Symantec EDR App for QRadar

App Architecture and Installation Guide

v.1.5.0

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, remediate complex attacks across endpoints, email, and your network, all from one console.

The *Symantec EDR App for QRadar* collects data from EDR to generate user-aggregated and individual visualizations for networks and endpoints. The app functionality is divided into three parts:

Data Collection	REST API calls are made to Symantec EDR server to retrieve data.
Parsing	Symantec EDR device support module (DSM) is used to parse data and correctly categorize it to the appropriate event name and event category. Symantec-specific parameters are extracted using custom properties.
Presentation	Dashboards - To visualize Symantec EDR data. Action- To perform custom EDR actions based on the received events.

Chapter 2

Data collection

This chapter includes the following topics:

Data collection

REST API calls are used to retrieve data from the EDR server. Using Python scripts, the application makes REST calls to the following APIs:

- /events
- /incidents
- /incidentevents
- /auditevents

The scripts are run on a user-defined schedule. By default, all the scripts are in disabled mode. The application supports data retrieval from multiple servers. The app configuration is managed on the setup page.

Note: Audit Events can be collected only if Symantec EDR user with Admin privileges is configured

Chapter 3

Parsing

This chapter includes the following topics:

Parsing

QRadar parses the received data using the suitable log source. The log source is made up of two components:

- Protocol- The protocol defines how data is moved into QRadar.
- DSM- The device support module defines how data is parsed. Log Source Extension and Custom Event Properties can be attached to a Log Source to extend its capability.

EDR DSM

The Symantec Endpoint Detection and Response (EDR) device support module (DSM) is used to assign event names and event categories to EDR events. The event name and event categories are identified with *QRadar Identifiers* (QIDS). EDR events to QID mapping lists the EDR events to QID mappings.

Note: Events with an event ID that differs from those in the table show “Unknown” for the event name and the event category.

Table 4-1 EDR events to QID mapping

Event ID	Category	QID Name	High-level Category	Low-level Category
1000	Symantec Events	Database error	Audit	General Audit Event
1000	Symantec Incident Events	Database error	Audit	General Audit Event
4096	Symantec Events	Reputation Request	System	Information
4096	Symantec Incident Events	Reputation Request	System	Information
4098	Symantec Events	Intrusion Prevention	System	Information
4098	Symantec Incident Events	Intrusion Prevention	System	Information
4099	Symantec Events	Suspicious File	Suspicious Activity	Suspicious Activity
4099	Symantec Incident Events	Suspicious File	Suspicious Activity	Suspicious Activity
4100	Symantec Events	SONAR	System	Information
4100	Symantec Incident Events	SONAR	System	Information
4110	Symantec Events	Network IOC Event	Suspicious Activity	Suspicious Activity
4110	Symantec Incident Events	Network IOC Event	Suspicious Activity	Suspicious Activity
4112	Symantec Events	Blacklist (IP/URL/ domain)	Risk	Loss of Confidentiality
4112	Symantec Incident Events	Blacklist (IP/URL/ domain)	Risk	Loss of Confidentiality
4113	Symantec Events	Vantage	Exploit	Web Exploit
4113	Symantec Incident Events	Vantage	Exploit	Web Exploit
4117	Symantec Events	Cynic	System	Information
4117	Symantec Incident Events	Cynic	System	Information
4118	Symantec Events	Blacklist File	Risk	Loss of Confidentiality
4118	Symantec Incident Events	Blacklist File	Risk	Loss of Confidentiality
4123	Symantec Events	Endpoint File Detection	Exploit	Misc Exploit
4123	Symantec Incident Events	Endpoint File Detection	Exploit	Misc Exploit

4353	Symantec Events	Antivirus(Network Detection)	Malware	Virus Detected
4353	Symantec Incident Events	Antivirus(Network Detection)	Malware	Virus Detected
8000	Symantec Events	Session	Suspicious Activity	User Activity
8000	Symantec Incident Events	Session	Suspicious Activity	User Activity
8001	Symantec Events	Process	Audit	General Audit Event
8001	Symantec Incident Events	Process	Audit	General Audit Event
8004	Symantec Events	Folder	Audit	General Audit Event
8004	Symantec Incident Events	Folder	Audit	General Audit Event
8005	Symantec Events	Registry Key	System	Successful Registry Modification
8005	Symantec Incident Events	Registry Key	System	Successful Registry Modification
8006	Symantec Events	Registry Value	System	Successful Registry Modification
8006	Symantec Incident Events	Registry Value	System	Successful Registry Modification
8080	Symantec Events	Session Query Result	Audit	General Audit Event
8080	Symantec Incident Events	Session Query Result	Audit	General Audit Event
8081	Symantec Events	Process Query Result	Audit	General Audit Event
8081	Symantec Incident Events	Process Query Result	Audit	General Audit Event
8082	Symantec Events	Module Query Result	Audit	General Audit Event
8082	Symantec Incident Events	Module Query Result	Audit	General Audit Event
8085	Symantec Events	Registry Key Query Result	Audit	General Audit Event
8085	Symantec Incident Events	Registry Key Query Result	Audit	General Audit Event
8086	Symantec Events	Registry Value Query Result	Audit	General Audit Event

8086	Symantec Incident Events	Registry Value Query Result	Audit	General Audit Event
8089	Symantec Events	Kernel Object Query Result	Audit	General Audit Event
8089	Symantec Incident Events	Kernel Object Query Result	Audit	General Audit Event
8090	Symantec Events	Service Query Result	Audit	General Audit Event
8090	Symantec Incident Events	Service Query Result	Audit	General Audit Event
8099	Symantec Events	Query Command Errors	System	Error
8099	Symantec Incident Events	Query Command Errors	System	Error
8103	Symantec Events	File Remediation	Audit	General Audit Event
8103	Symantec Incident Events	File Remediation	Audit	General Audit Event
8119	Symantec Events	File Remediation Errors	System	Error
8119	Symantec Incident Events	File Remediation Errors	System	Error
Symantec Action	Symantec Action	Symantec Action	Audit	General Audit Event
Symantec Incidents	Symantec Incidents	Symantec Incidents	System	Notice
4102	Symantec Events	Antivirus (Endpoint Detection)	Malware	Virus Detected
4102	Symantec Incident Events	Antivirus (Endpoint Detection)	Malware	Virus Detected
4109	Symantec Events	File IOC Event	Suspicious Activity	Suspicious Activity
4109	Symantec Incident Events	File IOC Event	Suspicious Activity	Suspicious Activity
4115	Symantec Events	Insight	Suspicious Activity	Information Leak
4115	Symantec Incident Events	Insight	Suspicious Activity	Information Leak
4116	Symantec Events	Mobile Insight	Suspicious Activity	Information Leak
4116	Symantec Incident Events	Mobile Insight	Suspicious Activity	Information Leak

4124	Symantec Events	Endpoint (IP/URL/Domain) Detection	Exploit	Misc Exploit
4124	Symantec Incident Events	Endpoint (IP/URL/Domain) Detection	Exploit	Misc Exploit
4125	Symantec Events	Email	Exploit	Mail Exploit
4125	Symantec Incident Events	Email	Exploit	Mail Exploit
8002	Symantec Events	Module	Audit	General Audit Event
8002	Symantec Incident Events	Module	Audit	General Audit Event
8003	Symantec Events	File	Audit	General Audit Event
8003	Symantec Incident Events	File	Audit	General Audit Event
8007	Symantec Events	Network	Access	Misc Network Communication Event
8007	Symantec Incident Events	Network	Access	Misc Network Communication Event
8009	Symantec Events	Named object	System	Information
8009	Symantec Incident Events	Named object	System	Information
8083	Symantec Events	File Query Result	Audit	General Audit Event
8083	Symantec Incident Events	File Query Result	Audit	General Audit Event
8084	Symantec Events	Directory Query Result	Audit	General Audit Event
8084	Symantec Incident Events	Directory Query Result	Audit	General Audit Event
20	Symantec Audit Event	Session Audit Event	Audit	General Audit Event
21	Symantec Audit Event	Entity Audit Event	Audit	General Audit Event

Network and endpoint event type IDs

The Network and Endpoint Protection dashboard panels display events with the following event type IDs:

Network	4096,4098,4099,4109,4100,4102,4111,4119,4120,4121,4122,4123,4124

Endpoint	4110,4112,4113,4115,4116,4117,4118,4126,4353

Overview dashboard panels pull events from all event IDs.

See the topic, *Event Summary Type IDs* in the *Symantec Endpoint Detection and Response (EDR) Security Operations Guide* for descriptions of the event type IDs.

Custom property extraction

A custom regular expression is used to extract various EDR properties. QRadar associates the custom property extraction to an event name or an event category. This association ensures that a field is extracted only for the matching event name. Property extraction associations lists the extracted properties, the expression that's used for the extraction, and the associated event names.

Table 4-2 Property extraction associations

Property Name	Regular Expression	Event Name
Application Category	"categories":\s*\[(.*?)\]	N/A
Application name	/“app_name”	N/A
Date_Time	/"time"	N/A
Email Subject	/"EmailSubject"	Email
Event Summary	/"summary"	N/A
File Hash	"filehash":\s*(\[[\"\w,\"]+\])	N/A
Filename	"name": "([\S\s]+?)"	N/A
Hostname	/"host_name"	N/A
MD5 Hash	"md5": "(\w*)"	N/A
Message	/"message"	N/A
MessageID	/”MessageId”	Email
URL	/"data_source_url"	N/A
VirusName	"virus_name":\s*\"(.*)\"	N/A
action_id	/"action_id"	N/A
actual_action	/"actual_action"	Endpoint File Detection
actual_action_idx	/"actual_action_idx"	Endpoint File Detection
agent_version	/"agent_version"	Endpoint File Detection
EDR_host	EDR_host=([\s\S]+?),	N/A
EDR_incident_id	//"EDR_incident_id"	N/A
av_date_detected	/"av"/"date_detected"	Antivirus (Endpoint Detection)
av_date_quarantined	/"av"/"date_quarantined"	Antivirus (Endpoint Detection)

