



Recorded Future App for Splunk

Recorded Future, Inc

Table of Contents

1. Overview	1
2. Upgrade App	5
3. Install	6
3.1. Requirements	6
3.2. Instructions	6
3.3. Install on a Search Head Cluster	7
4. Data collection	8
5. Malware Threat Hunts	9
5.1. Threat Hunt Dashboard	9
5.2. Malware Threat Hunt	10
6. Attack Surface Intelligence	12
6.1. Configuration	12
6.2. Key Use Cases	13
7. Alert Center	17
7.1. Limitation for the number of alerts	18
8. Alerting Rules	19
8.1. Setup	19
9. Create Notables for Ingested Alerts	20
9.1. Ingestion	20
9.2. Setup (ES - 8.0+)	20
9.3. Setup pre ES - 8.0	25
9.4. Classic Alerts Dashboard	31
9.5. Playbook Alerts Dashboard	32
10. Correlations	33
10.1. Correlation Types	33
10.2. When a correlation rule is saved	33
10.3. Correlation Dashboards	40
10.4. Shifting Correlation window to mitigate indexing lag	41
10.5. Technical Information	42
10.6. Disabling Automatic Correlation Searches	42
11. Enrichment Dashboards	44
11.1. Technical Information	44
11.2. rfenrich	44
12. Sigma Rules	45
12.1. Setup	45
13. Sigma Detections	47
14. Splunk Enterprise Security Integration	48
14.1. Install	48
14.2. Configure Enterprise Security Correlations	48
14.3. Configure TI framework ingestion	49

14.4. Create Notables for Ingested Alerts	50
15. Adaptive Response Actions	66
15.1. Recorded Future Collective Insights	66
15.2. Recorded Future Enrichment	66
15.3. Recorded Future Threat Hunt	66
16. Collective Insights	68
16.1. Limit Detection Sharing for Organisations within a Multi-org Enterprise	69
17. Features Settings	70
18. Custom Search Commands	71
18.1. rfenrich	71
19. Troubleshoot	72
19.1. Reports	72
19.2. Logs	72
19.3. Report Issue	73
19.4. Troubleshooting Package	73
20. Further Help	75
Technical documentation	76
21. Server-side dashboard generation	77
22. Customization of savedsearches	78
23. Threat Hunting API	79
23.1. Threat hunt profiles	79
23.2. Threat hunt runs	81
24. Change Log	83
24.1. [2.8.0] (2025-04-02)	83
24.2. [2.7.2] (2025-03-05)	84
24.3. [2.7.1] (2025-02-05)	84
24.4. [2.7.0] (2025-01-08)	84
24.5. [2.6.3] (2025-02-05)	85
24.6. [2.6.2] (2024-12-16)	85
24.7. [2.6.1] (2024-11-26)	86
24.8. [2.6.0] (2024-10-07)	86
24.9. [2.5.1] (2024-09-04)	87
24.10. [2.5.0] (2024-04-19)	87
24.11. [2.4.3] (2024-09-04)	87
24.12. [2.4.2] (2024-04-24)	87
24.13. [2.4.1] (2024-03-14)	88
24.14. [2.4.1] (2024-03-14)	88
24.15. [2.4.0] (2024-02-08)	88
24.16. [2.3.3] (2024-03-14)	89
24.17. [2.3.2] (2024-01-18)	89
24.18. [2.3.1] (2023-11-16)	89
24.19. [2.3.0] (2023-10-13)	90

24.20. [2.2.2] (2023-09-20).....	91
24.21. [2.2.1] (2023-08-18).....	91
24.22. [2.2.0] (2023-07-10).....	91
24.23. [2.1.4] (2023-06-07).....	93
24.24. [2.1.3] (2023-03-20).....	94
24.25. [2.1.2] (2023-02-13).....	94
24.26. [2.1.1] (2022-12-15).....	94
24.27. [2.1.0] (2022-12-15).....	95
24.28. [2.0.8] (2023-02-01).....	95
24.29. [2.0.7] (2023-01-17).....	95
24.30. [2.0.6] (2022-12-13).....	96
24.31. [2.0.5] (2022-10-11).....	96
24.32. [2.0.4] (2022-09-13).....	96
24.33. [2.0.3] (2022-09-05).....	96
24.34. [2.0.2] (2022-06-16).....	97
24.35. [2.0.1] (2022-05-11).....	97
24.36. [2.0.0] - 2021-12-25.....	97

Chapter 1. Overview



Recorded Future for Splunk 2.6 officially only support **python3**.

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.

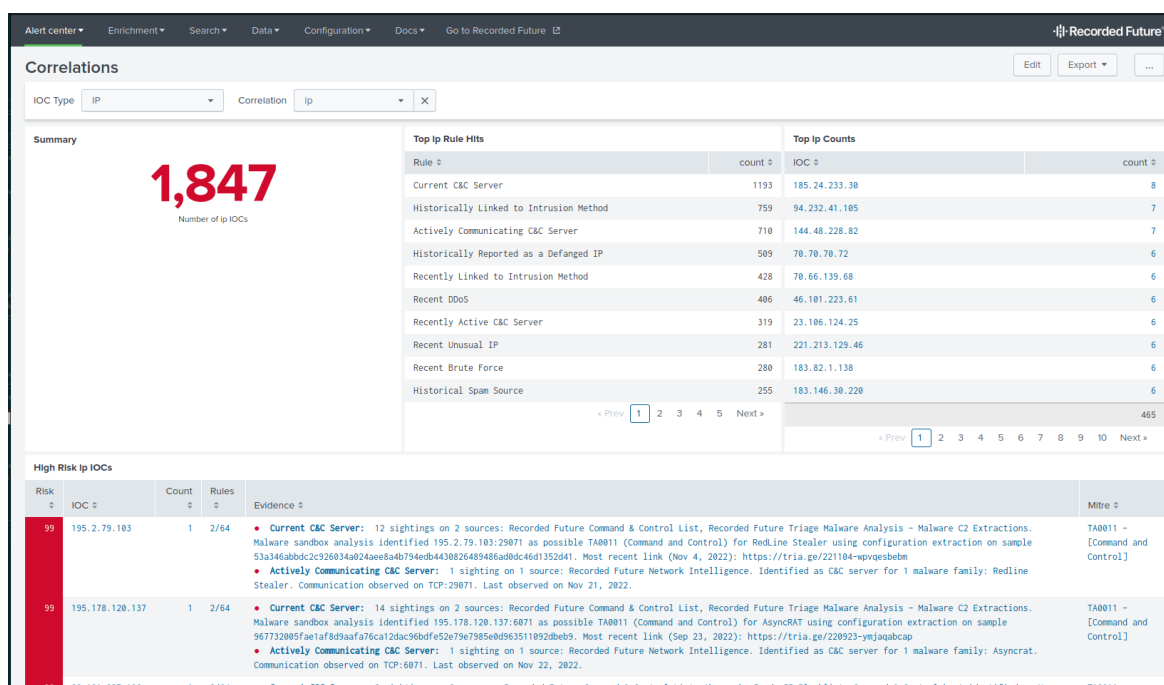


Figure 1. Correlation view

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.

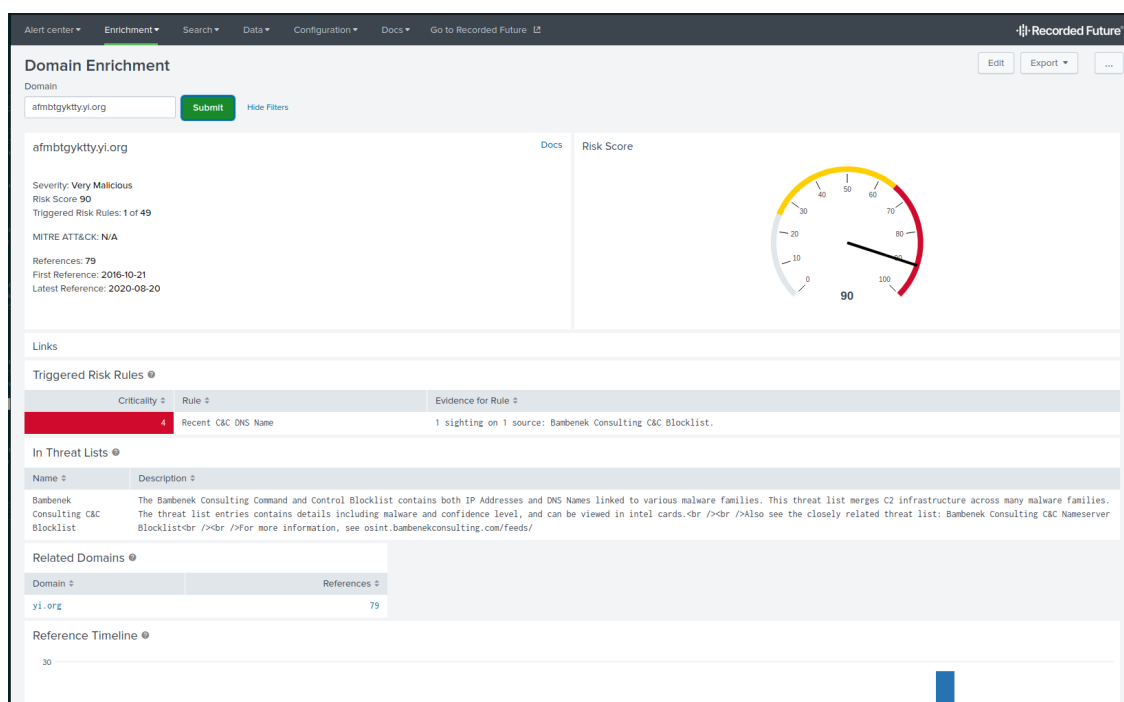


Figure 2. Enrichment view provides ample context for a suspicious IOC

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.

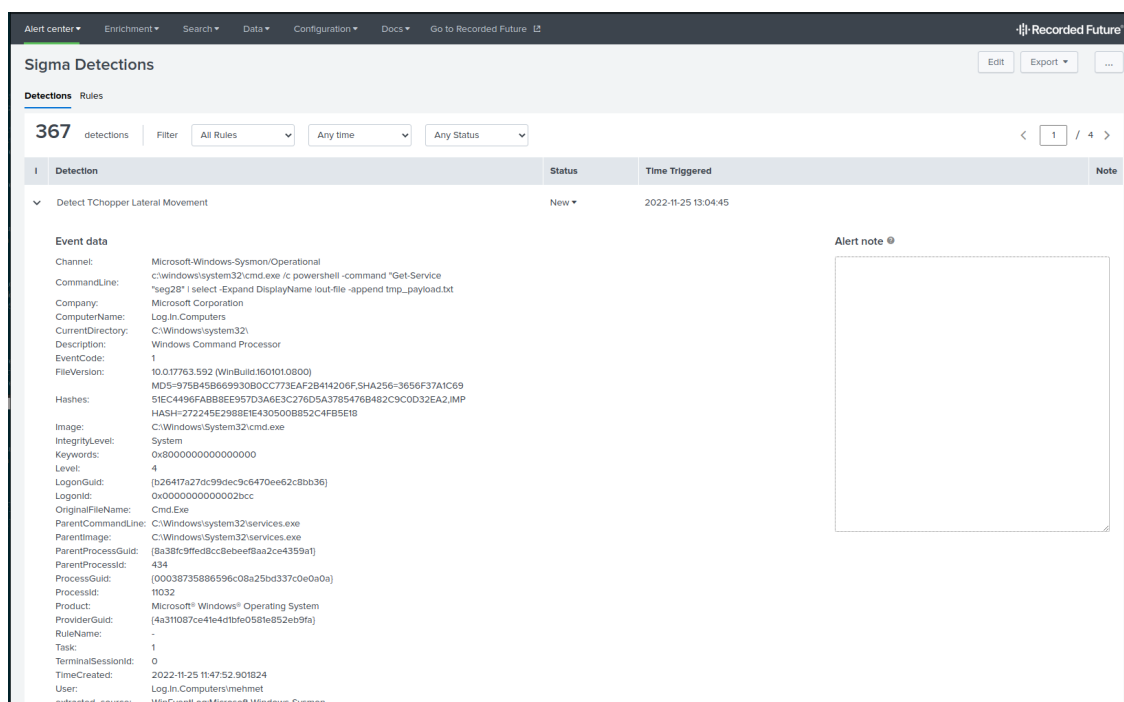


Figure 3. Sigma Detection Rules

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 Center

EditExport...

945 alerts

Alert Type

Any Alert Type

Filter

Last 24 hours

Any Status

< 1 / 10 >

I	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 - 114.34.17.53	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

Threat Hunts

Recorded Future for Splunk combines the SIEM platform with world-class threat intelligence to provide a tool to rapidly start with fundamental threat hunting. Utilize the wizard to run indicator based threat hunts, or use the API documentation in the documentation to automate the process outside the scope of the integration.

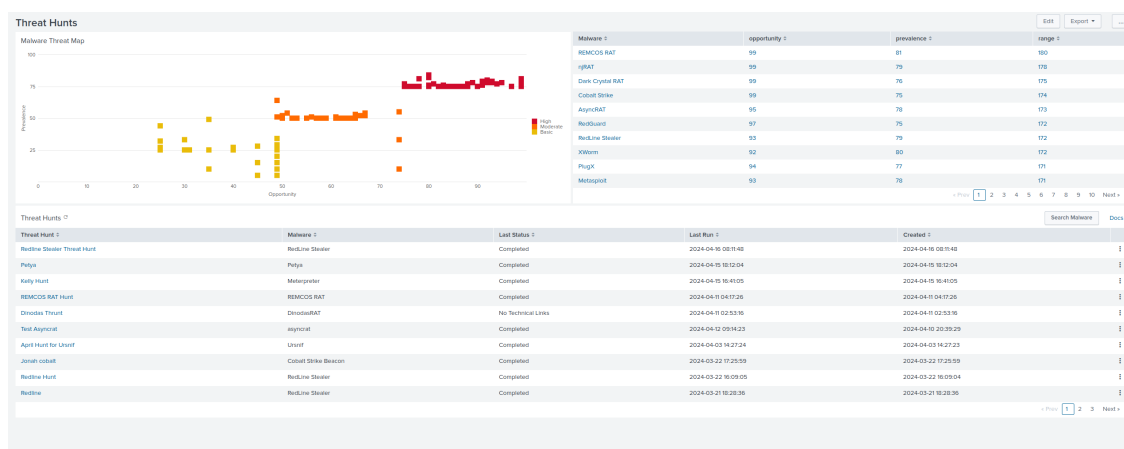


Figure 5. Recorded Future Threat Hunt

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 a Finding (Notable event) automatically. It's also possible to run the action ad-hoc.

Correlation search with Risk Based Alerting (RBA) 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...](#) Tag: [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 \(3334\)](#) [Add Selected to Investigation](#) [Prev](#) 1 2 3 4 5 ... [Next](#) [20 per page](#) [Refresh](#)

	Title	Risk Object	Risk Score	Risk Events	Type	Time	Disposition	Security Domain	Urgency	Status	Owner	Actions
<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 Fields

Additional	Value	Action
Destination	103.229.64.132 60	
Name	103.229.64.132	
Original	threatmatch://dest	
Splunk Source		
RF Triggered Rules	2/64	
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 TCP: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 60	
Source User	unknown 882189.0	
Threat	ip	
Category		
Threat Collection	ip_intel	
Threat Collection Key	p_default_ip_risklist103.229.64.132	

Related Investigations:
Currently not investigated.

Correlation Search:
[Recorded Future Correlationip](#)

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:

i No next steps defined.

Figure 6. Risk Based Alerting: Notable event created with additional Context and Risk assessment.

Chapter 2. 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.

Chapter 3. Install

3.1. 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; though designed to run on **Search Heads**
- **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.

See [Splunk Products Version Compatibility Matrix](#) for more details on compatibility between splunk products.

3.1.1. 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.

3.2. 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 > Settings**.

1. Select **General** option on the left menu
2. Verify that the application is connected with Recorded Future's API. "Status: Verified" will show when the connection is successful.
3. If the Status is "Not verified", the connection can require a proxy. Check "Use a proxy server" to activate a connection via proxy.
4. Enter the required fields. If the proxy server requires authentication, enter a valid username and password, otherwise leave these fields blank.



If your proxy is accessed via an IPv6 address, please enclose the IPv6 address in brackets.

5. Connect by clicking [**Verify API URL**]. The Status should be "Verified", if it isn't, review the proxy settings.
 - Only change the API URL or disable SSL verification if asked by your Recorded Future point of contact.
6. Enter the API Token. Contact Recorded Future to receive one.
7. Click [**Verify API Token**].

3.3. 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 zxvpf recorded-future-app-for-splunk_280.tgz`
3. Remove the package file:
`rm recorded-future-app-for-splunk_280.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 4. Data collection

Recorded Future collects unattributed data regarding application performance and feature usage in order to continuously improve the application.

For more information, please see Frequently Asked Questions at www.recordedfuture.com/faq/security

Chapter 5. Malware Threat Hunts

5.1. Threat Hunt Dashboard

You can start a Threat Hunt in two ways:

- 1. **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.
- 2. **By clicking on Threat Map marker or Threat Table row** and pressing **Create Threat Hunt** button. 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.

