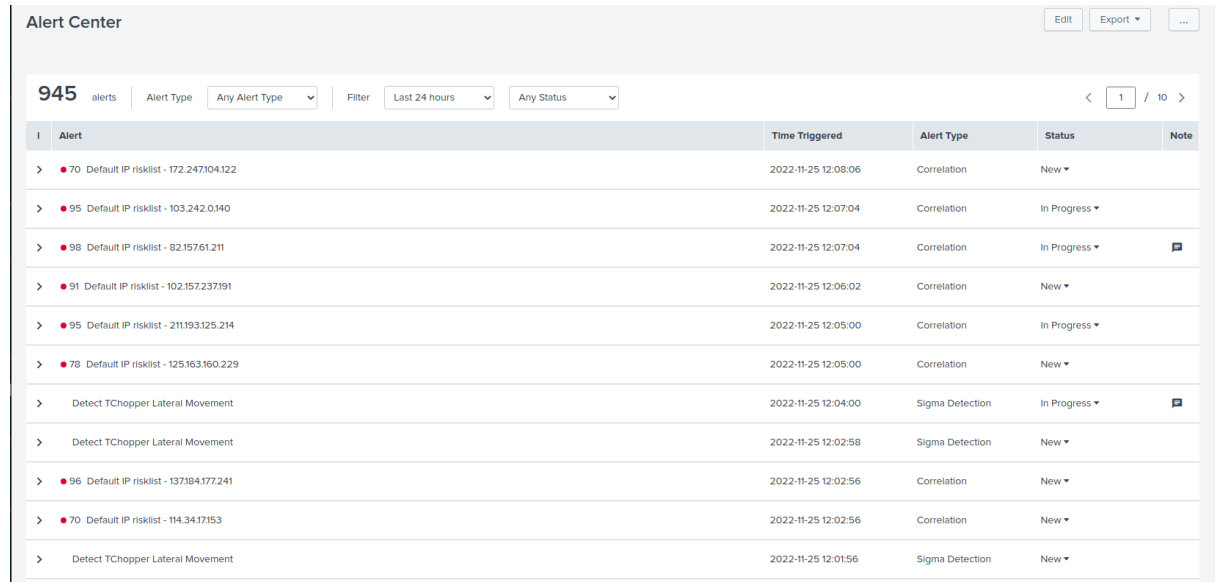
5.2.3. Edit Threat Hunt Storage Settings

To edit threat hunt storage settings, open `recordedfuture_settings.conf` and modify the value of

`threat_hunt_result_age_out`. By default, the app stores the last 100,000 runs and deletes older ones to save new hunts.

Chapter 6. Alert Center

The Alert Center is a new addition to Recorded Future for Splunk 2.1 and is the new home screen of the app. The Alert Center pulls data from cached Correlations and Sigma Rule Detections and displays all alerts in one combined list. Please configure Correlations and/or Sigma detection rules to start using the Alert Center.



The screenshot shows the Alert Center interface with 945 alerts. The table below represents the data shown in the interface:

Alert	Time Triggered	Alert Type	Status	Note
70 Default IP risklist - 172.247104.122	2022-11-25 12:08:06	Correlation	New	
95 Default IP risklist - 103.242.0.140	2022-11-25 12:07:04	Correlation	In Progress	
98 Default IP risklist - 82.157.61.211	2022-11-25 12:07:04	Correlation	In Progress	
91 Default IP risklist - 102.157.237191	2022-11-25 12:06:02	Correlation	New	
95 Default IP risklist - 211.193.125.214	2022-11-25 12:05:00	Correlation	In Progress	
78 Default IP risklist - 125.163.160.229	2022-11-25 12:05:00	Correlation	New	
Detect TChopper Lateral Movement	2022-11-25 12:04:00	Sigma Detection	In Progress	
Detect TChopper Lateral Movement	2022-11-25 12:02:58	Sigma Detection	New	
96 Default IP risklist - 137.184.177.241	2022-11-25 12:02:56	Correlation	New	
70 Default IP risklist - 114.34.17153	2022-11-25 12:02:56	Correlation	New	
Detect TChopper Lateral Movement	2022-11-25 12:01:56	Sigma Detection	New	

The interface will fetch new alerts every five minutes while the dashboard is open. Actively using the Alert Center will block this action.

Any alert in the Alert Center can be expanded by **clicking on the alert** and contains details about the alert. Furthermore, each rule has a note and a status that is tied to the specific alert and is synchronized between all views in the app. Possible statuses are **new**, **in-progress** and **resolved**.

The analyst note may contain up to 1,000 characters.

Filter options

The Alert Center, by default, shows alerts with the status **new** and **in-progress**, while alerts whose status is set to **resolved** are hidden from the default view. Resolved alerts can be viewed by selecting **resolved** in the status filter dropdown.

There exist correlation-specific filters which allow for filtration on indicator type (ip, domain, url, hash or vulnerability). To access this filter option first filter on **alert type > Correlation** and the additional filter option will appear.

The following filter options currently exist

- Alert type: Dynamically list the types of alerts available in the list, currently **Sigma Detection** and **Correlation**
- Time: Narrow down the scope of alerts via a list of time presets

- Status: Filter on status
- Correlation IOC type: If **Correlation** is selected, allows for filtering on IOC entity type.

6.1. Limitation for the number of alerts

The Alert Center has a limitation on the number of correlation alerts that can be displayed. The number depends on the configuration of your Splunk system, but in most cases, it is 50,000 alerts per type of correlation.

The limit exists because the Alert Center uses `| append subsearch` under the hood to aggregate alerts from different sources.