av_threat_categories	/"av"/"threat_categories"	Antivirus (Endpoint Detection)
bash_recommended_action	/"bash"/"recommended_action"	SONAR
bash_signature_version	/"bash"/"signature_version"	SONAR
bash_virus_id	/"bash"/"virus_id"	SONAR
count	/"count"	N/A
cynic_targeted_data	/"cynic"/"targeted_data"/"is_targeted"	Cynic
cynic_task_id	/"cynic"/"cynic_task_id"	Cynic
cynic_verdict	/"cynic"/"verdict"	Cynic
cynic_verdict_type	/"cynic"/"verdict_type"	Cynic
data_direction	/"data_direction"	N/A
data_source_ip	/"data_source_ip"	N/A
data_source_url_domain	/"data_source_url_domain"	N/A
deviceUid	"deviceUid":\s*(\[[\"A-Za-z0-9-,\"]+\])	N/A
device_end_time	/"device_end_time"	N/A
device_ip	/"device_ip"	N/A
device_name	/"device_name"	N/A
device_os_name	/"device_os_name"	N/A
device_os_ver	/"device_os_ver"	N/A
device_time	/"device_time"	N/A
device_type	/"device_type"	N/A
device_uid	/"device_uid"	N/A
direction	/"direction"	Email
emailaction	/"EmailAction"	Email
emailreceiveddate	/"EmailReceivedDate"	Email
event_count	/"event_count"	N/A
event_desc	/"event_desc"	N/A
event_id	/"event_id"	Endpoint (IP/URL/Domain) Detection
external_ip	/"external_ip"	N/A
external_port	/"external_port"	N/A
file_accessed	"accessed": "([\S\s]+?)"	N/A
file_age	"file_age": "([\S\s]+?)"	N/A
file_attributes	"attributes": "([\S\s]+?)"	N/A
file_company_name	"company_name": "([\S\s]+?)"	N/A
file_created	"created": "([\S\s]+?)"	N/A

file_desc	"desc": "([\S\s]+?)"	N/A
file_folder	"folder": "([\S\s]+?)"	N/A
file_mime_type	"mime_type": "([\S\s]+?)"	N/A
file_modified	"modified": "([\S\s]+?)"	N/A
file_prevalence_band	"prevalence_band": "([\S\s]+?)"	N/A
file_reputation_band	"reputation_band": "([\S\s]+?)"	N/A
file_sha2	"sha2": "([\S\s]+?)"	N/A
file_sig_com_name	"signature_company_name": "([\S\s]+?)"	N/A
file_sig_serial_num	"signature_serial_name": "([\S\s]+?)"	N/A
file_signature_issuer	"signature_issuer": "([\S\s]+?)"	N/A
file_size	"size": "([\S\s]+?)"	N/A
file_targeted_attack	"targeted_attack": "([\S\s]+?)"	N/A
file_threat_name	/"file"/"threat_name"	N/A
file_version	"version": "([\S\s]+?)"	N/A
first_event_seen	/"first_event_seen"	Symantec Incidents
incident rela	/"incident"	N/A
infected	/"infected"	Intrusion Prevention
internal_hostname	/"internal_hostname"	N/A
internal_ip	/"internal_ip"	N/A
internal_port	/"internal_port"	N/A
intrusion_attacker_local_remote	/"Intrusion"/"attacker_local_remote"	Intrusion Prevention
intrusion_date_detected	/"Intrusion"/"date_detected"	Intrusion Prevention
intrusion_detail_id	/"Intrusion"/"detail_id"	Intrusion Prevention
intrusion_protocol_id	/"Intrusion"/"protocol_id"	Intrusion Prevention
intrusion_signature_properties	/"Intrusion"/"signatures_properties"	Intrusion Prevention
intrusion_url	/"intrusion_url"	Endpoint (IP/URL/Domain) Detection
last_event_seen	/"last_event_seen"	N/A
local_host_mac	/"local_host_mac"	N/A
log_name	/"log_name"	N/A
log_time	/"log_time"	N/A
manual_submit	/"manual_submit"	Cynic
network_scanner_type	/"network_scanner_type"	N/A
no_of_viruses	/"no_of_virus"	Endpoint File Detection
origmessageheaderid	/"OrigMessageHeaderId"	Email

parent_file_sha2	/"parent_file_sha2"	Reputation Request
priority_level	/"priority_level"	Symantec Incidents
reason	/"reason"	N/A
recommended_action	/"recommended_action"	Symantec Incidents
recv_delivered	/"receivers"/"delivered"	Email
recv_email_address	/"receivers"/"EmailAddress"	Email
recv_internal	/"receivers"/"internal"	Email
releasedfromquarantine	/"receivers"/"ReleasedFromQuarantine"	Email
remote_host_mac	/"remote_host_mac"	Endpoint (IP/URL/Domain) Detection
scan_signatures_version	/"Scan"/"signatures_version"	N/A
scanner_name	/"scanner_name"	N/A
scanners	"scanners":\s*(\[[\"\w,\"]+\])	N/A
sender_email_address	/"sender"/"EmailAddress"	Email
sender_internal	/"sender"/"internal"	Email
sender_ip	/"sender"/"SenderIP"	Email
sep_installed	/"sep_installed"	N/A
severity	/"severity"	Endpoint (IP/URL/Domain) Detection
severity_id	/"severity_id"	N/A
signature_id	/"signature_id"	N/A
signature_name	/"signature_name"	N/A
source	/"source"	N/A
source_url_referer	/"data_source_url_referer"	N/A
state	/"state"	N/A
threat_category_id	/"threat"/"category_id"	Antivirus (Endpoint Detection)
threat_id	/"threat"/"id"	N/A
threat_name	/"threat"/"name"	vlan_id
threat_risk	/"threat"/"risk"	Antivirus(Network Detection)
type_id	/"type_id"	N/A
updated	/"updated"	N/A
user_uid	/"user_uid"	N/A
uuid	/"uuid"	N/A
virus_def	/"virus_def"	Endpoint File Detection
vlan_id	/"vlan_id"	N/A

The following table lists the properties that are extracted for the dashboards, and their associated queries.

Table 4-3 Queries for dashboards

Dashboard Name	Panel Name	Query
Domain Investigation	Top 10 Domain Information	SELECT LONG(UNIQUECOUNT("uuid")) AS 'COUNT' , DATEFORMAT("log_time",'yyyy-MM-dd') AS LOGDATE, "data_source_ip" as 'Device IP', "URL" as 'URL',"data_source_url_domain" as 'Domain', FIRST(DATEFORMAT("log_time", 'dd-MM-yyyy HH:mm:ss')) as 'FirstAccessInternally', LAST(DATEFORMAT("log_time", 'dd-MM-yyyy HH:mm:ss')) as 'LatestAccessInternally' FROM events WHERE LOGSOURCENAME(logsourceid) = 'Symantec ATP' AND "data_source_url_domain" IS NOT NULL GROUP BY Domain ORDER BY "COUNT" DESC LIMIT 10 Last 60 minutes
	Top 10 Related Connections on Domain	SELECT LONG(UNIQUECOUNT("uuid")) AS 'COUNT' , DATEFORMAT("log_time",'yyyy-MM-dd') AS 'LOGDATE', "URL" as 'DataSourceURL', "data_source_url_domain" as 'Domain', "data_source_ip" as 'LastIPAssociatedwithDomain', "Username" as 'Users', "device_name" as 'Devices' FROM events WHERE URL IS NOT NULL AND "data_source_url_domain" IS NOT NULL AND LOGSOURCENAME(logsourceid) = 'Symantec ATP' GROUP BY Domain ,"device_name" ORDER BY "COUNT" DESC LIMIT 10 Last 60 minutes
	Top 10 Files Downloaded on Domain	SELECT LONG(UNIQUECOUNT("uuid")) AS 'COUNT' , DATEFORMAT("log_time",'yyyy-MM-dd') AS LOGDATE, "Filename" as 'FileName', "data_source_url_domain" as 'Domain',"file_sig_com_name" as 'CompanyCertificate', "file_sha2" as 'SHA256', "MD5 Hash" as 'MD5', "URL" as 'URL', "Username" as 'Users' FROM events WHERE Filename IS NOT NULL AND "data_source_url_domain" IS NOT NULL AND LOGSOURCENAME(logsourceid) = 'Symantec ATP' GROUP BY "Filename", Domain ORDER BY "COUNT" DESC LIMIT 10 Last 60 minutes
Endpoint Investigation	Top 10 Endpoint Information	select LONG(UNIQUECOUNT("uuid")) AS 'TOTAL',"device_ip" as 'Device IP',"device_name" as 'device_name',"local_host_mac" as 'MAC Address',if LAST("sep_installed") is null then '' else "sep_installed" as 'SEP Installed', if LAST("infected") is null then '' else infected as

		'Infected', LAST(DATEFORMAT(log_time, 'dd-MM-yyyy HH:mm:ss')) as 'Last Seen' from events where LOGSOURCENAME(logsourceid)='Symantec ATP' AND device_ip is not NULL AND type_id is not NULL group by "device_ip","device_name" order by TOTAL DESC LIMIT 10 Last 60 minutes
	Top 10 Related Files	select "Username" as 'Username',"file_sha2" as 'file_sha2',"MD5 Hash" as 'file_md5',"Filename" as 'Filename',"device_ip" as 'device_ip' , "device_name" as 'device_name', "actual_action" as 'actual_action', "threat_name" as 'threat_name', "VirusName" as 'virus_name', LONG(UNIQUECOUNT("uuid")) AS 'COUNT' from events where LOGSOURCENAME(logsourceid)='Symantec ATP' AND "device_ip" IS NOT NULL AND "Filename" is NOT NULL GROUP BY "device_ip","Filename","file_sha2" ORDER BY "COUNT" DESC LIMIT 10 Last 60 minutes
	Top 10 Related Connections	select "device_ip" as 'device_ip',"data_source_url_domain" as 'data_source_url_domain', "Username" as 'Username' , "device_name" as 'device_name', "URL" as 'URL' , LONG(UNIQUECOUNT("uuid")) AS 'COUNT' from events where LOGSOURCENAME(logsourceid)='Symantec ATP' AND "device_ip" is NOT NULL AND "URL" is NOT NULL AND "type_id" != 4096 GROUP BY "device_ip" ORDER BY "COUNT" DESC LIMIT 10 Last 60 minutes
	Top 10 Related Threats	select LONG(UNIQUECOUNT("Filename")) AS 'File_Count', LONG(UNIQUECOUNT("uuid")) AS 'COUNT', "Username" as 'Username' , "threat_name" as 'threat_name', "device_ip" as 'device_ip' , "device_name" as 'device_name' from events where LOGSOURCENAME(logsourceid)='Symantec ATP' AND "device_ip" is NOT NULL AND "threat_name" is not NULL group by "device_ip" ORDER BY "COUNT" DESC LIMIT 10 Last 60 minutes
Endpoint Protection	IPS (Vantage)	select UNIQUECOUNT("device_ip") as 'COUNT' from events where LOGSOURCENAME(logsourceid)='Symantec ATP' AND "device_ip" is NOT NULL AND "type_id" in (4124,4098) Last 60 minutes
	File Reputation (Insight)	select UNIQUECOUNT("file_sha2") as 'COUNT' from events where LOGSOURCENAME(logsourceid)='Symantec ATP' AND "type_id" = 4123 AND "VirusName" MATCHES 'WS.Reputation.*' AND "file_sha2" is not NULL Last 60 minutes