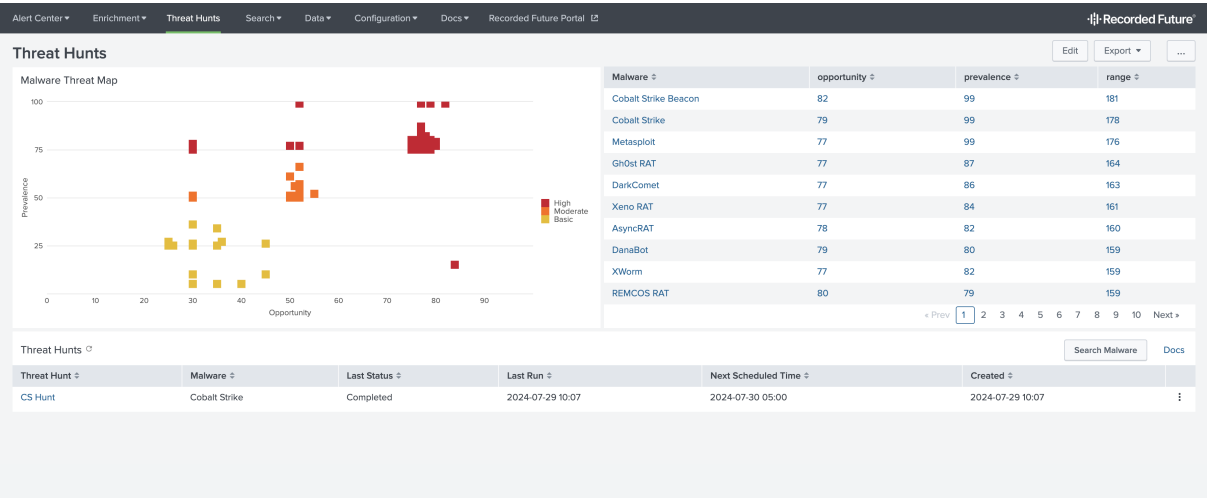
You can also schedule a Threat Hunt. To do this, toggle on the "Schedule search" input and set your desired schedule. This will create a scheduled saved search with the owner set to the current user, binding the schedule to the owner's local time zone.

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

Starting the hunt creates a new job in Splunk which may take some time to complete depending on the size of your index and how many source types and event fields you 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. It does not affect the schedule of the Threat Hunt.

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.

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 **Threat Hunts**.
2. Click on the Threat Map marker or Threat Table row and select **Create Threat Hunt** in the dropdown.
3. Configure the hunt:
 - Name the hunt
 - Select IOC types to search for
 - Select Splunk Events to search in
 - Set up the schedule (optional)
4. Click **Save and Run**.

5. Done.

Alternatively, you can follow these steps:

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
 - Set up the schedule (optional)
5. Click **Save and Run**.
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. Attack Surface Intelligence

The Attack Surface Intelligence (ASI) Integration with Splunk allows you to collect and analyze your attack surface data within the Splunk environment as you would natively within the Recorded Future Portal. It will query for your latest project data with appropriate visuals and actions.

6.1. Configuration

To configure Attack Surface Intelligence go to **Configuration › Settings › Attack Surface Intelligence**)

There you will be able to set up the API key and the Project ID required for Attack Surface Intelligence.

6.1.1. API Key

1. Go to **Account** under Security Trails portal.

The screenshot shows the Recorded Future Attack Surface Intelligence interface. At the top, there's a header with the Recorded Future logo, a 'Company Domain' dropdown, a search bar, and navigation links for 'Projects', 'SQL', 'Browse', and a user profile icon. Below the header, the main content area is titled 'Bank Demo' and includes a 'Summary' tab and several sub-tabs: 'Explorer', 'IP Explorer', 'Inventory', 'Risk Rules', 'Activity', and 'Export'. On the right side, there are 'Notifications' and 'Account' links, along with a 'View downloads' button. A summary card shows '1,845 Hostnames'. The main dashboard is divided into two sections: 'Risks' and 'Recent Assets Feed'. The 'Risks' section displays three risk levels: Critical (2), Moderate (22), and Informational (14). Below this is a table of risks with columns for Severity, Name, and Hosts. The 'Recent Assets Feed' section shows a table of assets with columns for Hostname and First Seen.

Severity	Name	Hosts
Critical	WordPress Contact Form 7 Plugin - Unrestricted File Upload (CVE-2020-35489)	1
Critical	Detect unpatched (CVE-2023-27997) FortiOS VPN Interface	1
High	Public Remote Desktops	2
High	Vanguard Marketplace CMS 2.1 - Cross-Site Scripting	2
High	Symfony Profiler - Detect	1

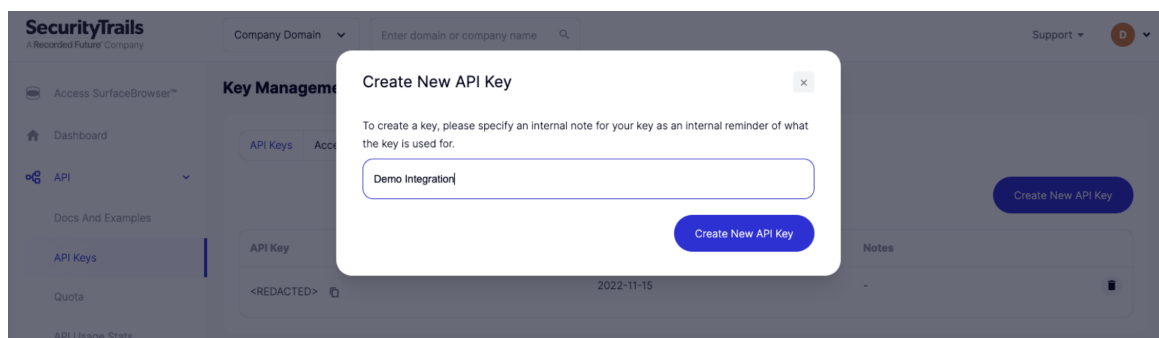
Hostname	First Seen
mobile-app.banescopagos.com	4d
auth-corpocard.alfabank.by	5d
corpocard.alfabank.by	6d
sinweb.banescosegurosonline.com.pa	1w
webmail.site.awashbank.com	2w

2. Click on **API Keys** under API on the left sidebar.

The screenshot shows the SecurityTrails Key Management page. The left sidebar contains navigation links: 'Access SurfaceBrowser™', 'Dashboard', 'API', 'Docs And Examples', 'API Keys', 'Quota', and 'API Usage Stats'. The main content area is titled 'Key Management' and has two tabs: 'API Keys' and 'Access Restrictions'. A 'Create New API Key' button is visible. Below the tabs is a table with columns for 'API Key', 'Created Date', and 'Notes'. The table contains one entry with a redacted API key and a creation date of 2022-11-15.

API Key	Created Date	Notes
<REDACTED>	2022-11-15	-

3. Click on **Create New API Key** button or copy the existing API key.



6.1.2. Project ID

1. Go to the project page under Security Trails portal
2. Copy the unique UID in the URI of the project page to be used for configuring the app in Splunk.

6.2. Key Use Cases

There are four use cases for attack surface intelligence.

- Monitor changes in your attack surface
- Analyze your attack surface makeup
- Understand identified exposures in your attack surface
- Investigate network artifacts

6.2.1. Monitor changes in your attack surface

The **Activity dashboard** will allow you to see the newly discovered and cleared risks within your attack surface. The bottom panel also allows you to see a stream of assets that Attack Surface Intelligence discovers in real time.

Activity

EditExport...

Recently Added Issues				Recently Cleared Issues			
Issue	Asset	Severity	Risk	Issue	Asset	Severity	Risk
Vulnerable Version of Sun ONE Web Server	banescoseguros.xyz	informational	26	Pypiserver 1.2.5 - CRLF Injection (CVE-2019-6802)	banescoseguros.xyz	moderate	65
Adobe Connect Username Exposure	vc.ansarbank.ir	informational	15	End of Life - PHP	www.wi-fi.alfabank.by	informational	35
WordPress Contact Form 7 Plugin - Unrestricted File Upload (CVE-2020-35489)	www.banescoseguros.org	high	99	End of Life - PHP	www.update.alfabank.by	informational	35
Detect unpatched (CVE-2023-27997) FortiOS VPN Interface	test-mb.sberbank.hr	high	99	End of Life - PHP	www.note.alfabank.by	informational	35
Detect unpatched (CVE-2023-27997) FortiOS VPN Interface	sxstest001.sberbank.hr	high	99	End of Life - PHP	www.life.alfabank.by	informational	35
Pre-auth Fully-responded SSRF (CVE-2018-1000600)	online.banescocom.cw	moderate	89	End of Life - PHP	www.docs.alfabank.by	informational	35
Exposed Kibana	search-node1.microdinc.com	moderate	65	End of Life - PHP	www.credits.alfabank.by	informational	35
Advanced Custom Fields PRO <= 6.1.5 - Reflected Cross-Site Scripting via 'post_status'	www.bcatech.com	moderate	65	End of Life - PHP	www.check.alfabank.by	informational	35
Advanced Custom Fields PRO <= 6.1.5 - Reflected Cross-Site Scripting via 'post_status'	qa.banescocom.pa	moderate	65	End of Life - PHP	www.banksepah.it	informational	35
Advanced Custom Fields PRO <= 6.1.5 - Reflected Cross-Site Scripting via 'post_status'	proaktesmbacs.pro-file.com	moderate	65	End of Life - PHP	wi-fi.alfabank.by	informational	35

« Prev12345678910Next»

Last update: 2023-07-26 02:20:01

6.2.2. Analyze your attack surface makeup

The **Inventory dashboard** will allow you to see notable segments of your attack surface to easily identify out-of-policy assets and those which stick out as inadvertent exposures. Filters at the top will allow you to easily isolate assets by hosting provider, country, and so on.

InventoryShow Filters

EditExport...

Hosts by Hosting Provider

Hosting Provider	Number of Hosts
IBANESCO_NAL BANK	2
Charter C...tions Inc	1
Domain na...gandi.net	1
ORANGE...S U.S. Inc.	1

Hosts by Country

Country	Number of Hosts
Venezuela	1
Panama	1
United States	1
France	1

Hosts by Hosting Server

Hosting Server	Number of Hosts
null	73
cloudflare	12
nginx	4
Apache	2
Apache/2	2
Microsoft-IIS/8.5	2
CE_E	1
Microsoft-IIS/10.0	1
Oracle-T.12.21.0.0	1
cPanel	1
openresty	1

Hosts by IP Address

IP Address	count
201.218.224.26	1
201.218.224.90	1
216.72.89.136	1
217.70.178.4	1
66.57.101.10	1

Hosts by Open Port

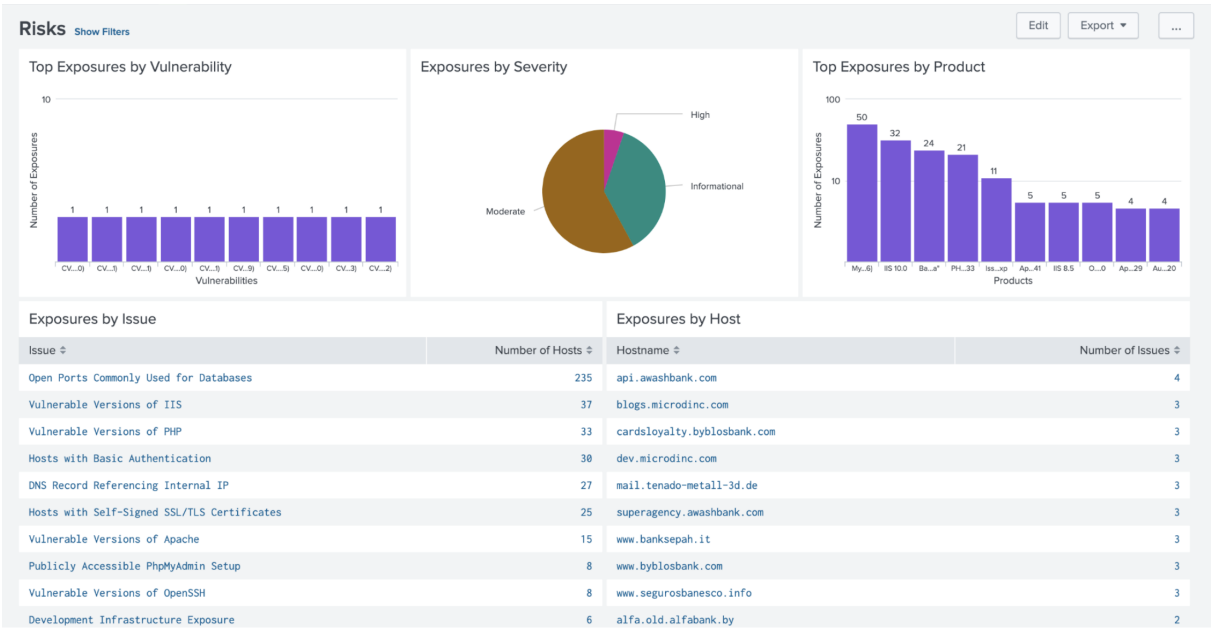
Open Port	Number of Hosts
143	1
993	1
995	1

Hosts by Certificate Issuer

Certificate Issuer	Number of Hosts
null	67
Cloudflare Inc ECC CA-3	8
Sectigo RSA Domain Validation Secure Server CA	7
COMODO ECC Domain Validation Secure Server CA 2	4
Certum Domain Validation CA SHA2	4

6.2.3. Understand identified exposures in your attack surface

The **Risks dashboard** will allow you to see where your attack surface exposes you to threats based on the most recent scan data. The filters at the top will also allow you to easily isolate assets and issues of interest in your investigation.



Hostname and Apex Domain Investigation

Enter Hostname

google.com

Submit

Hide Filters

Edit

Export

...

Hostname Investigation

DNS

A Records	AAAA Records
172.253.122.100	2607:f8b0:4004:c09::64
172.253.122.101	2607:f8b0:4004:c09::65
172.253.122.102	2607:f8b0:4004:c09::71
172.253.122.113	2607:f8b0:4004:c09::8b
172.253.122.138	
172.253.122.139	

IP Resolution

IP Address	IP Block	ASN Number	ASN Owner	Country
172.253.122.100	172.253.64.0/18	15169	Google LLC	United States
172.253.122.101	172.253.64.0/18	15169	Google LLC	United States
172.253.122.102	172.253.64.0/18	15169	Google LLC	United States
172.253.122.113	172.253.64.0/18	15169	Google LLC	United States
172.253.122.138	172.253.64.0/18	15169	Google LLC	United States
172.253.122.139	172.253.64.0/18	15169	Google LLC	United States

HTTP Crawl

Copyright	Email	Title	Content-Type	Server	MD5	Headers
		Google	text/html	gws	85b66f6c71b735baefd5a3b574e82865	cache-control:private, max-age=0 content-type:text/html; charset=ISO-8859-1 content-security-policy:report-only;object-src 'none';base-uri 'self';script-src 'nonce-koxk5oJGbuysT0pK90UIg' 'strict-dynamic' 'report-sample' 'unsafe-https://csp.withgoogle.com/csp/gws/other-hp' accept-ch:Sec-CH-Prefers-Color-Scheme p3p:CP="This is not a P3P policy! See g.co/p3phelp for more info." server:gws x-xss-protection:0 x-frame-options:SAMEORIGIN set-cookie:AEC=AVc:jaZeQh9xKpz_PaUsP5lbdwMXas0YKIVT8qH8JgdEZDya8go3azhu5w; expires=Mon, 18-Aug-2025 14:49:42 GMT; path=/; domain=.google.com; Secure; HT1 set-cookie:NTD=521=TAx44yJKr6buhevApP4MGhNtLxEVpJBjx5Itp0t1bwDuulwa1AltnVQvAKKzanZEAfK2M_zU6AwUJZF57abzrfdZ0foc9RvBQCmMItouuQcyz0_ENVUis8fuu_9XRJbnTJ30KAN00 expires=Thu, 21-Aug-2025 14:49:42 GMT; path=/; domain=.google.com; HttpOnly alt-svc:h3=":443"; ma=2592000,h3-29=":443"; ma=2592000 accept-ranges:none vary:Accept-Encoding

SSL Crawl

No results found.

Apex Domain Investigation

Subdomain Count

5,016,862

Subdomains

Subdomains

maps

support

play

plus

docs

drive

developers

policies

accounts

sites

« Prev

1

2

3

4

5

6

7

8

9

10

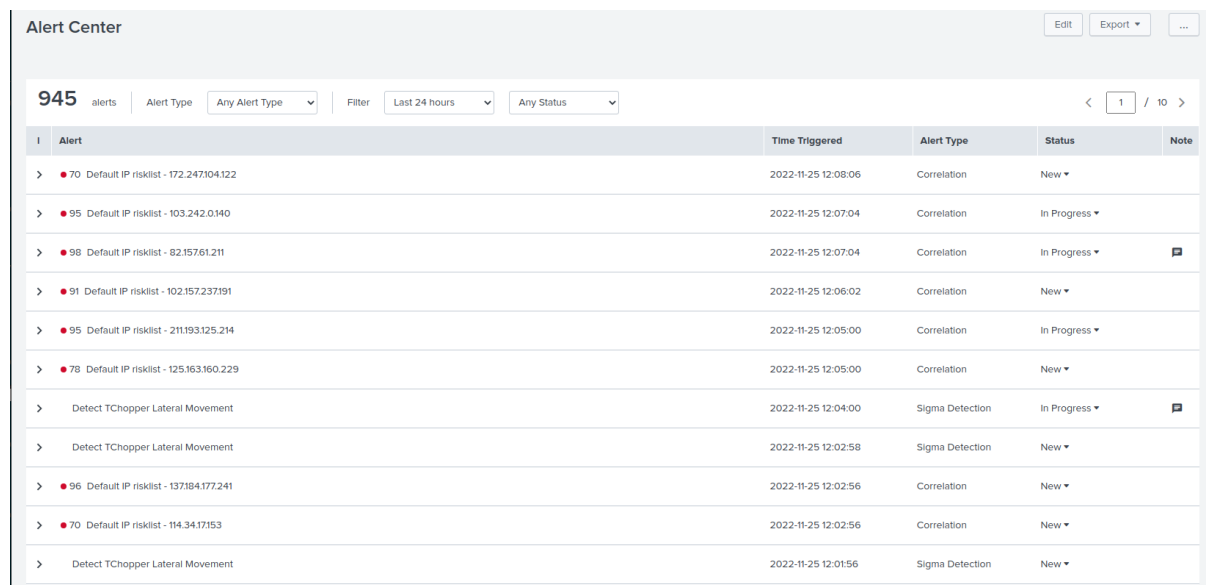
Next »

Whois

Organization	Country	Registrar	Registration Date	Expiry Date
Google LLC		MarkMonitor Inc.	1997-09-15T04:00:00Z	2028-09-14T04:00:00Z

Chapter 7. 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.



