Symantec EDR App for QRadar

App Architecture and Installation Guide

v1.3.0

Chapter 1

Architecture

This chapter includes the following topics:

Architecture

IBM QRadar SIEM is a network security management platform that provides situational awareness and compliance support.

Symantec Endpoint Detection and Response (EDR) helps you uncover, prioritize, investigate, re-mediate complex attacks across endpoint, email, and network from one console.

The Symantec EDR App for QRadar provides user aggregated as well as individual visualizations for Network and Endpoint by collecting data from Symantec EDR. The Symantec EDR app's functionality can be distributed in three parts as follows:

Data Collection

We use REST API calls to onboard data from Symantec EDR server. The application contains python scripts, which makes REST calls to following APIS. These scripts are run on user-defined schedule. By default, all the scripts are in disabled mode. The application supports data onboarding from multiple servers. This configuration can be managed via setup page.

- /events
- /incidents

- /incidentevents

Log Source

Symantec EDR App for QRadar creates log source called “Symantec ATP” automatically when the app is installed. This log source will identify all events that are coming to QRadar with this log source because all events have log source identifier - “symantecapp”.

Symantec EDR DSM

Separate DSM is built as part of this integration. The custom DSM is used for correctly assigning event name and event categories to Symantec EDR events. The event name and event categories are identified using QIDS. Following table lists EDR event to QID mapping. All the events with event id other than one mentioned in below table will have “Unknown” for event name and event category.

Event Id	QidName	Low-level Category	High-level Category
1000	Database error	Error	System
4096	Reputation Lookup	Information	System
4098	Intrusion Prevention	Information	System
4099	Suspicious File Detection	Suspicious Activity	Suspicious Activity
4100	SONAR Detection	Information	System
4102	Antivirus (Endpoint Detection)	Virus Detected	Malware
4109	File IoC Event	Suspicious Activity	Suspicious Activity
4110	Network IoC Event	Suspicious Activity	Suspicious Activity
4112	Blacklist (IP/URL/Domain)	Loss Of Confidentiality	Risk
4113	Vantage Detection	Web Exploit	Exploit
4115	Insight Detection	Information Leak	Suspicious Activity
4116	Mobile Insight	Information Leak	Suspicious Activity
4117	Sandboxing Detection	Information	System
4118	Blacklist (file)	Loss Of Confidentiality	Risk
4123	Endpoint File Detection	Misc Exploit	Exploit
4124	Endpoint (IP/URL/Domain) Detection	Misc Exploit	Exploit
4125	Email Detection	Misc Exploit	Exploit

4353	Antivirus (Network) Detection	Virus Detected	Malware
8000	Session Event	User Activity	Suspicious Activity
8001	Process Event	General Audit Event	Audit
8002	Module Event	General Audit Event	Audit
8003	File Event	General Audit Event	Audit
8004	Directory Event	General Audit Event	Audit
8005	Registry Key Event	Registry Key	System
8006	Registry Value Event	Registry Value	System
8007	Network Event	Misc Network Communication Event	Access
8009	Kernel Event	Information	System
8080	Session Query Result	General Audit Event	Audit
8081	Process Query Result	General Audit Event	Audit
8082	Module Query Result	General Audit Event	Audit
8083	File Query Result	General Audit Event	Audit
8084	Directory Query Result	General Audit Event	Audit
8085	Registry Key Query Result	General Audit Event	Audit
8086	Registry Value Query Result	General Audit Event	Audit
8089	Kernel Object Query Result	General Audit Event	Audit
8090	Service Query Result	General Audit Event	Audit
8099	Query Command Errors	Error	System
8103	File Remediation	General Audit Event	Audit
8119	File Remediation Errors	Error	System
Symantec Action	Symantec Action	General Audit	Audit
Symantec Incidents	Symantec Incidents	Notice	System

Network and Endpoint Event Type IDs

We have bifurcated Network and Endpoint Protection dashboard panels based on below event type IDs. Overview dashboard panels pull events from all event IDs.

Endpoint: 4096,4098,4099,4109,4100,4102,4111,4119,4120,4121,4122,4123,4124
Network: 4110, 4112, 4113,4115,4116,4117,4118,4126,4353

Chapter 2

Visualization, Dashboards and Actions

This chapter includes the following topics:

Visualization, Dashboards and Actions

Visualization

This application uses python's flask framework and various open source JavaScript framework to extend the capability of QRadar to visualize Symantec EDR events. It also includes four custom actions, which helps SOC in the closing loop by connecting Symantec EDR with QRadar.

Dashboards

All the dashboards consist of individual panels which plot specific metric related to the events from Symantec EDR server. All the dashboards allow the user to filter events by time. In addition to this first three dashboards also have the capability to filter events by Host since this application can support multiple EDR instances.

Overview Dashboard

This dashboard is built to provide overall visibility into EDR deployment. It gives count of suspicious files, open incidents, Top 10 event contributors etc.

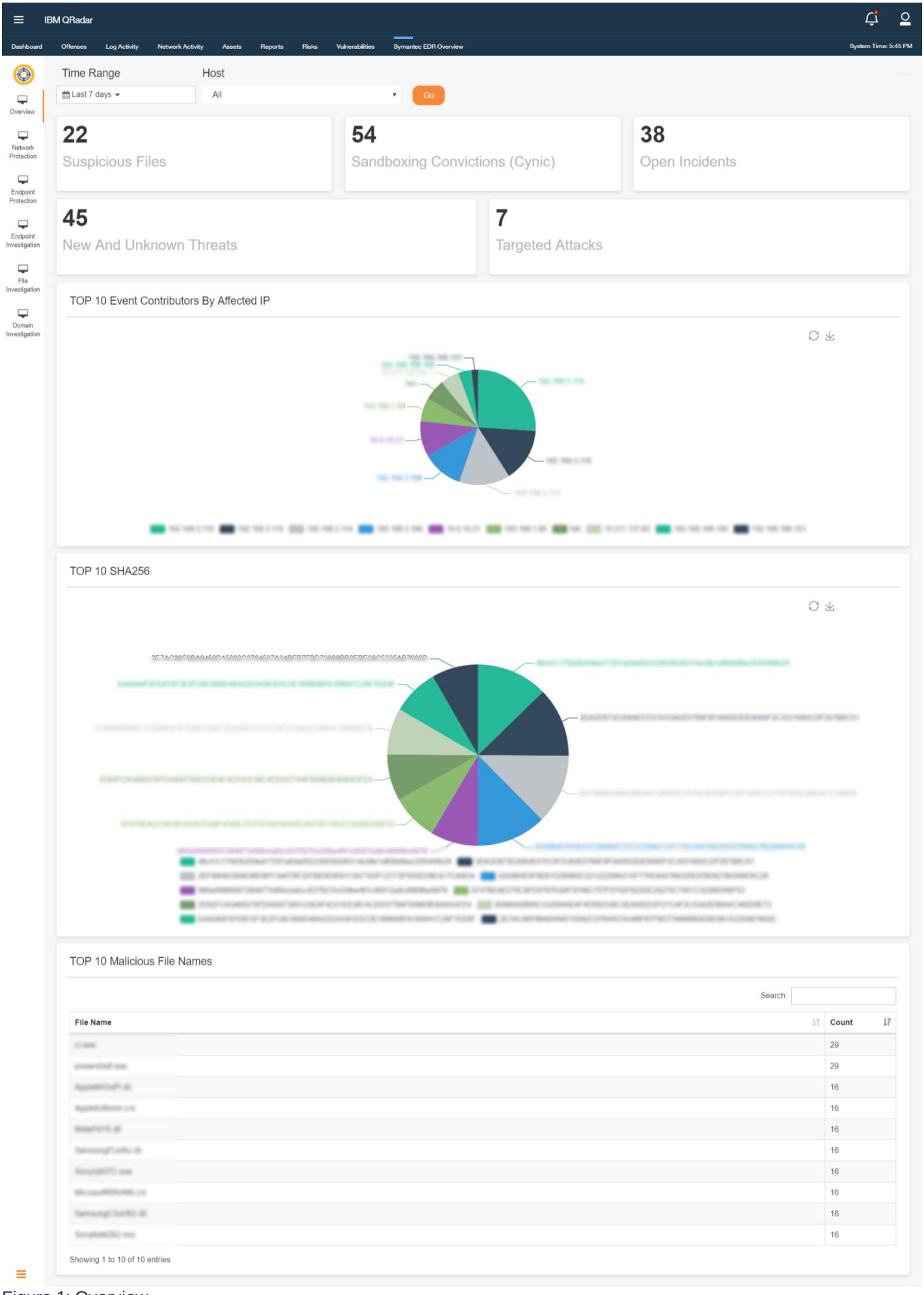


Figure 1: Overview

Network Protection Dashboard

This dashboard is built to provide visibility into network events collected by EDR.