However, you can change this limit to the desired number. To do so, proceed with the following steps:

1. Open the existing or create the missing `limits.conf` file at `$SPLUNK_HOME/etc/system/local/limits.conf`
2. Add `searchresults` stanza into the file if it is missing
3. Under the `searchresults` stanza, add `maxresultrows` field with the desired number. You should have the following content:

```
[searchresults]
maxresultrows = <integer>
```

4. Restart Splunk to apply the changes



It is not recommended to set the limit that exceeds 50,000. More information can be found in [the official documentation](#).

The application will display the warning message if the limit exceeds after loading the Alert Center page.

The screenshot shows the Alert Center interface. At the top, there is a navigation bar with 'Administrator' and 'Messages' (with a notification icon). Below the navigation bar, a yellow warning message is displayed: "The list is incomplete because the total number of events found by the underlying subsearch exceeded limit of 50000. Limit is set in the 'limits.conf' file of the Splunk system in 'searchresults' stanza under 'maxresultrows' field." Below the warning, there are filter controls: a 'Filter' dropdown menu showing 'Last week' and another dropdown menu showing 'Any Status'.

Chapter 7. Alerting Rules



This section covers both Recorded Future 'Classic' and Playbook Alerts. Playbook Alerts requires a Module Account. If you don't see an alert of the type "Playbook Alert", contact your account manager to discuss this option.

The Recorded Future app can display alerts (Classic and Playbook Alerts) from the Recorded Future platform. Alerts will appear in the Alert Center, after you have enabled alerting.

7.1. Setup

To activate Recorded Future Alerts in the Recorded Future app, follow these steps:

- Open the Recorded Future Portal.
- Go to **Intelligence Goals Library**
- Configure the desired Intelligence Goals / Alerting Rules.
- Open The Recorded Future app for Splunk.
- Go to **Configuration › Alerting Rules**.
- If no Alerting Rules appear, verify that Alerting Rules have been enabled in the Recorded Future portal.
- Activate the desired Alerting Rules.
- Once Alerting Rules are activated, alerts will appear in the **Alert Center**

The app will continually add support for more types of Playbook Alerts.

7.2. Classic Alerts Dashboard

The Dashboard displays Recorded Future Classic alerts. To edit the types of Classic alerts you receive, go to **Configuration › Alerting Rules**).

In the configuration for Alert Rules, you've selected specific alerting rules. Alerts for all of these rules will show up on the dashboard. Each Alert Rule will contain a maximum of 100 alerts which will show up on the dashboard.

In the dashboard, you can filter alerts based on the alert rule, time or status, or a combination of those.

The dashboard consists of a list of alerts. Click an alert to see more detailed information.

Alerts					
300 alerts		Alert rule: All alerts	Filter: Any time	Any Status	Docs
Alert Title	Status	Assignee	Triggered	Note	
> Global Trends, Trending Methods - Spike: QakBot, BlackBasta Ransomware and ...	New	None assigned	11/25/22, 5:03 AM		
> Infrastructure and Brand Risk, Potential Typosquatting Watch List Domains ...	New	None assigned	11/25/22, 5:03 AM		
> Global Third-Party Risk, Trend - Spike: Eurocámara, Fenbushi Capital and Co...	New	None assigned	11/24/22, 5:03 PM		
> Global Trends, Trending Methods - Surge: QakBot, Infostealer, Denial-of-Ser...	New	None assigned	11/24/22, 5:02 AM		
> Global Third-Party Risk, Trend - Spike: European Parliament and All-India L...	New	None assigned	11/23/22, 5:02 PM		

7.2.1. Alert Details

Clicking on an Alert title in the list will open the Alert's detail section and show you what the Alert contains.

The state of the Alert can be changed using the dropdown in the Status field.

Use the text field to save comments about the alert.

Alert center
Enrichment
Search
Data
Configuration
Docs
Go to Recorded Future
Recorded Future

Alerts
Edit
Export
...

300 alerts
Alert rule: All alerts
Filter: Any time
Any Status
Docs

Alert Title	Status	Assignee	Triggered	Note
> Global Trends, Trending Methods - Spike: QakBot, BlackBasta Ransomware and ...	New	None assigned	11/25/22, 5:03 AM	

References

Black Basta Ransomware Gang Actively Infiltrating U.S. Companies with Qakbot Malware New research indicates that half of all phishing scams are now hosted on Web sites whose Internet address includes... #PhishLabs #Cybersecurity #Politics #Technology <https://t.co/KSxF090J6n>

Malware	BlackBasta Ransomware, QakBot
Country	United States
Attack Vector	Phishing
URL	https://buzzsec.blogspot.com/2022/11/the-hacker-news-black-basta-ransomware.html
Hashtag	#PhishLabs, #politics, #cybersecurity, #Technology
Technology	internet

Black Basta Ransomware Gang Actively Infiltrating U.S. Companies with Qakbot Malware | Cyberfeed.io.

Malware	BlackBasta Ransomware, QakBot
Country	United States
Domain	cyberfeed.io

Black Basta Ransomware Gang Actively Infiltrating U.S. Firms with Qakbot Malware - Crypto News.

Malware	BlackBasta Ransomware, QakBot
Country	United States
Industry Term	crypto

Black Basta Ransomware Gang Actively Infiltrating U.S. Companies with Qakbot Malware | The Cyber Security News.

Malware	BlackBasta Ransomware, QakBot
Technology	Cyber Security
Country	United States

Analyst note

7.3. Playbook Alerts Dashboard

The Dashboard displays Recorded Future Playbook alerts. To edit the types of Playbook alerts you receive, go to **Configuration > Alerting Rules**.

- *Filter alerts* based on category, time, status, or assignee.
- *Enrich an IOC* by clicking on it. Supported IOCs appear as links.

