

McAfee ESM Configuration

Table of Contents

| | |
|---------------------------------|---|
| Introduction | 2 |
| Requirements | 2 |
| Configuration | 3 |
| Output: Watchlists | 6 |
| Output: Cyber Threat Indicators | 7 |
| Conclusion | 7 |

Introduction

Recorded Future is continually collecting and analyzing information from all over the internet to deliver the largest commercial security intelligence repository available. From this, Recorded Future creates frequently updated lists of high risk, malicious Indicators of Compromise (IOCs). These IOCs are delivered via STIX/TAXII and can be ingested as Watchlists within ESM, one for each IOC type(i.e., IP's, URL's, Hash and Domains).

These watchlists can then be correlated against internal telemetry for threat detection. When potential threats are discovered, Recorded Future can further assist with triage by providing additional context, such as indicator Risk Score and the associated evidence.

Please note that this configuration represents a basic integration setup. Fine tuning of both the risk indicators ingested and the associated detection rules can result in a more efficient and organization-specific security posture.

Requirements

- ESM version 10.3 and higher
- ESM Cyber Threat Module
- Access the Recorded Future Taxii server at <https://api.recordedfuture.com/taxii/>
- Recorded Future API Access via an integration subscription

Configuration

1. Create a "Cyber Threat Feed"

Cyber Threat Feed Wizard

Main Source Frequency Watchlist Backtrace

Fill out the information for retrieval of IOCs from a particular feed.

Name: Recorded_Future_Custom_IP

Enabled: ☒

Cancel < Back Next > Finish

Name the field unique and specific

2. Connect to the TAXII Server

- Server: <https://api.recordedfuture.com/taxii/>
- Basic Authorization
- Username: Can be anything here
- Password: valid Recorded Future API Token
- Collection Name: "ip_full" for IP Collection, "domain_full" for domains, "hash_full" for hashes and "url_full" for URLs

Cyber Threat Feed Wizard

Main Source Frequency Watchlist Backtrace

From the type combo box choose the correct driver to connect to your external source and then fill in the appropriate connection fields that will be needed.

Type: TAXII

URL: https://api.recordedfuture.com/taxii/

Authentication: ☐ None ☒ Basic

Username: anyusername

Password: *****

Method: ☒ GET ☐ POST

Ignore Invalid Certificates: ☒

Collection Name: full

Start Date: 01/01/1970 00:00:00

Test Connection:

Cancel < Back Next > Finish

Collection name for the TAXII server

URL for Recorded Future's Taxii Server

Use Basic Authentication

Username can be anything

Password is your Recorded Future Token

Once all the fields are entered, hit "Connect".

3. Schedule the collection, default is every two hours

- Pull Frequency: "Every So Many Minutes"

- Trigger Rate: 2 Hours

Cyber Threat Feed Wizard

Main Source Frequency Watchlist Backtrace

Choose the appropriate time when the Cyber Threat Manager should check for new indicators.

Pull Frequency: Every So Many Minutes

Periodic Trigger Rate

Hour: 2 Minute: 0

Cancel < Back Next > Finish

4. Map to watchlist. We recommend creating a new watchlist to age out duplicate data.

Cyber Threat Feed Wizard

Main Source Frequency Watchlist Backtrace

Optionally select the possible indicator types from the incoming IOC files and the watchlist to append the data to. These watchlists can potentially be used to filter throughout the product, as well as, create correlation rules.

Indicator Type

append to

Watchlist

Create New Watchlist

Cancel < Back Next > Finish

5. The watchlists should have indicative names representing the threat intelligence source and IOC type, whilst also selecting the associated Indicator type.

Values must be set to expire in a timeframe relative to the frequency of the Cyber Threat Feed, i.e if you are pulling data every 1 hour then ensure the data is timed

out every hour. This prevents excessive data consumption on ESM whilst also maintaining relevant high quality intelligence and rich content.

Name of the watchlist should be detailed and specific:

- Set "Static"
- For IP
 - Type: "IP Address"
 - Indicator Type: "IPv4"
- For Domain
 - Type: "Domain"
 - Indicator Type: "Fully Qualified Domain Name"
- For Hash
 - Type: "Hash"
 - Indicator Type: "MD5"
 - Or
 - Indicator Type: "SHA-256"
- For URL
 - Type: "URL"
 - Indicator Type: "URL"

Add Watchlist

Main Values

Select the type of values this watchlist will contain.

Type: **IP Address**

Values:

Match the indicator type with the data type you are collecting from the TAXII server

Hit finish when complete

Clear Values Export Import

Cancel < Back Next > Finish

Add Watchlist

Main Values

Enter a name for the watchlist.

Name: Recorded_Future_Custom_IP_WL

☒ Static ☐ Dynamic

☐ Values Expire

Duration: 1 Hours

Cancel < Back Next > Finish

Cyber Threat Feed Wizard

Main Source Frequency Watchlist Backtrace

Optionally select the possible indicator types from the incoming IOC files and the watchlist to append the data to. These watchlists can potentially be used to filter throughout the product, as well as, create correlation rules.

| Indicator Type | append to | Watchlist |
|----------------|-----------|------------------------------|
| IPv4 | append to | Recorded_Future_Custom_IP_WL |
| | append to | |

Map the Indicator types from the collection data to the watchlist(s) you created

Hit finish when done with the mapping

Create New Watchlist

Cancel < Back Next > Finish

Output: Watchlists

System Properties

System Information

Alarms

Content Packs

Custom Settings

Custom Types

Cyber Threat Feeds

Data Enrichment

Database

Email Settings

ESM Management

Event Forwarding

File Maintenance

Global Blacklist

Hosts

Login Security

Network Settings

Profile Management

Reports

SNMP Configuration

System Log

Users and Groups

Watchlists

Watchlists:

| Name | Type | State |
|------------------------------|------------|--------------|
| GTI Malicious IPs | IP Address | Inactive |
| GTI Suspicious IPs | IP Address | Inactive |
| Recorded_Future_Custom_IP_WL | IP Address | 10659 values |

Edit Watchlist

Main Values

Select the type of values this watchlist will contain.

