Recorded Future Azure Sentinel Install Guide

Overview

The Recorded Future integration with Azure Sentinel includes four major parts:

1. Logic apps to import malicious IP Addresses, File Hashes, URLs, and Domains to the ThreatIntelligenceIndicator table in Sentinel
2. Logic Apps/playbooks to enrich IP Addresses, File Hashes, URLs, and Domains in Sentinel incidents with Recorded Future Data
3. Sentinel Analytic rules to correlate Recorded Future Threat Intelligence against client telemetry to detect threat
4. Workbooks to visualize and summarize threat detection in a client tenant

Prerequisites

Roles

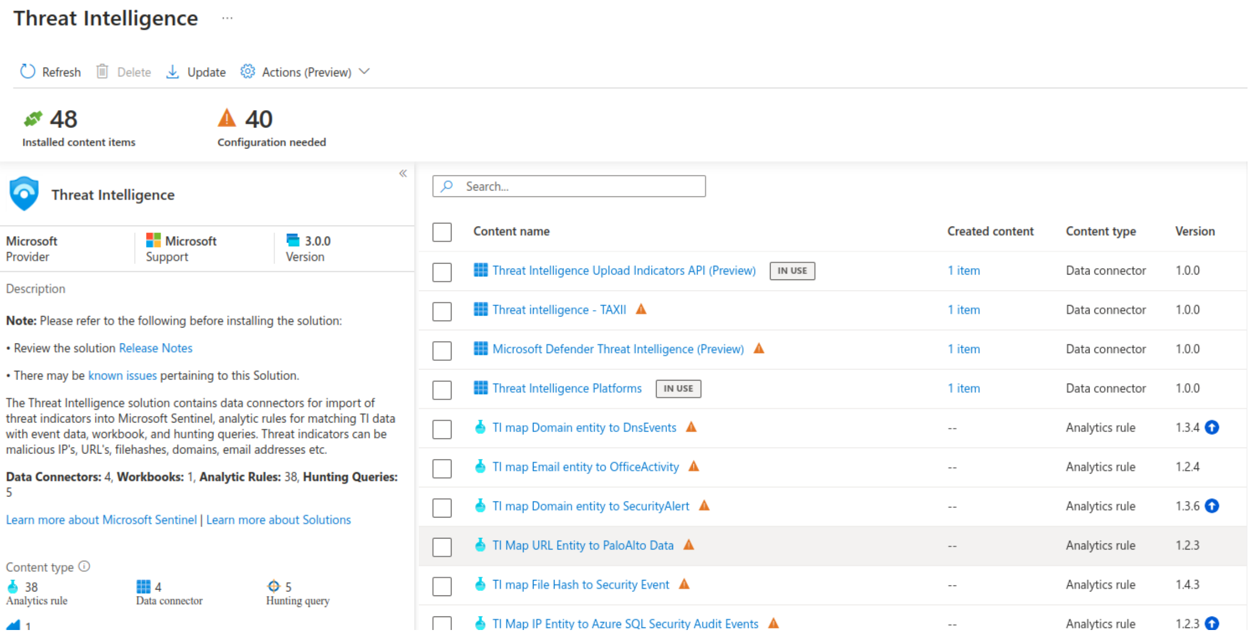
The following Azure roles and permissions will be needed at various stages of installation. This install guide will specify at each step which specific permission is required

- Microsoft Sentinel Contributor
- Logic app contributor
- “Owner” of the resource group where the logic apps will be deployed
- Template Spec Contributor
- Log Analytics Contributor

Threat Intelligence Solution

It is recommended, though not required, that you first install the solution **Threat Intelligence** (created by Microsoft) from the Sentinel Content Hub. This will create the following resources which will be useful for this integration

- The Data Connector **Threat Intelligence Upload Indicators API**, which will track the connectors ingested via the Recorded Future integration (and potentially other TI vendors as well).
- Templates for a number of Analytic rules, which will correlate client telemetry against Recorded Future Threat Intelligence to generate incidents when malicious behavior is detected.



Threat Intelligence ···

Refresh | Delete | Update | Actions (Preview)

48 Installed content items

40 Configuration needed

Threat Intelligence

Microsoft Provider | Microsoft Support | 3.0.0 Version

Description

Note: Please refer to the following before installing the solution:

• Review the solution Release Notes

• There may be known issues pertaining to this Solution.

The Threat Intelligence solution contains data connectors for import of threat indicators into Microsoft Sentinel, analytic rules for matching TI data with event data, workbook, and hunting queries. Threat indicators can be malicious IP's, URL's, filehashes, domains, email addresses etc.

Data Connectors: 4, **Workbooks:** 1, **Analytic Rules:** 38, **Hunting Queries:** 5

Learn more about Microsoft Sentinel | Learn more about Solutions

Content type

38 Analytics rule | 4 Data connector | 5 Hunting query | 1

Search...

□	Content name	Created content	Content type	Version
□	Threat Intelligence Upload Indicators API (Preview) IN USE	1 item	Data connector	1.0.0
□	Threat intelligence - TAXII ⚠	1 item	Data connector	1.0.0
□	Microsoft Defender Threat Intelligence (Preview) ⚠	1 item	Data connector	1.0.0
□	Threat Intelligence Platforms IN USE	1 item	Data connector	1.0.0
□	TI map Domain entity to DnsEvents ⚠	--	Analytics rule	1.3.4 ↑
□	TI map Email entity to OfficeActivity ⚠	--	Analytics rule	1.2.4
□	TI map Domain entity to SecurityAlert ⚠	--	Analytics rule	1.3.6 ↑
□	TI Map URL Entity to PaloAlto Data ⚠	--	Analytics rule	1.2.3
□	TI map File Hash to Security Event ⚠	--	Analytics rule	1.4.3
□	TI Map IP Entity to Azure SQL Security Audit Events ⚠	--	Analytics rule	1.2.3 ↑

Token

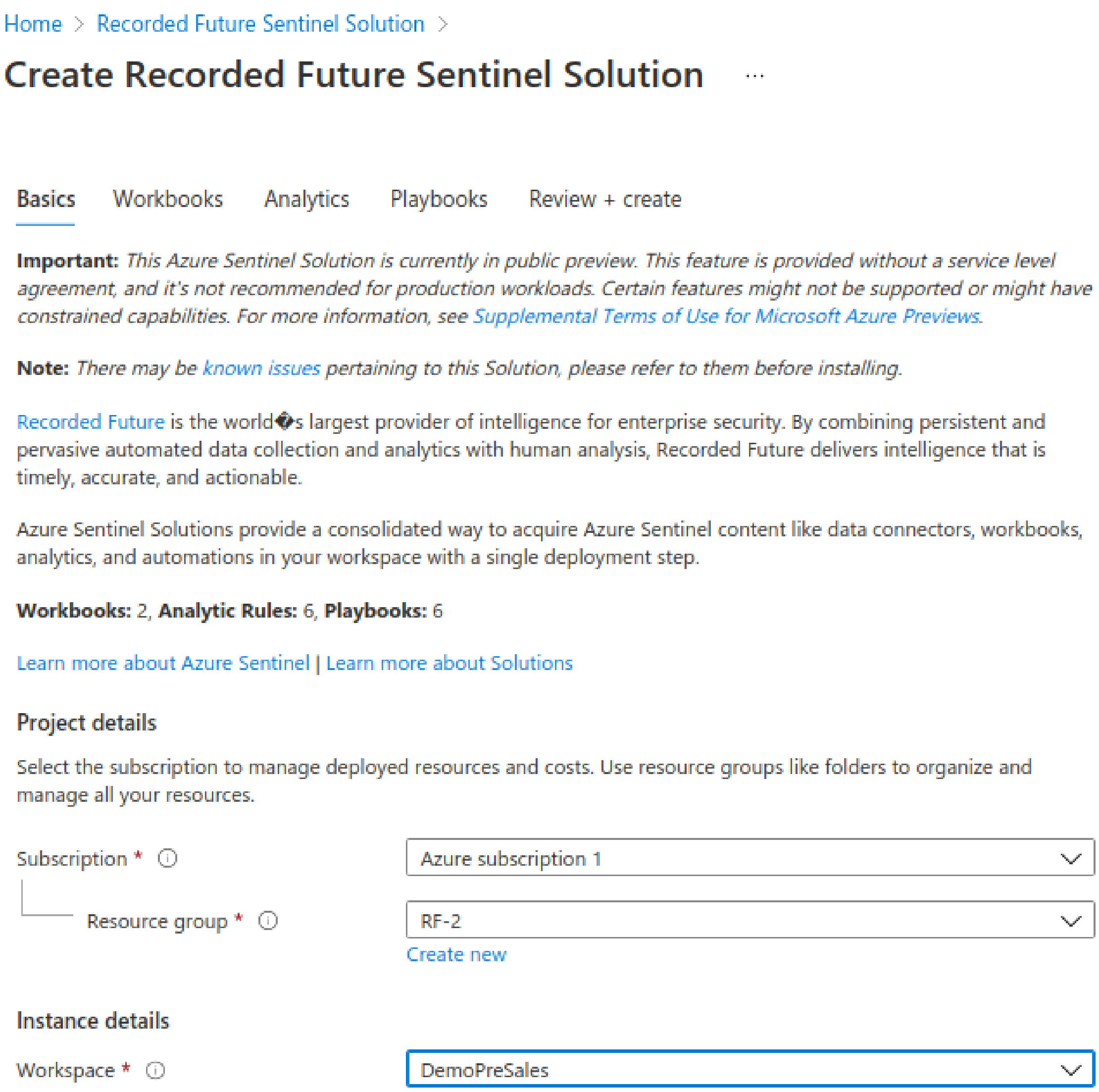
Three API tokens from Recorded Future are required for this integration