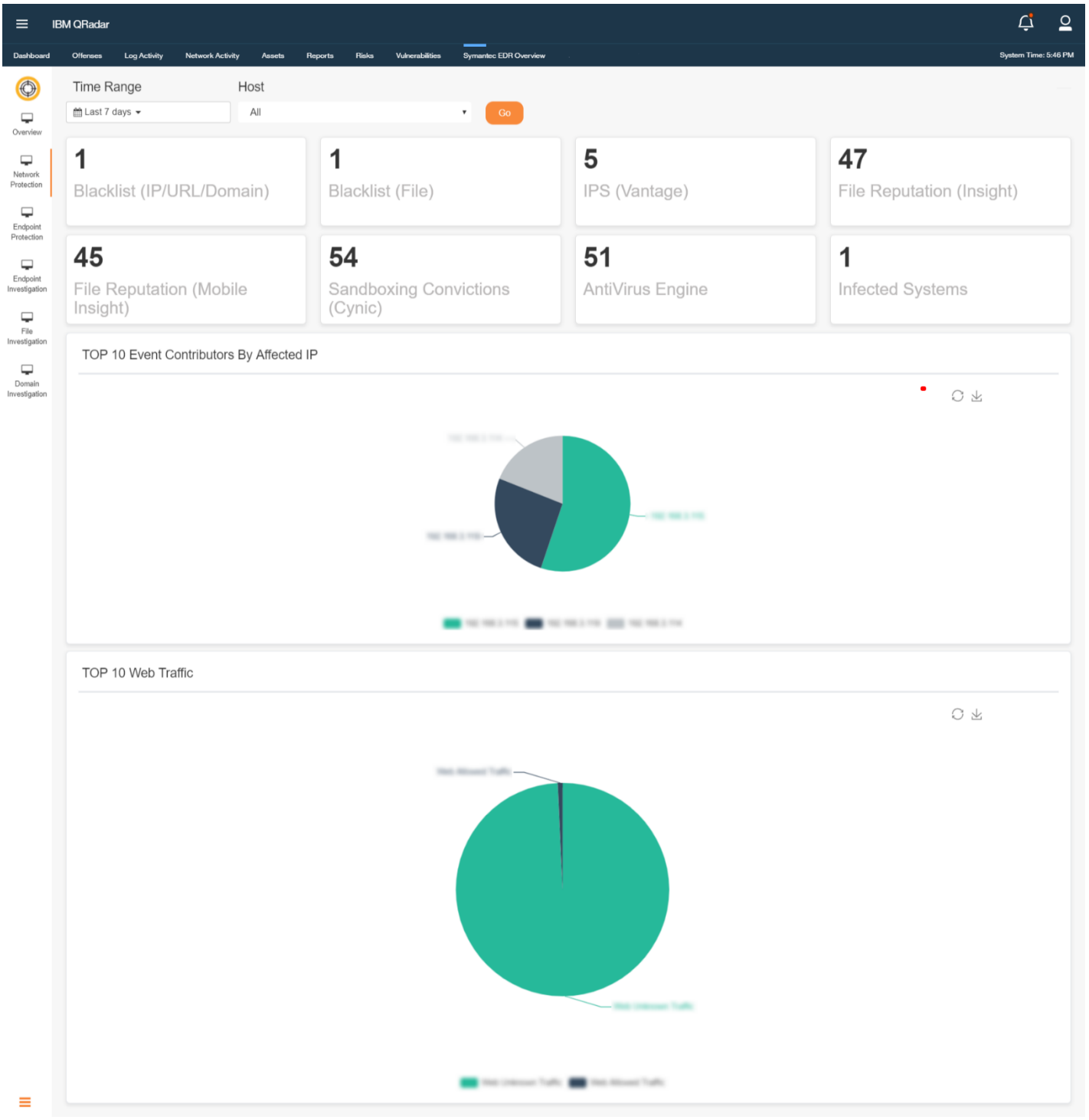


Figure 2: Network Protection at Glance

Endpoint Protection Dashboard

This dashboard is built to provide visibility into various endpoints managed by EDR.

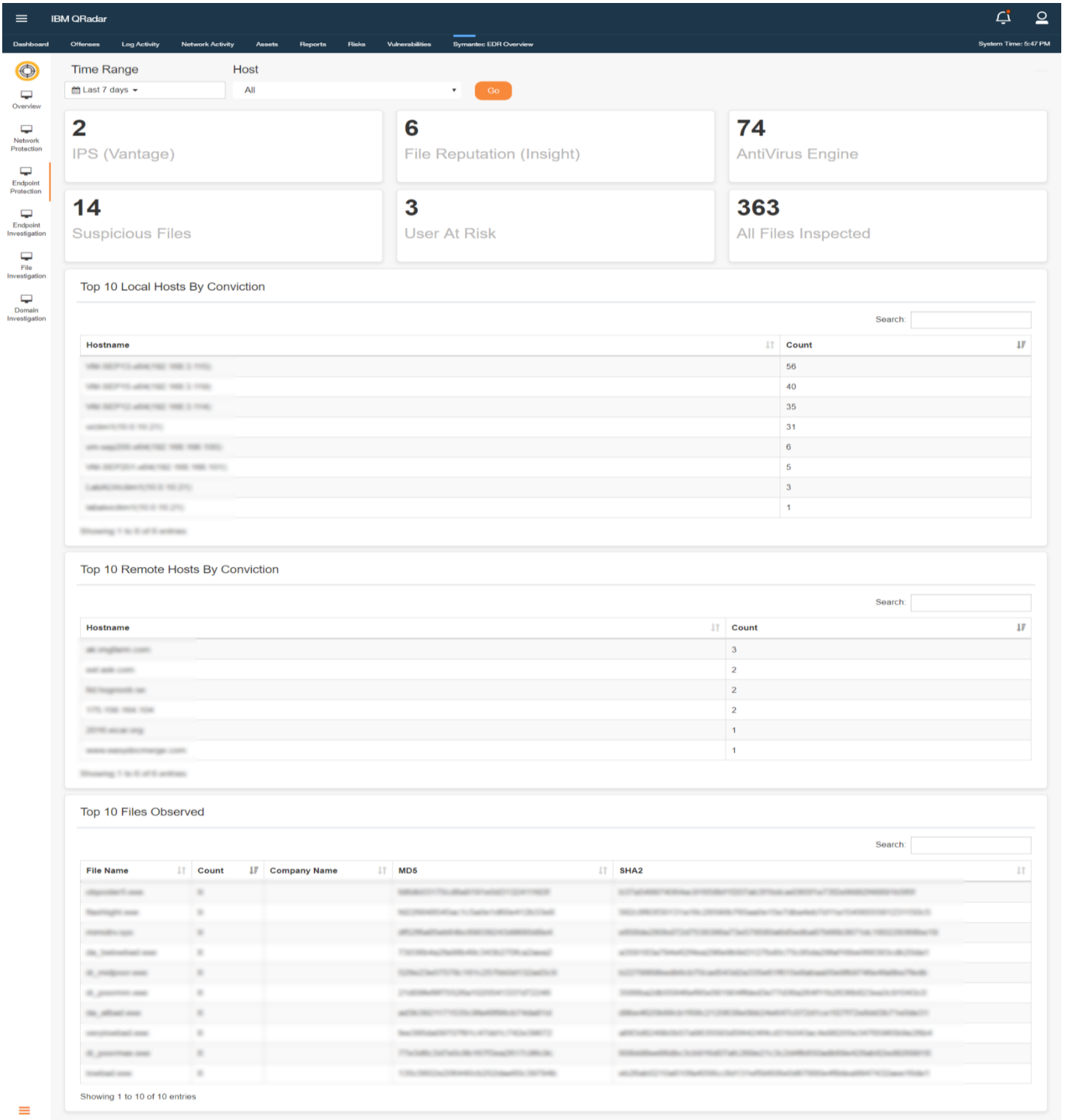


Figure 3: Endpoint Protection at Glance

Endpoint Investigation Dashboard

This dashboard is built for user to investigate a particular endpoint. User can type in the endpoint he wants to investigate and filter the data