	Suspicious Files	select UNIQUECOUNT("file_sha2") as 'COUNT' from events where LOGSOURCENAME(logsourceid)='Symantec ATP' AND "type_id" =4099 AND "file_sha2" is not NULL Last 60 minutes
	User At Risk	select UNIQUECOUNT("Username") as 'COUNT' from events where LOGSOURCENAME(logsourceid)='Symantec ATP' AND "type_id" in (4124,4123) AND "Username" is not NULL Last 60 minutes
	All Files Inspected	select UNIQUECOUNT("file_sha2") as 'COUNT' from events where LOGSOURCENAME(logsourceid)='Symantec ATP' AND "file_sha2" is not NULL AND "type_id" in (4096,4098,4099,4109,4100,4102,4111,4119,4120,4121,4122,4123,4124) Last 60 minutes
	AntiVirus Engine	select UNIQUECOUNT("file_sha2") as 'COUNT' from events where LOGSOURCENAME(logsourceid)='Symantec ATP' AND "type_id" in (4123,4102) AND "file_sha2" is not NULL Last 60 minutes
	Top 10 Local Hosts By Conviction	select LONG(COUNT("uuid")) AS 'COUNT' ,IF "device_name" == STR("device_ip") OR device_name ='N/A' THEN STR("device_ip") else CONCAT("device_name",CONCAT('(',CONCAT(STR("device_ip"),')'))) AS 'HostName' from events where LOGSOURCENAME(logsourceid)='Symantec EDR' AND "type_id" in (4123,4124) AND "device_ip" is NOT NULL AND devicetime BETWEEN <<start-time>> and <<end-time>> GROUP BY 'HostName' ORDER BY "COUNT" DESC LIMIT 10 START <<start-time>>
	Top 10 Remote Hosts By Conviction	select LONG(UNIQUECOUNT("uuid")) as 'COUNT', IF "data_source_url_domain" IS NOT NULL AND "data_source_url_domain" != '' THEN "data_source_url_domain" ELSE "data_source_ip" AS 'HostName' from events where LOGSOURCENAME(logsourceid)='Symantec ATP' AND "type_id" in (4124,4123) AND HostName is NOT NULL group by "HostName" ORDER BY "COUNT" DESC LIMIT 10 Last 60 minutes
	Top 10 Files Observed	select "Filename" as 'Filename', "file_sha2" as 'file_sha2', "MD5 Hash" as 'file_md5', "file_company_name" as 'file_company_name', LONG(UNIQUECOUNT("uuid")) as 'COUNT' from events where LOGSOURCENAME(logsourceid)='Symantec ATP' AND "type_id" =4096 AND "FileName" is

		NOT NULL group by "Filename" ORDER BY "COUNT" DESC LIMIT 10 Last 60 minutes
File Investigation	Top 10 File Information	SELECT LONG(UNIQUECOUNT("uuid")) AS 'COUNT', DATEFORMAT("log_time",'yyyy-MM-dd') AS LOGDATE, "data_source_ip" as 'Device IP' ,"Filename" as 'FileName', "file_size" as 'FileSize', "file_sha2" as 'SHA256', "MD5 Hash" as 'MD5' FROM events WHERE LOGSOURCENAME(logsourceid) = 'Symantec ATP' AND "Filename" IS NOT NULL GROUP BY FileName ORDER BY "COUNT" DESC LIMIT 10 Last 60 minutes
	Top 10 File Overview	SELECT LONG(UNIQUECOUNT("uuid")) AS 'COUNT', DATEFORMAT("log_time",'yyyy-MM-dd') AS LOGDATE, "Filename" as 'FileName', LONG(COUNT("uuid")) as "CynicDetections", CASE "file_reputation_band" WHEN 1 THEN 'Symantec-trusted' WHEN 2 THEN 'Good' WHEN 3 THEN 'Trending Good' WHEN 4 THEN 'Unproven' WHEN 5 THEN 'Poor' WHEN 6 THEN 'Untrusted' ELSE 'other' END as "ReputationBand", LAST(file_age) as "GlobalFirstSeen", CASE "file_prevalence_band" WHEN 1 THEN 'Fewer than 5 users' WHEN 2 THEN 'Fewer than 50 users' WHEN 3 THEN 'Fewer than 100 users' WHEN 4 THEN 'Hundreds of users' WHEN 5 THEN 'Thousands of users' WHEN 6 THEN 'Tens of thousands of users' WHEN 7 THEN 'Hundreds of thousands of users' WHEN 8 THEN 'Millions of users' ELSE 'New File' END as "GlobalPrevalenceBand", FIRST(DATEFORMAT(log_time, 'dd-MM-yyyy HH:mm:ss')) as "LocalFirstSeen", LONG(UNIQUECOUNT(device_ip)) as "LocalPrevalence", CASE file_targeted_attack WHEN 'true' THEN 'Yes' WHEN 'false' THEN 'No' ELSE '' END as "TargetedAttack" FROM events WHERE LOGSOURCENAME(logsourceid) = 'Symantec ATP' AND "Filename" IS NOT NULL GROUP BY Filename ORDER BY "COUNT" DESC LIMIT 10 Last 60 minutes
	Seen on Top 10 Endpoint	SELECT LONG(UNIQUECOUNT("uuid")) AS 'COUNT' , DATEFORMAT("log_time",'yyyy-MM-dd') AS LOGDATE, "Filename" as 'FileName',"device_ip" as 'IPAddress', "device_name" as 'HostName', "Username" as 'Users', "URL" as "URL", CASE "action_id" WHEN 0 THEN 'Yes' WHEN 1 THEN 'No' ELSE "action_id" END as "Blocked" FROM events WHERE LOGSOURCENAME(logsourceid) = 'Symantec ATP' AND "device_ip" IS NOT NULL AND "Filename" IS NOT NULL GROUP BY FileName, IPAddress ORDER BY "COUNT" DESC LIMIT 10 Last 60 minutes

	Top 10 Related Connections on File	SELECT LONG(UNIQUECOUNT("uuid")) AS 'COUNT' , DATEFORMAT("log_time",'yyyy-MM-dd') AS 'LOGDATE',"Filename" as 'FileName', "URL" as 'URL', "data_source_ip" as 'EndpointIPAddress' , device_name as 'EndpointHostName', "data_source_url_domain" as "Domain", "Username" as "Users" FROM events WHERE LOGSOURCENAME(logsourceid) = 'Symantec ATP' AND "URL" IS NOT NULL AND "Filename" IS NOT NULL GROUP BY URL, FileName ORDER BY "COUNT" DESC LIMIT 10 Last 60 minutes
Network Protection	Blacklist (File)	SELECT UNIQUECOUNT("file_sha2") AS 'COUNT' FROM events WHERE LOGSOURCENAME(logsourceid) = 'Symantec ATP' AND "file_sha2" is NOT NULL AND type_id = 4118 Last 60 minutes
	Blacklist (IP/URL/Domain)	SELECT UNIQUECOUNT("device_ip") AS 'COUNT' FROM events WHERE LOGSOURCENAME(logsourceid) = 'Symantec ATP' AND type_id = 4112 AND "device_ip" is not NULL Last 60 minutes
	IPS (Vantage)	SELECT UNIQUECOUNT("signature_id") AS 'COUNT' FROM events WHERE LOGSOURCENAME(logsourceid) = 'Symantec ATP' AND "signature_id" is NOT NULL AND type_id = 4113 Last 60 minutes
	File Reputation (Insight)	SELECT UNIQUECOUNT("file_sha2") AS 'COUNT' FROM events WHERE LOGSOURCENAME(logsourceid) = 'Symantec ATP' AND type_id = 4115 AND "file_sha2" IS NOT NULL Last 60 minutes
	File Reputation (Mobile Insight)	SELECT UNIQUECOUNT("file_sha2") AS 'COUNT' FROM events WHERE LOGSOURCENAME(logsourceid) = 'Symantec ATP' AND "file_sha2" is NOT NULL AND type_id = 4116 Last 60 minutes
	Sandboxing Convictions (Cynic)	SELECT UNIQUECOUNT("file_sha2") AS 'COUNT' FROM events WHERE LOGSOURCENAME(logsourceid) = 'Symantec ATP' AND "file_sha2" is NOT NULL AND type_id = 4117 Last 60 minutes
	AntiVirus Engine	SELECT UNIQUECOUNT("file_sha2") AS 'COUNT' FROM events WHERE LOGSOURCENAME(logsourceid) = 'Symantec ATP' AND "file_sha2" is NOT NULL AND type_id = 4353 Last 60 minutes
	Infected Systems	SELECT UNIQUECOUNT("signature_id") AS 'COUNT' FROM events WHERE LOGSOURCENAME(logsourceid) = 'Symantec