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 - 114.34.17.153	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.

7.1. 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:

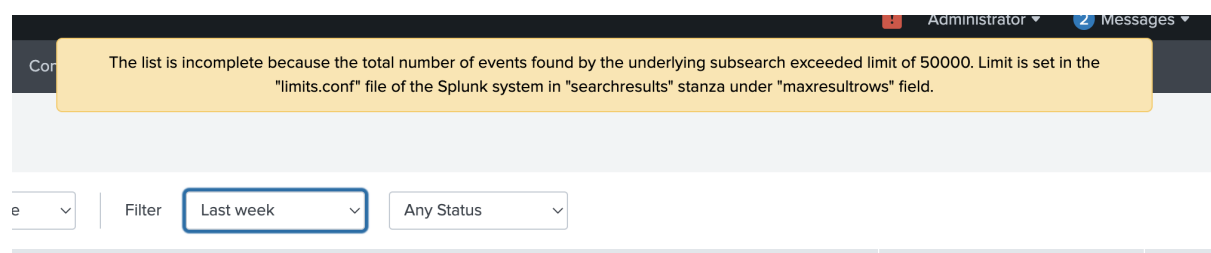
```
[searchresults]
maxresultrows = <integer>
```

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.



Chapter 8. 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.

8.1. 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.

Chapter 9. Create Notables for Ingested Alerts

9.1. Ingestion

After enabling the rule on the **Alerting Rules** page, you automatically start ingestion for this rule. The saved search with name **Recorded Future - Ingest Alerts** runs every 10 minutes. It retrieves the enabled rules and writes newly created alerts to the corresponding KV store collection:

- **alert_ingested** - for Classic Alerts
- **playbook_alert_ingested** - for Playbook Alerts

The application does not automatically set an initial time period for the first ingestion. This means that the ingestion will begin only after the associated rule is enabled for ingestion.

By default, ingested alerts are retained in the KV store collection for up to **365 days** or **10,000 records**, whichever limit is reached first. You can modify these retention settings:

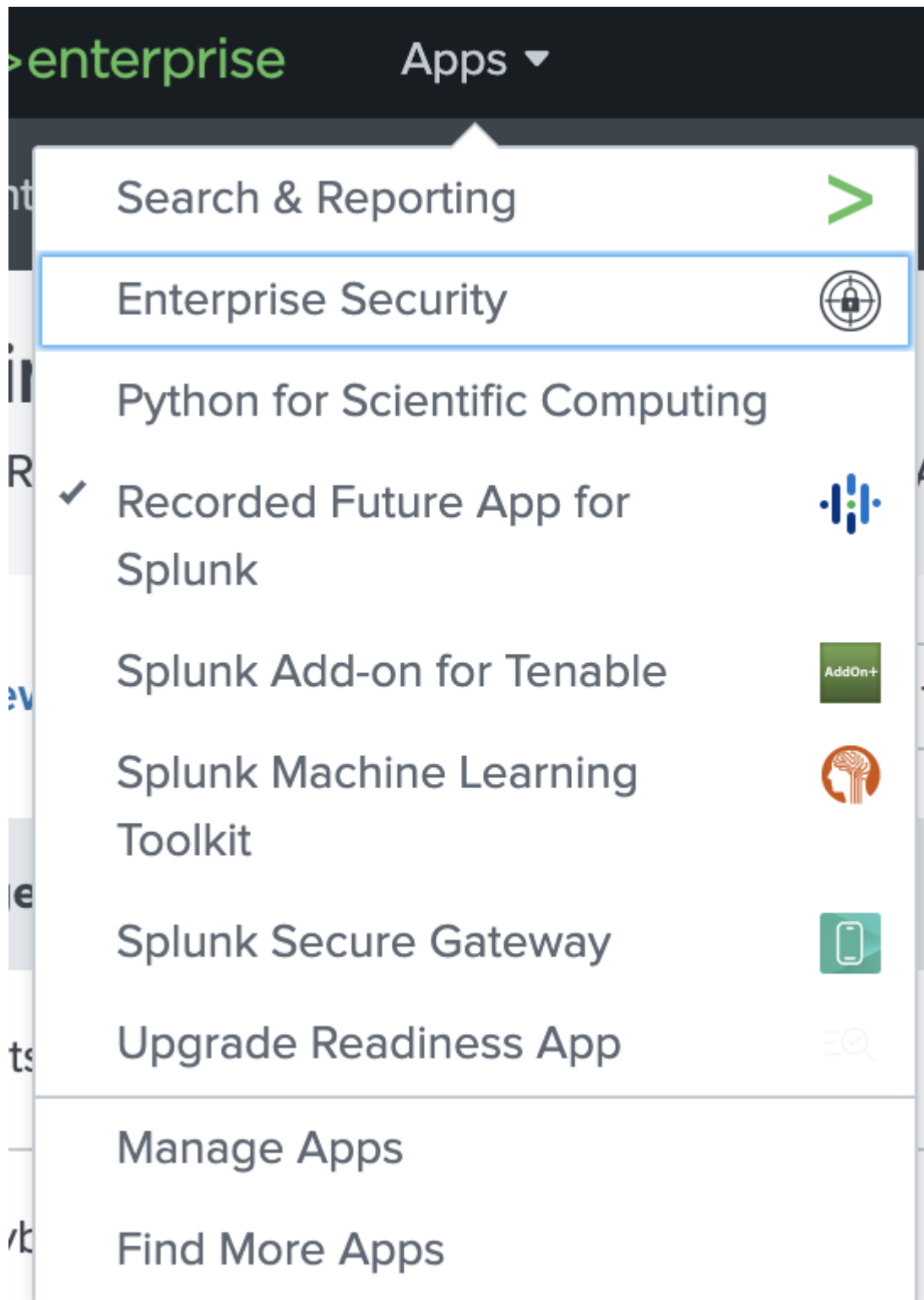
- Navigate to **Configuration › Settings › Features** to adjust the retention period and record limits.

9.2. Setup (ES - 8.0+)

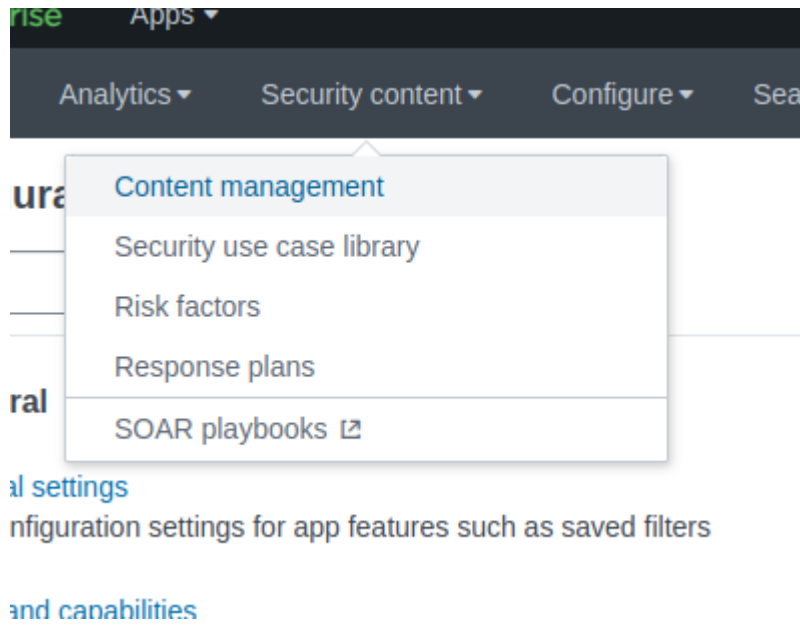
For older version of ES see [Setup pre ES - 8.0](#)

We will set up the creation of Findings (Notable Events) based on the new records in the corresponding collection.

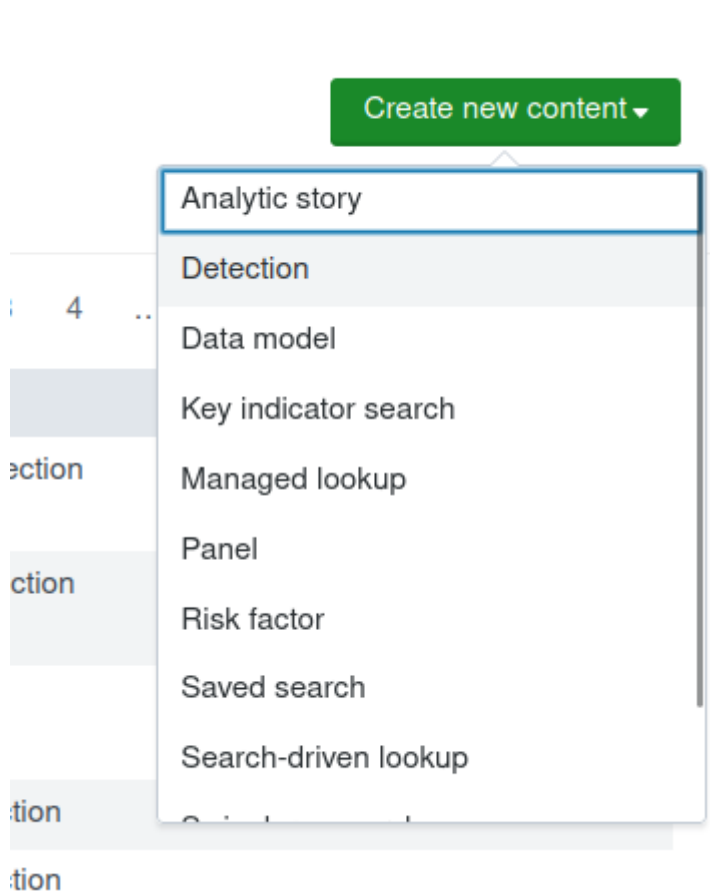
1. Open "Enterprise Security" application
-



2. Go to **Security Content** › **Content Management**



3. Press [**Create New Content**] and select [**Detection**]



4. Select **Event-based detection**
5. Make sure that **Finding** is the selected output type.

*** Finding output type**
Set up event-based detections to triage security threats. [Findings documentation](#)

☐ **Intermediate finding** RECOMMENDED
Records or observations created by event-based detections that indicate anomalies but might not be standalone security incidents.
Intermediate findings do not appear on the analyst queue until grouped by a [finding-based detection](#).

☒ **Finding**
Alerts that might be a security incident. Created by event-based or finding-based detections and displayed in the analyst queue.

6. In **2 › Event-based Detection**, set the **Detection name** (e.g. "New Ingested Classic Alerts") and set the **Detection description**.

7. In **2 › Event-based Detection**, set the **Detection search** (assuming we want to run the detection every 6 hours):

- Classic Alerts

```
| inputlookup alert_ingested
| eval new_record = if(_time > relative_time(now(), "-6h@h"), 1, 0)
| search new_record=1
```

- Playbook Alerts

```
| inputlookup playbook_alert_ingested
| eval new_record = if(_time > relative_time(now(), "-6h@h"), 1, 0)
| eval id = _key
| search new_record=1
```

8. Go to **3 › Analyst queue**

9. Set the **Title** and **Description** for new Findings, optionally set other fields. Example **Title** for Classic Alert:

New Alert Finding for \$rule.name\$



You can use fields of the alerts collection lookup, as defined in [transforms.conf](#) file, surrounded by dollar signs as in the example above.

10. In **Drill-down Dashboards** select the **[+ Add Drill-down Dashboard]**

Drill-down dashboards

[+ Add drill-down dashboard](#)

Add a drill-down dashboard for additional context to view multiple drill-down searches for a finding during an investigation.

11. In the dropdown list in **Dashboard** select the appropriate alerts dashboard:

- [TA-recordedfuture/rfes_alerts_list_v2](#) - for Classic Alerts
- [TA-recordedfuture/playbook_alerts](#) - for Playbook Alerts

12. Set the **Name** (e.g. "Alert details")
13. Press [**Edit Tokens**] and in the modal window press [**+ Drill-Down Token**]

Edit tokens documentation'. Below this is a table with two columns: 'Token Name' and 'Token Value'. Under 'Token Name' is a button '+ Drill-Down Token'. At the bottom right are two buttons: 'Cancel' and 'Save'."/>

14. Set **Token Name** as **deeplink** and set **Token Value** to **\$id\$**.

15. Press [**Save**] on the modal window.
16. Go to **4** › **Assign risk**, ES 8.0.2 forces you to configure this block to save the configuration. Since this detection is **finding** based these values will not have impact. Suggested values:
17. Set **Risk message** to "Recorded Future Alert"
18. Set **Entity** to "id"; this will group risk on the alert ID.
19. Set **Entity Type** to "other"
20. Go to **6** › **Cron Schedule** and set the desired schedule for this search, in our case it is every 6 hours:

* */6 * * *

21. Go to **7** › **Conditions** and pick [**For each result**].

Conditions
Trigger conditions to create a finding. [Conditions documentation](#)

Create when: Number of Results

is greater than 0

Create: Once | For each result

Adaptive response actions are created for each detection result.

22. Press [Save].

Now you have set up the creation of Notable Events for ingested alerts. After the detection runs, you should see the Notables on the **Incident Review** page of the Enterprise Security application.

Analyst queue: New Alert | Last 24 hours | Saved Views: Select... | Charts | Hide Timeline

Time Range: Last 24 hours | Search: New Alert | Clear All | Save

Updating: Auto refresh on | 20 per page

notable_title	ID	notable_type	risk_object	PK	F	F	F	_time	disposition
New Alert Notable for Brand Mentions with Cyber entities	3C2Cw4	3C2Cw4	3C2Cw4	3C2Cw4	3C2Cw4	3C2Cw4	3C2Cw4	Today, 9:10 AM	Undetected
New Alert Notable for Identify Similar Domains	3C2CwX	3C2CwX	3C2CwX	3C2CwX	3C2CwX	3C2CwX	3C2CwX	Today, 9:10 AM	Undetected
New Alert Notable for Analysis from Inskt Group	3C2CwM	3C2CwM	3C2CwM	3C2CwM	3C2CwM	3C2CwM	3C2CwM	Today, 9:10 AM	Undetected
New Alert Notable for Global Trends, Trending Targets	3C2CwQ	3C2CwQ	3C2CwQ	3C2CwQ	3C2CwQ	3C2CwQ	3C2CwQ	Today, 9:10 AM	Undetected
New Alert Notable for Malware Intelligence from Inskt Group	3C2CwR	3C2CwR	3C2CwR	3C2CwR	3C2CwR	3C2CwR	3C2CwR	Today, 9:10 AM	Undetected
New Alert Notable for Global Vulnerability Risk, New Critical or Pre-WVD Vulnerabilities	3C2CwN	3C2CwN	3C2CwN	3C2CwN	3C2CwN	3C2CwN	3C2CwN	Today, 9:10 AM	Undetected
New Alert Notable for Leaked Credential Monitoring	3C2CwL	3C2CwL	3C2CwL	3C2CwL	3C2CwL	3C2CwL	3C2CwL	Today, 9:10 AM	Undetected
New Alert Notable for IP Address Mentions	3C2CwK	3C2CwK	3C2CwK	3C2CwK	3C2CwK	3C2CwK	3C2CwK	Today, 9:10 AM	Undetected
New Alert Notable for Company Email on Code Repository	3C2CwJ	3C2CwJ	3C2CwJ	3C2CwJ	3C2CwJ	3C2CwJ	3C2CwJ	Today, 9:10 AM	Undetected
New Alert Notable for Leads and TTPs from Inskt Group	3C2CwI	3C2CwI	3C2CwI	3C2CwI	3C2CwI	3C2CwI	3C2CwI	Today, 9:10 AM	Undetected
New Alert Notable for Vulnerability Intelligence from Inskt Group	3C2CwH	3C2CwH	3C2CwH	3C2CwH	3C2CwH	3C2CwH	3C2CwH	Today, 9:10 AM	Undetected

New Alert Notable for Identify Similar Domains

Owner: Unassigned | Status: New | Urgency: Medium

Sensitivity: Select... | Disposition: Undetermined

Time: Feb 4th, 2025 9:10 AM

Last updated: N/A

Reference ID: 6cd7c318-b93b-4979-4500-9cdedf866fcb@notable@6cd7c318-b93b-4979-4500-9cdedf866fcb

Detection: Threat - New Ingested Classic Alerts - Rule

Detection name: Threat - New Ingested Classic Alerts - Rule

Related investigations: No related investigations

Drill-down dashboard: Alert Details

History: View all review activity

Adaptive responses: Obtaining list of adaptive responses...