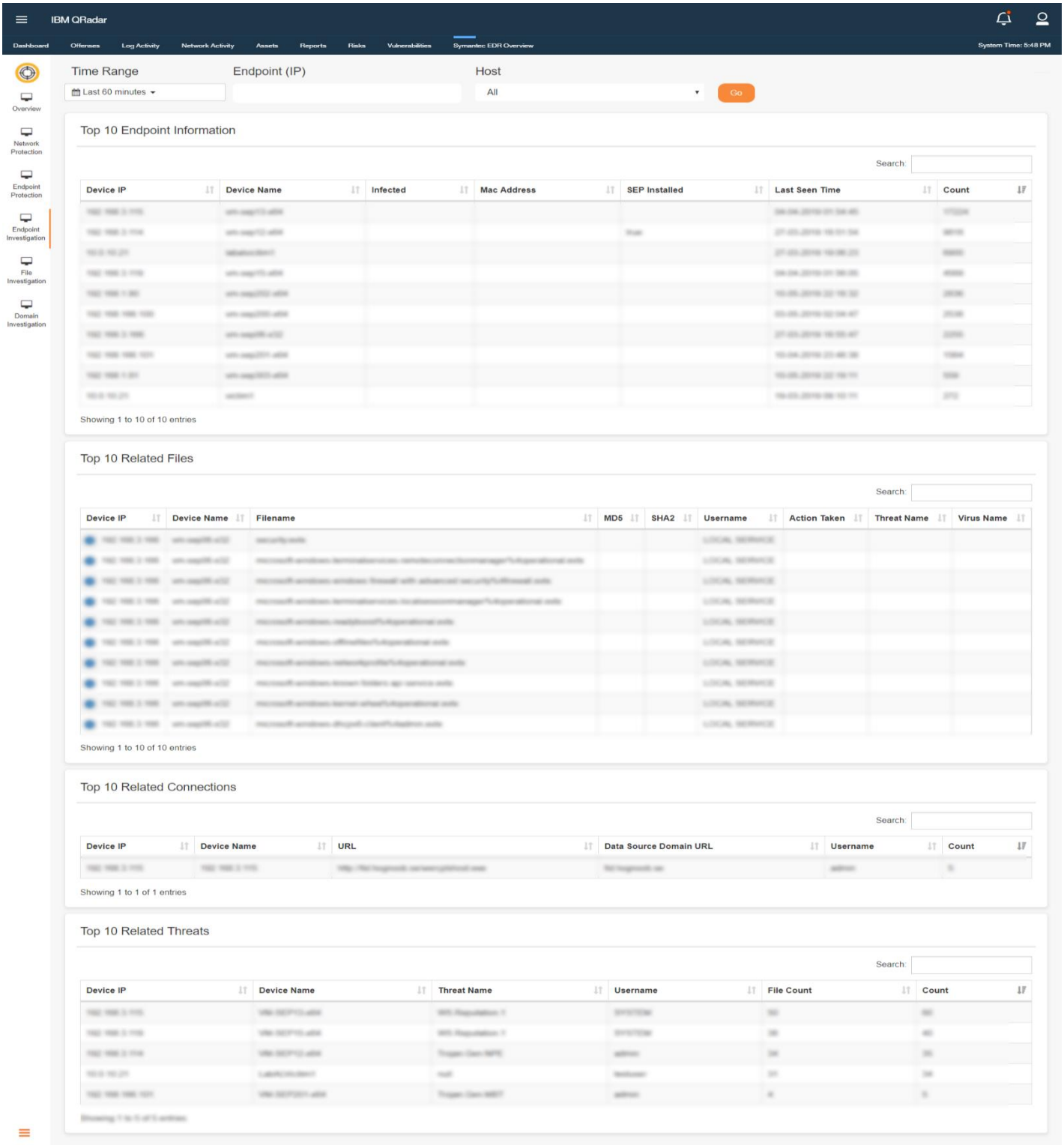


Figure 4: Endpoint Investigation

File Investigation Dashboard

This dashboard is built for user to investigate a particular file. User can type in the file hash or file URL he wants to investigate and filter the data.

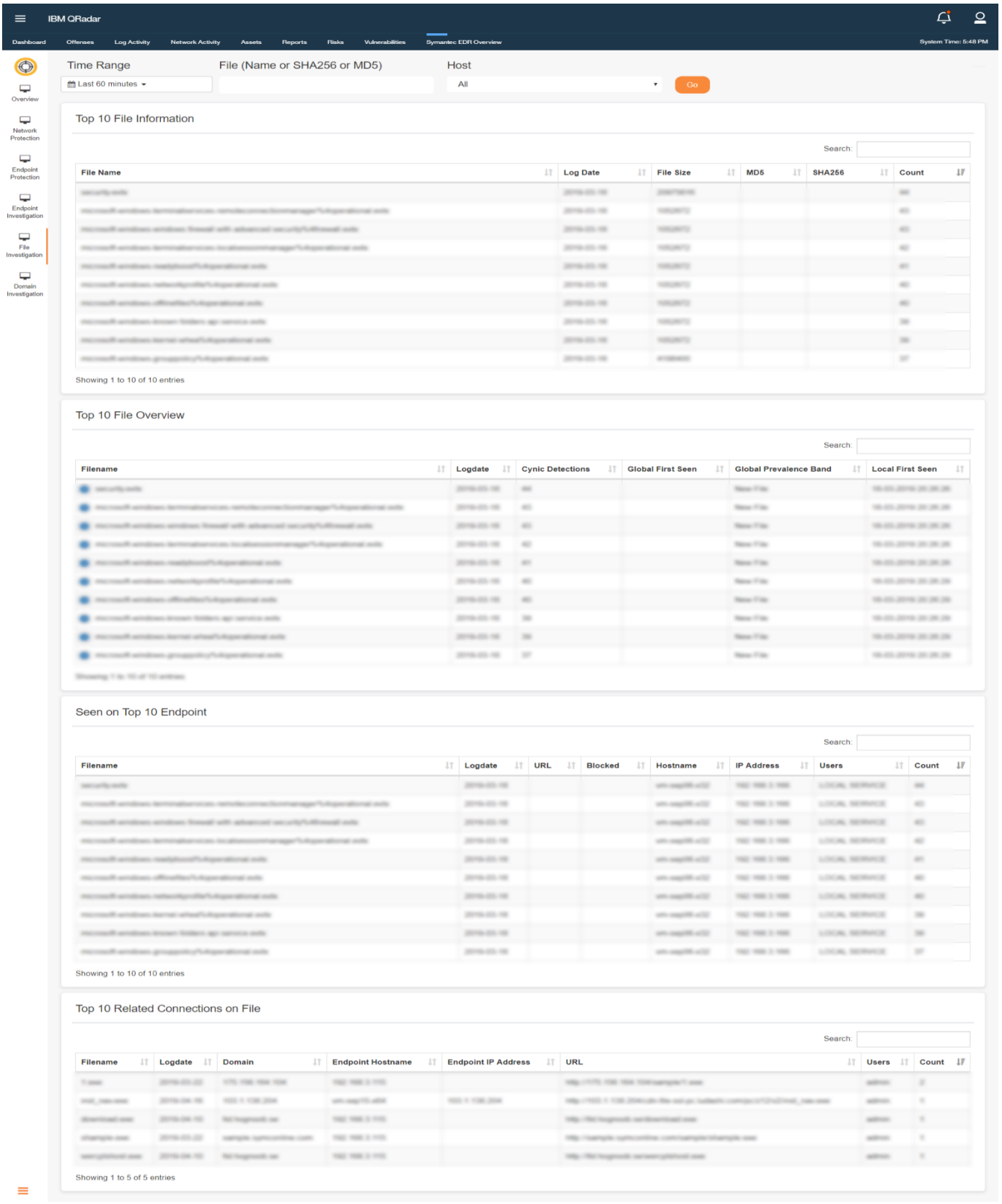


Figure 5: File Investigation

Domain Investigation Dashboard

This dashboard is built for user to investigate a particular domain. User can type in the domain he wants to investigate and filter the data.