		ATP' AND type_id = 4113 AND "Signature" MATCHES 'System Infected:.*' AND "signature_id" IS NOT NULL Last 60 minutes
	TOP 10 Web Traffic	SELECT UNIQUECOUNT("uuid") AS 'TOTAL' , CASE "action_id" when 0 THEN 'Web Blocked Traffic' when 1 THEN 'Web Allowed Traffic' ELSE 'Web Unknown Traffic' END as 'ACTION' from events WHERE LOGSOURCENAME(logsourceid) = 'Symantec ATP' AND "type_id" in (4112,4113,4115,4116,4117,4118,4126,4353) GROUP BY "action_id" ORDER BY TOTAL DESC LIMIT 10 Last 60 minutes
	TOP 10 Event Contributors By Affected IP	SELECT UNIQUECOUNT("uuid") AS 'TOTAL', "device_ip" AS 'DEVICE_IP' from events WHERE LOGSOURCENAME(logsourceid) = 'Symantec ATP' AND "type_id" in (4112,4113,4115,4116,4117,4118,4126,4353) AND "device_ip" is NOT NULL GROUP BY device_ip ORDER BY TOTAL DESC LIMIT 10 Last 60 minutes
Overview	Suspicious Files	SELECT UNIQUECOUNT("file_sha2") AS 'COUNT' FROM events WHERE LOGSOURCENAME(logsourceid) = 'Symantec ATP' AND type_id = 4099 AND "file_sha2" IS NOT NULL Last 60 minutes
	Sandboxing Convictions (Cynic)	SELECT UNIQUECOUNT("file_sha2") AS 'COUNT' FROM events WHERE LOGSOURCENAME(logsourceid) = 'Symantec ATP' AND type_id = 4117 AND "file_sha2" IS NOT NULL Last 60 minutes
	Open Incidents	SELECT UNIQUECOUNT("atp_incident_id") AS 'COUNT' FROM events WHERE LOGSOURCENAME(logsourceid) = 'Symantec ATP' AND QIDNAME(qid) = 'Symantec Incidents' AND "atp_incident_id" is NOT NULL AND state = 1 Last 60 minutes
	Targeted Attacks	SELECT UNIQUECOUNT("atp_incident_id") AS 'COUNT' FROM events WHERE LOGSOURCENAME(logsourceid) = 'Symantec ATP' AND QIDNAME(qid) = 'Symantec Incidents' AND "atp_incident_id" is NOT NULL AND ("Event Summary" MATCHES '.*Targeted.*attack.*detected.*') Last 60 minutes
	New And Unknown Threats	SELECT UNIQUECOUNT("uuid") AS 'COUNT' FROM events WHERE LOGSOURCENAME(logsourceid) = 'Symantec ATP' AND type_id IN (4123,4115,4116,4117) AND VirusName MATCHES '.*WS.Reputation.*' Last 60 minutes
	TOP 10 Event Contributors By Affected IP	SELECT UNIQUECOUNT("uuid") AS 'TOTAL', "device_ip" AS DEVICE_IP from events WHERE

		LOGSOURCENAME(logsourceid) = 'Symantec ATP' and “device_ip” is not null GROUP BY device_ip ORDER BY TOTAL DESC LIMIT 10 Last 60 minutes
	TOP 10 Malicious File Names	SELECT "Filename", LONG(UNIQUECOUNT("uuid")) as "COUNT" FROM events WHERE LOGSOURCENAME(logsourceid) = 'Symantec ATP' AND "Filename" is not NULL AND type_id in (4125, 4113, 4123, 4112, 4115, 4116, 4124, 4353, 4117) GROUP BY "Filename" ORDER BY "COUNT" DESC LIMIT 10 Last 60 minutes
	TOP 10 SHA256	SELECT "file_sha2", UNIQUECOUNT("uuid") as "TOTAL" FROM events WHERE LOGSOURCENAME(logsourceid) = 'Symantec ATP' AND "file_sha2" is not NULL AND "action_id" != 1 GROUP BY "file_sha2" ORDER BY "TOTAL" DESC LIMIT 10 Last 60 minutes

Chapter 4

Visualization

This chapter includes the following topics:

Visualization

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

Dashboards

All of the dashboards use individual panels to plot the metrics that are related to the events from the EDR server. All of the dashboards let you filter events by time. Because the application can support multiple EDR instances, the Protection, Network Protection, and Endpoint Protection dashboards let you filter events by Host.