Chapter 8. Correlations

The app does correlation (Threat Detection) by correlating a log source with Recorded Future lookup files; these files are available in the Splunk system. The App has a number of Correlation Use Cases available for different Threat profiles. The App has several Correlation Use Cases available for different Threat profiles. The saved search responsible for detection can be disabled via the **toggle** in **Configuration > Correlation**. Disabled correlations will keep the risk lists up to date but not generate any new alerts.

8.1. Correlation Types

When setting up a correlation, there are three types.

- "Correlation" - looks at a specific index and specific source type. This also gives you the flexibility of using an entirely custom search if you so want to.
- "Data model correlation" - When you have a specific data model that you want to correlate with.
- "Splunk Enterprise Security Correlation" - This is looking at default ES data models, such as network traffic and web data models.

8.2. When a correlation rule is saved

When you save a correlation the following happens in the background.

- The app fetches the Risk List associated with the Use Case. After the initial download, the Risk List will be kept in sync with the Recorded Future API.
- The app creates a Saved Search.
 - This search uses a Lookup file to correlate events from the search with the content of the lookup file.
 - The search is run once with a -7d time frame. After that the search will run on a three-minute schedule correlating logs from three minutes at a time.
 - Matches, or Correlations, are stored in a KV store collection file on the Splunk server called `correlation_cache_<datatype>`
 - The correlation caches are split up based on the data type they contain (ip, domain, hash, etc.) and each file has a defined age-out setting defining how much data can be stored. By default these values are set to 365 days or 100,000 rows but this can be modified in `recordedfuture_settings.conf`.
- The Correlation dashboard is dynamically populated with correlations from the correlation cache lookup files.



Do not edit the Saved Search created by the app or the View created by the app. They may be updated at any time and your edits will be lost.

Setup Default Correlations

1. Go to **Configuration** › **Correlations**
2. Click **New Correlation** › **Add Correlation**
3. Add a title for the Correlation
4. Select an IOC: The correlated entity type can be an IP, domain, hash, vulnerability or URL
5. Select the source of the events that are to be inspected:
 - Index: this is the index that is used by the sourcetype. Once selected, the UI will show the number of events that have been indexed over the last 24 hours.
 - Sourcetype: this is the sourcetype of the events that are being inspected. Once selected, the UI will show how many events this sourcetype has produced over the last 24 hours.
 - Field: the field containing IOCs that we will correlate against the Risk List. Once selected, the UI will show how many events with this field the sourcetype has produced over the last 24 hours. The UI will also show the percentage of IOCs found that can be used in a correlation (e.g., the percentage of IOCs that are valid IP addresses). Select a Correlation Use Case. Hover over the line of a Correlation Use Case to show more details.



The correlation setup pages use a sampled SPL query to populate the field dropdown to improve performance. As a consequence, fields from rare events might not be listed. Under such circumstances, consider using the **Search String** option.

6. Click [**Save**]

[← All Correlations](#)

New Correlation

[Docs](#)

Title * ?

Recorded Future Intelligence Goal

IOC ?

Select IOC to view related Intelligence goals

Intelligence Goal

Events

Selection mode

Guided selection

Search String

Index ?

Source type ?

Field ?

Correlation: ?

Save

Setup Data Model Correlations

1. Go to **Configuration** › **Correlations**
 2. Click **New Correlation** › **Add Data Model Correlation**
 3. Add a title for the Correlation
 4. Select an IOC: The correlated entity type can be an IP, domain, hash, vulnerability or URL
 5. Select a Correlation Use Case. Hover over the line of a Correlation Use Case to show more details.
 6. Select the source of the events that are to be inspected:
 - Data Model: This is the name of the Data Model that contains the events. A green check mark indicates that the data model contains events from the last 24 hours.
 - Section: This is the section of the events that are being inspected. Once selected, the UI will indicate that the section has produced over the last 24 hours with a green check mark.
 - Field: The field containing IOCs that we will correlate against the Risk List. Once selected, the UI will show how many events with this field the sourcetype has produced over the last 24 hours.
 7. Click [**Save**]
-

← All Correlations

New Data Model Correlation

[Docs](#)

Title * ?

Recorded Future Intelligence Goal

IOC ?

Select IOC to view related Intelligence goals

Intelligence Goal

Select risklist

General

- Default IP risklist**
- Default IP risklist hourly
- Indicators Frequently Linked to Malware
- Large IP risklist
- Log4Shell_Potentially_Malicious_Scanners_Risklist
- Log4Shell_Related_Scanners_Risklist
- Threat Actor IP Risklist
- Credentials/Bruteforce attacks
- Indicators Found in Honeypots

Events

Data Model ?

✓ ok

Section ?

✓ ok

Field ?

✓

8.3. Correlation Dashboards

The Correlation Dashboard displays correlations between customer logs and Recorded Future Risk Lists.



The Correlation Dashboard is not available until after the first correlation rule has been configured.

The top of the Correlation Dashboard has two dropdowns where you select the IOC type and correlation rule you wish to show detections for.



Please note that recently configured correlations will not be selectable in the Correlation dropdown until they make their first detection.

The correlation dashboard contains four elements:

- "Summary" shows the number of entities that the correlation found to match one or more events.
- "Top Rule Hits" shows the rules triggered by these entities.
- "Top Counts" displays the entities with the number of events found by the correlation.
- "High Risk" contains matching entities with their risk information.

Field	Description
Risk	The risk score assigned to the entity by Recorded Future
Entity	The matched entity
Count	The number of events matched to the entity
Rules	The number of Recorded Future rules triggered for the entity out of the total number of rules set up for this type of entity by Recorded Future.
Evidence	Each of the triggered rules is listed in descending criticality. The criticality is signaled by a color coded dot at the start of the line. The rule is written in bold followed by the details in regular text.
Mitre	Any MITRE ATT&CK codes attached to the Risk Rules.