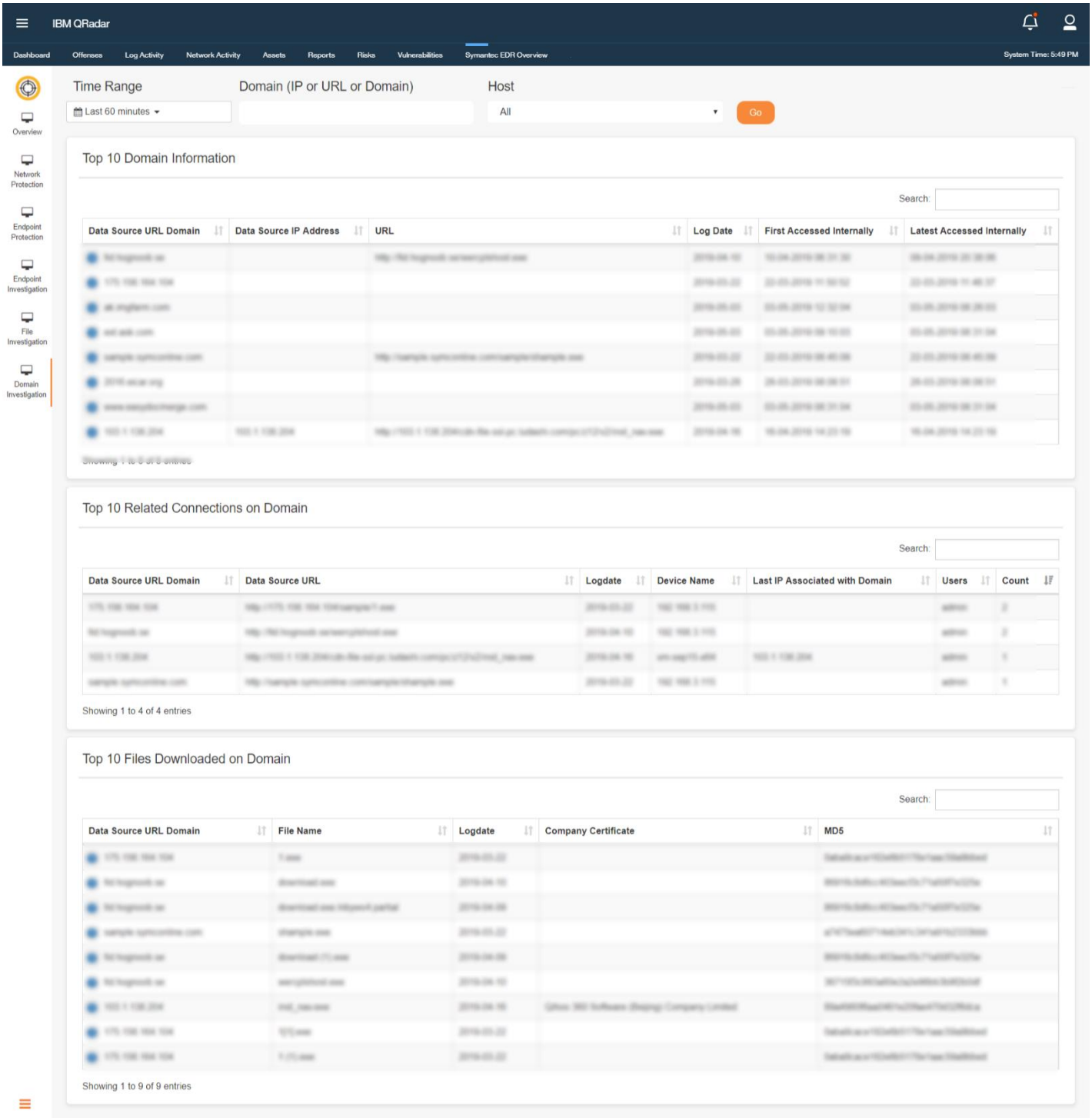


Figure 6: Domain Investigation

Actions

In the current environment, security analyst prefers the capability to perform monitoring and action from a single interface. This application allows the user to take following actions from QRadar events only: Note: This is allowed only from Log Activity Tab.

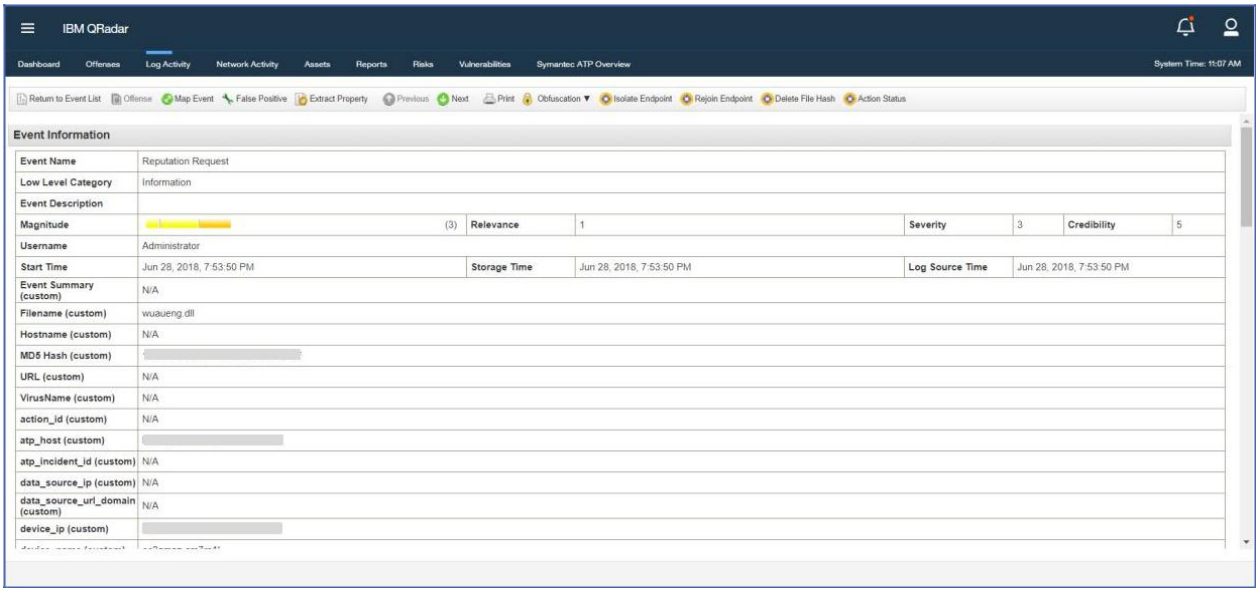


Figure 7: Take Action

- Isolate Endpoint: Quarantines the endpoint offline/off the network, while maintaining communication to the EDR appliance for additional instructions or actions.
- Rejoin Endpoint: Brings the endpoint back online, allows you to rejoin the network
- Delete File Hash: Remediates by removing the file off the endpoint, as well as reversing any actions the file has taken on the endpoint
- Action Status: This action allows security analyst in keeping track of action taken on the EDR instance. It uses REST API to fetch the status of the last action taken on a particular event.