Figure 5-1 Overview At Glance

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

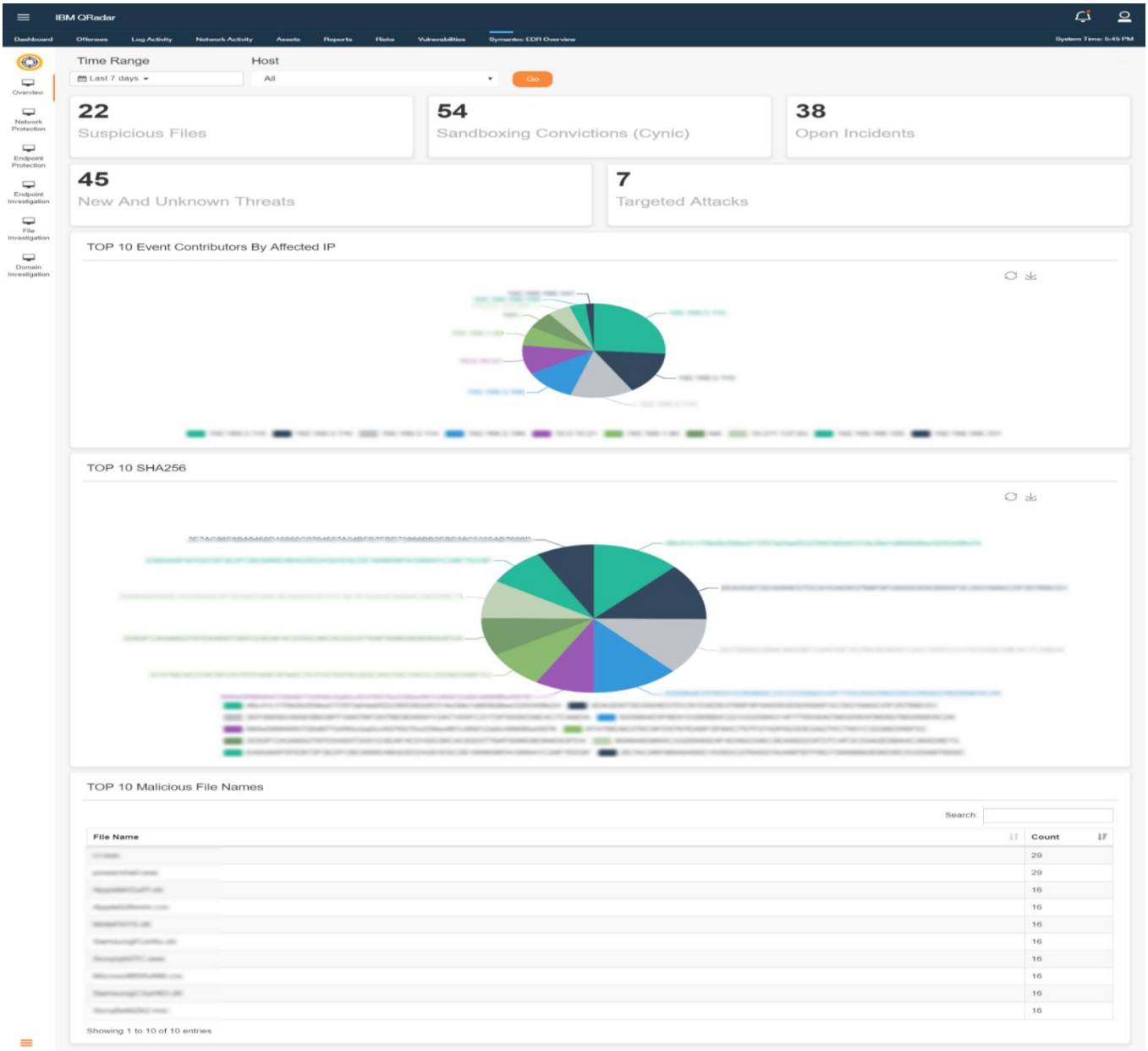


Figure 5-2 Network Protection at Glance

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

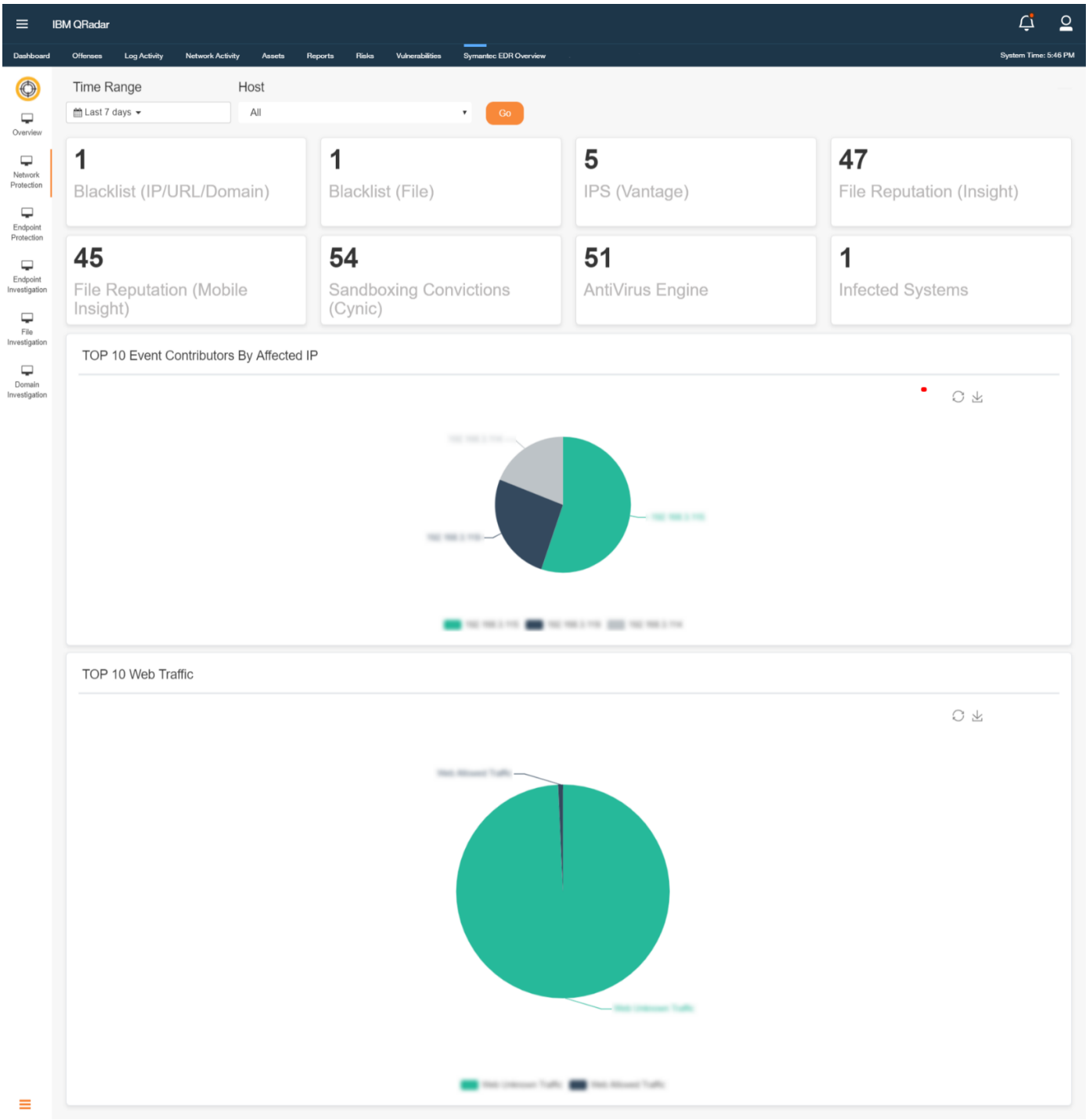


Figure 5-3 Endpoint Protection at Glance

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

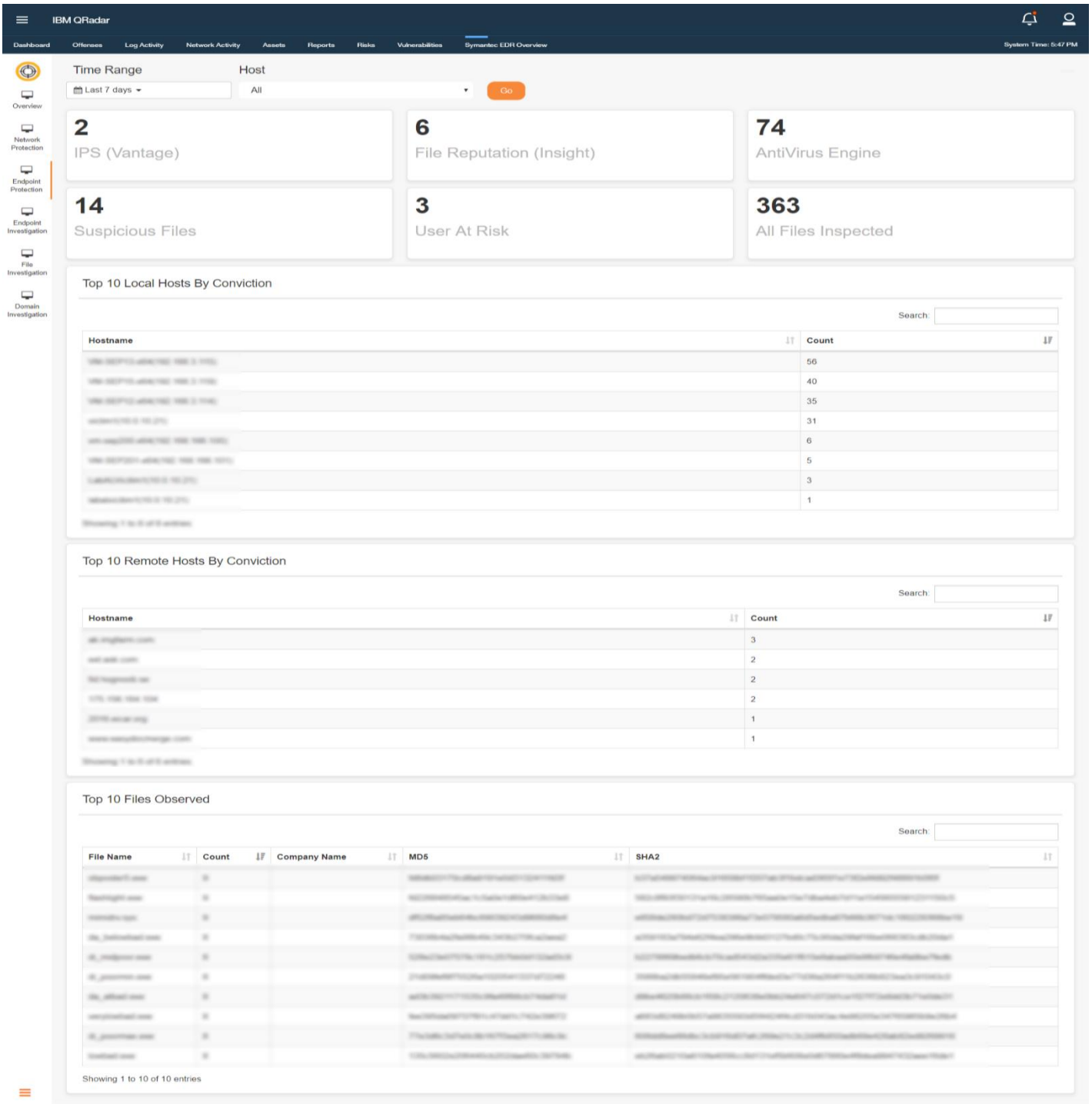


Figure 5-4 Endpoint Investigation

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

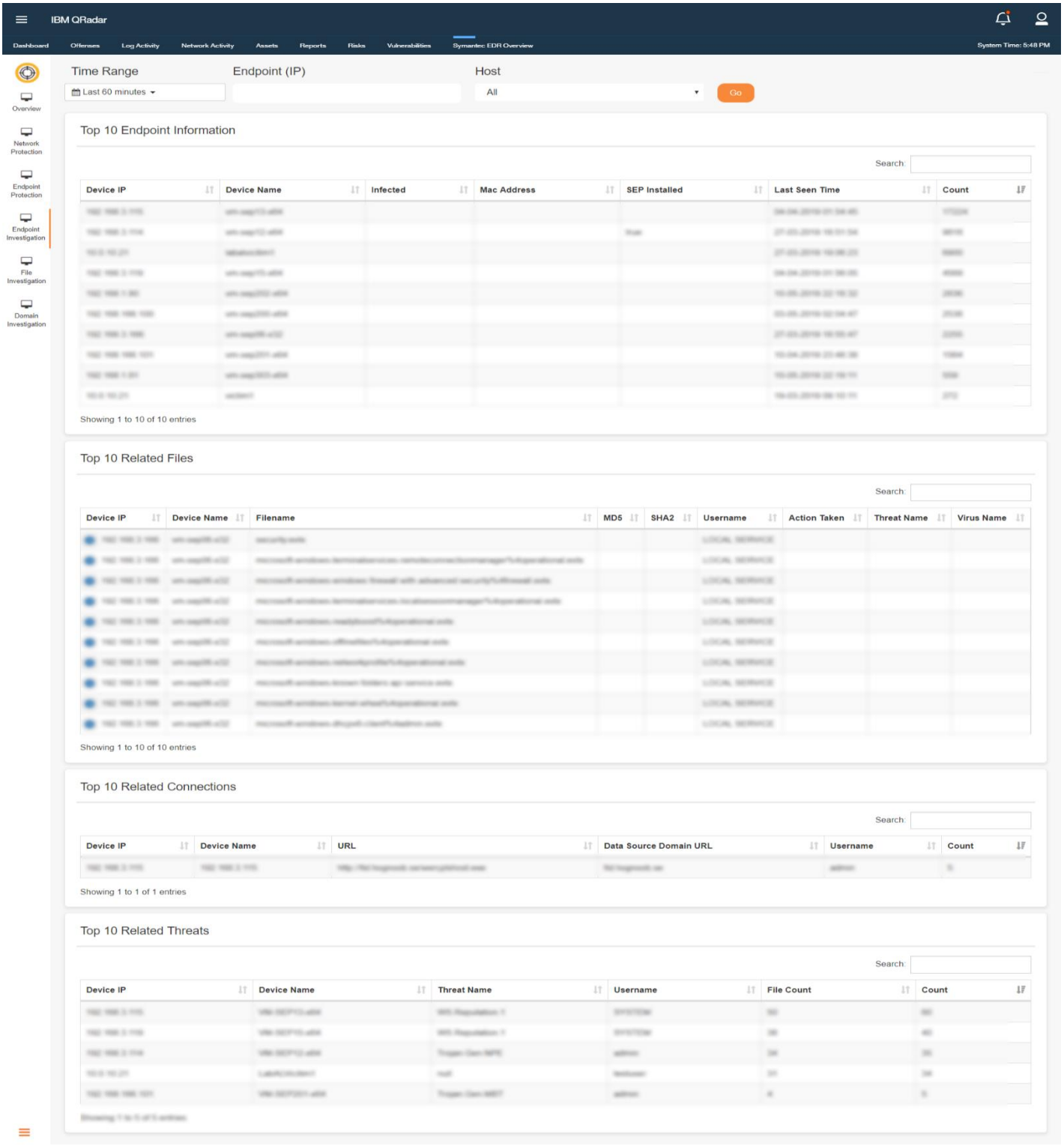


Figure 5-5 File Investigation

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.