Further information can be obtained by two drill down options:

- Click on the entity, such as the IP address or the Domain, to open a new Search window looking for events involving the entity.
- Click on any other part of the line to open the Enrichment Dashboard for the entity.

8.4. Technical Information

For each Correlation Use Case, Recorded Future provides a Risk List. A Risk List is a CSV file in which each line contains information about an IOC that has an associated risk.

The following columns are part of the file:

Column	Description
Name	The IOC (e.g. an IP, domain).
Risk	The Risk score that Recorded Future has assigned to the IOC. A value between 0 and 99.
RulesCount	The number of triggered Recorded Future Risk Rules for an IOC. Rules are used to calculate the Risk Score.
RulesTotal	This is the number of rules used to assess the risk for these types of IOCs.
EvidenceDetails	A structure with evidence for why Recorded Future assigns the risk. It is a structure encoded in JSON.
Mitre	A structure with the MITRE ATT&CK codes associated with the IOC. It is a structure encoded in JSON.

Chapter 9. Enrichment Dashboards

An enrichment dashboard shows Recorded Future intelligence on an IOC. The displayed elements vary based on the IOC type and available information.

The Enrichment Dashboards can include the following panels:

- **Summary:** provides a brief overview of the entity, including the number of references, criticality, Risk Score, linked Mitre ATT&CK Codes, and dates of the first and last reference.
- **Threat Research Insikt Group:** displays Analyst Notes related to the IOC.
- **Triggered Risk Rules:** shows an entities triggered Risk Rules, sorted by severity.
- **Total Reference Count:** graphically represents the timestamps of references related to the entity.
- **Related Entities:** up to 15 tables containing related entities are displayed, including attacker, target, actors, malware, vulnerabilities, IP addresses, domains, products, countries, hashes, technologies, email addresses, attack vectors, malware categories, and operations.
- **References:** two tables that display the first reference and the most recent references.
- **IOC-specific Panels:** additional elements specific to certain entity types, including GEOIP and CIDR details for IP addresses, information on other Risk Lists that contain an IP address or domain, NVD summary for vulnerabilities, affected versions for vulnerabilities, and links to documents containing more information about vulnerabilities.
- **Infrastructure Detections:** shows past detections of an IOC within your organisation's infrastructure, based on information from applications connected to Collective Insights. To use this panel [activate Collective Insights](#).



Click **activate Collective Insights** to open the Collective Insights Settings page

9.1. Technical Information

When you enrich an IOC, the Enrichment Dashboard fetches IOC information via a custom REST handler that makes a call to Recorded Future's API.

Chapter 10. Sigma Rules

Sigma rules are a YAML-based signature standard created to detect malicious behaviour. While typical indicators are static and easy for an adversary to change, behavioural indicators are much stronger and therefore carry higher confidence when it comes to detection.

The Recorded Future Insikt group creates Sigma rules for detection as part of their malware analysis, and these rules will now be distributed directly into the Splunk integration as of version 2.1. When enabled they will carry out searches in your Splunk environment looking for events that match the behaviour defined in the Insikt Sigma rules.

Unsupported badge on the sigma rule indicates that the rule is no longer served by the API. The unsupported rule is not automatically removed from the list because it has been configured before by the customer.

10.1. Setup

To configure Sigma rule detection please navigate to the **Sigma Rule** configuration page via **Configuration > Sigma Rules**, this brings up a list of available Sigma rules. Clicking **Configure** of any of the listed rules present a popup menu. To the left in the popup is the search query, derived from the Sigma rule, and to the left is an event mapper. The event mapper allows for customization of the query using the fields available in any given index.

The screenshot shows a configuration window for a Sigma Rule titled "Sigma Rule: T-RAT 2.0 DNS queries". The window is divided into two main sections: "Splunk Search" and "Event Mapping".

Splunk Search: This section contains a text area with the following search query:

```
index=main
EventID=22
Message IN ("api.telegram.org",
"ifconfig.me", "ipinfo.io", "api.ipify.org",
"ip.42.pl", "ipapi.co", "www.sslproxies.org")
Image="*sihost.exe"
```

Below the text area is a toggle switch labeled "Edit search query (disables Event Mapping)" which is currently turned off. At the bottom left of this section is a "Run search" button with an external link icon.

Event Mapping: This section has a heading "Event Mapping" and a sub-heading "Event Mapping attempts to automatically find the event fields required by the Sigma Rule in Splunk." Below this are two tables:

Source	Matched source
✓ Index=main	main

Event Field	Matched Event Field
✓ Image	Image
EventID	EventID
Message	Message

At the bottom right of the configuration window is a green "Activate Rule" button.

To activate a rule, please select an index on which you wish to enable detection. The app will populate the event mapper with recent fields from this index. Clicking **Activate rule** enables the rule as is, and detections will be presented in the **Detections** tab or in the **Alert Center**.

The screenshot displays the Sigma Rules interface. At the top, there are 'Edit', 'Export', and '...' buttons. Below is a filter section with '96 rules' and dropdowns for 'Any Product', 'Any MITRE code', and 'Any Status'. The main table has columns for 'Sigma Rule', 'Status', and 'Tags'. The first rule is 'Sigma Rule: Ransomware Shadow Copy manipulations' with a status of 'In Use' and a green toggle switch. Below the rule name, there are details: Status (N/A), Level (High), Malware Category (Ransomware), Product (Windows), and Alerts triggered (0). There are 'Run Search' and 'Edit' buttons. At the bottom, there is a 'Configure' button.

Clicking on any given rule allows for editing of detection query and ad-hoc search. Sigma detection for any given rule can be disabled by toggling the green toggle to the left.