- One for the Recorded Future v2 logic app connector
- One for the Recorded Future Sandbox logic app connector
- A token retrieved from sandbox.recordedfuture.com, to be used in the Malware Sandbox logic app

Installing the Content Hub Solution

All component parts of the Recorded Future integration can be found in the Sentinel Content Hub. Navigate to Microsoft Sentinel->Content Hub->Recorded Future->Install->Create. Select the Resource Group and Sentinel Workspace where the solution will be deployed, and page through the tabs to view the component parts of the integration.If more detail is required, you can view the source templates for the logic apps/analytic rules/workbooks here. Click Review+Create to deploy the solution.

The **Logic App Contributor, Sentinel Contributor,** and **Template Spec Contributor** roles are required to deploy the solution.



Home > Recorded Future Sentinel Solution >

Create Recorded Future Sentinel Solution ...

Important: *This Azure Sentinel Solution is currently in public preview. This feature is provided without a service level agreement, and it's not recommended for production workloads. Certain features might not be supported or might have constrained capabilities. For more information, see Supplemental Terms of Use for Microsoft Azure Previews.*

Note: *There may be known issues pertaining to this Solution, please refer to them before installing.*

Recorded Future is the world�s largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable.

Azure Sentinel Solutions provide a consolidated way to acquire Azure Sentinel content like data connectors, workbooks, analytics, and automations in your workspace with a single deployment step.