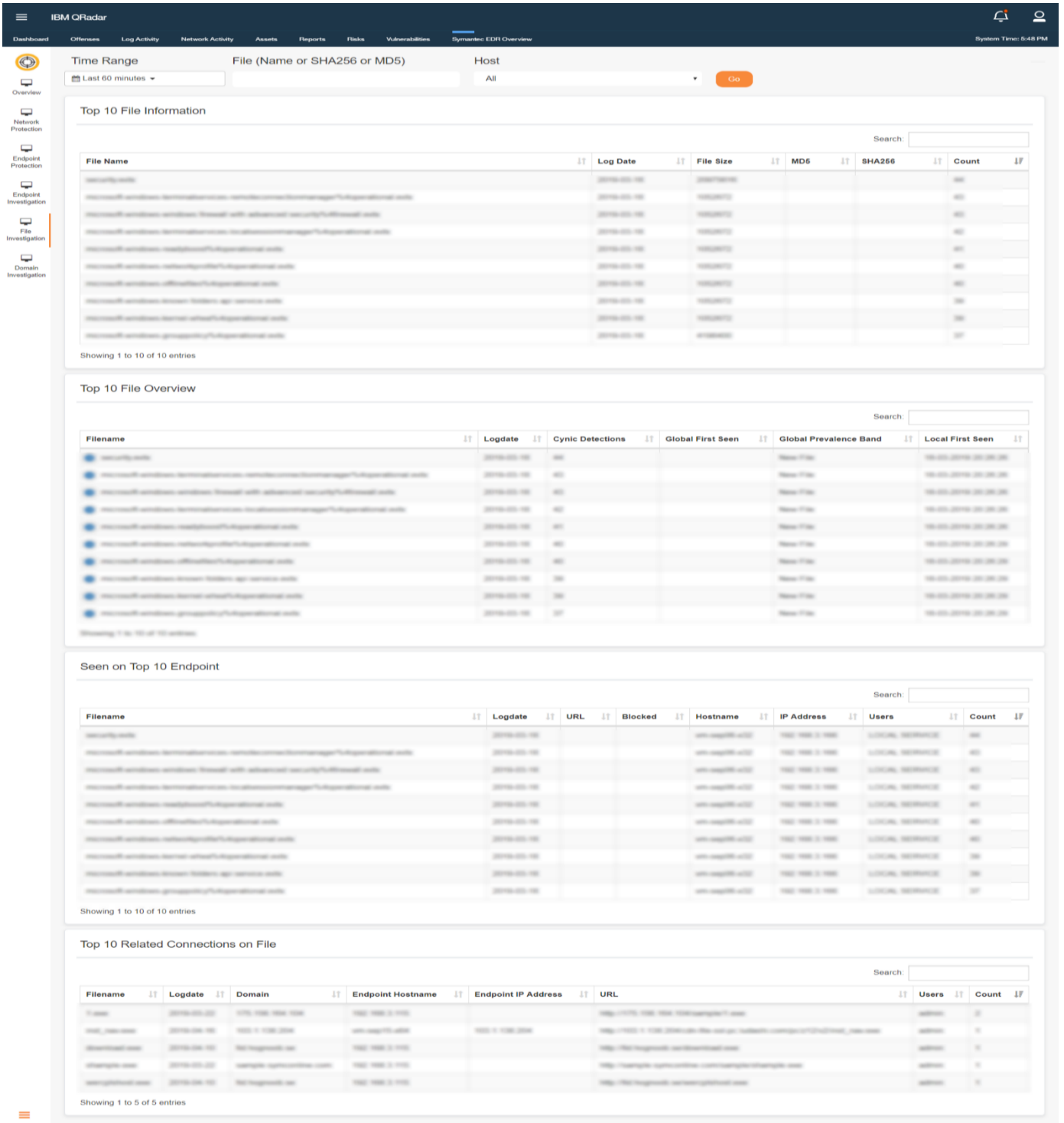
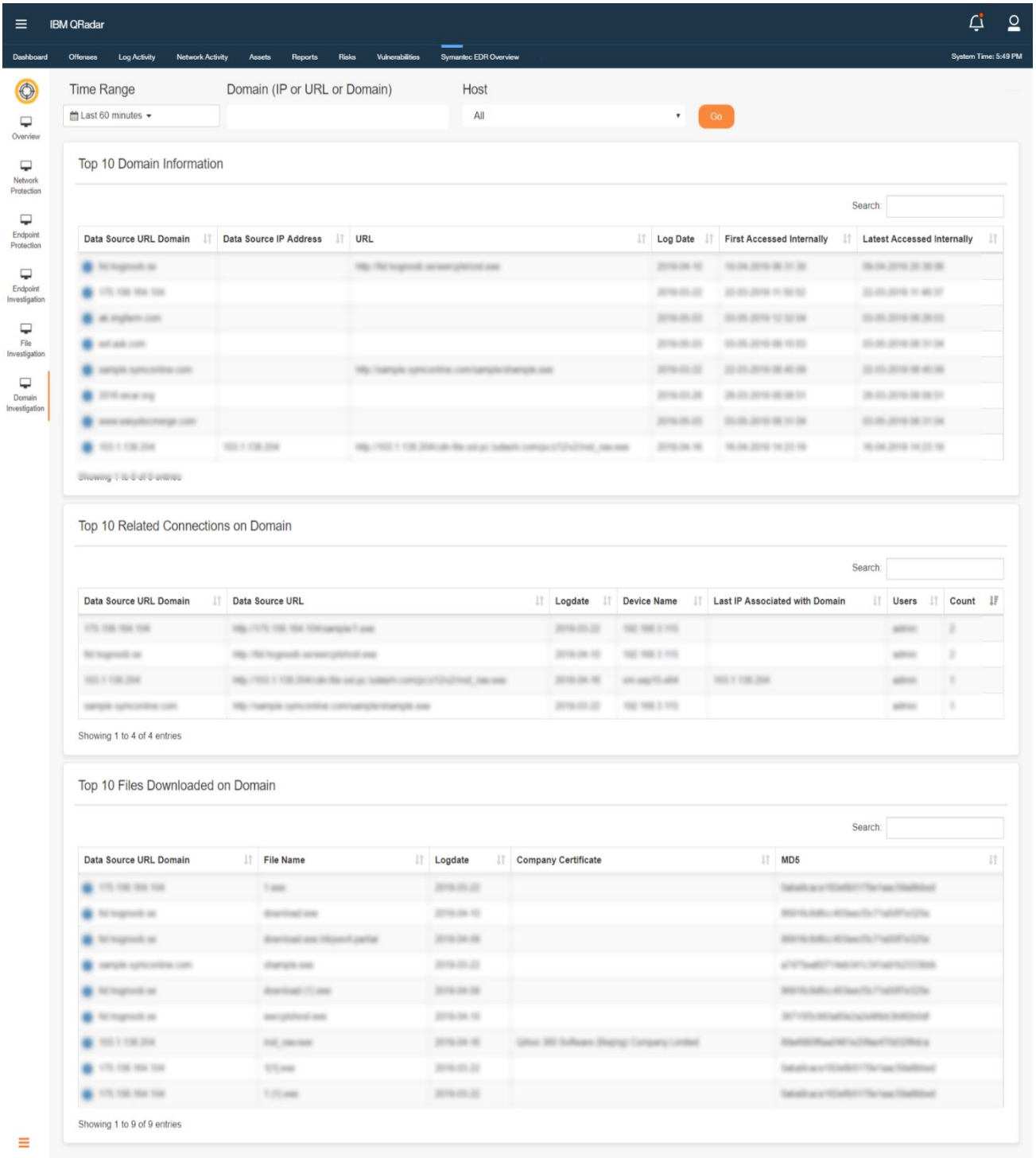


Figure 5-6 Domain Investigation

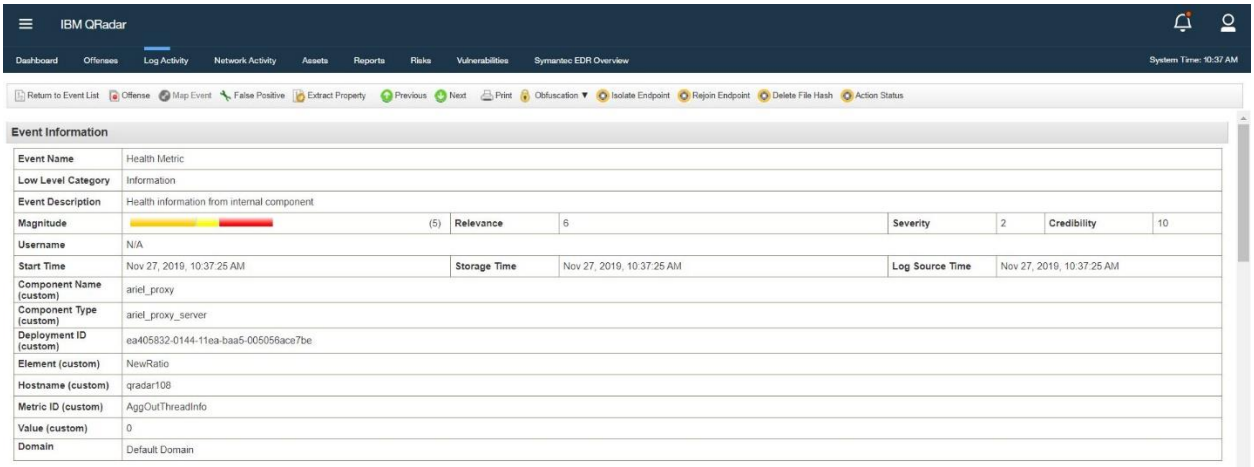
This dashboard is built for user to investigate a particular domain. User can type in the domain he wants to investigate and filter the data.



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. Application lets you take the following actions from QRadar events only:

Note: Actions are only allowed from the Log Activity tab.



- Isolate Endpoint- Quarantines the endpoint offline and from the network, while communication to the EDR appliance is maintained for additional instructions or actions.
- Rejoin Endpoint- Brings the endpoint online and lets you rejoin the endpoint to the network.
- Delete File Hash- Removes the file from the endpoint and reverses any actions the file has taken on the endpoint.
- Action Status- Allows the security analyst to keep track of an action taken on the EDR instance. The action uses a REST API to fetch the status of the last action that is taken on a particular event.

Chapter 5

Installation

This chapter includes the following topics:

Pre-Requisites

Symantec EDR App for QRadar v1.5.0 version supports EDR product version 3.2 to 4.1. User requires QRadar version 7.3.1 or above

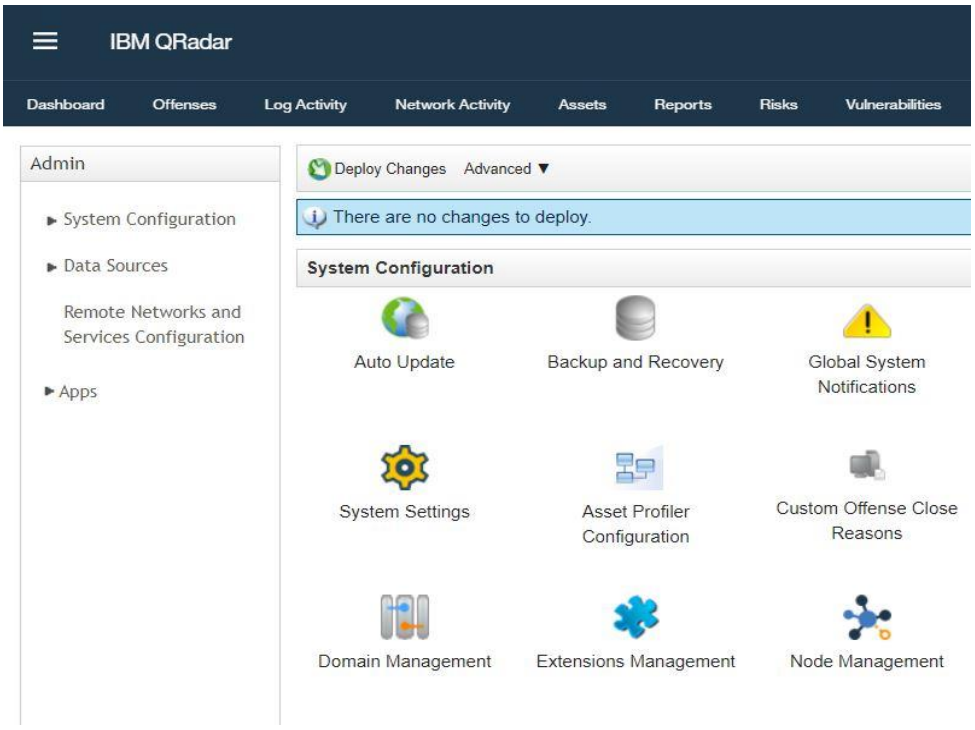
Note: User must configure token from Symantec EDR product and get corresponding client id and client secret that supports Symantec API version v2. API Version v1 came to EOL dated May 2019.