The search query can be customized by either using the event mapper or by toggling the **Edit search query** toggle. This toggle unlocks the text box, allowing for direct modification of the search query. Be mindful when making direct changes, as errors can either introduce false positives or cause detection to fail.



The Sigma setup pages use a sampled SPL query to populate the event mapper with available fields in order to improve performance. As a consequence, fields from rare events might not be listed. Under circumstances where a field does not appear, consider using the **Edit search query** option.

A more reliable customization approach is to use the event mapper. The event mapper is a convenient way to customize the search query, without the risk of negatively affecting the detection query. In order to use the event mapper, first select an index as previously described. Then find the field you wish to substitute in the column to the right, titled **Event Field**. In the dropdown adjacent to this select the field you wish to use instead. Upon selecting the field you wish to use the query and UI will be updated to reflect this change.

The Sigma detection cache is pruned after 100,000 entries, and entries older than one year are removed. The settings regarding pruning can be modified in the `recordedfuture_settings.conf` file.

Chapter 11. Sigma Detections

Based on the activated Sigma Rules detections are generated. These detections will contain information gathered from the machine.

Chapter 12. Splunk Enterprise Security Integration

The Recorded Future integration with Splunk Enterprise Security (ES) provides Splunk ES correlations with Recorded Future Risk Lists. Additionally, by leveraging Splunk's Threat Intelligence framework, correlation detections can be classified as notable events.

The integration offers two methods for enriching Notable events:

- **Risk Based Alerting (RBA)** (Recommended method)
 - RBA directly enriches Notable with Recorded Future data, ideal for detection.
- **Recorded Future Enrichment - Adaptive Response (AR)**
 - Enrich Notable Events generated by any non-RBA intelligence source, including sources from other providers.

The integration offers one method to perform ad-hoc searches on Recorded Future links data.

- **Recorded Future Threat Hunt - Adaptive Response (AR)**
 - Fetch linked indicators from any field in a Notable event and perform a one-time search. Results are written as a notable- or risk event.

12.1. Install



- The Recorded Future app and Splunk Enterprise Security (ES) must be installed on the same search head.
- The app automatically detects if Splunk ES is installed.

Activate the Recorded Future Integration with Splunk ES.

1. Open the Recorded Future Splunk app
2. In the top-level menu, click **Configuration** › **App Settings**.
3. In the section **Splunk Enterprise Security (ES) Integration**, check **Use Recorded Future's integration with Splunk ES**.
4. Done.

12.2. Setup Correlations

To activate correlations in Splunk Enterprise Security you only need to configure a threat feed. A threat feed contains indicators used for detection. Recorded Future correlations in ES require these feeds to function, as they contain indicator and risk data.

The Recorded future app supplies two types of threat feeds, Risk Based Alerting and Adaptive Response feeds. It is not recommended to use both types of feeds simultaneously as this will produce duplicate detections.

Risk based alerting feeds provide both detection and enrichment; while Adaptive Response feeds rely on a secondary Splunk correlation search for detection.

12.2.1. Risk Based Alerting feed

How to configure and enable an RBA feed:

1. In the Recorded Future App, go to **Configuration › Splunk Enterprise Security Feeds**.
2. Confirm that you are on the **Risk Based Alerting** tab.
3. Click the button **Add Threat Feed**
4. Complete the required configuration
5. Click [**Save**] at the bottom of the panel
6. Done

Generate Notable Events from IOC Detections

By default, RBA feeds generate Risk Events when they detect an IOC. Feeds can also be configured to generate Notable Events if the severity of a detected IOC is above a defined level. Configure a RBA feed to generate Notable Events, by following these steps:

1. Open the configuration page of the RBA feed to modify.
2. Add a IOC severity threshold to define which IOC detections that generate Notable Events.

Disabling **Generate Risk Events** will cause the feed to only generate Notable Events.

Estimate

RBA feed setup allows for the estimation of daily alert count. This estimation will download risklists that are not available which might take some time.

12.2.2. Adaptive Response feed

How to configure and enable an Adaptive response feed

1. In the Recorded Future App, go to **Configuration › Splunk Enterprise Security Feeds**.
2. Navigate to the **Adaptive Response** tab.
3. Click the button **Add Threat Feed**
4. Complete the required configuration
5. Click [**Save**] at the bottom of the panel
6. Done

Adaptive Response feeds rely on the Splunk correlation search "Threat Activity Detected" to produce detections. To enable this please proceed with the following steps:

1. In ES, Go to **Configure › Content Management**
 2. In the filter bar, type "Threat Activity Detected"
-

3. Enable the correlation search "Threat Activity Detected"
4. Click on "Threat Activity Detected"
5. Scroll to the bottom of the *Adaptive Response Actions* section and click [**Add New Response Action**].
6. Select "Recorded Future Enrichment".
7. Click [**Save**].
8. (Optional) If the error "*There was an error saving the correlation search: Risk-Modifier fields are required.*" appears: Open the "Risk Analysis" action, scroll to the bottom and remove the last modifier by clicking on the X. Click Save.
9. Done

Correlations via Adaptive Response have now been configured; any correlations will appear as Notable Events in the ES incident review table.

Configuration Options

Please proceed with the following steps to display Recorded Future risk rule data in the Incident Review table of ES.

1. In ES, Go to **Incident Management** › **Incident Review Settings**.
2. Under **Incident Review - Event Attributes** click **Add new entry**. Add the following Label and Field Combinations:

Field	Label
<code>rf_a_risk</code>	RF Risk Score
<code>rf_b_rules</code>	RF Triggered Rules
<code>rf_evidence_critical</code>	RF Very Malicious Evidence
<code>rf_evidence_malicious</code>	RF Malicious Evidence
<code>rf_evidence_suspicious</code>	RF Suspicious Evidence
<code>rf_evidence_unusual</code>	RF Unusual Evidence

12.2.3. Risk Based Alerting

Setting up a threat feed, as described in is the only step required to activate Risk Based Alerting.