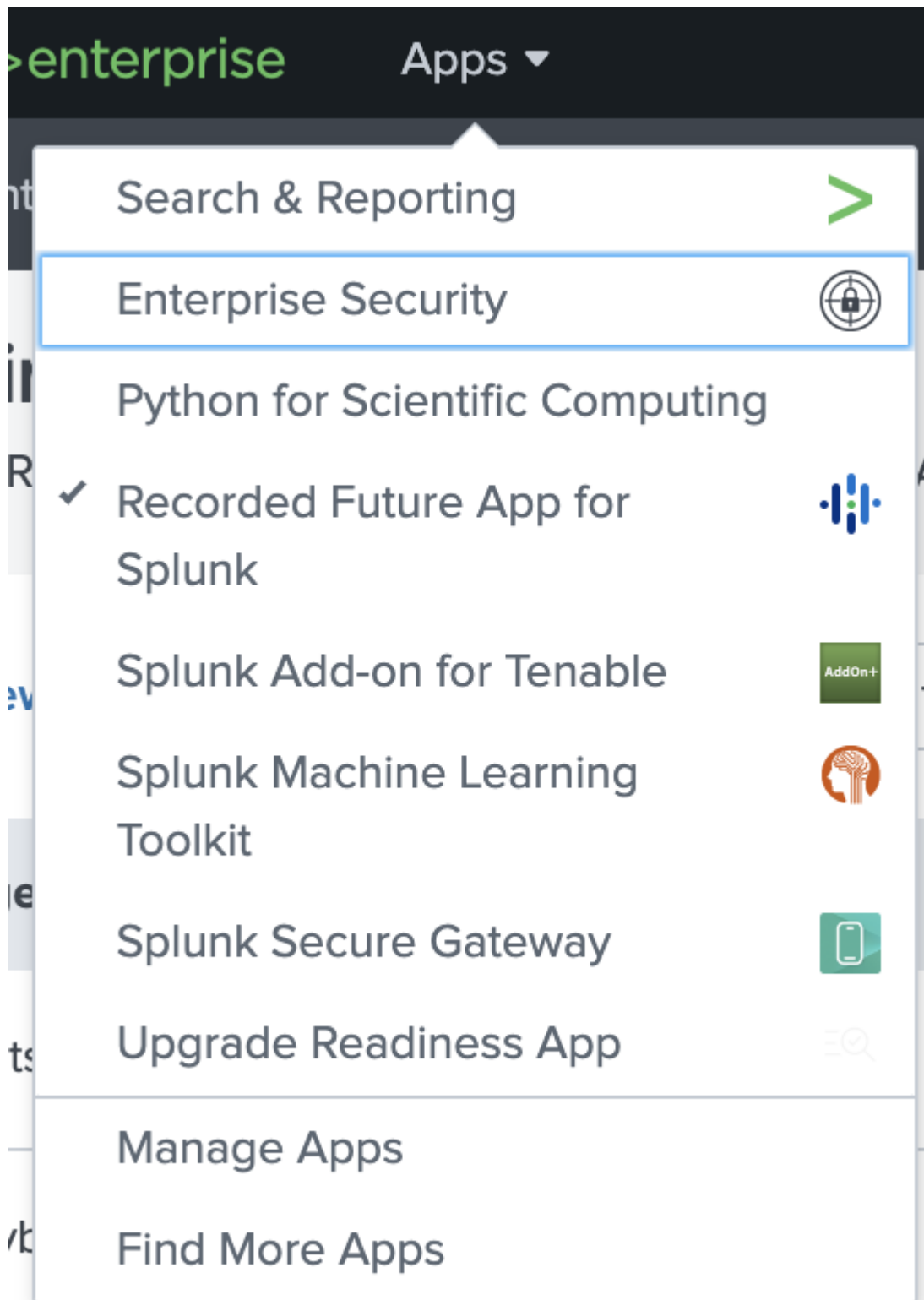
View Adaptive Response Invocations

Notes

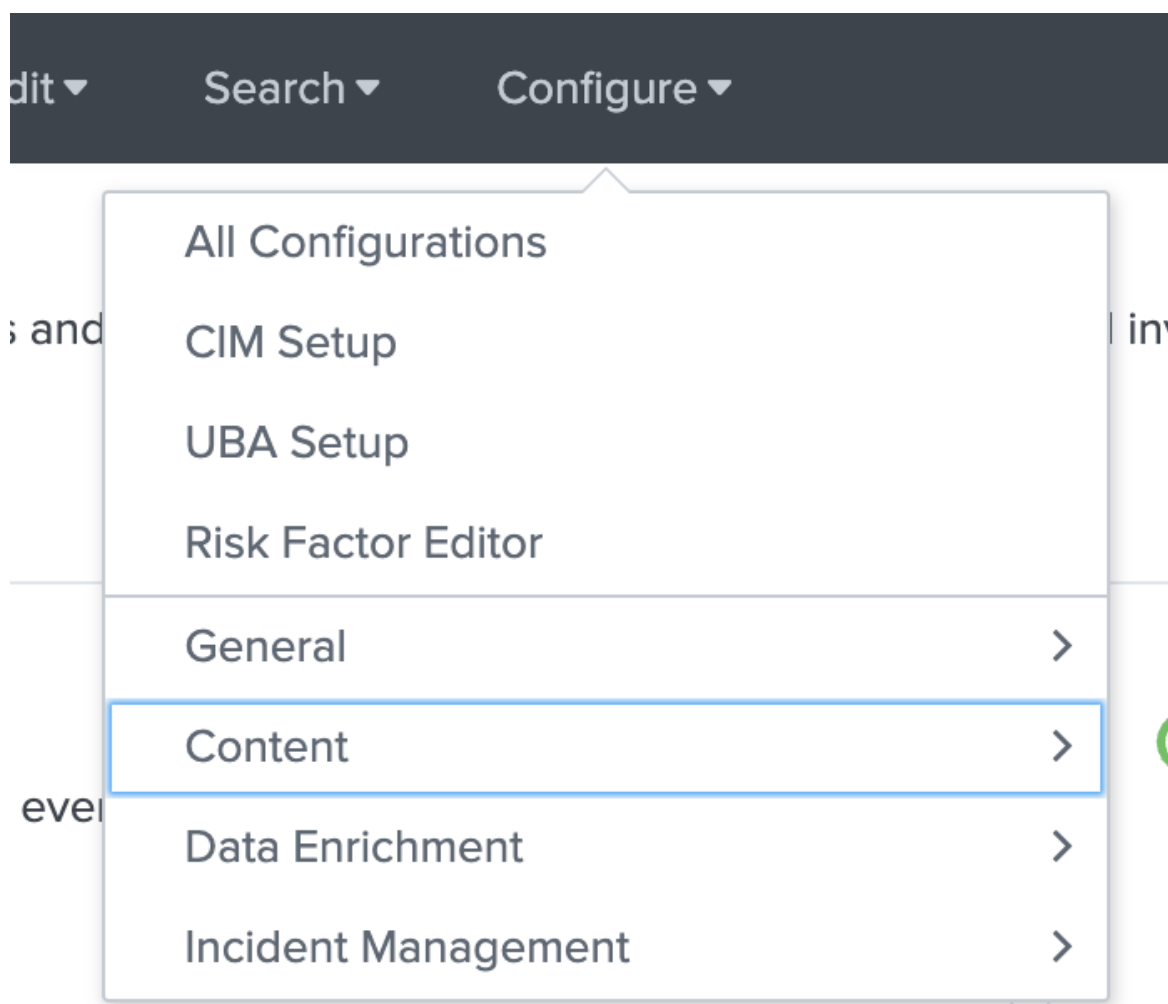
9.3. Setup pre ES - 8.0

We will set up the creation of Notable Events based on the new records in the corresponding collection.

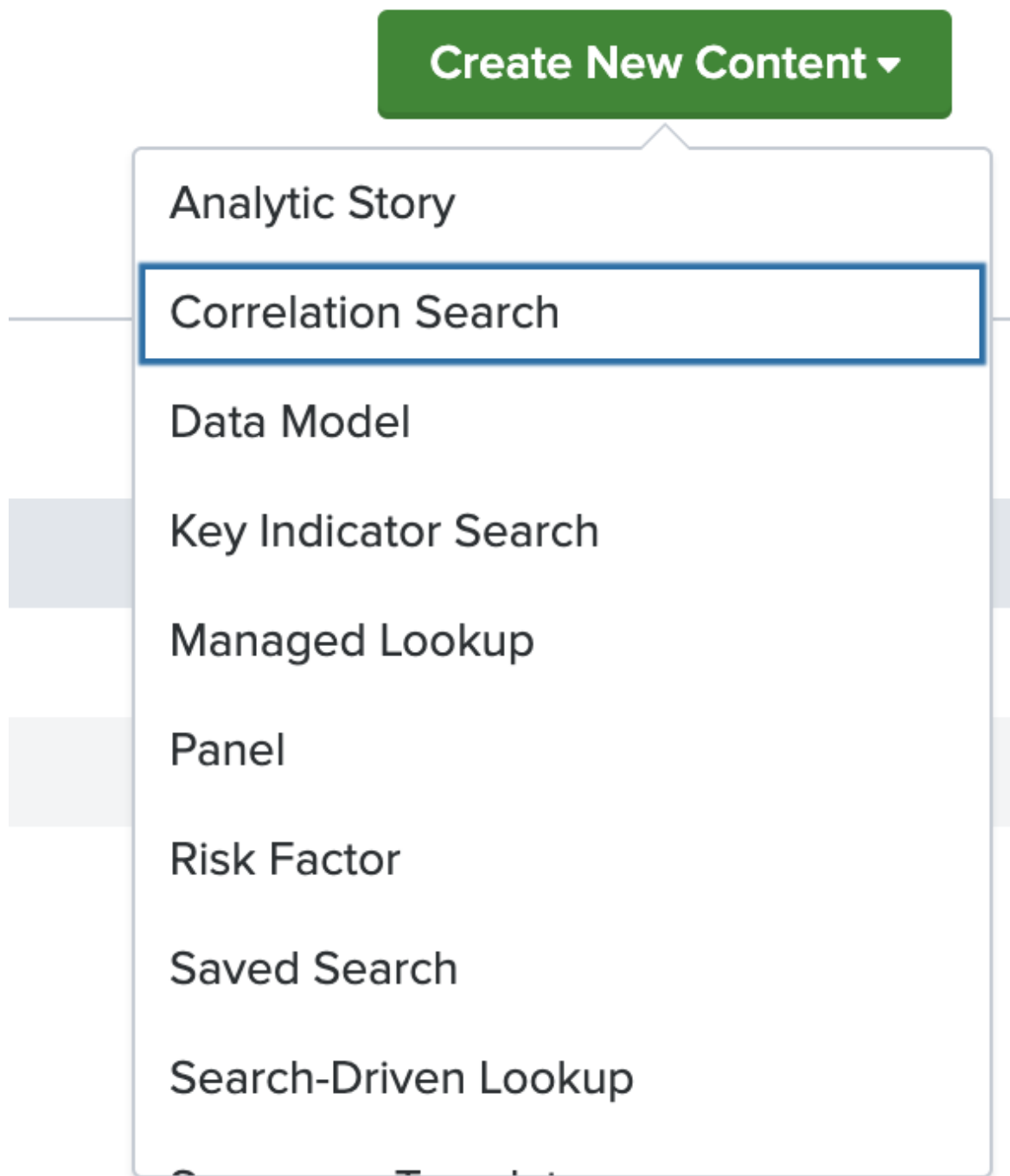
1. Open "Enterprise Security" application



2. Go to **Configure** › **Content** › **Content Management**



3. Press [**Create New Content**] and select [**Correlation Search**]



4. Set the **Search Name** (e.g. "New Ingested Classic Alerts") and optionally set the **Description**.
5. Set the **Search** (assuming we want to run the correlation search every 6 hours):
 - Classic Alerts

```
| inputlookup alert_ingested  
| eval new_record = if(_time > relative_time(now(), "-6h@h"), 1, 0)  
| search new_record=1
```

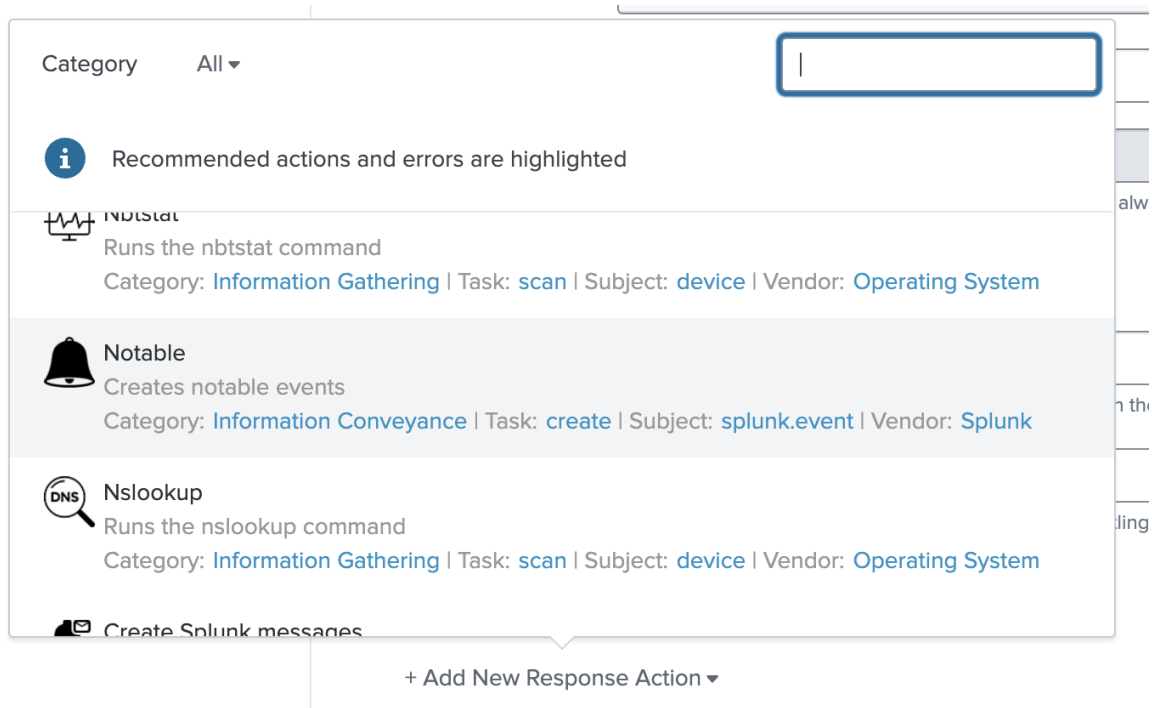

- Playbook Alerts

```
| inputlookup playbook_alert_ingested
| eval new_record = if(_time > relative_time(now(), "-6h@h"), 1, 0)
| eval id = _key
| search new_record=1
```

6. Go to **Time Range** › **Cron Schedule** and set the desired schedule for this search, in our case it is every 6 hours:

```
* */6 * * *
```

7. Go to **Trigger Conditions** › **Trigger** and pick [**For each result**].
8. In **Adaptive Response Actions** select [**+ Add New Response Action**] and pick **Notable**.



9. Set the **Title** for new Notable Events (example for Classic Alert):

```
New Alert Notable for $rule.name$
```



You can use fields of the alerts defined in `transforms.conf` file surrounded by dollar signs as in the example above.

10. Optionally set the **Description** and other fields.
11. In **Drill-down Dashboards** select the [**+ Add Drill-down Dashboard**]

Drill-down
Dashboards

+ Add Drill-down Dashboard

12. In the dropdown list in **Dashboard** select the appropriate alerts dashboard:

- **TA-recordedfuture/rfes_alerts_list_v2** - for Classic Alerts
- **TA-recordedfuture/playbook_alerts** - for Playbook Alerts

13. Set the **Name** (e.g. "Alert details")

14. Press [**Edit Tokens**] and in the modal window press [**+ Drill-Down Token**]

Edit tokens documentation'. Below this is a table with two columns: 'Token Name' and 'Token Value'. Under 'Token Name' is a '+ Drill-Down Token' button. At the bottom right are 'Cancel' and 'Save' buttons."/>

15. Set **Token Name** as **deeplink** and set **Token Value** to **\$id\$**.

16. Press [**Save**] on the modal window.

17. Press [**Save**].

Now you have set up the creation of Notable Events for ingested alerts. After the correlation search runs, you should see the Notables on the **Incident Review** page of the Enterprise

Security application.

98 Notables

Unselect all |
Edit Selected |
Edit All Matching Events (98) |
Add Selected to Configuration

Last refresh at 10:09 AM

Q

Auto-Refresh Off

< Prev

1

2

3

...

Next >

20 per page

<input type="checkbox"/>	<input type="checkbox"/> i	Title	Risk Object	Risk Score	Risk Events	Type	Time	Disposition	Security Domain	Urgency	Status	Owner	Actions
<input type="checkbox"/>	▼	New Alert Notable for Global Vulnerability Risk, New Critical or Pre NVD Vulnerabilities	--	--	--	Notable	Today, 10:06	Undetermined	Threat	Low	New	unassigned	▼

Description

unknown

Additional Fields

Value

Action

Event Details

event_hash

5d75f549e9b4f23a36d18176b2b28a0c

▼

event_id

AEACA880-D1B9-4A05-B448-7FBE9399577A@notable@@5d75f549e9b4f23a36d18176b2b28a0c

▼

eventtype

modnotable_results

▼

notable

▼

Short ID

[Create Short ID](#)

Related Investigations

Currently not investigated.

Correlation Search

[Threat - New Ingested Classic Alerts - Rule](#)

History

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

Drill-down Dashboard

[Alert details](#)

Adaptive Responses

Response	Mode	Time	User	Status
Notable	saved	2024-08-09T10:06:10+0000	admin	success

[View Adaptive Response Invocations](#)

Next Steps

i

No next steps defined.

9.4. 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, Fenbush1 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 I...	New	None assigned	11/23/22, 5:02 PM	

9.4.1. 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.

Alerts

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

Alert Title	Status	Assignee	Triggered	Note
Global Trends, Trending Methods - Spike: OakBot, 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

9.5. 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 10. Correlations

The app does correlation (Threat Detection) by correlating a log source against KV store populated with Recorded Future threat intel. 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.

10.1. 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.

10.2. 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 KV store.



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 name for the Correlation
4. Select a Correlation Use Case, optionally filter the list on type from the dropdown on the right.
5. Select the source of the events that are to be inspected:
 - a. Click **+ Add Index**, and select an index. This is the index that is used by the sourcetype.
 - b. Sourcetype: this is the sourcetype of the events that are being inspected.
 - c. Field: the field containing IOCs that we will correlate against the Risk List. The UI will show the number of events which fields matches the IOC of the selected Correlation Use Case.
 - d. Repeat from **a** if you wish to correlate on more than one field.
6. Optional, add a **+ Filter Search**, which filter or tunes out correlations from the results of the query.
7. Optional, view the **Search Preview** and press **Run Search** to validate that the query is implemented as expected.
8. Click **[Save Correlation]**



The lookup for any given Correlation Use Case is not available until after the rule has been saved. The **Run Search** redirect will comment out any lookup that would otherwise fail.

← All Correlations

New Correlation

Docs

Default IP correlation

▼ Risk List

Default IP risklist (ip)

Choose Recorded Future IOC Risk List to correlate with Splunk events. List names describe their use case.

ip ▼

default_ip_enriched (ip)
Default IP risk list with enriched fields for location, threatLists, and analystNotes...

Default IP risklist (ip)
The default risk list for IP

Default IP risklist hourly (ip)
The default risk list for IP

Indicators Frequently Linked to Malware (ip)
Identify communication with IPs known for generating malicious traffic.