Installation

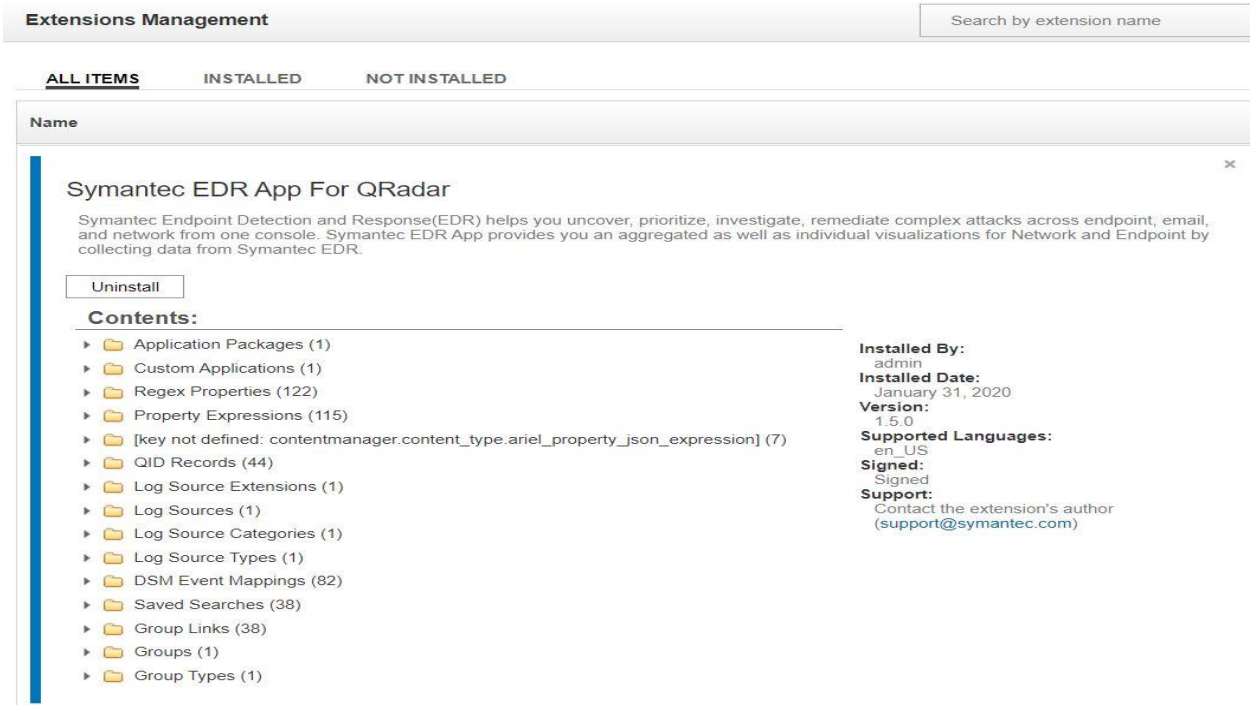
The application installation requires access to the QRadar console computer, using a web interface. The web interface is accessed at https://*QRadarconsoleIP*/. To install the application, do the following:

Application installation

1. Log on to the QRadar console.
2. Go to **Admin > Extension Management**.



3. Click **Browse** and then choose the downloaded zip file.
4. Click **Install**. Upon installation, the app displays all of the components as shown in the following screen shot:



5. Clear the cache and reload the page.

Upgrade

Upgrade App to version 1.5.0

1. Log on to the QRadar console.
2. Before upgrading Symantec EDR App for QRadar to v1.5.0 from any installation before v1.4.2, please follow below steps. If you are upgrading from v1.4.2 follow Installation steps.
3. Go to Admin > Custom Event Properties.
4. In the search box enter keyword “domain” Log on to the QRadar console.
5. Select the custom property named “domainid”, verify that the associated log source is Symantec ATP, and click on the delete button.
6. Select the custom property named “Domain”, verify that the associated log source is Symantec ATP, and click on the delete button.
7. Go to Admin Panel and click on Deploy Changes.
8. Clear the cache and reload the page.
9. Follow the same steps of Installation to install new version

Note: Custom Property “Domain” exist only for versions v1.0.0 and v1.1.0

QRadar Cloud Support

Symantec EDR QRadar v1.5.0 supports all its functionalities on QRadar cloud

Release Notes

v1.5.0

- Added support to collect Audit Events from Symantec EDR.
- Added support for configurable SSL verification in configuration page.

Chapter 6

Configuration

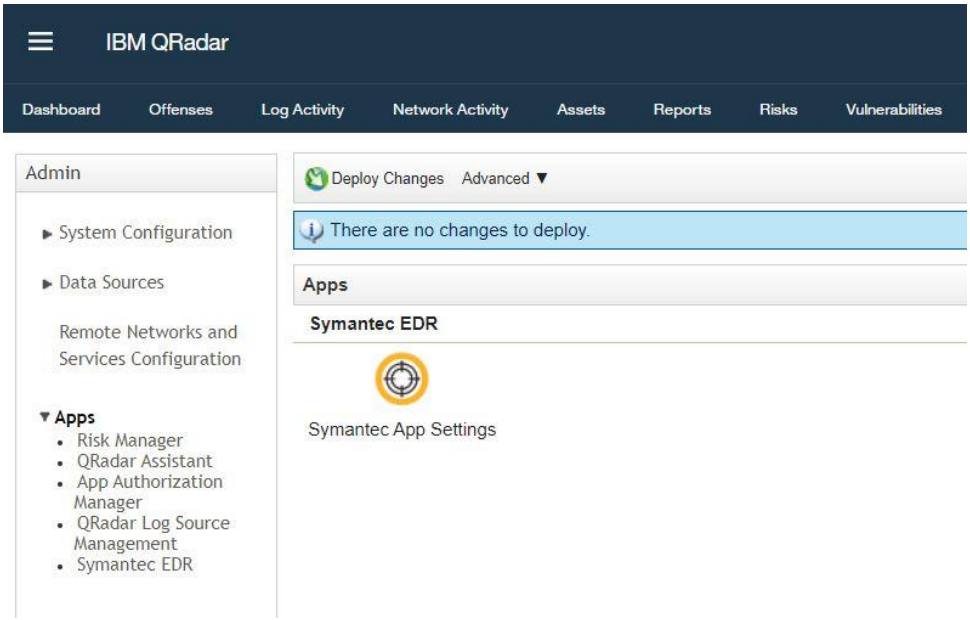
This chapter includes the following topics:

Configuration

The visualization dashboards are available after installation. For QRadar to start receiving data from EDR, data collection must be enabled. To enable data collection, do the following:

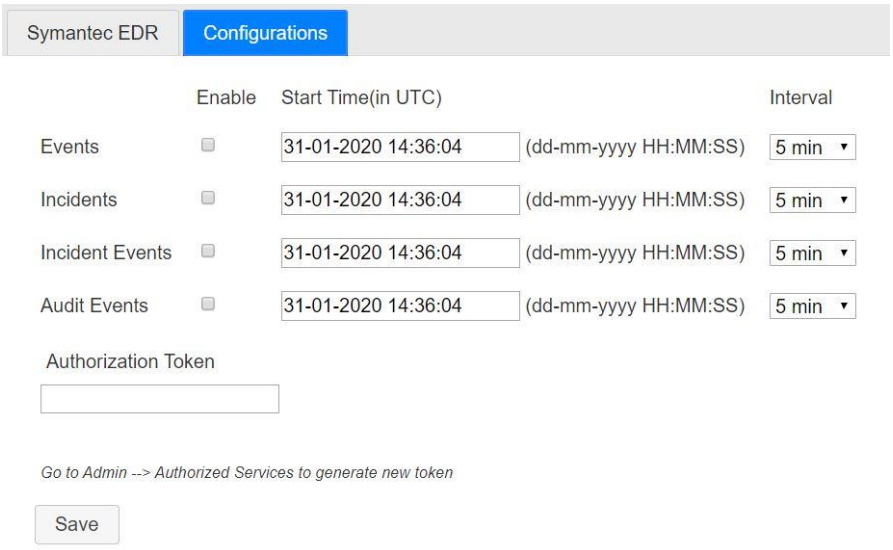
Enabling data collection

1. Log on to the QRadar console.
2. Go to Admin > Plug-ins > Symantec EDR.



3. Enter the details about the EDR server. If required, you can add multiple EDR instances.

4. Go to the Configuration tab and enable the data collection as required.
5. Enter the authorization token that is used to fetch data through the REST API.