The following Automatic actions occurs for events detected by the ES via the TI framework

- Enrich the event with: **Recorded Future intelligence** and **Mitre ATT&CK** codes
- Generate a Notable event
- Generate a Risk Event (if applicable)

Splunk's "Risk Based Alerting" framework uses these objects to automatically group related events. The framework can automatically promote the Risk Event into Notable events if needed.

Technical Information

- `saved_searches.conf` stores all correlation configurations
- For each configured threat feed the app sets up a TI-framework feed, which is ingested by ES and is the basis of detection.
- Search frequency: 1/hour

Edit frequency in **Splunk ES › Content Management**

Setup Risk Factors

Edit Risk Factors in Splunk ES by going to Configure → Risk Factor Editor. Risk Factors are conditional logic that affects the risk score of Risk Notables.

12.2.4. Accelerated Data Model Correlations

Correlations of events from Accelerated Data Models is a high performance correlation. The data model used will depend on what entity type is correlated on. Furthermore, the correlations are currently limited in scope to one given field in the data model. This differs from the threat matching searches performed by Splunk ES which use multiple fields and data models.

IOC type	Data Model	Correlating on field
ip	Network_Traffic.All_Traffic	dest
domain	Network_Resolution.DNS	dns.query
hash	Malware.Malware_Attack	Malware_Attacks.file_hash
url	Web	Web.url

To use this form of correlation, the events must be available from Accelerated Data Models (which can be configured in Splunk). The output is a Saved Search and a dashboard in the application.

In Splunk Enterprise Security, Recorded Future recommends that the events from each Scheduled Correlation search are promoted to "Notable Events". This is described in the Configuration of the app for Splunk Enterprise.

12.2.5. How to configure

Using the Correlation Configuration panel, complete the following steps to setup a Correlation Use Case:

1. Go to **Configuration › Correlations**
2. Click **New Correlation › Add Splunk Enterprise Security Correlation**
3. Add a title for the Correlation:
 - Title: This is the name of the Correlation View that will be created. The view will be available via a dropdown in the **Alert Center › Correlations** menu.
 - IOC: This is the type of IOC that will be correlated. Currently this can be an IP, domain, hash, vulnerability or URL.

- The Saved Search will be created that drives the Correlation view. This search can also be used outside of the view or to be run from a schedule with the option of creating alerts when suspicious events are found.
4. Select a Correlation Use Case. Hover over the line of a Correlation Use Case to show more details.
 5. Click [**Save**]

← All Correlations

New Splunk Enterprise Security Correlation Docs

Title * ?

Example IP correlation

Recorded Future Intelligence Goal

IOC ? ip ▼

Select IOC to view related Intelligence goals

Intelligence Goal

- Threat Actor IP Risklist
- Credentials/Bruteforce attacks
- Indicators Found in Honeypots
- Traffic From Connections (IPs) Linked to Malware
- Malware Detection
- Communication With Anonymizing Web Proxies
- Indicators Linked to Malware C&C Servers
- Indicators Linked to Malware
- Indicators Linked to Malware Using TOR
- Insider Threat
- Network Devices Using TOR to Anonymize Traffic

Save

Once the Correlation Use Case is saved, the following is done:

- The app is configured to fetch the Risk List associated with the Use Case. After the initial download, the Risk List will be kept in sync with the Recorded Future API.
- A Saved Search is created. This is named as the ID that was automatically generated for the correlation. You can see the generated ID when you press Edit button on the corresponding

correlation. The search can be run from search using this command: | `savedsearch correlation:correlation_id`

- A Correlation View is created.
- The menu is updated to reflect the new Correlation view.

12.2.6. Enrich Notable Events

The AR action operates in one of three modes:

1. Enrich using real-time data from Recorded Future's API. In this mode, calls are made to Recorded Future's API to fetch up-to-date intelligence about the detected IOCs.
2. Enrich using cached data - share the data with Recorded Future, and the Collective Insights. In this mode, enrichment is based on information from Recorded Future Risk Lists. The TI framework will use all the data it can extract from the lists. This mode notifies Recorded Future's API about which IOC was detected.
3. Enrich using cached data - do not share data with Recorded Future. This is identical to the previous mode, except the IOCs are not shared with Recorded Future.

12.2.7. Ad-hoc Enrichment

Ad-hoc invocations of the Adaptive Response are possible, for example, via the Incident Review dashboard. Invoking the AR ad-hoc requires a Splunk account with `list_storage_passwords` capability.

12.2.8. Adaptive Response Title Prefix option

When using Adaptive Response action a new Notable is created in ES that is enriched with Recorded Future risk rules. By default, this new notable is created with the title "Threat Activity Enriched (IOC)". The title prefix options allow users to customize this naming scheme.

Any value entered into the "Title Prefix" option box will replace the "Threat Activity Enriched" string in the produced Notable Event.

12.3. Adaptive Response Threat Hunt



Running the Adaptive Response as an automatic action may cause a significant load on the Splunk system. Each IOC detection will trigger a new Splunk search for linked IOCs.

The Adaptive Response action searches for IOCs linked to an indicator present in any Notable Event. The searches are based on intelligence provided by Recorded Future's Technical Links. The AR contains several parameters to control the threat hunt. These are:

- Entity field: field of the notable on which to perform links lookup.
- Entity category: The category of indicator, 'auto' is selected on default, please specify if you encounter issues.
- Index: comma separated list of indexes to search, e.g. "main,firewall,edr". No spaces.

- Earliest: how far back the search will look; uses splunk time format.