Large IP risklist (ip)
The large risk list for IP

Low-Medium Risk Malware Generated IP List (ip)

▼ Events

Selection mode

Guided (Recommended)

Custom Search

Select indexes with events to correlate. For each index, select specific events based on Sourcetype and EventType.

main xmain x+ Add index

Sourcetype

netscreen:firewall▼

Event Field

src▼

Matching Events (last 5 minutes)

30 of 30

+ Filter Search

> Search Preview

Save Correlation

Setup Data Model Correlations

1. Go to **Configuration › Correlations**
2. Click **New Correlation › Add Data Model Correlation**
3. Add a name for the Correlation
4. Select a Correlation Use Case, optionally filter the list on type from the dropdown on the right.
5. Select the source of the events that are to be inspected:
 - a. Data Model: This is the name of the Data Model that contains the events.
 - b. Section: This is the section of the events that are being inspected.
 - c. Field: the field containing IOCs that we will correlate against the Risk List. The UI will show the number of events which fields matches the IOC of the selected Correlation Use Case. Ctrl+click to select more than one field.
6. Optional, select the **Delay Correlation search** and set the delay in minutes. This instructs the application to look for events further in time to compensate for event indexing delays.
7. Optional, add a **+ Filter Search**, which filter or tunes out correlations from the results of the query.
8. Optional, select fields under **Event Field Visibility** to include in the query output. Data model correlation utilise **tstats** queries, and fields of interest must be known at searchtime. Any fields selected here can be shown on the correlation dashboard.
9. Optional, view the **Search Preview** and press **Run Search** to validate that the query is implemented as expected.
10. Click [**Save Correlation**]



The lookup for any given Correlation Use Case is not available until after the rule has been saved. The **Run Search** redirect will comment out any lookup that would otherwise fail.

All Correlations

New Data Model Correlation

Docs

Name*

Name for correlation

> Risk List

default_ip_enriched (ip)

< Events

Select Data Model, Section and Event Fields that contain events to correlate.

Data Model

Network Resolution (DNS)

Section (Child Dataset)

DNS (DNS)

Event Fields

Ctrl-click to select multiple fields

Select Event Fields

additional_answer_count

answer

answer_count

authority_answer_count

dest

dest_bunit

dest_category

dest_port

dest_priority

duration

message_type

name

query

query_count

query_type

record_type

reply_code

☒ Delay Correlation search

Offset correlation search time to compensate for event indexing delays

0

minutes

+ Filter Search

> Event Field Visibility

> Search Preview

Save Correlation

Setup Correlations using Accelerated Models

- Go to **Configuration › Correlations**
 - Click **New Correlation › Add Splunk Enterprise Security Correlation**
 - 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.
 - Select a Correlation Use Case. Hover over the line of a Correlation Use Case to show more details.
 - Optional, select the **Delay Correlation search** and set the delay in minutes. This instructs the application to look for events further in time to compensate for event indexing delays.
 - Optional, add a **+ Filter Search**, which filter or tunes out correlations from the results of the query.
 - Optional, view the **Search Preview** and press **Run Search** to validate that the query is implemented as expected.
 - Click [**Save Correlation**]
-

← All Correlations

New Splunk Enterprise Security Correlation

[Docs](#)

Name*

Default ES correlation

▼ Risk List

default_ip_enriched (ip)

Choose Recorded Future IOC Risk List to correlate with Splunk events. List names describe their use case.

All IOC Types ▼

- default_ip_enriched (ip)**
Default IP risk list with enriched fields for location, threatLists, and analystNotes...
- Domain risklist INTEGR3572 (domain)**
The default risk list for domain INTEGR3572 – [65, 80]
- marty_third_party_risklist_pull (domain)**
Retrieves a TD Bank's third party watchlist and generates a risklist for Splunk wi...
- Default domain risklist (domain)**
The default risk list for domain
- Default domain risklist hourly (domain)**
The default risk list for domain
- Default bank risklist (bank)**

- ☒ Delay Correlation search
Offset correlation search time to compensate for event indexing delays

0 minutes

+ Filter Search

> Search Preview

Save Correlation

Nightly back-fill search

The app ships with a nightly search to attempt to back-fill any correlations that occurs outside the search window. Events can occur outside the search window due to indexing lag. This search only applies for Datamodel and ES correlations. In order to disable this search:

1. Navigate to Splunk **Settings › Searches › reports › and alerts**
2. Filter on settings created by the app, and search for **Recorded Future - Back-fill Correlation Search**.
3. Click "Edit" in the action column.
4. Select disable

This search will no longer run.

10.3. 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.

The following are the default columns displayed. Any field available in the matched correlation event can be selected as a column. Columns are controlled via the **view columns** icon on the top right of the primary table. Displayed columns are persistent on a per-rule basis.

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.

10.3.1. Filter Search

Content of the table can be filtered via the **+ Search filter** option, present in the top bar. Clicking it reveals a filter menu with a text input. Any text entered into will be treated as SPL and control what correlations are displayed. For example, **Risk > 90** will only include correlation with risk over 90 and **Name="x.x.x.x"** only includes the ip x.x.x.x.

Selecting any value in **Available Event Fields** will include the selected field in the SPL query.

10.4. Shifting Correlation window to mitigate indexing lag.



Shifting the detection window will cause delay in correlation.

Out of the box the applications correlation search assumes very low indexing lag, 1 min. The app performs a search in the interval **-4m@m** to **-1m@m** every three minutes.

In the presence of indexing lag this interval can be shifted in time. Assume an 15 minutes index lag, that would result in a shift by 15m to **-19m@m** to **-16m@m**.

The settings for the correlation search can be changed via the splunk GUI.

1. Navigate **Settings > Searches, Reports, and Alerts**
2. Find the search **Recorded Future - Correlation Search**
3. Click **Edit > Edit Search**
4. Modify **Earliest time** and **Latest time** to match the new shifted cycle. Be sure that the difference between earliest and latest is 3 minutes.

10.5. 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.

10.6. Disabling Automatic Correlation Searches

Our app includes a powerful correlation search feature that performs automatic searches every 3 minutes. This ensures that relevant correlations are identified and surfaced in real time. By default, this automatic search runs to continuously monitor your data and provide timely insights.

However, for customers utilizing Splunk's Workload Pricing model, frequent searches may incur unnecessary resource usage. To address this, we've introduced an option to disable automatic correlation searches and run them on demand.

By disabling the automatic correlation feature, you can prevent correlation searches from running every 3 minutes. Instead, you can execute these searches manually when you need them, directly from the correlation dashboard.

When you visit the Correlations dashboard, you can:

- Specify correlation rules you want to apply.
- Set a custom time range for the data analysis.

This option allows you to take full control over when and how searches are executed, ensuring that you optimize your resource usage based on your operational needs.

10.6.1. Disabling Correlation feature

1. Navigate to **Configuration > Settings**
2. Select **Features** section on the left menu
3. Press [**Enabled**] button next to **Correlations**, this will make the feature **Disabled**

With this feature, you have the flexibility to manage your searches based on your specific requirements while minimizing unnecessary resource consumption in environments with compute-based pricing.

Chapter 11. 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 Insight 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.
- **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

11.1. 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.

11.2. rfenrich

This command enriches events based on the specified entity type and field name using Recorded Future intelligence. The command adds 2 new fields to the events: `rf_risk` and `rf_rules`. The supported entity types are: ip, domain, hash, url, and vulnerability. You should specify only one entity type per command invocation.



The command processes a maximum of 10,000 events per invocation.

11.2.1. Usage

This example enriches events based on IP addresses.

```
... | rfenrich ip=src_ip
```


Chapter 12. 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.

12.1. 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** on any of the listed rules presents 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 titled "Sigma Rule: T-RAT 2.0 DNS queries". It is divided into two main sections: "Splunk Search" and "Event Mapping".

Splunk Search: 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: Includes a descriptive text: "Event Mapping attempts to automatically find the event fields required by the Sigma Rule in Splunk." Below this is a table for mapping fields:

Source	Matched source
✓ Index=main	main

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

At the bottom right of the 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 management interface. At the top, there are buttons for 'Edit', 'Export', and a menu icon. Below the header, there's a filter section with '96 rules' and dropdowns for 'Any Product', 'Any MITRE code', and 'Any Status'. The main table lists rules with columns for 'Sigma Rule', 'Status', and 'Tags'. The first rule, 'Sigma Rule: Ransomware Shadow Copy manipulations', is expanded, showing its details: Status (N/A), Level (High), Malware Category (Ransomware), Product (Windows), and Alerts triggered (0). There are 'Run Search' and 'Edit' buttons. Below the details, the rule's description and publication date (9/24/2020) are shown. At the bottom, another rule is partially visible with tags T1490 and T1486.

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 13. Sigma Detections

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

Chapter 14. Splunk Enterprise Security Integration

The Recorded Future integration with Splunk Enterprise Security (ES) provides Splunk ES correlations with Recorded Future Risk Lists. Indicators are managed by Splunk's Threat Intelligence framework. Any correlation made generates both Finding (Notable) and Intermediary-Finding (Risk) events.

The integration offers several Adaptive Response actions:

- **Recorded Future Threat Hunt**
 - Fetch linked indicators from any field in a Notable event and perform a one-time search. Results are written as a Finding (Notable Event) or Intermittent-Finding (Risk event)
- **Recorded Future Enrichment**
 - Performs an API enrichment of any field in a finding (notable); results are returned as a new finding (notable event).

14.1. 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.

14.2. Configure Enterprise Security Correlations

Correlations for Enterprise Security relies on the TI framework to handle data ingestion and production of initial detection. Any threats matched this way will be enriched and then produce a Finding and/or Intermediary-Finding (Notable event and/or Risk event.)

All correlations by an Enterprise Security correlation rule produce both Notable and Risk events. A Risk event is always generated unless explicitly disabled, while Notable events are produced only for indicators with a risk score exceeding a predefined threshold.

These parameters are set during the configuration of a new rule. Disabling **Generate Risk Events** will cause the feed to only generate Notable Events.

This is how to configure and enable a new correlation rule for Enterprise Security.

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

14.2.1. Estimate

Splunk Enterprise Correlation setup allows for the estimation of the daily alert count. This process may involve downloading unavailable risklists, which could take some time.

14.2.2. Correlations in Splunk ES

Setting up a threat feed, as described above, is the only step required to activate correlations in ES.

The following Automatic actions occurs for events detected

- Query Threat Activity datamodel for threats
- Enrich any events found with: **Recorded Future intelligence** and **Mitre ATT&CK** codes
- Generate a Finding (Notable event)
- Generate a Intermediary-Finding (Risk Event) (if applicable)

Correlations utilise the Risk Framework. The Risk Based framework uses these objects to automatically group related events. The framework can automatically promote the Intermediary-Findings (Risk Event) into Findings (Notable events) if a threshold is met.

Technical Information

For each configured threat feed

- Detections (Correlation searches) are saved to `savedsearches.conf`
- Metadata about selected risk lists are stored in `recordedfuture_settings.conf`; responsible for pushing data to TI framework.
- 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 Findings.

14.3. Configure TI framework ingestion

The application can be configured to ingest indicators in the ES TI framework. Adding an ingestion rule on this page will simply populate the TI framework KV stores with indicators.

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, data will be ingested into the TI framework.

These are the TI framework KV stores where data is ingested:

IoC category	KV store
ip	ip_intel
hash	file_intel
domain	ip_intel
url	http_intel

Configure Incident Review table

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
rf_a_risk	RF Risk Score
rf_b_rules	RF Triggered Rules
rf_evidence_critical	RF Very Malicious Evidence
rf_evidence_malicious	RF Malicious Evidence
rf_evidence_suspicious	RF Suspicious Evidence
rf_evidence_unusual	RF Unusual Evidence

14.4. Create Notables for Ingested Alerts

14.4.1. Ingestion

After enabling the rule on the **Alerting Rules** page, you automatically start ingestion for this rule. The saved search with name **Recorded Future - Ingest Alerts** runs every 10 minutes. It retrieves the enabled rules and writes newly created alerts to the corresponding KV store collection:

- `alert_ingested` - for Classic Alerts
- `playbook_alert_ingested` - for Playbook Alerts

The application does not automatically set an initial time period for the first ingestion. This means that the ingestion will begin only after the associated rule is enabled for ingestion.

By default, ingested alerts are retained in the KV store collection for up to **365 days** or **10,000 records**, whichever limit is reached first. You can modify these retention settings:

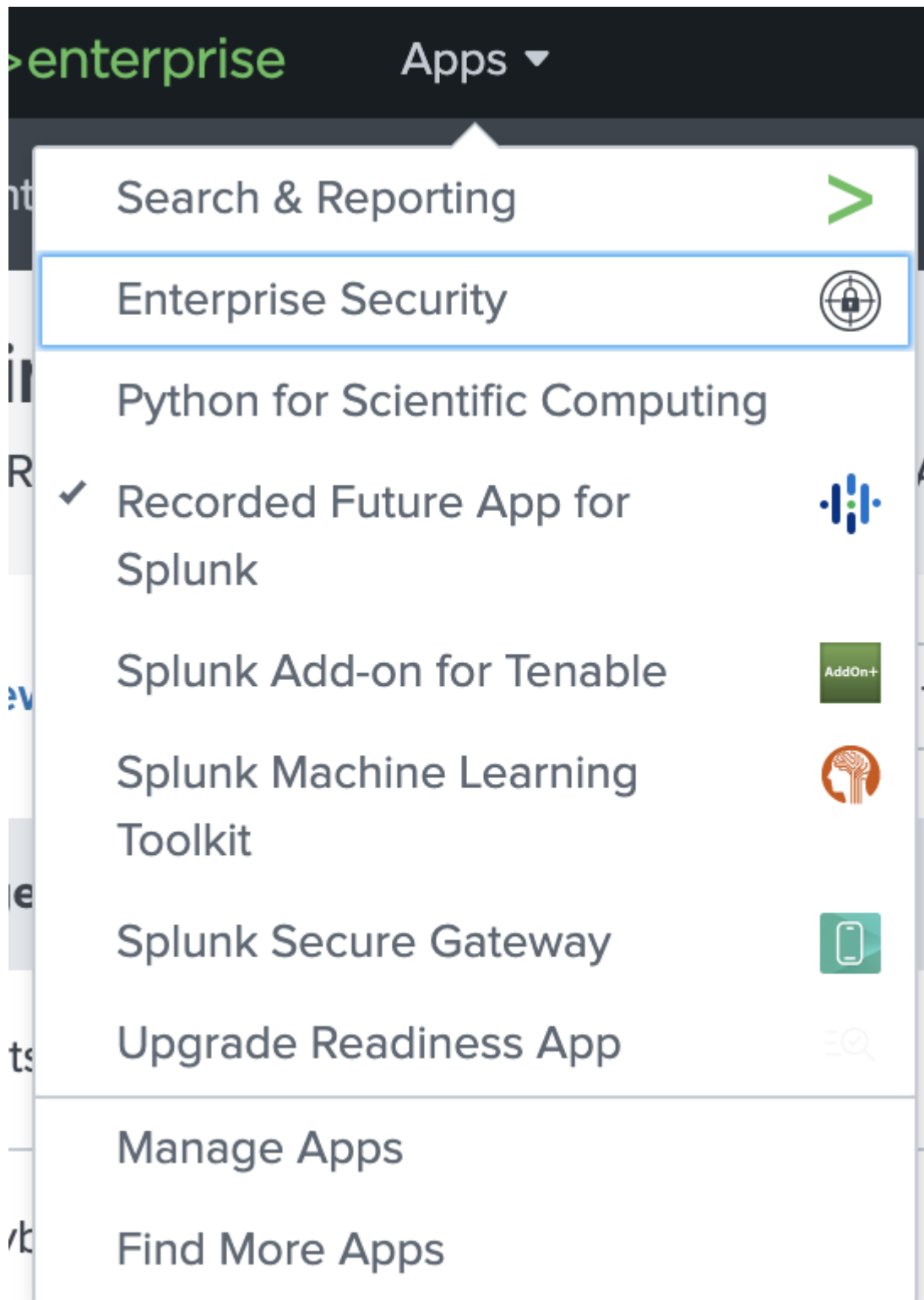
- Navigate to **Configuration › Settings › Features** to adjust the retention period and record limits.

14.4.2. Setup (ES - 8.0+)

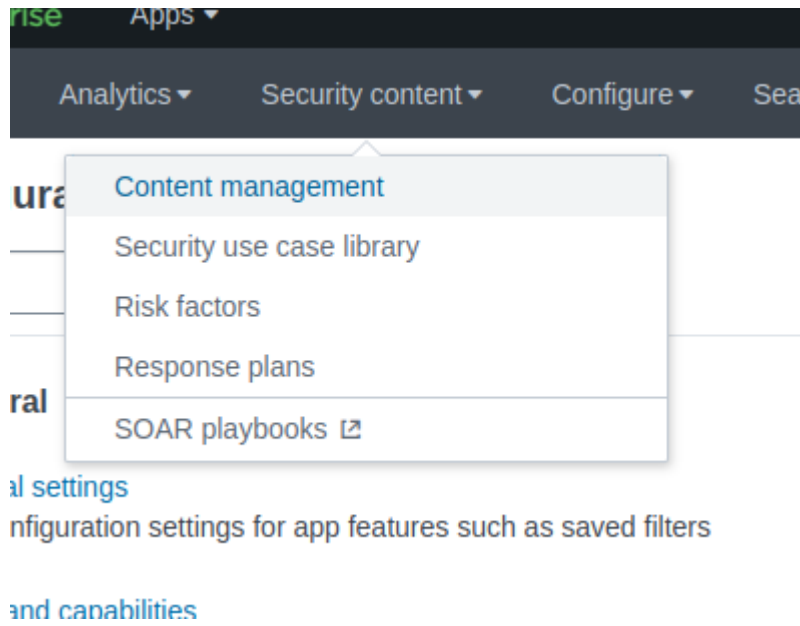
For older version of ES see [Setup pre ES - 8.0](#)

We will set up the creation of Findings (Notable Events) based on the new records in the corresponding collection.