Workbooks: 2, **Analytic Rules:** 6, **Playbooks:** 6

Learn more about Azure Sentinel | Learn more about Solutions

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : Azure subscription 1

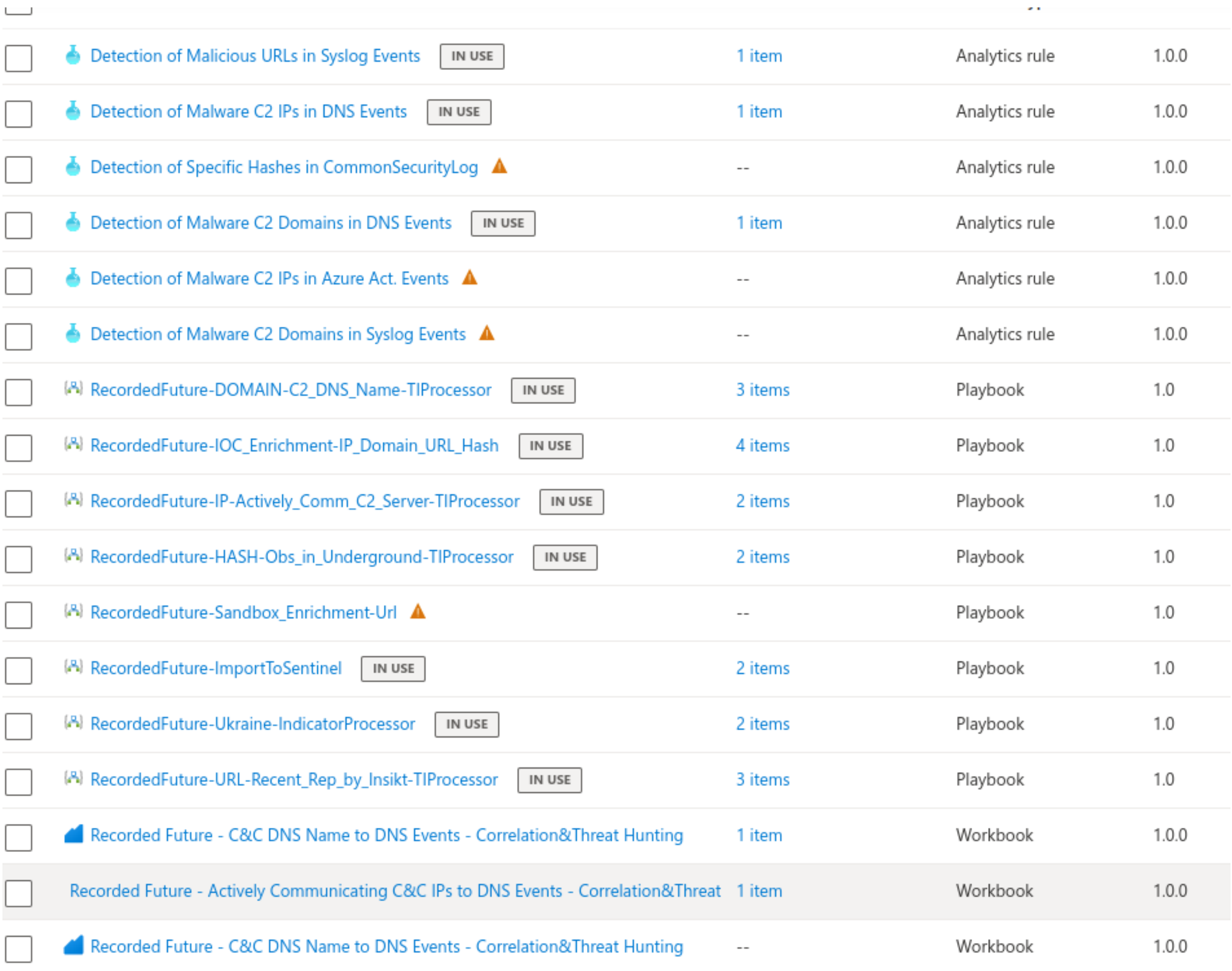
Resource group * : RF-2

Instance details

Workspace * : DemoPreSales

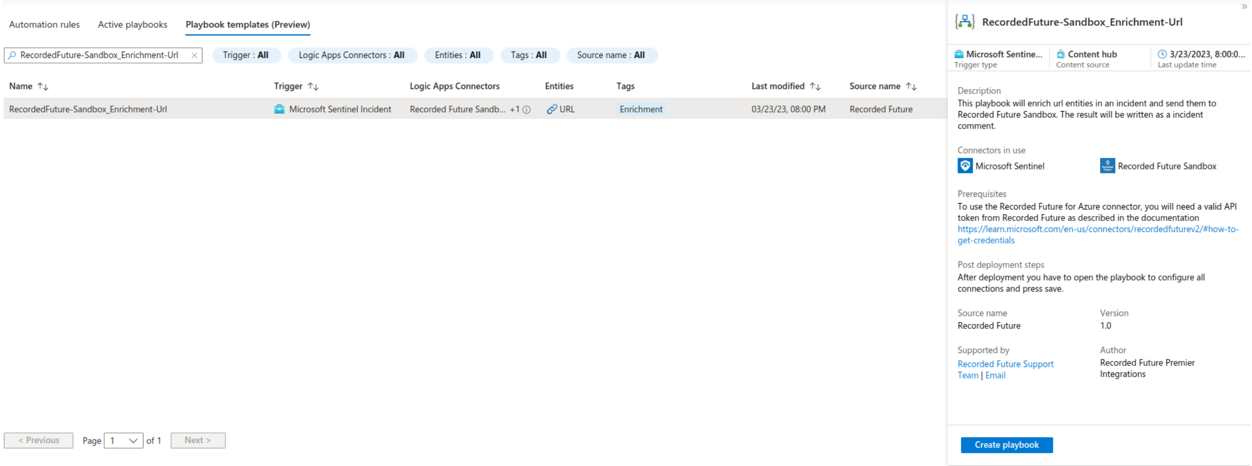
Deploying Templates

Deploying the Content Hub Solution does not directly create the Logic Apps, Workbooks, and Analytic Rules that make up the integration. Instead, it simply deploys the templates locally in your Azure subscription. Those templates can be viewed by navigating to Sentinel->Content Hub->Recorded Future (installed)->Manage.



□	Detection of Malicious URLs in Syslog Events IN USE	1 item	Analytics rule	1.0.0
□	Detection of Malware C2 IPs in DNS Events IN USE	1 item	Analytics rule	1.0.0
□	Detection of Specific Hashes in CommonSecurityLog ⚠	--	Analytics rule	1.0.0
□	Detection of Malware C2 Domains in DNS Events IN USE	1 item	Analytics rule	1.0.0
□	Detection of Malware C2 IPs in Azure Act. Events ⚠	--	Analytics rule	1.0.0
□	Detection of Malware C2 Domains in Syslog Events ⚠	--	Analytics rule	1.0.0
□	RecordedFuture-DOMAIN-C2_DNS_Name-TIProcessor IN USE	3 items	Playbook	1.0
□	RecordedFuture-IOC_Enrichment-IP_Domain_URL_Hash IN USE	4 items	Playbook	1.0
□	RecordedFuture-IP-Actively_Comm_C2_Server-TIProcessor IN USE	2 items	Playbook	1.0
□	RecordedFuture-HASH-Obs_in_Underground-TIProcessor IN USE	2 items	Playbook	1.0
□	RecordedFuture-Sandbox_Enrichment-Url ⚠	--	Playbook	1.0
□	RecordedFuture-ImportToSentinel IN USE	2 items	Playbook	1.0
□	RecordedFuture-Ukraine-IndicatorProcessor IN USE	2 items	Playbook	1.0
□	RecordedFuture-URL-Recent_Rep_by_Insikt-TIProcessor IN USE	3 items	Playbook	1.0
□	Recorded Future - C&C DNS Name to DNS Events - Correlation&Threat Hunting	1 item	Workbook	1.0.0
□	Recorded Future - Actively Communicating C&C IPs to DNS Events - Correlation&Threat	1 item	Workbook	1.0.0
□	Recorded Future - C&C DNS Name to DNS Events - Correlation&Threat Hunting	--	Workbook	1.0.0

Here, you can view and deploy all logic apps, workbooks, and analytic rules associated with the integration. You must deploy each resource individually by selecting the template, clicking Configuration, clicking the template name again, clicking “Create Playbook,” and following the deployment wizard



Name ↑↓	Trigger ↑↓	Logic Apps Connectors	Entities	Tags	Last modified ↑↓	Source name ↑↓
RecordedFuture-Sandbox_Enrichment-Url	Microsoft Sentinel Incident	Recorded Future Sandb... +1	URL	Enrichment	03/23/23, 08:00 PM	Recorded Future

RecordedFuture-Sandbox_Enrichment-Url

Microsoft Sentine...
Trigger type

Content hub
Content source

3/23/2023, 8:00:0...
Last update time

Description
This playbook will enrich url entities in an incident and send them to Recorded Future Sandbox. The result will be written as a incident comment.

Connectors in use
Microsoft Sentinel
Recorded Future Sandbox

Prerequisites
To use the Recorded Future for Azure connector, you will need a valid API token from Recorded Future as described in the documentation https://learn.microsoft.com/en-us/connectors/recordedfuturev2/#how-to-get-credentials

Post deployment steps
After deployment you have to open the playbook to configure all connections and press save.

Source name
Recorded Future

Version
1.0

Supported by
Recorded Future Support Team | Email

Author
Recorded Future Premier Integrations

Please Note that you must deploy the “RecordedFuture-ThreatIntelligenceImport” playbook before deploying any of the “IndicatorImport” playbooks

Importing the Risk Lists

Overview

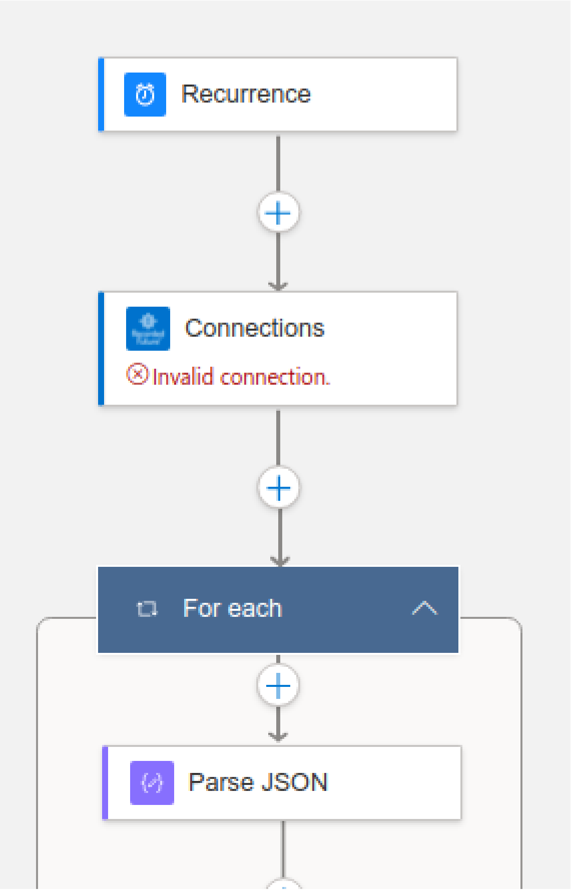
The logic apps that end in “IndicatorImport” pull risk lists from the Recorded Future API, and formats the indicators in STIX2 for the Threat Intelligence Upload API. For performance optimization, these indicators are then sent to the RecordedFuture-ThreatIntelligenceImport logic app for batching. The Indicators are then bulk uploaded to the GraphSecurityAPI, which will forward them to your Microsoft Sentinel ThreatIntelligenceIndicator table.

For all of the following steps editing logic apps, the **Logic App Contributor** and **Microsoft Sentinel** roles are required.

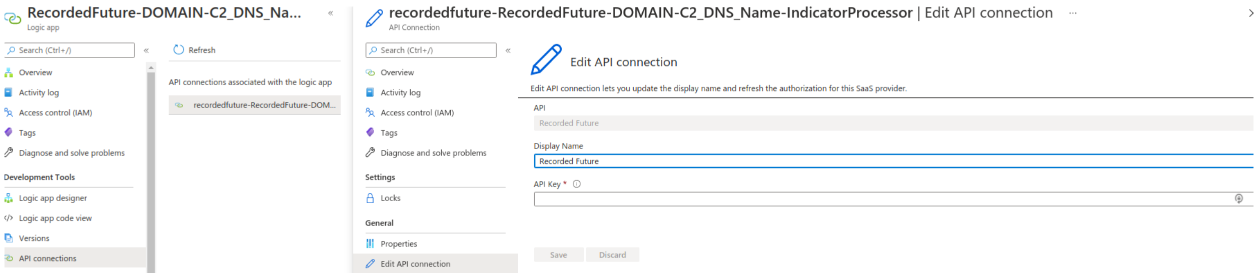
Authorizing connections

In general, logic app connections can be authorized one of two ways.