Chapter 3

Installation

This chapter includes the following topics:

Installation

Pre-Requisites

Symantec EDR App for QRadar v1.3.0 version supports EDR product version 2.0, 3.0 and 4.0.
User requires QRadar version 7.3.1 or above

Upgrading the App from previous Installation

Before upgrading to Symantec EDR App for QRadar v1.3.0 from v1.0.0 or v1.1.0 please delete the custom property named “Domain” by performing the following steps:

1. Navigate to Custom Event Properties via Admin panel
2. In the search box enter keyword “Domain”
3. Select the custom property named “Domain”, verify that the associated log source is Symantec ATP, and click on the delete button

Deleting “Domain” custom property

Installing App for the First Time

The application installation requires access to QRadar console machine via a web interface. The web interface can be accessed via https://QRadarconsoleIP/. The installation process is as follows:

a. Login to QRadar console
b. Go to Admin -> Extension Management

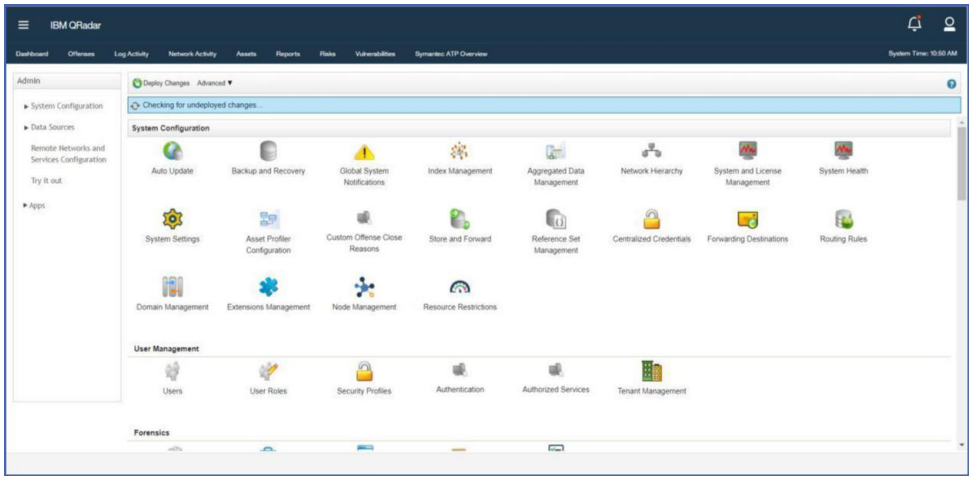


Figure 8: Extension Management

c. Choose the downloaded zip file by clicking on browse.
d. The QRadar will prompt list of changes being made by the app. Click on install button. After the Application is installed it will show all the components as shown below.

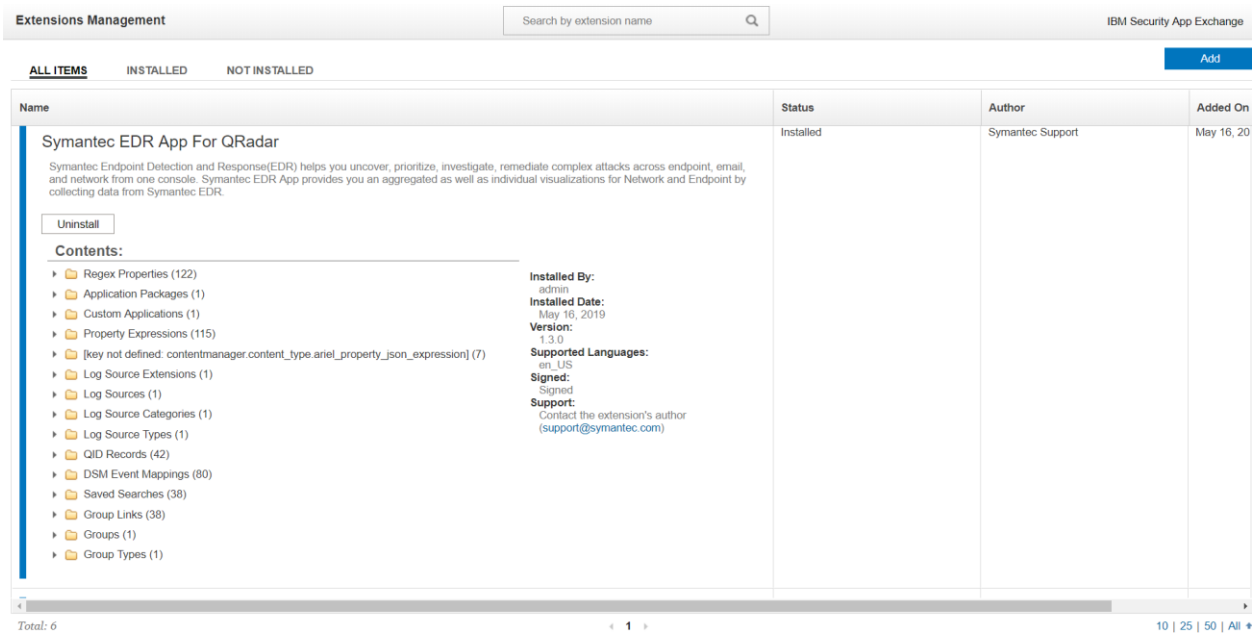


Figure 9: App Extensions

Configuration

The visualization dashboards will be available after application installation. In order for QRadar to start receiving data from Symantec EDR data collection must be enabled. To enable data collection, perform the following steps:

a. Login to QRadar console.
b. Go to Admin -> Plugins -> Symantec EDR

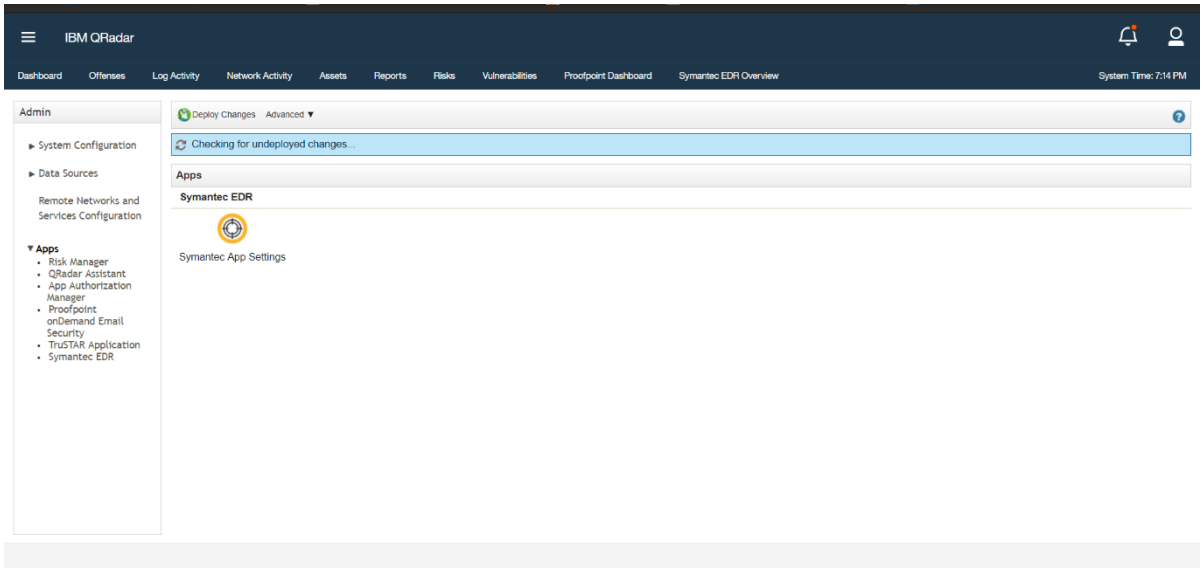


Figure 10: App Configuration Page

c. Click on “New” to setup a new Symantec EDR Server. And then enter following details:
   i: EDR Server URL for example : https://<<Your Server Host or IP/
   ii. Password: It must be in client_id:client_secret format, which is generated using Symantec EDR Server.