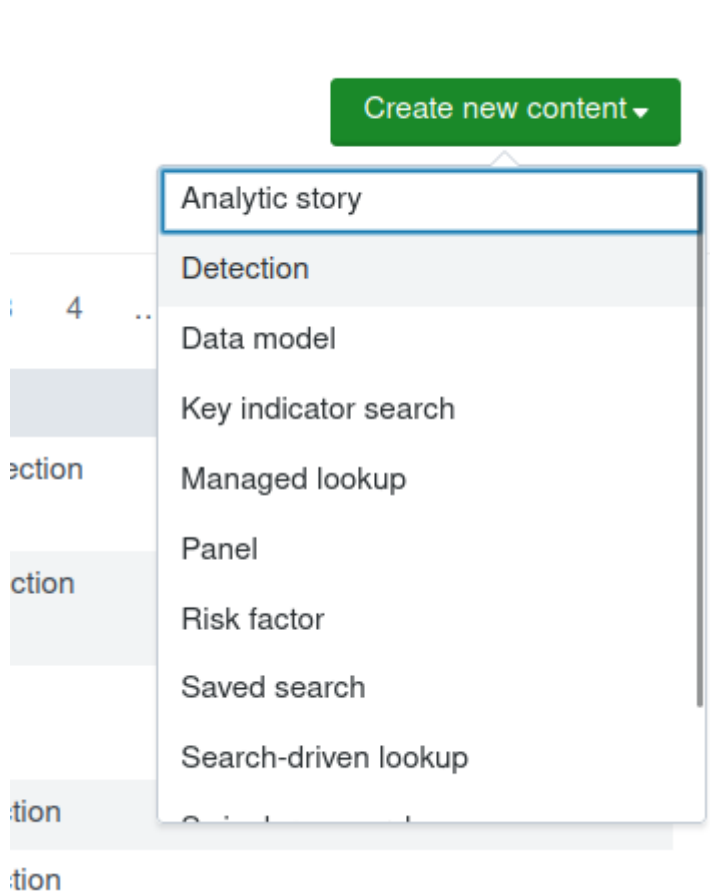
1. Open "Enterprise Security" application
-



2. Go to **Security Content** › **Content Management**



3. Press [**Create New Content**] and select [**Detection**]



4. Select **Event-based detection**
5. Make sure that **Finding** is the selected output type.

*** Finding output type**
Set up event-based detections to triage security threats. [Findings documentation](#)

☐ **Intermediate finding** RECOMMENDED
Records or observations created by event-based detections that indicate anomalies but might not be standalone security incidents.
Intermediate findings do not appear on the analyst queue until grouped by a [finding-based detection](#).

☒ **Finding**
Alerts that might be a security incident. Created by event-based or finding-based detections and displayed in the analyst queue.

6. In **2 › Event-based Detection**, set the **Detection name** (e.g. "New Ingested Classic Alerts") and set the **Detection description**.

7. In **2 › Event-based Detection**, set the **Detection search** (assuming we want to run the detection every 6 hours):

- Classic Alerts

```
| inputlookup alert_ingested
| eval new_record = if(_time > relative_time(now(), "-6h@h"), 1, 0)
| search new_record=1
```

- Playbook Alerts

```
| inputlookup playbook_alert_ingested
| eval new_record = if(_time > relative_time(now(), "-6h@h"), 1, 0)
| eval id = _key
| search new_record=1
```

8. Go to **3 › Analyst queue**

9. Set the **Title** and **Description** for new Findings, optionally set other fields. Example **Title** for Classic Alert:

New Alert Finding for \$rule.name\$



You can use fields of the alerts collection lookup, as defined in [transforms.conf](#) file, surrounded by dollar signs as in the example above.

10. In **Drill-down Dashboards** select the **[+ Add Drill-down Dashboard]**

Drill-down dashboards

[+ Add drill-down dashboard](#)

Add a drill-down dashboard for additional context to view multiple drill-down searches for a finding during an investigation.

11. In the dropdown list in **Dashboard** select the appropriate alerts dashboard:

- [TA-recordedfuture/rfes_alerts_list_v2](#) - for Classic Alerts
- [TA-recordedfuture/playbook_alerts](#) - for Playbook Alerts

12. Set the **Name** (e.g. "Alert details")

13. Press [**Edit Tokens**] and in the modal window press [**+ Drill-Down Token**]

Edit tokens documentation'. Below this is a table with two columns: 'Token Name' and 'Token Value'. Under 'Token Name', there is a '+ Drill-Down Token' button. At the bottom right are 'Cancel' and 'Save' buttons."/>

14. Set **Token Name** as **deeplink** and set **Token Value** to **\$id\$**.

15. Press [**Save**] on the modal window.

16. Go to **4 › Assign risk**, ES 8.0.2 forces you to configure this block to save the configuration. Since this detection is **finding** based these values will not have impact. Suggested values:

17. Set **Risk message** to "Recorded Future Alert"

18. Set **Entity** to "id"; this will group risk on the alert ID.

19. Set **Entity Type** to "other"

20. Go to **6 › Cron Schedule** and set the desired schedule for this search, in our case it is every 6 hours:

* */6 * * *

21. Go to **7 › Conditions** and pick [**For each result**].

Conditions
Trigger conditions to create a finding. [Conditions documentation](#)

Create when: Number of Results

is greater than 0

Create: Once | For each result

Adaptive response actions are created for each detection result.

22. Press [Save].

Now you have set up the creation of Notable Events for ingested alerts. After the detection runs, you should see the Notables on the **Incident Review** page of the Enterprise Security application.

Analyst queue: New Alert | Last 24 hours | Saved Views: Select... | Charts | Hide Timeline

Time Range: Last 24 hours | Search: New Alert | Clear All | Save | Stop

Updating: Auto refresh on | 20 per page

checkbox	rule_title	ID	notable_type	risk_object	PK	F...	F...	F...	_time	disposition
<input type="checkbox"/>	New Alert Notable for Brand Mentions with Cyber entities	3C2Cw4	Threat	3C2Cw4	1				Today, 9:10 AM	Undo
<input type="checkbox"/>	New Alert Notable for Identify Similar Domains	3C2Cw4	Threat	3C2Cw4	1				Today, 9:10 AM	Undo
<input type="checkbox"/>	New Alert Notable for Analysis from Inskt Group	3C2CwX	Threat	3C2CwX	1				Today, 9:10 AM	Undo
<input type="checkbox"/>	New Alert Notable for Global Trends, Trending Targets	3C2CwM	Threat	3C2CwM	1				Today, 9:10 AM	Undo
<input type="checkbox"/>	New Alert Notable for Malware Intelligence from Inskt Group	3C2Cwq	Threat	3C2Cwq	1				Today, 9:10 AM	Undo
<input type="checkbox"/>	New Alert Notable for Global Vulnerability Risk, New Critical or Pre-WVD Vulnerabilities	3C2C8r	Threat	3C2C8r	1				Today, 9:10 AM	Undo
<input type="checkbox"/>	New Alert Notable for Leaked Credential Monitoring	3C2CwN	Threat	3C2CwN	1				Today, 9:10 AM	Undo
<input type="checkbox"/>	New Alert Notable for IP Address Mentions	3C2C4L	Threat	3C2C4L	1				Today, 9:10 AM	Undo
<input type="checkbox"/>	New Alert Notable for Company Email on Code Repository	3C2C46	Threat	3C2C46	1				Today, 9:10 AM	Undo
<input type="checkbox"/>	New Alert Notable for Leads and TTPs from Inskt Group	3C2CvK	Threat	3C2CvK	1				Today, 9:10 AM	Undo
<input type="checkbox"/>	New Alert Notable for Vulnerability Intelligence from Inskt Group	3C2C8b	Threat	3C2C8b	1				Today, 9:10 AM	Undo

New Alert Notable for Identify Similar Domains

Owner: unassigned | Status: New | Urgency: Medium

Sensitivity: Select... | Disposition: Undetermined

Time: Feb 4th, 2025 9:10 AM

Last updated: N/A

Reference ID: 6cd7c318-b93b-4979-a500-9cdedf866fcb@notable@66cd7c318b03b4979a5009cdedf866fcb

Detection: Threat - New Ingested Classic Alerts - Rule

Detection name: Threat - New Ingested Classic Alerts - Rule

Related investigations: No related investigations

Drill-down dashboard: Alert Details

History: View all review activity

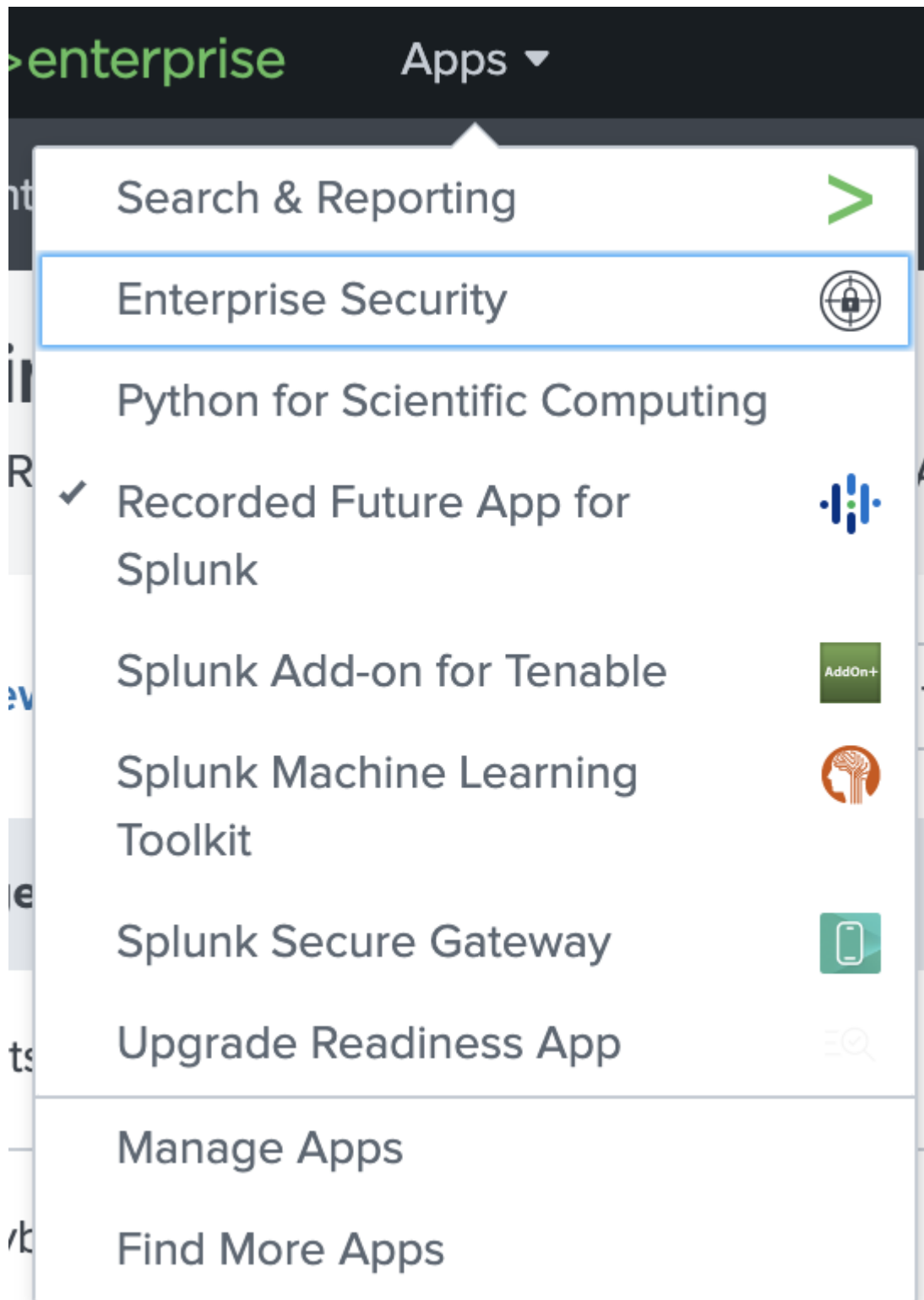
Adaptive responses: Obtaining list of adaptive responses... View Adaptive Response Invocations

Notes

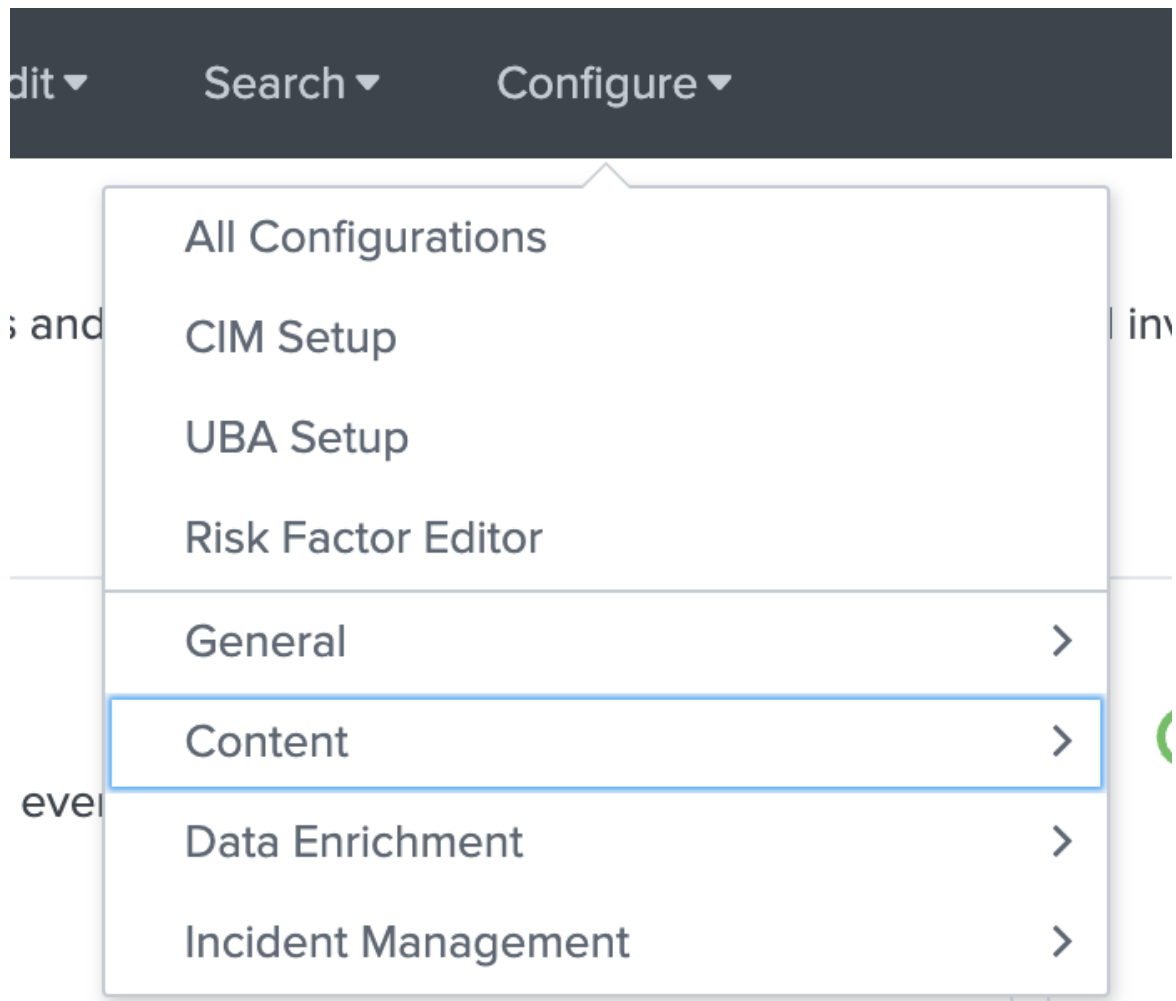
14.4.3. Setup pre ES - 8.0

We will set up the creation of Notable Events based on the new records in the corresponding collection.