1. Navigate to the logic app->Overview->Edit. Click on the block(s) that says “Connections.”



2. Navigate to the logic app->API Connections. In each of the listed connections, navigate to edit API connection



RecordedFuture-DOMAIN-C2_DNS_Na...

API connections associated with the logic app

recordedfuture-RecordedFuture-DOM...

recordedfuture-RecordedFuture-DOMAIN-C2_DNS_Name-IndicatorProcessor | Edit API connection

Edit API connection

Edit API connection lets you update the display name and refresh the authorization for this SaaS provider.

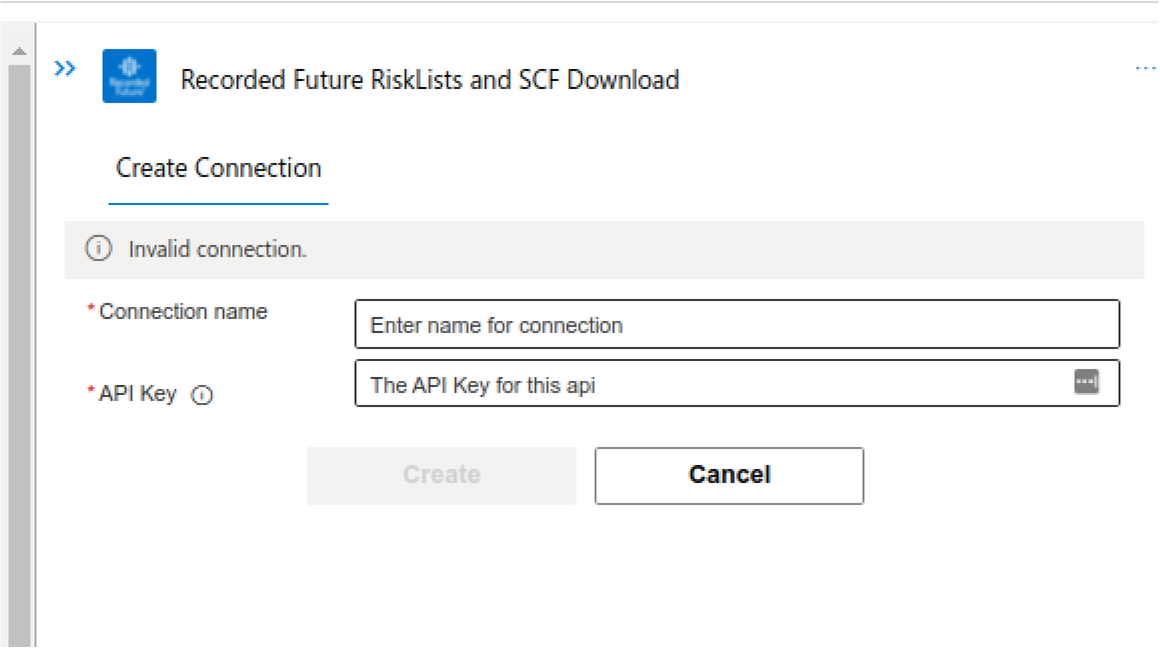
API: Recorded Future

Display Name: Recorded Future

API Key *

Recorded Future

Each of the four “IndicatorImport” apps must be authorized to communicate with the Recorded Future API. Following one of the paths above, you will be prompted to enter in a Recorded Future API key and Connection Name. Paste in your API key and choose an arbitrary name.



Recorded Future RiskLists and SCF Download

Create Connection

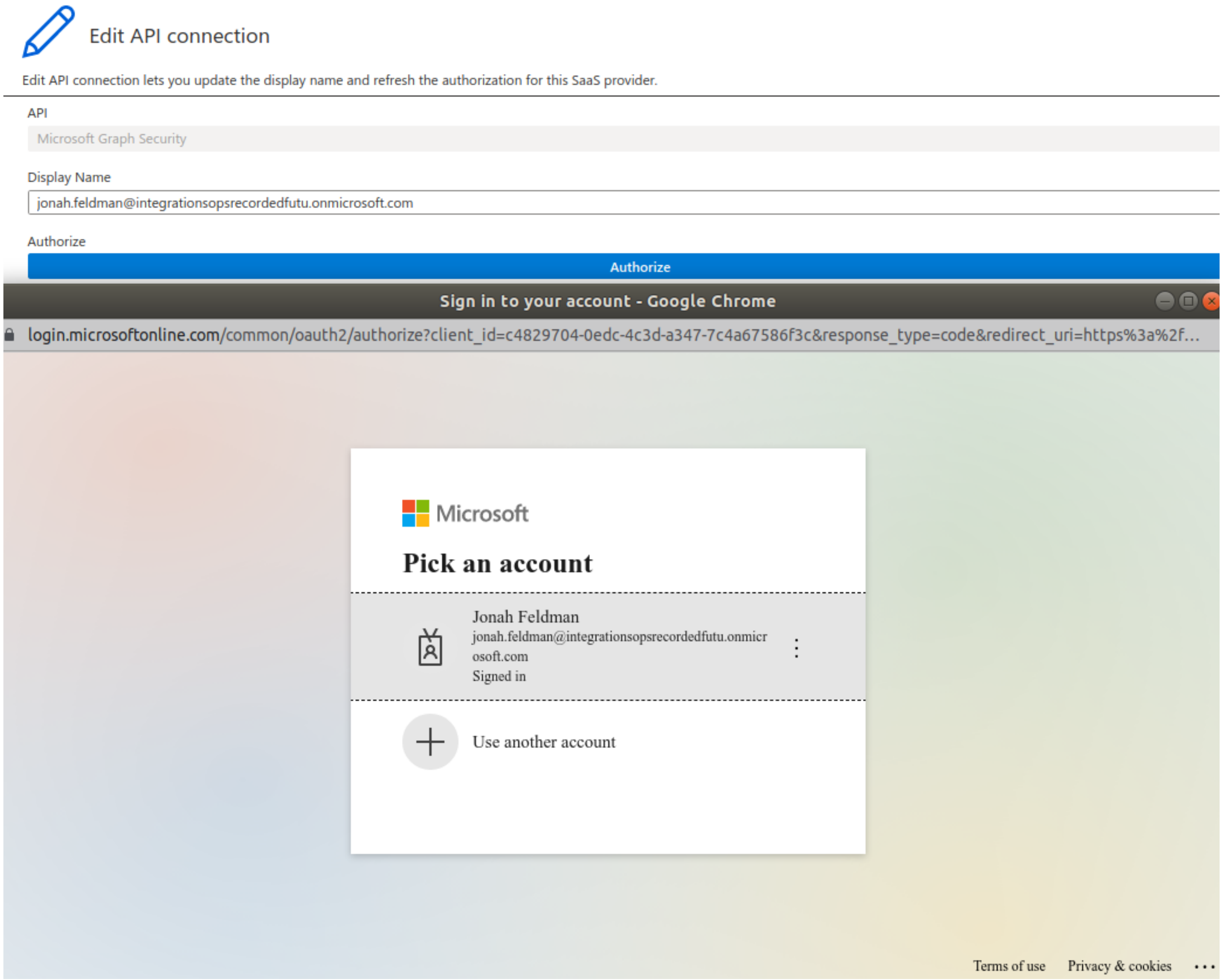
Invalid connection.

* Connection name: Enter name for connection

* API Key: The API Key for this api

Threat Intelligence Upload Indicator API

The RecordedFuture-ThreatIntelligenceImport logic app must be authorized to communicate with the Threat Intelligence Upload Indicator API . Following one of these paths, you will be prompted to Authorize the connection by signing into your Azure AD account.



Edit API connection

Edit API connection lets you update the display name and refresh the authorization for this SaaS provider.

API: Microsoft Graph Security

Display Name: jonah.feldman@integrationsopsrecordedfutu.onmicrosoft.com

Authorize

Sign in to your account - Google Chrome

login.microsoftonline.com/common/oauth2/authorize?client_id=c4829704-0edc-4c3d-a347-7c4a67586f3c&response_type=code&redirect_uri=https%3a%2f...