The Links Adaptive Response (Links AR) action can be used ad-hoc or in conjunction with a Correlation search to perform automatic threat hunting based on the results of a correlation search, such as Recorded Future's RBA correlations. Any results are presented as Notable Events.

Chapter 13. Collective Insights

The Recorded Future Collective Insights provides complete Intelligence coverage across adversaries, their infrastructure, and the organizations they target, so business and security leaders can take action quickly and confidently. Organizations tap into the Collective Insights, forming a network that creates more value for everyone as the community grows.

This version of our app enables sharing of correlations and sigma rule detections back into the intelligence cloud to further improve the quality of our intelligence. The data we store is encrypted by individual enterprise keys and stored separate. This feature can be disabled by going to **Configuration › Recorded Future Intelligence Cloud Settings**. If sharing is enabled, we write back the following information whenever a new correlation is found or a sigma rule detection is made:

- Correlations:
 - The indicator triggering the correlation
 - The type of log source that the correlation rule was configured with
 - The event field that the correlation rule was configured with
 - The name of the use case that the correlation rule was configured with
- Sigma Rule Detections:
 - The type of log source that the sigma detection was found in
 - The name of the use case that the sigma detection rule is configured with
- Matches in the Splunk ES TI framework data model (ES only):
 - The indicator triggering the match (`threat_match_value`)
 - The type of log source from the correlated event(`orig_sourcetype`)
 - The event field of the correlated event(`threat_match_field`)
 - The id of the TI feed of the correlated event (`threat_key`)
- Recorded Future Threat Hunt (ES only):
 - The indicators found by threat hunt search
 - The indicator which was the starting point of the threat hunt
 - The type of log source of any events found by the search
 - The event field of any events found by the search
 - The id of the TI feed of the correlated event

13.1. Limit Detection Sharing for Organisations within a Multi-org Enterprise



This setting applies to Recorded Future accounts with multi-org enabled.

By default, all organizations within a multi-org that are accessible from the Recorded Future

integration for Splunk will share Collective Insight detections with each other.

To prevent detection sharing with other organizations, follow the steps below.

1. Contact Recorded Future support to obtain organisation IDs
 2. Open Splunk Enterprise.
 3. Add configuration that adds `rf_multiorg_org=<org-id>` to any event or source where sharing should be limited to a specific organization. This can be done in various ways, ex as a Calculated field (Settings→Fields→Calculated Fields).
 4. Done
-

Chapter 14. Troubleshoot

The issues involving the Recorded Future for Splunk can be divided into two categories. To ease troubleshooting, the app contains one report for each type:

14.1. Reports

14.1.1. Validate App Deployment

Run the report "Validate App Deployment" when the Recorded Future for Splunk has been deployed and configured or as an initial step during troubleshooting. The built-in validator performs several tests and collects troubleshooting information. "Ok" and "NA" indicate that the app's connectivity setup is working. Investigate other codes, such as "Warning" or "Error". This can also be accessed on the troubleshooting page.

14.1.2. All logs from the app

The report "All logs from the app" lists all the events created by the app. You can adjust the log level on the **Configuration** › **App Settings** page. The default is INFO. Setting the log level to DEBUG may ease troubleshooting.

A good starting place is to look for errors (log level ERROR). The report can be opened in the search view: select **Open in Search** via the [**Edit**] button.

14.2. Logs

The logs generated by the Recorded Future app are located in the default Splunk log directory `$SPLUNK_HOME/var/log/splunk` and will be written to the following file:

- `ta_recordedfuture_rest.log`

The information contained in the log files can be viewed either in the Splunk GUI or as files on the Splunk server.

14.2.1. Search queries

Search app logs

```
index=* sourcetype="tarecordedfuture:app:log"
```

Search logs from Adaptive Response actions (Splunk ES)

```
index=* sourcetype="modular_alerts:ta_recordedfuture"
```

Search for app references in Splunk logs

```
index=* sourcetype=splunkd recordedfuture
```

14.3. Report Issue

When reporting an issue to Recorded Future, the following steps help us analyze and solve the issue:

1. Write a brief summary of the issue.
 - what is or is not happening?
 - Is it happening all the time, is it intermittent or limited to a subset of entities?
2. Please include screenshots with the result from running the reports:
 - Validate App Deployment
 - Latest Update of all Risk Lists
3. Please include screenshots of the developer console to show any javascript errors that may have been triggered.
4. Increase the log level to DEBUG.
5. Trigger the issue.
6. Note the date and time the issue was triggered. Make sure to include this in the report to Recorded Future.
7. Run the report "All logs from the App"
 - Export the results as a CSV file.
8. Reset the log level.

Chapter 15. Further Help

The Recorded Future App for Splunk is developed by Recorded Future.

You find further information and support on our support site: support.recordedfuture.com

Chapter 16. Technical documentation

Chapter 17. Server-side dashboard generation

The application contains a number of dashboards that are generated server-side and then sent to the application. Modifications directly to these dashboards will be overwritten.

- **Alert Center › Correlation** (`rfes_correlation_cached`)
- **Enrichment › Domain Enrichment** (`rfes_enrich_domain`)
- **Enrichment › Vulnerability Enrichment** (`rfes_enrich_vulnerability`)
- **Enrichment › URL Enrichment** (`rfes_enrich_url`)
- **Enrichment › Malware Enrichment** (`rfes_enrich_malware`)
- **Enrichment › IP Enrichment** (`rfes_enrich_dip`)
- **Enrichment › Hash Enrichment** (`rfes_enrich_hash`)
- **Threat Hunts** (`rfes_threathunt_dashboard`)
- **Search › Recorded Future Search** (`rfes_search_pivot`)
- **Data › Recorded Future for Splunk Overview Page** (`rfes_landing_page`)
- **Configuration › Correlation** (`correlations_list`)
- **Configuration › New Correlation** (`rfes_correlation_edit_reg`)
- **Configuration › New Data Model Correlation** (`rfes_correlation_edit_model`)
- **Configuration › New Threat Feed** (`ti_framework_edit`)

Any other dashboard or searches found in the app are client side and can be freely modified without having to worry that changes will be overwritten.