Note: To generate OAuth Credentials for Symantec EDR Please following this URL:
https://help.symantec.com/cs/symantecedr_4.1/EDR/v118551314_v130949130/Generating-an-OAuth-client?locale=EN_US

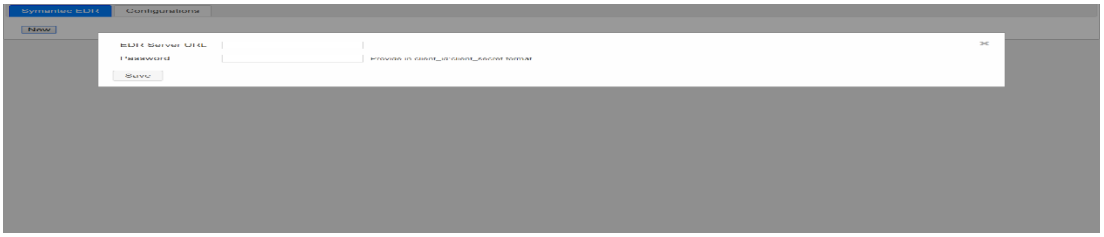


Figure 11: EDR Configurations

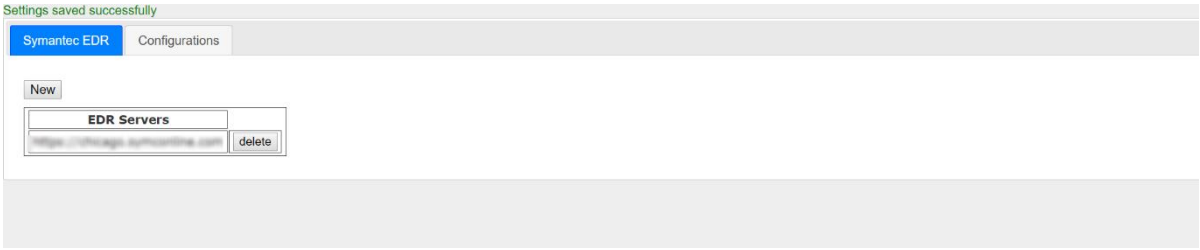


Figure 12: EDR Instance Details

d. Go to Admin Panel -> Authorized Services
e. Create a new Authorization token and click on the checkbox No Expiry

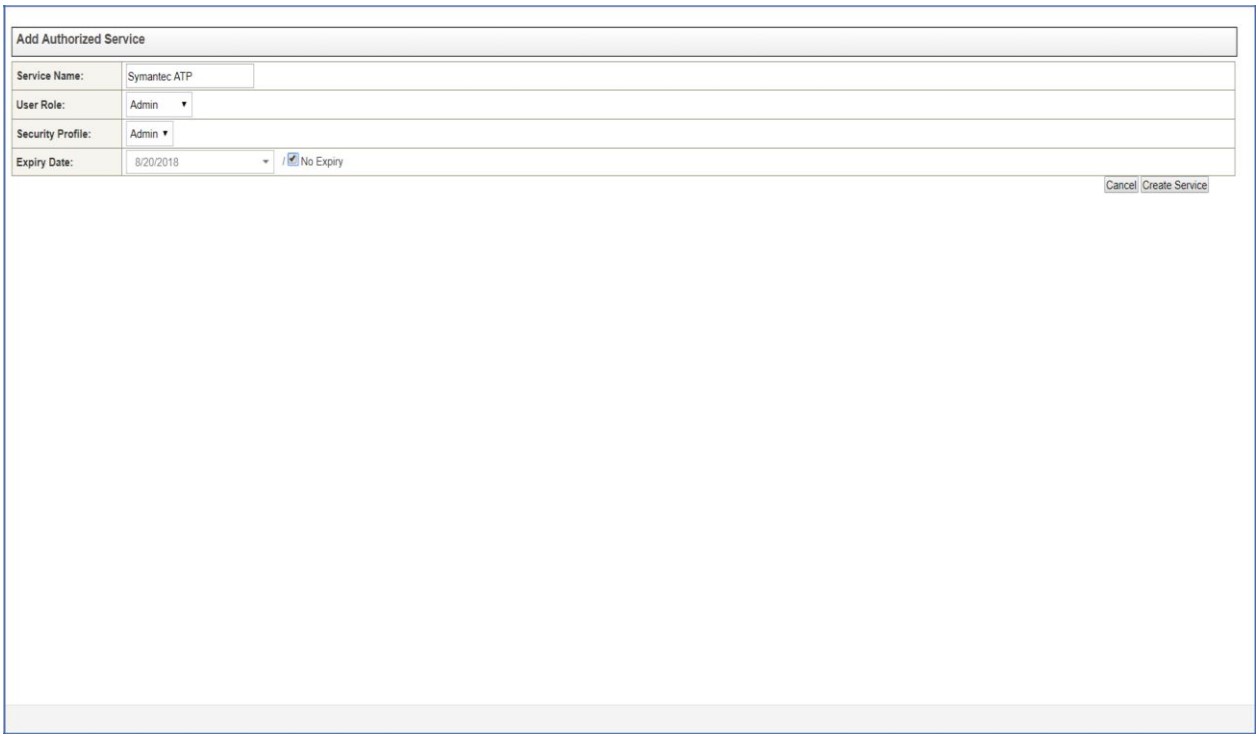


Figure 13: Authorization Token

f. Now click on Deploy changes
g. Go to configuration tab and enable the data collection as required.
h. Enter Authorization token that is used for fetching data via REST API.
i. The user is recommended to keep the start time as “now” else there will be discrepancy in the dashboards and user may have to wait for some time until dashboards get populated fully
j. The user is recommended to keep the start time as “now” else there will be discrepancy in the dashboards and user may have to wait for some time until dashboards get populated fully
k. It is recommended that "Start Time" should not be older than last 3 months for data collection in the Configuration

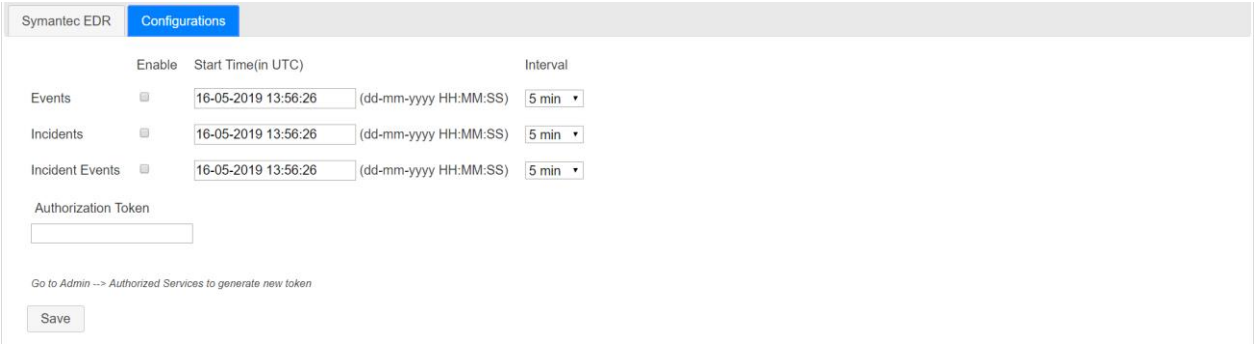


Figure 14: Data Collection Configuration

User Roles / Capabilities

The QRadar supports ACL configurations for restricting access different actions/dashboards. This app adds new capability called Symantec EDR, which controls access to different Symantec EDR actions. For accessing Symantec EDR actions, the user should be assigned a role that has this capability. By default, admin users have access to all the capabilities. To configure Role in QRadar, use following steps.