Microsoft

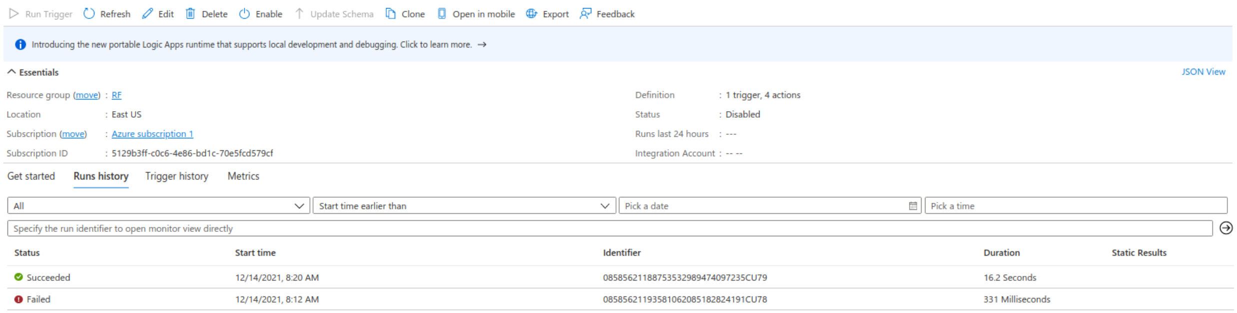
Pick an account

Jonah Feldman
jonah.feldman@integrationsopsrecordedfutu.onmicrosoft.com
Signed in

The **Microsoft Sentinel Contributor** role is required to authorize a connection. Alternatively, you can use a managed identity to authenticate, as described in our appendix.

Running the logic apps

For each of the IndicatorImport logic apps, click run->run trigger to begin importing risk lists into Sentinel. If you do not manually trigger a run, the logic apps will still run on a schedule. Do not attempt to run the RecordedFuture-ThreatIntelligenceImport logic app directly, as it is called downstream by the IndicatorImport apps and so will run automatically. To ensure there were no errors, view the past runs of both the IndicatorImport and ThreatIntelligenceImport apps to see if there were any failures.



Resource group (move) : RF
Location : East US
Subscription (move) : Azure subscription 1
Subscription ID : 5129b3ff-c0c6-4e86-bd1c-70e5fcd579cf

Definition : 1 trigger, 4 actions
Status : Disabled
Runs last 24 hours : ---
Integration Account : -- --

All | Start time earlier than | Pick a date | Pick a time

Specify the run identifier to open monitor view directly

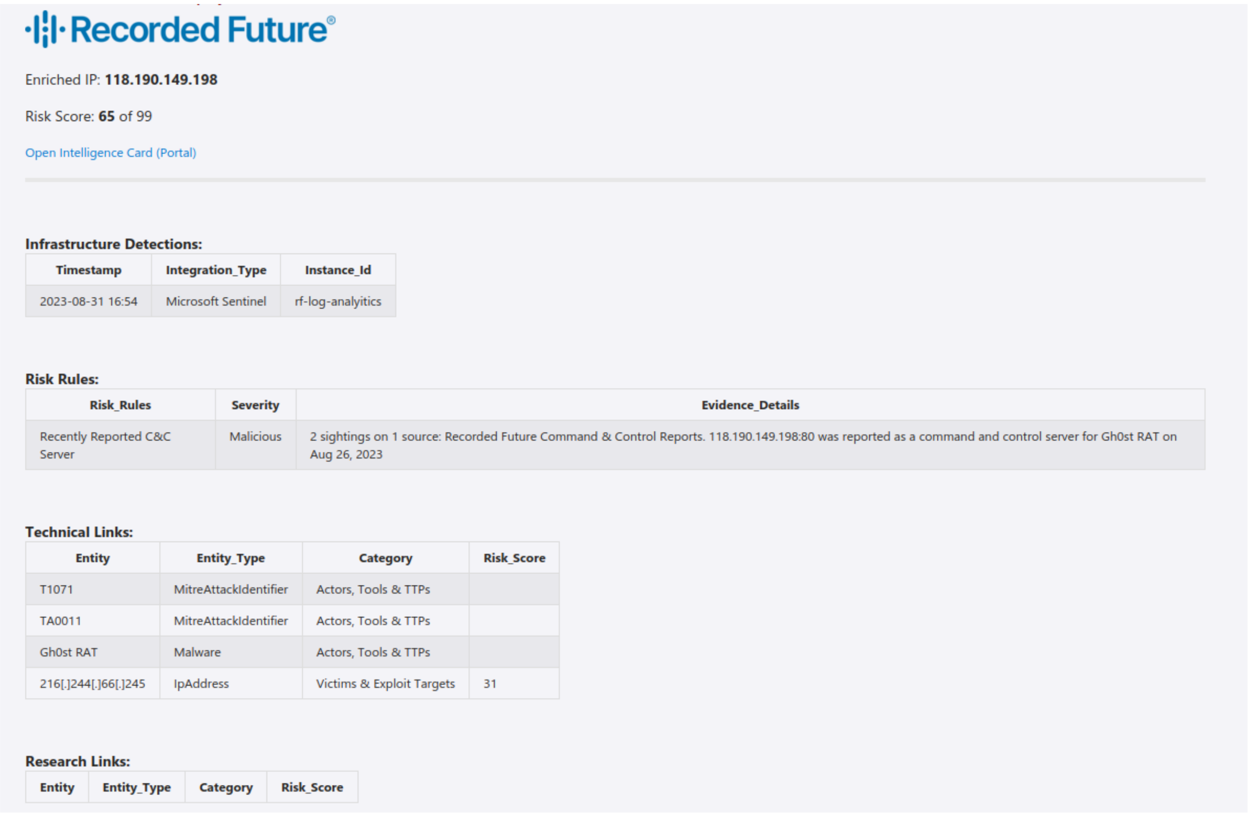
Status	Start time	Identifier	Duration	Static Results
Succeeded	12/14/2021, 8:20 AM	08585621188753532989474097235CU79	16.2 Seconds	
Failed	12/14/2021, 8:12 AM	08585621193581062085182824191CU78	331 Milliseconds	

Data should begin populating in the ThreatIntelligenceIndicator table in Sentinel. Please note that it can take up to 10-15 minutes for this data to populate the first time.

Enriching Incidents

Overview

The RecordedFuture-IOC_Enrichment-IP_Domain_URL_Hash logic app can be folded into a Sentinel Automation rule to enrich all IOCs in an incident with Recorded Future data. For each IOC in an incident, a comment will be written containing the Recorded Future Risk score, Risk Rules, links, infrastructure/collective insights detections, and intelligence card link.



Enriched IP: **118.190.149.198**

Risk Score: **65** of 99

Open Intelligence Card (Portal)

Infrastructure Detections:

Timestamp	Integration_Type	Instance_Id
2023-08-31 16:54	Microsoft Sentinel	rf-log-analyitics

Risk Rules:

Risk_Rules	Severity	Evidence_Details
Recently Reported C&C Server	Malicious	2 sightings on 1 source: Recorded Future Command & Control Reports. 118.190.149.198:80 was reported as a command and control server for Gh0st RAT on Aug 26, 2023

Technical Links:

Entity	Entity_Type	Category	Risk_Score
T1071	MitreAttackIdentifier	Actors, Tools & TTPs	
TA0011	MitreAttackIdentifier	Actors, Tools & TTPs	
Gh0st RAT	Malware	Actors, Tools & TTPs	
216[.]244[.]66[.]245	IpAddress	Victims & Exploit Targets	31

Research Links:

Entity	Entity_Type	Category	Risk_Score

Authorizing Connections

The RecordedFuture-IOC_Enrichment-IP_Domain_URL_Hash logic app required connections to be authorized to Recorded Future and Microsoft Sentinel.