Type: IP Address

Values:

- 1.109.105.144
- 1.160.121.212
- 1.160.98.76
- 1.162.177.98
- 1.163.211.97
- 1.163.6.149
- 1.168.204.177
- 1.170.24.181
- 1.172.172.253
- 1.172.20.161
- 1.173.137.63
- 1.174.149.91
- 1.179.156.149
- 1.179.190.36
- 1.186.137.174
- 1.186.184.163
- 1.186.185.77

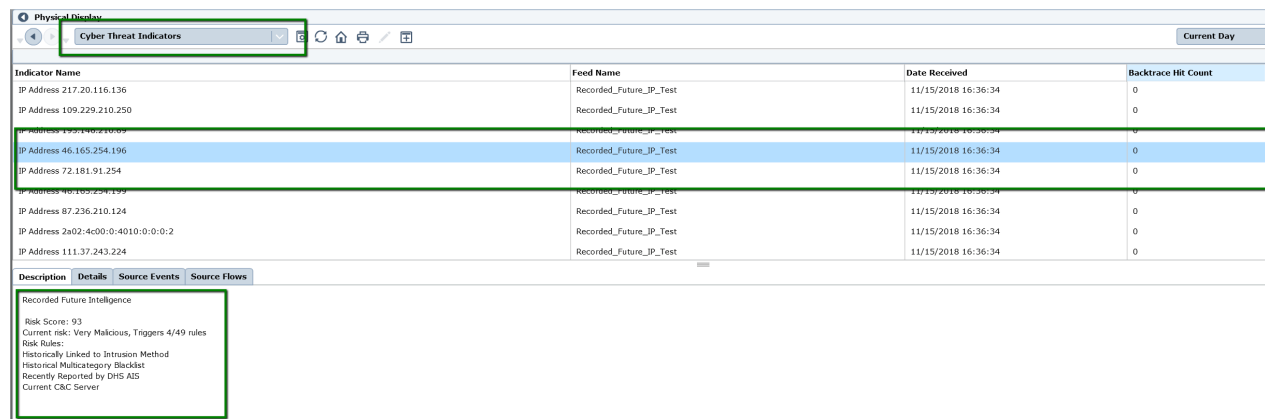
Clear Values

Export Import

Cancel < Back Next > Finish

OK Cancel Apply

Output: Cyber Threat Indicators



| Indicator Name | Feed Name | Date Received | Backtrace Hit Count |
|-------------------------------------|-------------------------|---------------------|---------------------|
| IP Address 217.20.116.136 | Recorded_Future_IP_Test | 11/15/2018 16:36:34 | 0 |
| IP Address 109.229.210.250 | Recorded_Future_IP_Test | 11/15/2018 16:36:34 | 0 |
| IP Address 193.107.10.69 | Recorded_Future_IP_Test | 11/15/2018 16:36:34 | 0 |
| IP Address 46.165.254.196 | Recorded_Future_IP_Test | 11/15/2018 16:36:34 | 0 |
| IP Address 72.181.91.254 | Recorded_Future_IP_Test | 11/15/2018 16:36:34 | 0 |
| IP Address 46.105.224.159 | Recorded_Future_IP_Test | 11/15/2018 16:36:34 | 0 |
| IP Address 87.236.210.124 | Recorded_Future_IP_Test | 11/15/2018 16:36:34 | 0 |
| IP Address 2a02:4c00:0:4010:0:0:0:2 | Recorded_Future_IP_Test | 11/15/2018 16:36:34 | 0 |
| IP Address 111.37.243.224 | Recorded_Future_IP_Test | 11/15/2018 16:36:34 | 0 |

| Description | Details | Source Events | Source Flows |
|---|---------|---------------|--------------|
| Recorded Future Intelligence Risk Score: 93 Current risk: Very Malicious, Triggers 4/49 rules Risk Rules: Historically Linked to Intrusion Method Historical Multicategory Blacklist Recently Reported by DHS AIS Current C&C Server | | | |

Conclusion

There are many elements of the data which may well require further explanation from the analyst's perspective. For example, to gain a better understanding around the scores and risk rules, it's advisable to visit the support panel on the Recorded Future platform. The following links will provide insight into scoring mechanisms, terminology and integration application specifics (a login to the Recorded Future portal is required to access these pages). Additionally there is a wealth of information that is maintained and updated regularly around threat intelligence which is well worth the time and consideration.

<https://support.recordedfuture.com/hc/en-us/articles/115004303128-TAXII-service>

<https://support.recordedfuture.com/hc/en-us/articles/360062518313-STIX-TAXII-Collection-Use-Cases>

<https://support.recordedfuture.com/hc/en-us/articles/115000897208-Risk-Scoring-in-Recorded-Future>

<https://support.recordedfuture.com/hc/en-us/articles/360051212654-Support-at-Recorded-Future>

Should support be required please email support@recordedfuture.com or use this [online form](#); our teams will respond to any concerns or queries promptly.