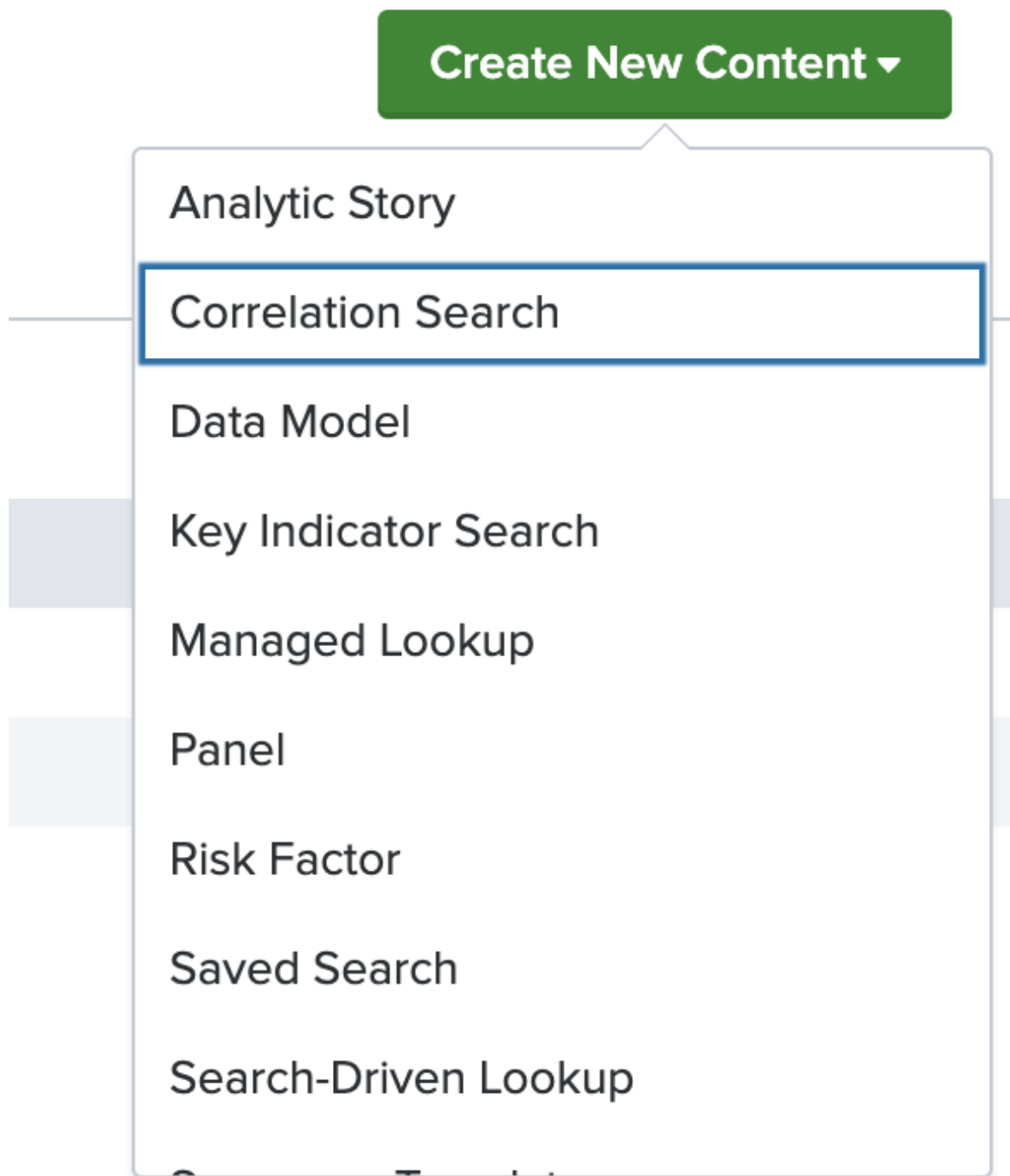
1. Open "Enterprise Security" application



2. Go to **Configure** › **Content** › **Content Management**



3. Press [**Create New Content**] and select [**Correlation Search**]



4. Set the **Search Name** (e.g. "New Ingested Classic Alerts") and optionally set the **Description**.
5. Set the **Search** (assuming we want to run the correlation search every 6 hours):
 - Classic Alerts

```
| inputlookup alert_ingested  
| eval new_record = if(_time > relative_time(now(), "-6h@h"), 1, 0)  
| search new_record=1
```

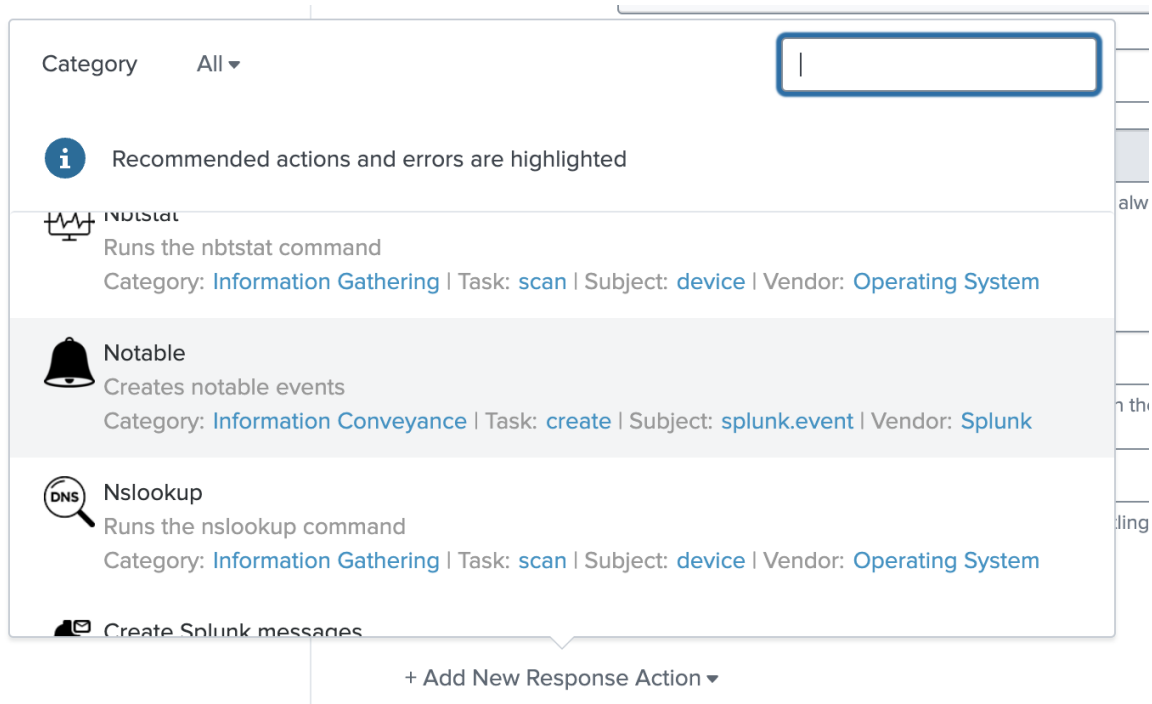
- Playbook Alerts

```
| inputlookup playbook_alert_ingested
| eval new_record = if(_time > relative_time(now(), "-6h@h"), 1, 0)
| eval id = _key
| search new_record=1
```

6. Go to **Time Range** › **Cron Schedule** and set the desired schedule for this search, in our case it is every 6 hours:

```
* */6 * * *
```

7. Go to **Trigger Conditions** › **Trigger** and pick [**For each result**].
8. In **Adaptive Response Actions** select [**+ Add New Response Action**] and pick **Notable**.



9. Set the **Title** for new Notable Events (example for Classic Alert):

```
New Alert Notable for $rule.name$
```



You can use fields of the alerts defined in `transforms.conf` file surrounded by dollar signs as in the example above.

10. Optionally set the **Description** and other fields.
11. In **Drill-down Dashboards** select the [**+ Add Drill-down Dashboard**]

Drill-down
Dashboards

+ Add Drill-down Dashboard

12. In the dropdown list in **Dashboard** select the appropriate alerts dashboard:

- **TA-recordedfuture/rfes_alerts_list_v2** - for Classic Alerts
- **TA-recordedfuture/playbook_alerts** - for Playbook Alerts

13. Set the **Name** (e.g. "Alert details")

14. Press [**Edit Tokens**] and in the modal window press [**+ Drill-Down Token**]

Edit tokens documentation'. Below this is a table with two columns: 'Token Name' and 'Token Value'. Under 'Token Name' is a button '+ Drill-Down Token'. At the bottom right are 'Cancel' and 'Save' buttons."/>

15. Set **Token Name** as **deeplink** and set **Token Value** to **\$id\$**.

16. Press [**Save**] on the modal window.

17. Press [**Save**].

Now you have set up the creation of Notable Events for ingested alerts. After the correlation search runs, you should see the Notables on the **Incident Review** page of the Enterprise

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](#)

Name*

▼ Risk List

Choose Recorded Future IOC Risk List to correlate with Splunk events. List names describe their use case.

All IOC Types ▼

default_ip_enriched (ip)

Default IP risk list with enriched fields for location, threatLists, and analystNotes...

Domain risklist INTEGR3572 (domain)

The default risk list for domain INTEGR3572 – [65, 80]

marty_third_party_risklist_pull (domain)

Retrieves a TD Bank's third party watchlist and generates a risklist for Splunk wi...

Default domain risklist (domain)

The default risk list for domain

Default domain risklist hourly (domain)

The default risk list for domain

Default bank risklist (bank)

☒ Delay Correlation search

Offset correlation search time to compensate for event indexing delays

minutes

[+ Filter Search](#)

> Search Preview

Save Correlation

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.
-

Chapter 15. Adaptive Response Actions

This section lists all adaptive response actions provided in the Recorded Future app.

Ad-hoc invocations of 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.

All provided adaptive response actions provide ad-hoc functionality.

15.1. Recorded Future Collective Insights

The Collective Insights adaptive response action allows you to contribute any Findings (Notable Events) to Collective Insights. The parameters in the setup of the action accepts field or free-text strings. The order of priority if `field` then, if there is no matching field in the Finding (Notable event), the `string` will be used.

Any findings will be sent either in batch, or one by one. This is controlled by the `Create` option in `Trigger condition` setup of the detection (correlation search). `Once` will send all findings as batch, while `For each result` will send each finding individually.

15.2. Recorded Future Enrichment

The enrichment adaptive response action can be used to enrich any notable with Recorded Future threat intelligence.

This is done by querying the Recorded Future API for each indicator detected by a finding. Any results found will create a new Finding (Notable event)

Adaptive Response Title Prefix option

When using Adaptive Response action a new Finding (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.

15.3. Recorded Future 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 Finding (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 finding 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 Detection (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 new Findings.

Chapter 16. 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 (ES and Enterprise):
 - 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 and id of the use case that the correlation rule was configured with
 - Action of the correlated event, if available.
 - Timestamp of the correlated event, if available.
 - 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
 - Action of the correlated event, if available.
 - Timestamp of the correlated event, if available.
 - 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:
 - The indicators found by threat hunt search
 - The indicator/malware 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
 - Action of the correlated event, if available.
 - Timestamp of the correlated event, if available.
-

16.1. 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 17. Features Settings

This page contains settings for different features of the **Recorded Future App for Splunk**.

Chapter 18. Custom Search Commands

Recorded Future app provides custom search commands that extend SPL to serve customer's specific needs.

18.1. rfenrich

This command enriches events based on the specified entity type and field name using Recorded Future intelligence. The command adds 2 new fields to the events: `rf_risk` and `rf_rules`. The supported entity types are: ip, domain, hash, url, and vulnerability. You should specify only one entity type per command invocation.



The command processes a maximum of 10,000 events per invocation.

18.1.1. Usage

This example enriches events based on IP addresses.

```
... | rfenrich ip=src_ip
```

Chapter 19. Troubleshoot

The issues involving the Recorded Future for Splunk can be divided into two categories; reports and logs.

All items related to troubleshooting can be found in the Troubleshooting tab on the Settings page.

To ease troubleshooting, the app contains one report for each type:

19.1. Reports

19.1.1. 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 Validation dashboard (**Configuration › Settings › Troubleshooting › Open Validation Dashboard**).

19.1.2. 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 › Settings › Troubleshooting** 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.

19.2. 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.

19.2.1. Search queries

Search app logs

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

Search logs from Adaptive Response actions (Splunk ES)

```
tag=modaction "[RF Adaptive]"
```

Search for app references in Splunk logs

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

19.3. 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 of the developer console to show any javascript errors that may have been triggered.
3. Increase the log level to DEBUG.
4. Trigger the issue.
5. Note the date and time the issue was triggered. Make sure to include this in the report to Recorded Future.
6. Download the troubleshooting package and include that in the information to send to us.
7. Reset the log level.

19.4. Troubleshooting Package



Exporting the package might take some time due to the inclusion of app log data. Please be patient after clicking the download button.

The "troubleshooting package" is a .zip archive that can be downloaded from menu:Configuration[Settings > Troubleshooting]. The package contains the following information:

- Application logs
- "Validation" report results
- "Last updated risklist" report results
- Mentions of the application in internal splunk logs
- KV store utilization
- alert_actions.conf
- app.conf
- recordedfuture_settings.conf

- savedsearches.conf
- transforms.conf

Chapter 20. 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

Technical documentation

The following sections contain technical details and API documentation for parts of the application.

Chapter 21. 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 22. 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 23. Threat Hunting API

23.1. 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`
- `is_scheduled`: `true/false`, specifying if the hunt is scheduled.
- `schedule`: configuration for scheduling the threat hunt. Examples: `{"type": "daily", "at_hour": 23, "at_minute": 0}, {"type": "weekly", "at_hour": 23, "at_minute": 0, "on_days": [1, 7]}, {"type": "monthly", "at_hour": 23, "at_minute": 0, "on_day": 1}.`

23.1.1. Create profile



Creating a profile only saves a threat hunt on that profile. If you want to also start the hunt automatically, you need to pass `save_and_run` query parameter with value set to `true`.

POST the following payload to `services/TA-recordedfuture/create_threat_hunt_config?save_and_run=true` to create and start 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"]}},
  "is_scheduled": "false",
  "schedule": {}
}
```

Example curl:

```
curl -X POST 'https://127.0.0.1:8089/services/TA-
recordedfuture/create_threat_hunt_config?save_and_run=true&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"
}
}
```

23.1.2. 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

23.2. 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.

23.2.1. Start threat hunt

GET `services/TA-recordedfuture/run_threat_hunt?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=b7613b6abba94981b507e8366e9776178ou
tput_mode=json' \
```

Response:

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

23.2.2. 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=e0d416d435cf4b0084b3e7ca48689a6d8&outpu  
t_mode=json' \
```

Response:

- 200 - OK
- 400 - Missing parameter :experimental: :icons: font :img_location: img :last-update-label!:

Chapter 24. Change Log

All notable changes to the Recorded Future for Splunk will be documented in this file.

24.1. [2.8.0] (2025-04-02)

24.1.1. Improvements

- Deeplink functionality for Recorded Future Alerts, Playbook Alerts, and Sigma Detections pages.
- Including multiorg owner-organization in the PBA redirect link for correct viewing in the portal.
- Added ASI feature including dashboards and settings page.
- Changed savedsearch name from "Recorded Future - Check Asynchronous Jobs" to "Recorded Future - Threat Hunt Result Collector" to resolve ambiguity.
- Support for Splunk ES 9.4.
- New enrichment command `rferrich` to enrich events in a search.
- Enriching Vulnerabilities now contains CSSVv3 and CSSVv4
- Introducing Adaptive Response Action to contribute Findings to Collective Insights.
- New home page replacing Alert Center as the default page when starting the app.
- Now FIPS compliant and can be run in a FIPS environment.
- Improvements to playbook alerts
- New tab for Settings page "Troubleshooting" allowing you to easily export logs and settings to send to support for further investigation.

24.1.2. Changes

- Moved Troubleshooting page from **Configuration** menu into **Configuration › Settings › Troubleshooting**.

24.1.3. Bug Fixes

- Fix an issue with RBA feeds where the risk threshold was set to 0 after upgrading from v2.6.x.
- Fix displaying of invoked Adaptive Response Actions in Mission Control.
- **IMPORTANT.** If you are using Sigma rules you are strongly encouraged to update to 2.8 or forthcoming 2.7.3. There was a bug where if the corresponding SPL for a sigma rule was broken, other sigma rule searches would not run correctly. All Sigma rules searches now run separately and when saving we validate that the SPL is valid, ie can run without issues. To check whether you are affected by this bug update to the latest version and look for the following error "Sigma search got 400 error investigate".

We have identified three problematic sigma rules, if you use any of these you are definitely affected.

- doc:v-9-ef - Insikt Validated TTP: Detecting NovaSentinel Using Sigma
- doc:1sioHH - Sigma Rule: Drive Overwriting with "cipher" Command
- doc:2uXk09 - Sigma Rule: Detecting Scheduled Tasks Named "Windows Update ALPHV", Used by Various Ransomware Families

We encourage you to disable these for the time being.

Once upgraded, if you have custom SPL in the sigma rules we encourage you to edit these rules and click save again, as this will validate that the SPL is indeed valid. If the SPL is invalid you will get an error and won't be able to save the rule.

24.2. [2.7.2] (2025-03-05)

24.2.1. Improvements

- Dynamic base url in javascript allowing for on-premise installations to have custom url paths.

24.2.2. Bug fixes

- Fix Technical Links occasionally not showing up for certain malware.
- Fix an upgrade issue when you're using an old 2.x version of the Recorded Future app.

24.3. [2.7.1] (2025-02-05)

24.3.1. Improvements

- Add support for Splunk ES 8.0
- Add support for Splunk Enterprise 9.4

24.3.2. Bug Fixes

- btool errors for sigma rules
- Error with "search preview"

24.4. [2.7.0] (2025-01-08)

24.4.1. Improvements

- Adding the option to pivot from the Threat Hunt result page to the Search itself via '...' menu. A "Search and Export" button is now available there.
 - Adding "Description" and "Timestamp" to third-party collective insights call.
 - Multiple indexes are now available to be selected for sigma rules.
 - Including multiorg owner-organization in the PBA redirect link for correct viewing in the portal.
 - Removing jQuery from our code. jQuery is still in use for Splunk provided components where
-

Splunk is responsible for updates.

- Change format for Mitre ATT&K Techniques on Sigma rules page to include the name of the technique.
- Renaming modules to better reflect what they do.
- Risk Based alerting has been renamed to Enterprise Security Correlations
- Adaptive response has been renamed to TI Framework Ingestion.
- Indexing of playbook alerts in KVstore
- Enrichment page now contains an AI summary
- Better UX for starting Threat hunts in both threat map and threat table.
- Threat hunting with threat actors in addition to hunting with malware.
- Data Model is now an option for configuring Threat Hunts
- Improved when a hunt is failing
- The `command | rest /services/TA-recordedfuture/migrate_remove_threat_intel_entries` will clean out all old threat intel data from Recorded Future.

24.4.2. Bug fixes

- Fix high runtimes for correlations in 2.6
- Change hashing function so that the Recorded Future app works in FIPS environment.
- Fixing the issue of old entries in the TI framework kvstores are left behind by reverting to a CSV solution for the TI framework.

24.5. [2.6.3] (2025-02-05)

24.5.1. Improvement

- Support for Splunk ES 8.0
- Support for Splunk Enterprise 9.4

24.5.2. Bug fixes

- Fix UI regression affecting Threat Hunt view when upgrading to Splunk 9.4.
- Revert Threat Intelligence Framework usage of kvstore; now using CSV as a ingestion.

24.6. [2.6.2] (2024-12-16)

24.6.1. Bug fixes

- Fix an issue where searches exceeded the search concurrency limit of historical searches. This affected the migration handler preventing us to run migrations needed when upgrading from one version to another.

24.6.2. Improvement

- Add the following rest command, making it accessible to easily update a conf file. | `rest /services/TA-recordedfuture/write_conf_file filename=recordedfuture_settings stanza=conf_version data="{\"fail_counter\": 0}"`

24.7. [2.6.1] (2024-11-26)

24.7.1. Bug fixes

- Risklist are now stored in .csv's again following abnormal increase in correlation_search runtime.
- Fixing a broken link on the settings page.

24.7.2. Improvements

- Changes to "Weekly Active User" metrics.

24.8. [2.6.0] (2024-10-07)

24.8.1. Improvements

- Risklist are now stored in KV store rather than .csv
- Optional KV store ingestion of Alerts.
- Optional KV store ingestion of Playbook Alerts.
- Threat Hunt Scheduling capability.
- Ability to disable continuous cached correlation searches in UI.
- Correlation dashboard "live mode" that runs correlation on dashboard visits when caching of correlation searches is disabled.
- Display v3 alerts on Recorded Future Alerts page.
- Collective insights storing event time rather than detection time.
- Collective insight will start recording "actions" seen in relation to a detection, i.e. firewall allowed/blocked for a firewall based correlation.
- Consolidation of adaptive response and app logfile. Errors and Warnings are still listed on the troubleshooting view.

24.8.2. UI improvements

- Configure threat hunt directly from Threat Map.
 - New UI for settings page.
-

24.9. [2.5.1] (2024-09-04)

24.9.1. Bug Fixes

- Adding quotes to mitigate the space in field used in default correlations.
- Splunk 9.3 issue where menu was not displayed correctly after app first-time-setup.
- Change to threat hunt where hunts could run outside specified time scope.
- Fixed an issue with disappearing Link block for enrichment pages.

24.10. [2.5.0] (2024-04-19)

24.10.1. Improvements

- Better Threat Hunt results grouping and representation.
- Fields selected for **Datamodel** correlations will now automatically be displayed on the correlation dashboard.
- Added input for custom correlation delay on Datamodel and ES correlation setup page.
- Added nightly search for correlations that picks up events with big indexing delay.

24.10.2. Bug Fixes

- **Index-based** correlation will now use `_index_time` instead of `_time`, removing the risks of index delay.

24.11. [2.4.3] (2024-09-04)

24.11.1. Bug Fixes

- Adding quotes to mitigate the space in field used in default correlations
- Splunk 9.3 issue where menu was not displayed correctly after app first-time-setup.
- Change to threat hunt where hunts could run outside specified time scope.
- Fixed an issue with disappearing Link block for enrichment pages.

24.12. [2.4.2] (2024-04-24)

- Added input for custom correlation delay on Datamodel and ES correlation setup page.
- Added nightly search for correlations that picks up events with big indexing delay.

24.12.1. Bug Fixes

- **Index-based** correlation will now use `_index_time` instead of `_time`, removing the risks of index delay.
-

24.13. [2.4.1] (2024-03-14)

24.13.1. Bug Fixes

- Removed `localop` in index search for sigma setup page.
- Renamed deprecated `distsearch.conf` stanza.
- Added query logic to process an empty response to clear the .csv risklists correlation feed file.
- Removed stray rename statement from ES correlation searches.
- Fixed Sigma Modal view when update to a rule is received.
- Fixed issue where Playbook Alerts released upon received empty API payload.

24.14. [2.4.1] (2024-03-14)

24.14.1. Bug Fixes

- Removed `localop` in index search for sigma setup page.
- Renamed deprecated `distsearch.conf` stanza.
- Added query logic to process an empty response to clear the .csv risklists correlation feed file.
- Removed stray rename statement from ES correlation searches.
- Fixed Sigma Modal view when update to a rule is received.
- Fixed issue where Playbook Alerts released upon received empty API payload.

24.15. [2.4.0] (2024-02-08)

24.15.1. Improvements

Correlation Dashboard

- Added the ability to select columns to display.
- Added SPL filter option to filter correlations.

Correlation Setup

- Added extra tuning options for correlations.
 - Added ability to correlate on any number of fields with one rule.
 - Added ability to correlate on multi-value fields with one rule.
 - Adding search preview to display the correlation search as it is being constructed.
 - Added pivot from setup page to Splunk search app to run and view results of correlation rule search.
-

General

- Configuration page will now automatically refresh after the app has been fully configured.
- Update the URI format for playbook alerts.
- Added `earliest_time` and `latest_time` parameters to the sigma savedsearch.
- Added support for "json" format of the response to `/fetch_single_alert` endpoint.

24.15.2. Bug Fixes

- Improved RBA exception handling to prevent naked/empty notables in Incident Review.
- Added more verbose logging for RBA searches.
- Reworked how indexes and sourcetypes were identified, no longer using `index=*` syntax, instead a different tstats query.

24.16. [2.3.3] (2024-03-14)

24.16.1. Bug Fixes

- Removed `localop` in index search for sigma setup page.
- Renamed deprecated `distsearch.conf` stanza.
- Added query logic to process an empty response to clear the .csv risklists correlation feed file.
- Fixed Sigma Modal view when update to a rule is received.
- Fixed issue where Playbook Alerts released upon received empty API payload.

24.17. [2.3.2] (2024-01-18)

24.17.1. Bug Fixes

- Improved RBA exception handling to prevent naked/empty notables in Incident Review.
- Added more verbose logging for RBA searches.
- Update `%-search` query on Correlation setup page to avoid undefined result value.
- Fixing Collective Insights support page link issue.
- Updated url format for the playbook alerts portal redirect.

24.18. [2.3.1] (2023-11-16)

24.18.1. Improvements

- Filtering out special fields from the configuration for the Threat Hunt:
 - tag
-

- tag:.*
- eventtype

24.18.2. Bug fixes

- Fixed error for the hidden Sigma rules that received the update.
- Added `splunk_server=local` to fix the problem for clustered environments with the next savedsearches:
 - Recorded Future - Send Weekly Active Users statistics
 - Recorded Future - Check Asynchronous Jobs
- Fixed the issue with never-ending failed Threat Hunt.

24.19. [2.3.0] (2023-10-13)

24.19.1. General

- "Intelligence Cloud" renamed to "Collective Insights"
- Removed mandatory "ID" field when configuring correlation, it is now auto-generated.
- Added 'Threat Hunt' feature support.
 - Added "Threat Hunts" dashboard.
 - Added "Threat Hunt Runs" results page.
 - Added Malware Threat Map.

24.19.2. Improvements

- The "new" badge disappears after two weeks of the import of the sigma rule.
- Added the ability to perform IP enrichment on CIDR ranges.
- Added improved loading indicators.
- Removed required ID field when setting up a new Correlation/TI Feed/RBA.
- Re-introducing the ability to not verify SSL certificates for on-prem setups. Not applicable for Cloud.

24.19.3. Bug fixes

- Be able to sort on status in Sigma configuration view.
 - Faster loading in correlation view
 - Added a missing collection.
 - Disabling a savedsearch pending a thorough investigation into reports of performance issues. Impact: correlation dashboard risk update is disabled until further notice.
 - Added purging of deprecated sigma rules.
-

24.20. [2.2.2] (2023-09-20)

24.20.1. Bug fixes

- Ensure that the collection `recordedfuture_conf` is added to `collections.conf`. The omission of this entry in `collections.conf` is an issue for Splunk Cloud.
- Increasing the timeout from 45s to 180s for requests to Recorded Future's api.

24.21. [2.2.1] (2023-08-18)

24.21.1. Improvements

- Include a new endpoint `/services/TA-recordedfuture/get_spl_sigma_rules`, to get sigma rules formatted for spl.

24.21.2. Bug Fixes.

- Fixed an issue where risklists could not be pulled into ES because of a default limit in ES.
- Fixed an issue where Notable events were not generated correct when using a threshold with RBA.

24.22. [2.2.0] (2023-07-10)

24.22.1. General

- Added support for Playbook Alerts, 2.2 ships with "Domain Abuse". Additional types will be distributed in the future without any need to upgrade the integration.
 - Separate page with Playbook Alerts in the Alert Center section
 - Configuration of Playbook Alerts on the same page as Classic Alerts.
 - Displaying of total count of alerts on the Overview page.
 - Updated RBA feature set
 - Added Threshold option to RBA feeds. This option sets a minimum severity for which notable events are created. Anything below threshold is only created as a risk event.
 - RBA feeds from versions 2.1.x will be migrated into an RBA feed which is only producing Notable events.
 - Added optional Estimate; when configuring splunk ES correlations with Risk Based Alerting this can be used to estimate daily notable event count.
 - Splunk ES adaptive response action that performs correlation on related indicators (Links). Correlations are displayed in ES as notables or ingested as risk events.
 - For customers that are sharing data, they also share the `recordedfuture_settings.conf`, so it becomes easier to debug.
 - The app produces statistics about how many users uses the different endpoints in the app and forwards those to Recorded Futures API. Only the number of users per endpoint along
-

with min/avg/max response times are sent.

24.22.2. Improvements

- Added the ability to contribute to Collective Insight with matches in the TI data model. Please visit Intelligence cloud configuration page and review settings.
- Updated Intelligence Cloud configuration page.
- UI update on the Tlfeed page to accommodate the Risk Based Alerting Threshold Option.
- Notable Events created by our Risk Based Alerting integration now contains the original event.
- Added multi-org support for Recorded Future alerts. Alerting rules and alerts will now display which organization owns the alert. Added filtering option on "owner".
- Added support for specifying organization when participating in Collective insight for clients that are multi-organization clients.
- RBA feeds without threshold now only produce notable events and not risk notables. Risk handling is left fully to splunk RBA based of events in the risk index. Feeds created before 2.2 will be upgraded accordingly.

24.22.3. Bug Fixes.

- Splunk ES sometimes derives IOC from Recorded Future indicators which have no risk in the Recorded Future platform. If the occurs a message will be displayed in the notable event.
- Bug with regexp in distsearch.conf that caused risklists to be replicated to indexers in cluster environments.
- Python2.7 compatibility issue with Adaptive Response Enrichment.
- For new installations, the collections `TA_recorded_future_incident_state` and `TA_recorded_future_detections` have the owner Nobody. If needed, you can change this manually in Settings > All configurations > Re-assign Knowledge object.
- Resolve an issue where the alert center view may trigger a jsondecode error. As updated risklists come in, the risk score in correlations and alert center gets updated. Initial risk is kept in cache in the field `initial_risk`
- IOCs that no longer exist in downloaded risklists will not show up in the correlation view. These IOCs will continue to be available in the alert center; but the risk score will be out of date.

24.22.4. Engineering

- Updated `metadata/default.meta` file by adding write permissions for `sc_admin` role which is an alternative `admin` role on cloud instances.
- A migration of the following collections `correlation_cache_{category}`, where category is either, vulnerability, url, domain, hash or ip. Only 50k of these collections will be migrated by default. If you require to migrate a larger amount of these collections ensure that larger values are set for the following entries in `limits.conf`. This will also ensure that out of date risk scores is being updated correctly.

When the migration happen it will normalize the `collection_cache_{category}`. This means that only one correlation hit will appear in a single correlation dashboard. So it may appear that correlations are missing compared to before the upgrade. However, that is not the case, duplicated correlations have with the correlation been deduplicated.

The following change needs to be added to `limits.conf` in `/etc/system/local/limits.conf`. You may adjust the values according to your system's need.

```
[searchresults]
maxresultrows = 10000000

[join]
subsearch_maxout = 10000000

[kvstore]
max_rows_per_query = 1000000
```

- Risk Based Alerting feeds from 2.1 will be migrated over to 2.2 as pure Notable Events feeds and will not produce any Risk events. Please recreate these to reintroduce risk event generation.
- Removed the ability to disable SSL verification of external traffic.

24.22.5. Changes

- Renamed "Configuration" → "Recorded Future Alerts" to "Alerting Rules".

24.23. [2.1.4] (2023-06-07)

24.23.1. Improvements

- Added multiorg support for Recorded Future alerts. Alerting rules and alerts will now display which organization owns the alert. Added filtering option on "owner".
- Added more in-app documentation

24.23.2. Bug fixes

- Bug with regexp in `distsearch.conf` that caused risklists to be replicated to indexers in cluster environments.
- Python2.7 compatibility issue with Adaptive Response Enrichment.
- Bug involving the conversion of Splunk event to JSON
- Increased timeout of a number of calls causing premature timeouts.
- For new installations, the collections `TA_recorded_future_incident_state` and `TA_recorded_future_detections` have the owner Nobody. If needed, you can change this manually in Settings > All configurations > Re-assign Knowledge object.

- Resolve an issue where the alert center view may trigger a jsondecode error.

24.24. [2.1.3] (2023-03-20)

24.24.1. Improvements

- Improved performance of Correlation Setup for massive log environments.
- Improved performance of Sigma Setup for massive log environments.
- Added documentation for new "Infrastructure Detections" enrichment panel.
- Improved in-app documentation for Correlation "Search String" option

24.24.2. Bug fixes

- Notifications text sometimes clipped outside its border.
- Subset of in-app correlation risked being missed.
- Risklist sync failure caused correlation setup to fail with an incorrect error message.

24.25. [2.1.2] (2023-02-13)

24.25.1. Improvements

- Ad-hoc invocations of Adaptive Response will now create Notable events.
- Title Prefix option which allows for customization of Notable event title.
- UI improvements for notifications.
- Added a quickstart guide for setting up the app.
- Removed save button in the configuration page.

24.25.2. Bug fixes

- Bug where events containing multi-value fields were incorrectly filtered out from results when the `make_json` macro was used.
- Fixed bug where previous correlation view ID were shown in dropdown.
- HTTPS-proxy support disabled for splunk 8 as it lacks support. Please upgrade to Splunk 9 to get the full HTTPS proxy support.

24.26. [2.1.1] (2022-12-15)

24.26.1. Changes

- Invalid config in app.manifest fixed.
-

24.27. [2.1.0] (2022-12-15)

24.27.1. Changes

- Removed the migration tool - migration is only supported between versions 1.x and 2.0.

24.27.2. General

- Added Sigma Rule Detection
- Top navigation menu reworked
- Added Alert Center displaying Sigma Detections and Correlations
- Correlations
 - Correlation now works via a cached approach, reducing load times of dashboards
 - All correlations available in a new dashboard
- Updated documentation.
- Reworked Recorded Future Alerts
- A new tab "Intelligence Cloud" added to Configuration. An option to either share or not share any unattributable data for analytical purposes can be made here. The default option is to share data.

24.27.3. Enterprise Security

- Added integration into the Risk Based Alerting framework
 - Notable events enriched directly - duplicate events are not created anymore
 - Notables also annotated with Mitre ATT&CK codes

24.28. [2.0.8] (2023-02-01)

24.28.1. Bug fixes

- HTTPS-proxy settings issue occurring for users of Splunk 8. Splunk 8 is using a version of urllib3 that does not support HTTPS proxies, and will use HTTP regardless of configuration. Please upgrade to Splunk 9 to get the full HTTPS proxy support.
- Fixed edgecase on migration from 1.1, where a setup without any usecases loaded cause the migration to fail.

24.29. [2.0.7] (2023-01-17)

24.29.1. Improvements

- Ad-hoc invocations of Adaptive Response will now create Notable events.
 - Title Prefix option which allows for customization of Notable event title.
-

- Updated UI for Recorded Future Alerting rule page.

24.30. [2.0.6] (2022-12-13)

24.30.1. Bug fixes

- Configured Correlation use cases that become unavailable confused the correlation configuration view.
- Tighter filter on what data is shared from Adaptive Response.

24.30.2. Improvements

- Tightened security in Python made any deployments using an HTTPS proxy to fail if the SSL certificates of the proxy were not properly signed. Implemented a setting to make it possible to disable verification of the proxy SSL certificates.

24.31. [2.0.5] (2022-10-11)

24.31.1. Bug fixes

- The Adaptive response code contained code that was not python2 compatible. Some instances of Splunk still runs Adaptive Responses using python2.

24.32. [2.0.4] (2022-09-13)

24.32.1. Bug fixes

- Change in 2.0.3 caused a degradation in performance for correlations of accelerated data models. This has been remedied.
- Calculated fields were missing when setting up a correlation for accelerated data models.

24.33. [2.0.3] (2022-09-05)

24.33.1. Bug fixes

- Machines that use self-signed certificates and upgrade to 2.0.x won't have issues upgrading.
 - Fix log parsing
 - Clicking on "Search string" button in correlation configuration will no longer give you an error.
 - Removal of all f-strings that cause issues for AR actions as it runs python 2.7.
 - Be able to filter on Network Traffic, allowed/block without issues.
 - Enrich action pivots from ES Notable events correctly.
-

24.34. [2.0.2] (2022-06-16)

24.34.1. Bug fixes

- Broken python2 compatibility exhibited in Adaptive response.
- Notable events that don't have threat_match_value will no longer throw an error
- "Event" text has been removed from Accelerated correlation configuration step.

24.34.2. Improvements

- Improved dialog options for Enterprise Security correlation writebacks with a new menu option "Intelligence Sharing".

24.35. [2.0.1] (2022-05-11)

24.35.1. Bug fixes

- Documentation fixes
- Javascript interoperability issues
- Collections are not replicated to indexers
- Correlation setup wizards now include calculated fields

24.35.2. Improvements

- Documentation improvements
- Performance improvements in the correlation setup views
- Usability improvements in the correlation setup views
- The Splunk system is now requested to reload configurations once a new ES thread feed has been added. This avoids having to restart the Splunk system for the new feed to become available
- Improved error messages
- Additional information available about Recorded Future alerts.

24.36. [2.0.0] - 2021-12-25

24.36.1. Improvements

24.36.2. General

- Correlation dashboards are now dynamically generated based on input from the user.
 - Added MITRE ATT&CK codes.
 - Support for accelerated data models.
-

- Enrichment dashboards are now dynamically generated.
- New overview page that shows statistics based on configuration of the app.
- Menu is dynamically generated to suit the current configuration.
- New and improved configuration pages.
 - Validation of API URL and token.
 - Separate pages for correlations and alerts.
- Now uses an API that is adapted to suit the integration app.
- Updated documentation.
- Updated workflow actions.
- Global Map dashboard removed.
- Added migration tool for users upgrading from version 1.x of this app.
- Refactored code and made more robust.
- Design updates.

24.36.3. Enterprise Security

- Improved Adaptive Response module

24.36.4. Bug fixes

- Stuff
-