Recorded Future

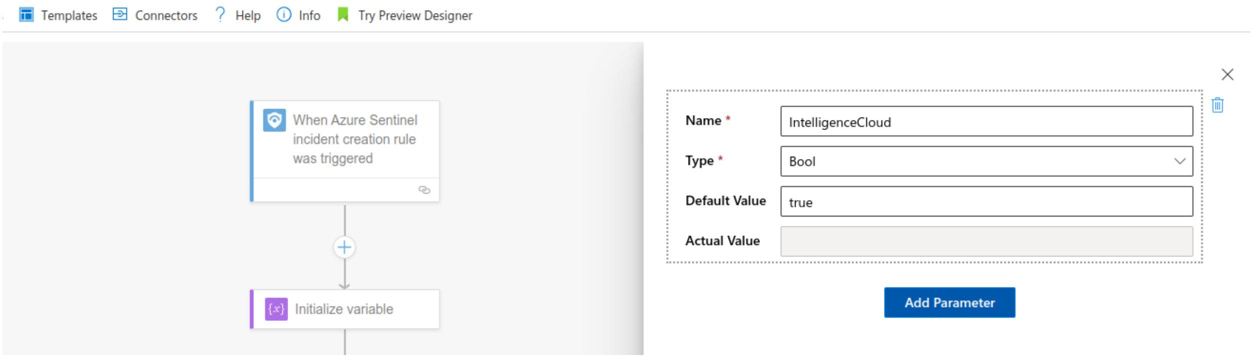
Same as before

Microsoft Sentinel

Identical process and permissions required as the Threat Intelligence Upload API

Collective Insights

Collective Insights can be enabled in the enrichment logic app by setting the "IntelligenceCloud" parameter to **true** .



Name * IntelligenceCloud

Type * Bool

Default Value true

Actual Value

This feature is enabled by default. Any IP Address, Domain, File Hash, or URL from an incident enriched by Recorded Future will be collected and used to track malicious activity and indicators over time in features like the SecOps dashboard

Creating the Automation Rule

In order to automate the enrichment process, the logic app needs to be attached to a Sentinel Automation rule. Navigate to Sentinel->Automation->Create->Automation rule. Fill out the fields using the examples below:

Automation rule name: A logical name like "Recorded Future Enrichment"

Conditions: If Analytic Rule Name “Contains” “All.” If you only want this logic app to operate on a subset of your analytic rules, please select those rules
Actions: Run playbook

Choose the RecordedFuture-IOC_Enrichment-IP_Domain_URL_Hash playbook.

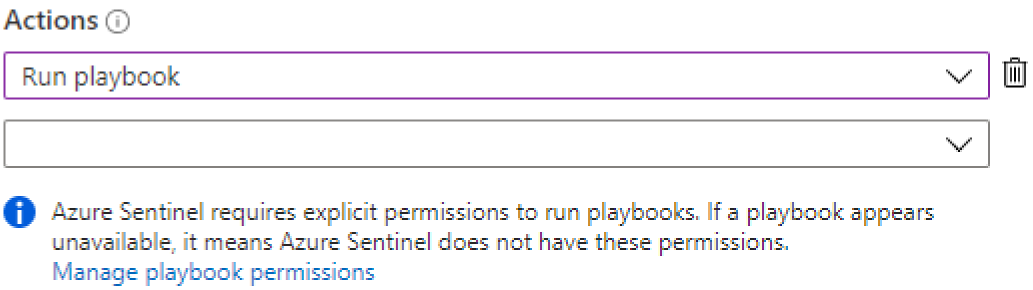
Click **Apply**.

Future Incidents should now be enriched with Recorded Future Data. This enrichment can also be run ad-hoc on past, current, and future incidents by navigating to Incidents->{Incident}->Actions->Run Playbook->Run

Creating an Automation rule requires the **Sentinel Contributor** role

Manage Permissions

If this Sentinel instance has never created an automation rule to run playbooks from this resource group before, the playbooks may be grayed out and unselectable. If you are an **owner of the resource group** where the logic apps are deployed, you will see a link to “Manage Permissions.” Click on that link and authorize running playbooks from that resource groups.



Azure Sentinel requires explicit permissions to run playbooks. If a playbook appears unavailable, it means Azure Sentinel does not have these permissions.
Manage playbook permissions

More details can be found in the Microsoft documentation here.

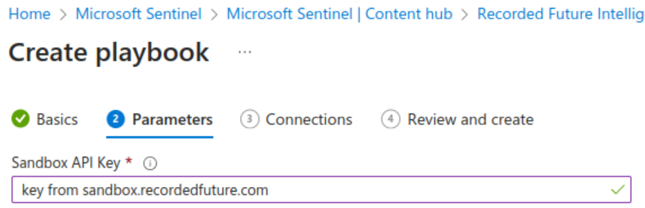
Utilizing the Malware Sandbox

Overview

The RecordedFuture-Sandbox_Enrichment-Url logic app operates similarly to the above enrichment logic app. Instead of simply fetching intelligence about an IOC, this logic app will detonate a URL in Recorded Future’s sandbox and write the results of the report to the incident as a comment

Inputting Sandbox token

During deployment of the logic app, make sure to input your Sandbox API Key as a parameter. This can be found at sandbox.recordeduture.com->Accounts->API Keys. You cannot securely enter your Sandbox API token once the logic app is deployed


Home > Microsoft Sentinel > Microsoft Sentinel | Content hub > Recorded Future Intelligence > Automation >
Create playbook ...
Basics
2 Parameters
3 Connections
4 Review and create

Sandbox API Key *: key from sandbox.recordedfuture.com

Authorizing connections

Microsoft Sentinel

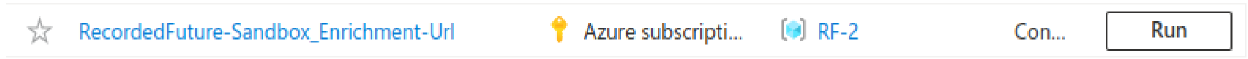
Identical process and permissions required as the Threat Intelligence Upload API

Recorded Future

Same as before, except you will need to use your Recorded Future Sentinel Sandbox API key, different from previous API keys used. This should be supplied by your Recorded Future point of Contact

Usage

We do not recommend setting up an automation rule to detonate every URL, as this may cause you to hit your limit of 10k daily submissions to the sandbox. Instead, detonate URLs of interest in an incident by navigating to Incident->Actions->Run Playbook-> RecordedFuture-Sandbox_Enrichment-Url



Importing alerts into Sentinel

The logic apps RecordedFuture-AlertImporter and RecordedFuture-Playbook-Alert-Importer will import classic alerts and playbook alerts from the Recorded Future portal. Those alerts will be stored in custom logs in Microsoft Sentinel. Optionally, classic alerts can be configured to generate incidents in Sentinel

Classic Alerts

The RecordedFuture-AlertImporter logic app imports classic alerts into the log table RecordedFuturePortalAlerts_CL. The **create_incident** parameter, that if set to True, will create a Sentinel Incident for each alert imported

Playbook Alerts

The RecordedFuture-Playbook-Alert-Importer logic app imports Playbook alerts into the log table RecordedFuturePlaybookAlerts . Current Domain Abuse Playbook alerts are supported

Authorizing connections

Microsoft Sentinel

Same as before

Recorded Future

Same as before

Azure Log Analytics Data Collector

This Connector will require your log analytics Workspace Key and ID for the Workspace your Sentinel instance is deployed in. These can be found under Log Analytics Workspaces->{Your workspace name}-Settings->Agents->Log Analytics Instructions. You will need the **Log Analytics Contributor** role to view these secrets

Azure Monitor logs

Use an OAuth login flow to authorize this connector, similar to the Microsoft Sentinel Connector. The **Log Analytics Reader** or **Microsoft Sentinel Reader** roles are required to authorize this connector

Detecting and Visualizing Malicious Activity

Modifying Analytic rules of Workbooks will require the **Sentinel Contributor** role.

Analytic Rules

Recorded Future’s integration provides a number of analytic rules to detect malicious indicators in your logs and generate incidents from them. Currently, the integration detects indicators in the following logs:

- DNSEvents
- SyslogEvents
- CommonSecurityLog
- AzureActivityEvents

If you have other log tables you want to detect malicious indicators in, you can utilize Microsoft’s built in [Threat Intelligence Detection rules](). These rules are compatible with Recorded Future’s threat intelligence.