1. Login to QRadar console, go to Admin User Roles.

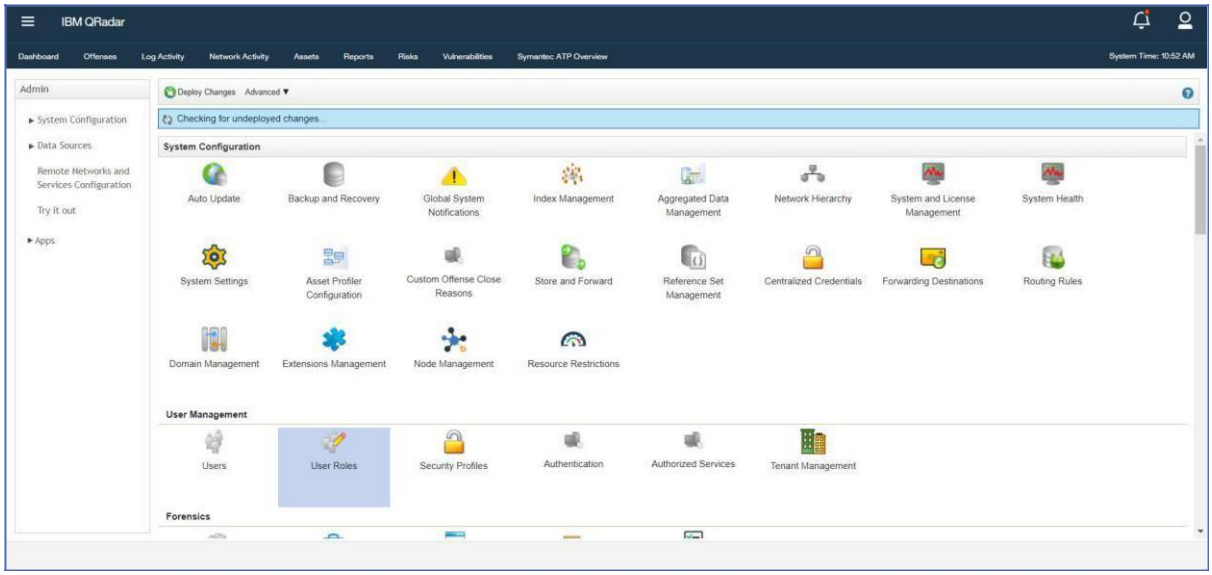


Figure 15: User Role

2. Click on New button.
3. Enter the name of the role. Assign required capabilities as shown in the screenshot. Assign these roles to Users who should be able to perform different Symantec EDR actions.

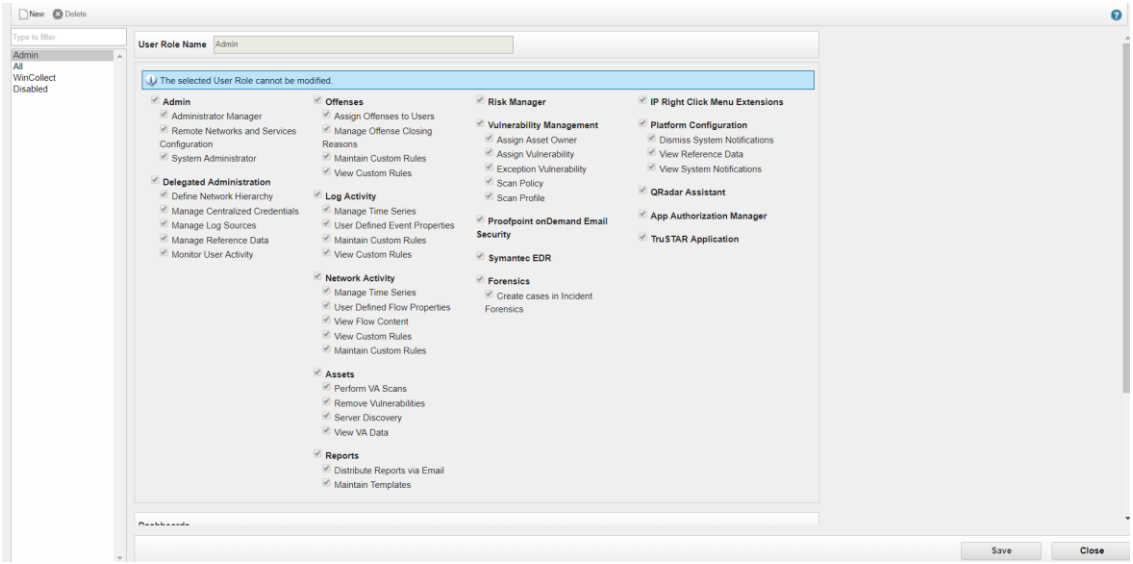


Figure 16: Assign App Permissions

Uninstalling the Application

To uninstall the application, the user needs to perform following steps.

1. Go to Admin Page
2. Open Extension Management
3. Select Symantec EDR application
4. Click on Uninstall

QRadar Cloud Support

Symantec EDR QRadar v1.3.0 supports all its functionalities on QRadar cloud

Chapter 4

Troubleshooting

This chapter includes the following topics:

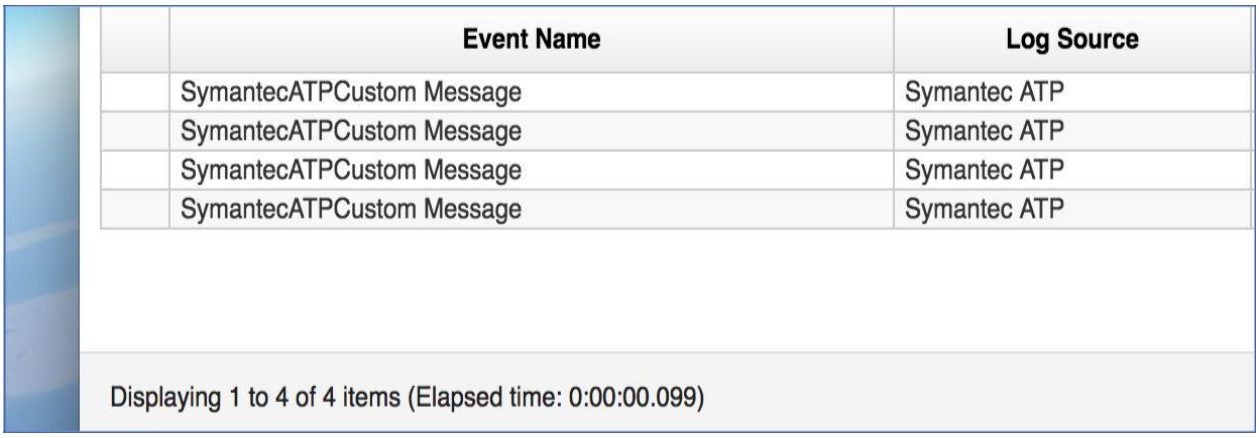
Troubleshooting

This section describes the common issues that might happen during the deployment or the running of the app and the steps to resolve the issues.

Case #1 – Symantec EDR events are shown up as SymantecATPCustom events

Problem: Symantec EDR events will show up as **SymantecATPCustom** rather than getting identified as the right QRadar category. This will be seen in “Log Activity” TAB in QRadar when user might be searching for event pertaining to Symantec ATP log source.

Below is a screenshot how it will look



	Event Name	Log Source
	SymantecATPCustom Message	Symantec ATP
	SymantecATPCustom Message	Symantec ATP
	SymantecATPCustom Message	Symantec ATP
	SymantecATPCustom Message	Symantec ATP

Displaying 1 to 4 of 4 items (Elapsed time: 0:00:00.099)

Figure 17: CustomMessage Issue

Troubleshooting Steps: This issue is caused when the payload size is more than 4096 bytes which leads to breaking of the event payload. 4096 is default size configured in QRadar platform. Following steps need to be followed to resolve this issue

1. Navigate to System settings by going to the admin panel.
2. Select advanced settings.
3. There is an option of **Max TCP Syslog Payload Length**.
4. Increase the value of this field according to need
5. Click on Deploy changes
6. Click on Restart Event Collection Services to set the changes into effect.