If local modifications are desired, then create a copy in the apps `/local/data/view` directory. This copy will be a snapshot of the dashboard at the time of copy. Note that the dashboards will *not* be updated automatically, and any improvements made after will need to be manually copied over. Removing the dashboard from `local/data/view` removes the snapshot and the app once more use the latest available dashboard from the API.

Chapter 18. Customization of savedsearches

The app comes delivered with a lot of savedsearches. These searches are stored in `/default/savedsearches.conf`. Any changes made directly to the `/default/savedsearches.conf` is at risk of being overwritten when the app is updated.

Modifying a savedsearch in the splunk UI creates an override in `local/savedsearches.conf`. Overrides are persistent over upgrades.

If you wish to modify a savedsearch in `.conf` file directly, create an override by adding a new stanza in `local/savedsearches.conf`. The name of the stanza must match that found in defaults. Proceed to add any properties to the stanza that you wish to override.

Chapter 19. API documentation

Chapter 20. Threat Hunting API

20.1. Threat hunt profiles

Profiles are stored in a collection, and can be accessed via the `threathunt_profile` lookup and contains all details needed to initiate future hunts. Each profile requires the following information:

- `name`: cleartext name that identifies the hunt
- `target`: target being hunted on, must match Recorded Future portal name.
- `target_type`: type of hunt, currently only `malware` is supported
- `iocs`: list of links types to hunt on, possible values: `["domain", "ip", "hash", "url", "vulnerability"]`
- `lookup_period_seconds`: how far back to hunt in seconds.
- `indexes_sourcetypes_event_fields_map`: json object used to map links to specific fields or sourcetypes. Example: ``{"index1": {"sourcetype1": ["field1"], "sourcetype2": ["field2"]}`` will produce a search `index=index1 (sourcetype=sourcetype1 AND (field1=IOC)) OR (sourcetype=sourcetype2 AND (field2=IOC))`
- `config_type`: `guided`

20.1.1. Create profile



Creating a profile also starts a threat hunt on that profile automatically.

POST the following payload to `services/TA-recordedfuture/create_threat_hunt_config` to create a threat hunt.

```
{
  "name":"Threat Hunt 1",
  "target":"Cobalt Strike",
  "target_type":"malware",
  "iocs":["domain","ip",
  "hash","url","vulnerability"],
  "config_type":"guided",
  "lookup_period_seconds":7776000,

  "indexes_sourcetypes_event_fields_map":{"main":{"netscreen:firewall":["dest"],
  "squid:access":["url"]}}
}
```

Example curl:

```
curl -X POST 'https://127.0.0.1:8089/services/TA-
recordedfuture/create_threat_hunt_config?output_mode=json' \
  -d '{"name":"Threat Hunt 1","target":"Cobalt
Strike","target_type":"malware","iocs":["domain","ip","hash","url","vulnerabil
ity"],"config_type":"guided","lookup_period_seconds":7776000,"indexes_sourcety
pes_event_fields_map":{"main":{"netscreen:firewall":["dest"],"squid:access":["
url"]}}}' \
```

Response:

- 200 - OK
- 400 - Missing parameter

200 response contains profile_key and threat hunt run_key.

```
{
  "links": {},
  "entry": {
    "content": "Threat Hunt successfully started",
    "sid": "1697017815.315",
    "profile_key": "f208713f7fdd4d1e86eb8a8de3c462bc",
    "run_key": "a7b6d18faaf34358b043fa36648612c6"
  }
}
```

20.1.2. Delete profile

POST the following payload to `services/TA-recordedfuture/delete_threat_hunt_config` to delete a threat hunt.

```
{
  "profile_key": "f208713f7fdd4d1e86eb8a8de3c462bc"
}
```

Example curl:

```
curl -X POST 'https://127.0.0.1:8089/services/TA-
recordedfuture/delete_threat_hunt_config?output_mode=json' \
  -d '{"profile_key":"f208713f7fdd4d1e86eb8a8de3c462bc"}' \
```

Response: * 200 - OK * 400 - Missing parameter

20.2. Threat hunt runs

Threat hunt runs are initiated threat hunts. Runs are stored in a collection, and may be accessed via the `threathunt_run` lookup. Runs can be initiated based on a profile, or stopped with a `run_key`.

Results are stored in a collection, and may be accessed via the `threathunt_result` lookup.

20.2.1. Start threat hunt

GET `services/TA-recordedfuture/create_threat_hunt_config?profile_key=<profile_key>` to start a threat hunt, where `profile_key` belongs to an existing profile.

Example curl:

```
curl -X GET 'https://127.0.0.1:8089/services/TA-recordedfuture/run_threat_hunt?profile_key=b7613b6abba94981b507e8366e977617&output_mode=json' \
```

Response:

- 200 - OK, response includes SID (Splunk ID) of primary threat hunt search.
 - 400 - Missing parameter
 - 500 - Unknown exception
-

20.2.2. Stop threat hunt

GET `services/TA-recordedfuture/stop_threat_hunt?run_key=<run_key>`, `run_keys` can currently only be found by reading the `threathunt_run` collection.

Example curl:

```
curl 'https://127.0.0.1:8089/services/TA-recordedfuture/stop_threat_hunt?run_key=e0d416d435cf4b0084b3e7ca48689a6d&output_mode=json' \
```

Response:

- 200 - OK
 - 400 - Missing parameter
-