Workbooks

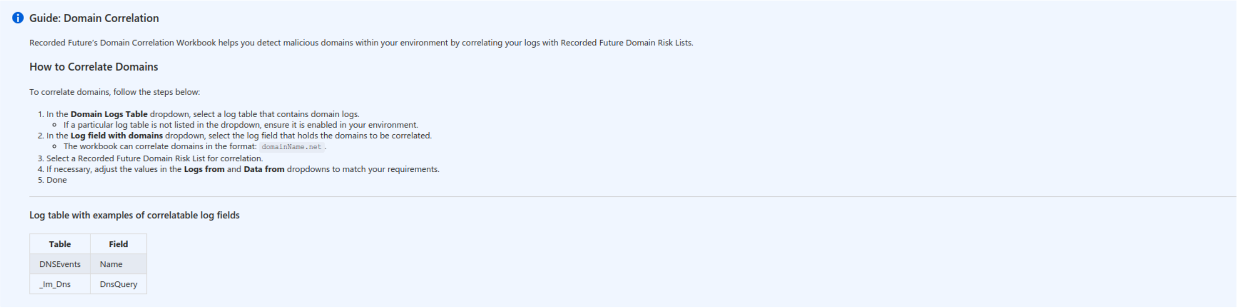
Recorded Future provides workbooks to aggregate, analyze and visualize Recorded Future data in your environment.

Correlation Workbooks

The Recorded Future Solution comes with four correlation workbooks (one each for IP Addresses, Domains, Hashes and URLs) which correlate Recorded Future threat intelligence with your telemetry.

For each workbook, select the log table and log field you want to correlate IOCs against, as well as the time picker. There is also an in-workbook guide to assist you

Please note that these workbooks are only compatible with log sources where an IOC is extracted into a separate field - correlations against IOCs that are part of a larger string are not currently supported



Guide: Domain Correlation

Recorded Future's Domain Correlation Workbook helps you detect malicious domains within your environment by correlating your logs with Recorded Future Domain Risk Lists.

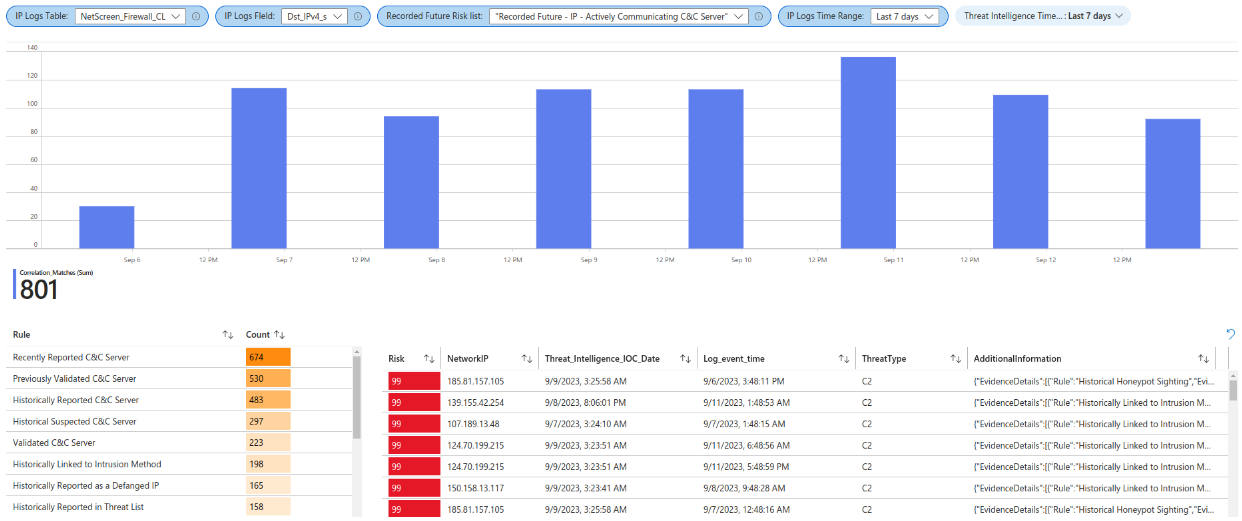
How to Correlate Domains

To correlate domains, follow the steps below:

1. In the **Domain Logs Table** dropdown, select a log table that contains domain logs.
   - If a particular log table is not listed in the dropdown, ensure it is enabled in your environment.
2. In the **Log field with domains** dropdown, select the log field that holds the domains to be correlated.
   - The workbook can correlate domains in the format: `domainName.net`.
3. Select a Recorded Future Domain Risk List for correlation.
4. If necessary, adjust the values in the **Logs from** and **Data from** dropdowns to match your requirements.
5. Done

Log table with examples of correlatable log fields

Table	Field
DNSEvents	Name
_Im_Dns	DnsQuery



IP Logs Table: NetScreen_Firewall_CL

IP Logs Field: Dst_IPv4_s

Recorded Future Risk list: "Recorded Future - IP - Actively Communicating C&C Server"

IP Logs Time Range: Last 7 days

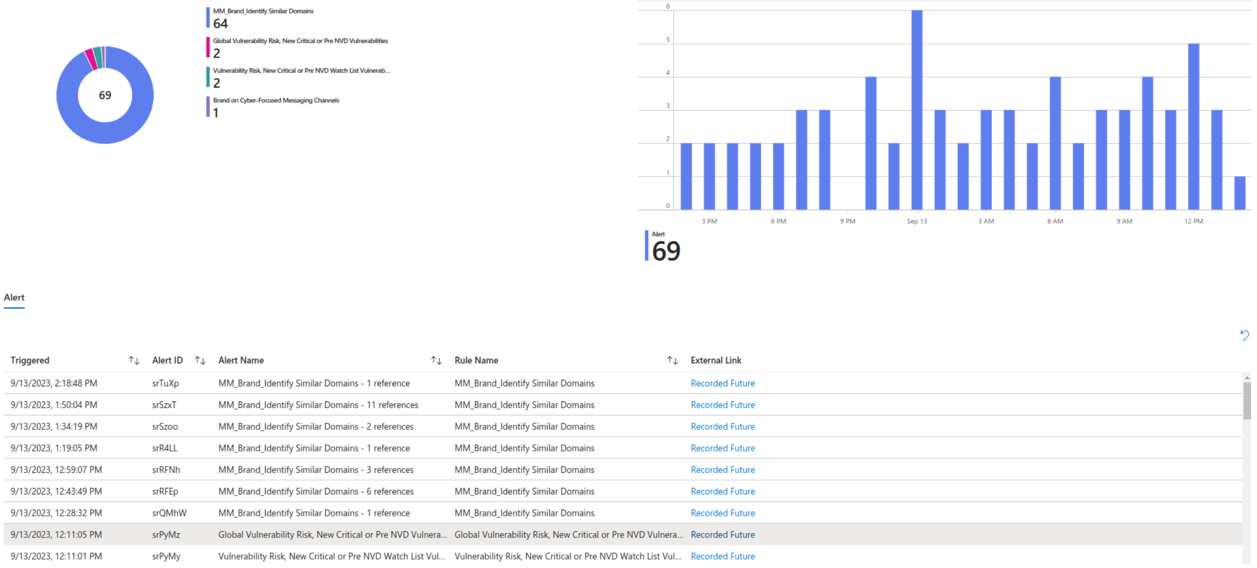
Threat Intelligence Time... : Last 7 days

Rule	Count
Recently Reported C&C Server	674
Previously Validated C&C Server	530
Historically Reported C&C Server	483
Historical Suspected C&C Server	297
Validated C&C Server	223
Historically Linked to Intrusion Method	198
Historically Reported as a Defanged IP	165
Historically Reported in Threat List	158

Risk	NetworkIP	Threat_Intelligence_IOC_Date	Log_event_time	ThreatType	AdditionalInformation
99	185.81.157.105	9/9/2023, 3:25:58 AM	9/6/2023, 3:48:11 PM	C2	{"EvidenceDetails":[{"Rule":"Historical Honeypot Sighting","Evi...
99	139.155.42.254	9/8/2023, 8:06:01 PM	9/11/2023, 1:48:53 AM	C2	{"EvidenceDetails":[{"Rule":"Historically Linked to Intrusion M...
99	107.189.13.48	9/7/2023, 3:24:10 AM	9/7/2023, 1:48:15 AM	C2	{"EvidenceDetails":[{"Rule":"Historically Linked to Intrusion M...
99	124.70.199.215	9/9/2023, 3:23:51 AM	9/11/2023, 6:48:56 AM	C2	{"EvidenceDetails":[{"Rule":"Historically Linked to Intrusion M...
99	124.70.199.215	9/9/2023, 3:23:51 AM	9/11/2023, 5:48:59 PM	C2	{"EvidenceDetails":[{"Rule":"Historically Linked to Intrusion M...
99	150.158.13.117	9/9/2023, 3:23:41 AM	9/8/2023, 9:48:28 AM	C2	{"EvidenceDetails":[{"Rule":"Historically Linked to Intrusion M...
99	185.81.157.105	9/9/2023, 3:25:58 AM	9/7/2023, 12:48:16 AM	C2	{"EvidenceDetails":[{"Rule":"Historical Honeypot Sighting","Evi...