Below is a screenshot for quick reference:

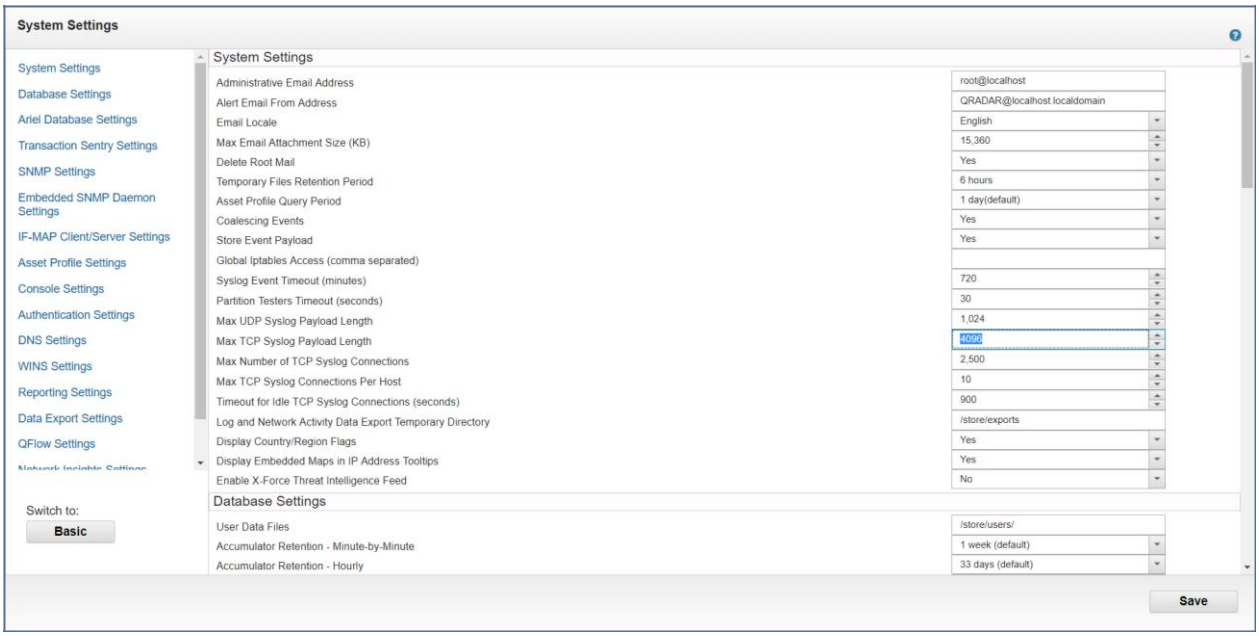


Figure 18: Max TCP Syslog Payload Length

Case #2 – Symantec EDR App configuration fails with various error messages

Problem: New configuration of EDR fails with error message “Fail: API server is already configured”. Below is a screenshot for quick reference.

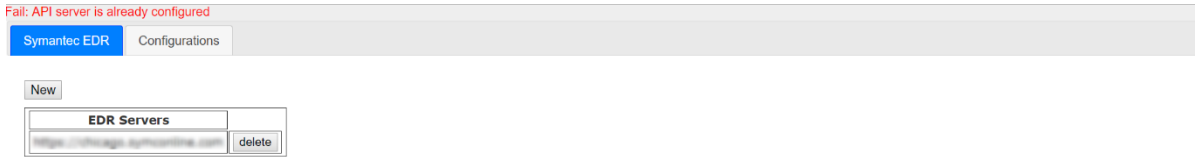


Figure 19: Duplicate credentials error

Troubleshooting Steps: User might have entered URL which is already configured. User is recommended to enter new credentials which is not already provided

Problem: New configuration of EDR fails with error message “Failed due to connection timeout”. Below is a screenshot for quick reference

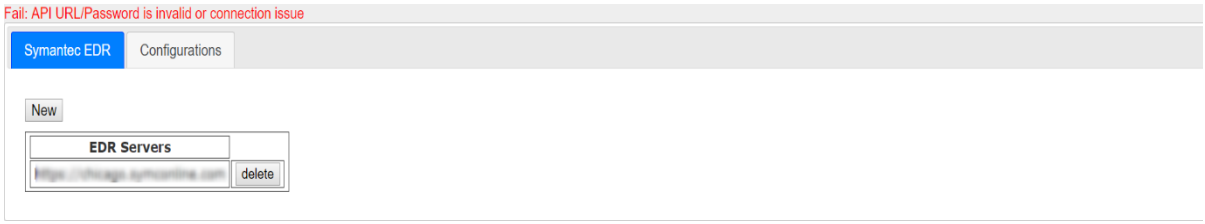


Figure 20: Connection Timeout

Troubleshooting Steps: This happens when there is connection issue while connecting to EDR instance. User is recommended to check the connectivity or firewall rules on the QRadar machine.

Problem: New configuration of EDR fails with error message “Fail: API password is invalid”. Below is a screenshot for quick reference

Troubleshooting Steps: This happens when user has entered wrong credentials so authentication failed while saving the configuration. User is recommended to check the credentials and try again

Case #3 – Symantec EDR events are coming as unknown

Problem: Events are seen as “unknown” in log activity screen.

Troubleshooting Steps: It is possible that EDR is sending events which are not mapped in DSM. Please execute following steps

1. Go to Log Activity.
2. Add Filter Log Source [Indexed] Equals to Symantec ATP
3. Select Last 7 Days in Views filter.
4. If any events come as unknown,
    a. Right click on that particular event.
    b. View in DSM editor.
    c. Check the value of Event ID and Event Category under Log activity Preview
5. Reach out to Symantec customer support to have this new event IDs added to DSM

Case #4 – Symantec EDR data is not getting collected

Problem: This could happen for many reason.

Troubleshooting Steps: Please follow below steps:

1. Click on System and License Management in Admin Panel
2. Select the host on which Symantec EDR App is installed
3. Click on Actions in top panel and select the option Collect Log Files
4. A pop-up named Log File Collection will open
5. Click on Advance Options
6. Select the checkbox to Include Debug Logs, Application Extension Logs , Setup Logs (Current Version)
7. Click on Collect Log Files Button after selecting 2 days as data input.
8. Click on "Click here to download the log files"
9. This will download all the log files in a single zip on your local machine
10. Create support case with Symantec and attach this log file

Case #5 – Symantec EDR UI related issues

Problem: Any dashboard panel, configuration pages, charts shows errors or unintended behavior.

Troubleshooting Steps:

1. Clear the browser cache and reload the webpage
2. Try reducing the time range of the filter and retry. It has been seen that QRadar queries expire if too much data is being matched in the query.

Case #6 – Re installation of the app

Problem: The application is exhibiting aberrant behavior and user wishes to perform clean installation again.

Troubleshooting Steps: To perform a reinstallation of the app please perform the following steps:

1. Remove all custom properties and saved searches associated with the log source Symantec ATP
2. Delete the log source named Symantec ATP by navigating to Log Sources via Admin panel
3. Uninstall the app
4. Refresh the page and check the Dashboard tab of Symantec EDR Overview is not seen after uninstallation
5. Now install the app from Extension Management

Case #7 – All other issues which are not part of the document

Problem: If the problem is not listed in the document, please follow below steps.

Troubleshooting Steps: Please follow below steps:

1. Click on System and License Management in Admin Panel
2. Select the host on which Symantec EDR App is installed
3. Click on Actions in top panel and select the option Collect Log Files
4. A pop-up named Log File Collection will open
5. Click on Advance Options
6. Select the checkbox to Include Debug Logs, Application Extension Logs , Setup Logs (Current Version)
7. Click on Collect Log Files Button after selecting 2 days as data input.
8. Click on "Click here to download files"
9. This will download all the log files in a single zip on your local machine
10. Create support case with Symantec and attach this log file