Chapter 7

User roles and capabilities

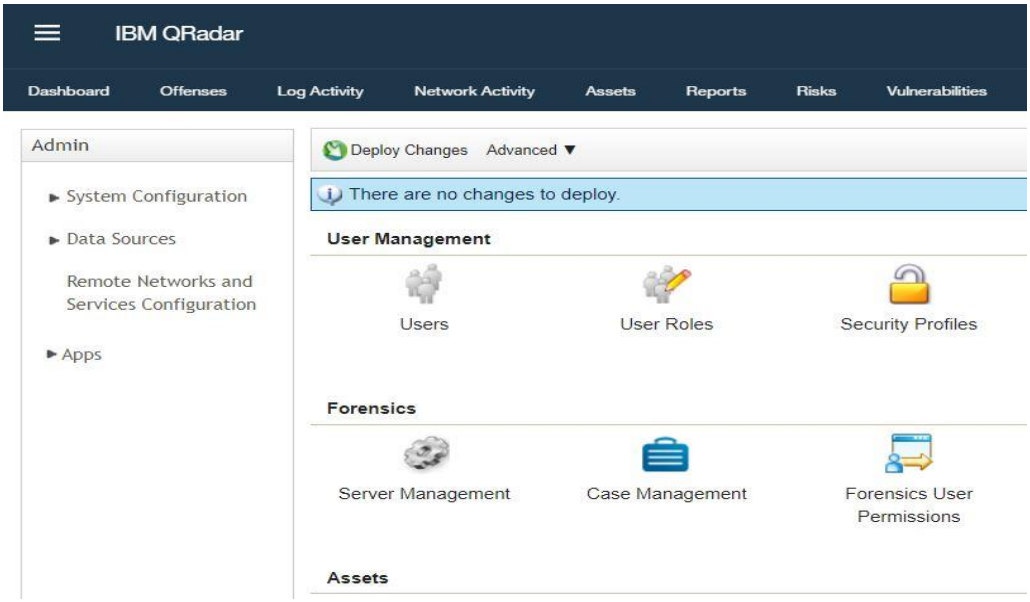
This chapter includes the following topics:

User roles and capabilities

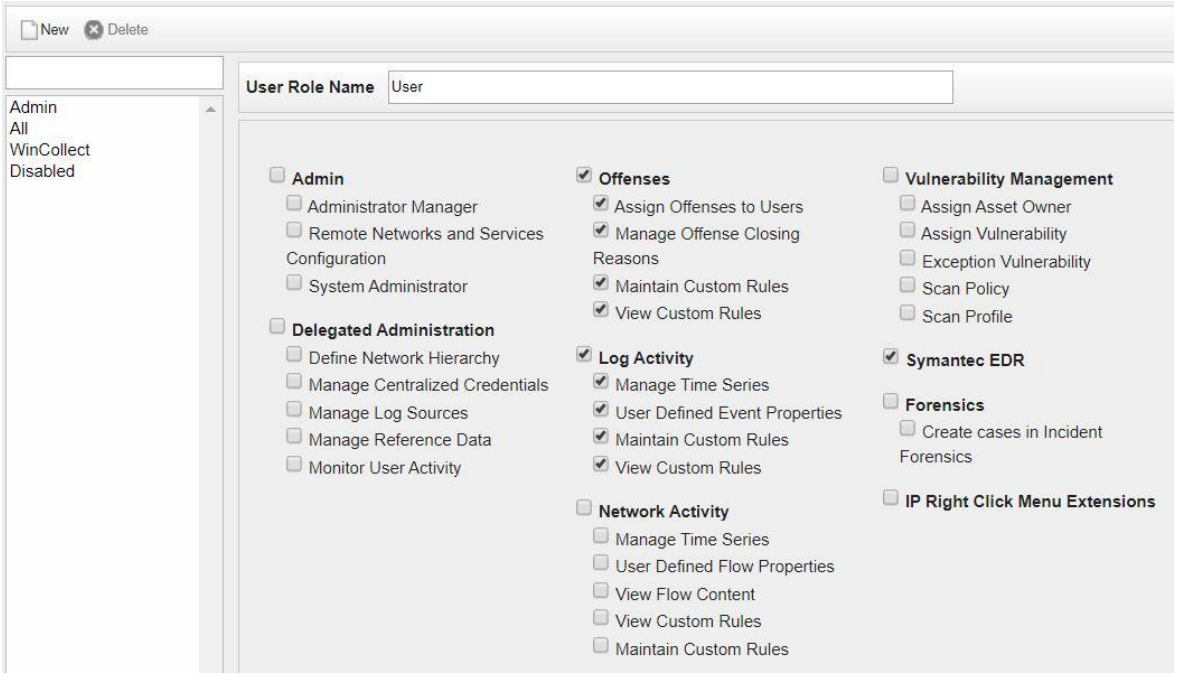
The QRadar app supports ACL configurations for restricting access different actions and dashboards. The app adds new capabilities (indicated as *Symantec EDR*) that controls access to different EDR actions. To access *Symantec EDR* actions, the user must be assigned a role that has permissions to run actions. By default, admin users have access to all of the *Symantec EDR* functions. To configure a role in QRadar, do the following:

Configuring roles

1. Log on to the QRadar console and go to **Admin > User Roles**.



2. Click **New**.
3. Enter the name of the role. Assign the desired functions as shown in the screen shot. Assign these roles to the users who are allowed to perform EDR actions.



4. Click **Save**.

Chapter 8

Uninstalling the application

This chapter includes the following topics:

Uninstalling the application

To uninstall the application, do the following:

Uninstalling the application

5. Log on to the QRadar console and go to the Admin Page.
6. Open **Extension Management**.
7. Select the Symantec EDR application.
8. Click **Uninstall**.

Chapter 9

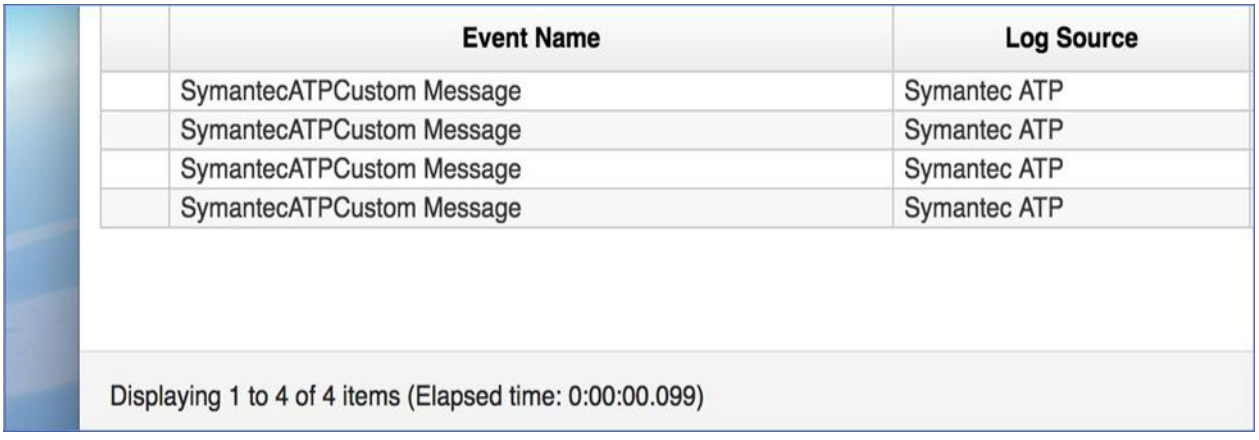
Troubleshooting

This chapter includes some 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

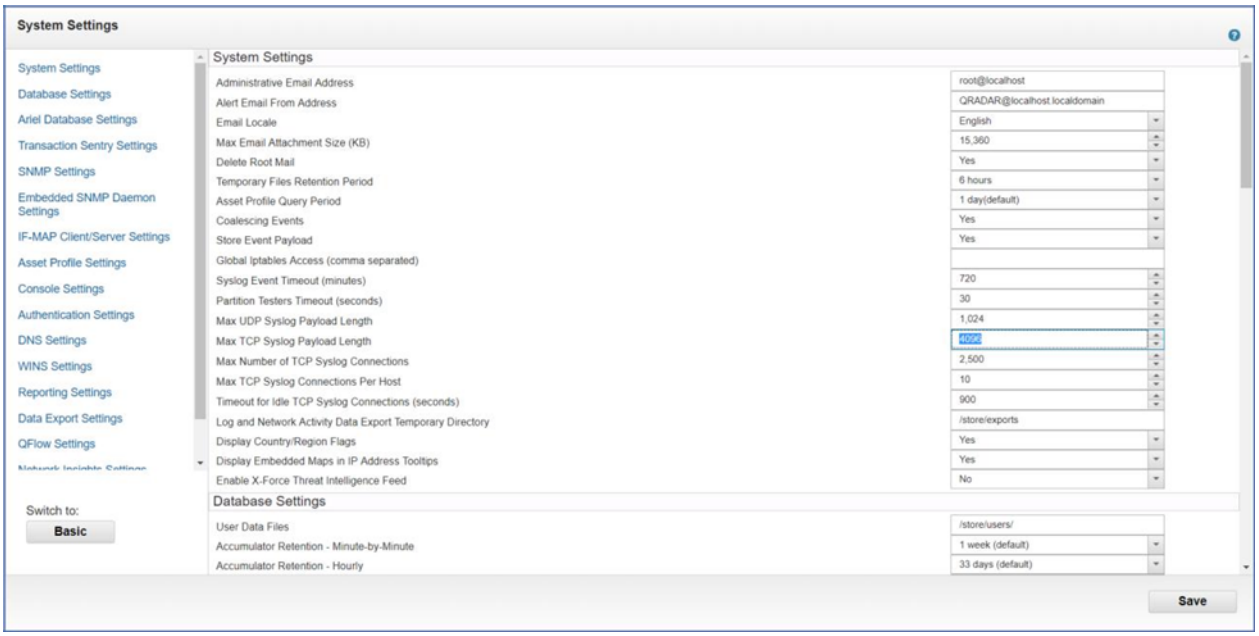
Displaying 1 to 4 of 4 items (Elapsed time: 0:00:00.099)

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:

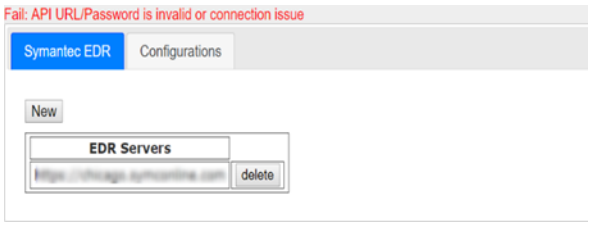


Case #2 – Symantec EDR App configuration fails with various error messages

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

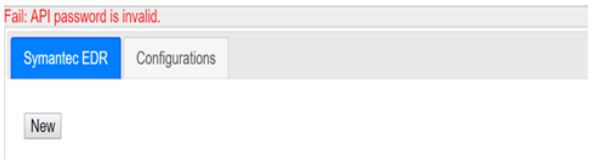
Troubleshooting Steps: User might have entered URL which is already configured. User is recommended to enter new credentials which is not already provided

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



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.

3. **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,
    - Right click on that event.
    - View in DSM editor.
    - 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: Please follow below 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: Please follow below 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