Classic Alerts

The workbook Recorded Future - Alerts Overview displays and visualizes alerts imported into a Sentinel custom log. Make sure to select the correct log table where the Alerts are stored, by default RecordedFuturePortalAlerts_CL

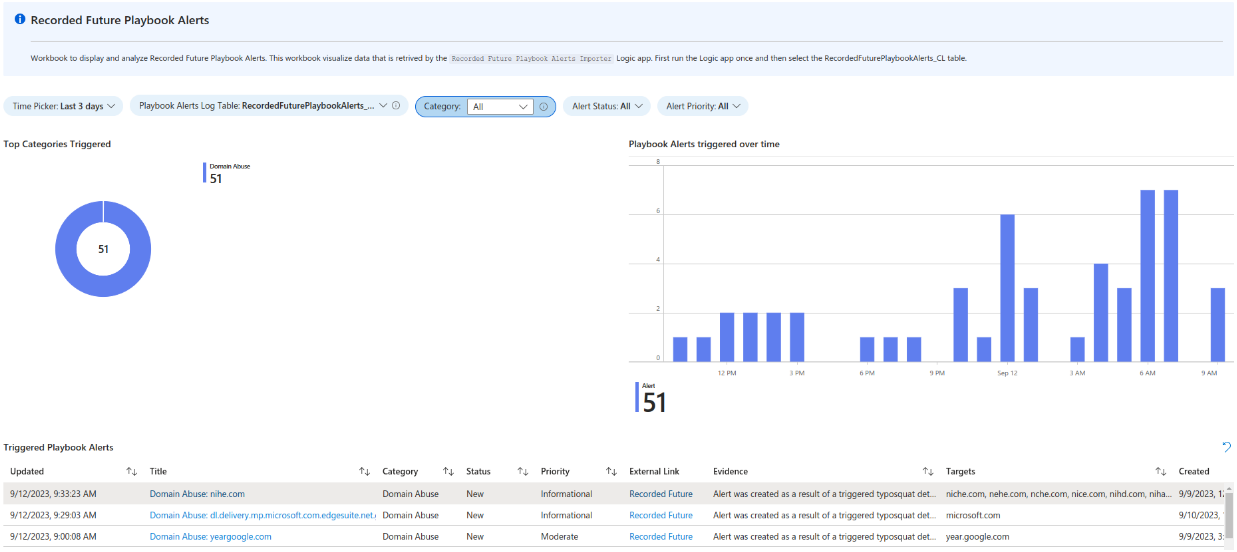


69
MM_Brand_Identify Similar Domains
64
Global Vulnerability Risk, New Critical or Pre NVD Vulnerabilities
2
Vulnerability Risk, New Critical or Pre NVD Watch List Vulnerab...
2
Brand on Cyber-Focused Messaging Channels
1
6
5
4
3
2
1
0
3 PM
6 PM
9 PM
Sep 13
3 AM
6 AM
9 AM
12 PM
Alert
69
Alert

Triggered	Alert ID	Alert Name	Rule Name	External Link
9/13/2023, 2:18:48 PM	srTuXp	MM_Brand_Identify Similar Domains - 1 reference	MM_Brand_Identify Similar Domains	Recorded Future
9/13/2023, 1:50:04 PM	srSzxT	MM_Brand_Identify Similar Domains - 11 references	MM_Brand_Identify Similar Domains	Recorded Future
9/13/2023, 1:34:19 PM	srSzoo	MM_Brand_Identify Similar Domains - 2 references	MM_Brand_Identify Similar Domains	Recorded Future
9/13/2023, 1:19:05 PM	srR4LL	MM_Brand_Identify Similar Domains - 1 reference	MM_Brand_Identify Similar Domains	Recorded Future
9/13/2023, 12:59:07 PM	srRFNh	MM_Brand_Identify Similar Domains - 3 references	MM_Brand_Identify Similar Domains	Recorded Future
9/13/2023, 12:43:49 PM	srRFEp	MM_Brand_Identify Similar Domains - 6 references	MM_Brand_Identify Similar Domains	Recorded Future
9/13/2023, 12:28:32 PM	srQMhW	MM_Brand_Identify Similar Domains - 1 reference	MM_Brand_Identify Similar Domains	Recorded Future
9/13/2023, 12:11:05 PM	srPyMz	Global Vulnerability Risk, New Critical or Pre NVD Vulnera...	Global Vulnerability Risk, New Critical or Pre NVD Vulnera...	Recorded Future
9/13/2023, 12:11:01 PM	srPyMy	Vulnerability Risk, New Critical or Pre NVD Watch List Vul...	Vulnerability Risk, New Critical or Pre NVD Watch List Vul...	Recorded Future

Playbook Alerts

The workbook Recorded Future - Playbook Alerts Overview operates similarly for playbook alerts



Recorded Future Playbook Alerts

Workbook to display and analyze Recorded Future Playbook Alerts. This workbook visualize data that is retrived by the `Recorded Future Playbook Alerts Importer` Logic app. First run the Logic app once and then select the RecordedFuturePlaybookAlerts_CL table.

Time Picker: **Last 3 days** | Playbook Alerts Log Table: **RecordedFuturePlaybookAlerts_...** | Category: All | Alert Status: **All** | Alert Priority: **All**

Top Categories Triggered

Playbook Alerts triggered over time

Triggered Playbook Alerts

Updated	Title	Category	Status	Priority	External Link	Evidence	Targets	Created
9/12/2023, 9:33:23 AM	Domain Abuse: nihe.com	Domain Abuse	New	Informational	Recorded Future	Alert was created as a result of a triggered typosquat det...	niche.com, nehe.com, nche.com, nice.com, nihd.com, niha...	9/9/2023, 1
9/12/2023, 9:29:03 AM	Domain Abuse: dl.delivery.mp.microsoft.com.edgesuite.net.	Domain Abuse	New	Informational	Recorded Future	Alert was created as a result of a triggered typosquat det...	microsoft.com	9/10/2023,
9/12/2023, 9:00:08 AM	Domain Abuse: yeargoogle.com	Domain Abuse	New	Moderate	Recorded Future	Alert was created as a result of a triggered typosquat det...	year.google.com	9/9/2023, 3:

FAQs and common issues

Can I detonate files in the malware sandbox using this integration?

Our logic app connector supports uploading files to the malware sandbox. Microsoft Sentinel does not allow you to extract file objects, so we have no prebuilt logic apps to detonate files from Sentinel. If you have another use case (like sending email attachments to be detonated), this can be supported. We have two sample logic app ARM templates that you can use as a base to build you custom solution

Can I adjust the cadence of my risk list pulls?

You can adjust the cadence in the Recurrence block of the IndicatorImport logic apps. However, if you do so it is **critical** that you also adjust the expirationDateTime parameter in the final block of that logic app to be synchronized with the recurrence timing. Failure to do so can result in either a) duplicate indicators or b) having no active Recorded Future indicators the majority of the time. If you are unsure of how to do this, please consult your Recorded Future point of contact.