

Symantec EDR App for QRadar

App Architecture and Installation Guide

v1.3.0

Chapter

Architecture

This chapter includes the following topics:

- <u>Architecture</u>
 - o Data Collection
 - o Log Source
 - o Symantec EDR DSM
 - o Network and Endpoint Event Type IDs

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 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
		User Activity	Suspicious
8000	Session Event		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
		Misc Network Communication	Access
8007	Network Event	Event	
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
 - o Overview Dashboard
 - o Network Protection Dashboard
 - o Endpoint Protection Dashboard
 - o Endpoint Investigation Dashboard
 - o File Investigation Dashboard
 - o Domain Investigation Dashboard
- <u>Actions</u>

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.

Symantec EDR App for QRadar



Figure 1: Overview

Network Protection Dashboard

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

≡ IB	8M QRadar			Ċ <u>°</u>
Dashboard	Offenses Log Activity Network Activity Assets	Reports Risks Vulnerabilities Symantec EDR Overview		System Time: 5:46 PM
P	mile Kange Host mile Last 7 days ▼ All	• G o		
Overview Network Protection	1 Blacklist (IP/URL/Domain)	1 Blacklist (File)	5 IPS (Vantage)	47 File Reputation (Insight)
Endpoint Protection Endpoint Investigation	45 File Reputation (Mobile Insight)	54 Sandboxing Convictions (Cynic)	51 AntiVirus Engine	1 Infected Systems
Investigation	TOP 10 Event Contributors By Affected	i IP		
Domain Investigation				。 ○ 不
	TOP 10 Web Traffic			
				Оъ
=		-		

Figure 2: Network Protection at Glance

Endpoint Protection Dashboard

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

fenses Log Activity Ne	ntwork Activity A	ussets Reports f	Risks Vu	Inerabilities Symantec EDR Overview				
ïme Range	Host							
Last 7 days 👻	All			Go				
_				-				
2				6		74		
PS (Vantage)				File Reputation (Insight)		AntiVi	rus Engine	
14				3		363		
I - I				Upor At Disk				
suspicious riles	5			USEI AL RISK		AILEIN	es inspecied	
Top 10 Local Hosts	By Convictio	n						
								Search:
Hostname						11	Count	
V80.00711-0042102 100.0							56	
100.00710.404(10).100.0							40	
100.00712.404(102.108.0							35	
activit(10.0.10.21)							31	
are suggifted addressed to a	100.1003						6	
100.007021.404(10).100	100.1011						5	
144403030101111111111111111111111111111							3	
Multi-cline 1(10.1.10.21)							1	
Top 10 Remote Hos	its By Convic	tion						
Top 10 Remote Hos	its By Convic	tion						Search:
Top 10 Remote Hos Hostname	its By Convic	tion				Count		Search:
Top 10 Remote Hos Hostname	its By Convic	tion			11	Count 3		Search:
Top 10 Remote Hos Hostname	its By Convic	tion			11	Count 3 2		Search:
Top 10 Remote Hos Hostname	ts By Convic	tion			11	Count 3 2 2		Search:
Top 10 Remote Hos Hostname	ts By Convic	tion			11	Count 3 2 2 2 2		Search:
Top 10 Remote Hos Hostname	its By Convic	tion			41	Count 3 2 2 2 1		Search:
Top 10 Remote Hos Hostname	its By Convic	tion			41	Count 3 2 2 2 2 2 1 1 1 1		Search:
Top 10 Remote Hos	ts By Convic	tion			11	Count 3 2 2 2 2 1 1 1		Search:
Top 10 Remote Hos Hostname	red	tion			11	Count 3 2 2 2 2 1 1 1		Search:
Top 10 Remote Hos Hostname	its By Convic	tion			11	Count 3 2 2 2 2 1 1 1		Search:
Top 10 Remote Hos Hostname Top 10 Files Observ	red	tion Company Name	11	MD5	11 11 11 11 11 11	Count 3 2 2 2 2 1 1 1		Search:
Top 10 Remote Hos Hostname Top 10 Files Observ	red	tion Company Name	11	MD5	11 11 11 11 11	Count 3 2 2 2 3 1 1 1		Search:
Top 10 Remote Hos Hostname Top 10 Files Observ	red	tion Company Name	11	MD5	11 11 11 SHA2	Count 3 2 2 2 1 1 1		Search:
Top 10 Remote Hos Hostname Top 10 Files Observ	red	tion Company Name	11	MD5	11 11 11 11 11 11 11	Count 3 2 2 2 3 1 1 1		Search:
Top 10 Remote Hos Hostname Top 10 Files Observ	red	tion	11	MD5	11 11 11 11 11 11 11	Count 3 2 2 2 1 1 1		Search:
Top 10 Remote Hos Hostname	red	tion	11	MD5	II SHA2	Count 3 2 2 2 1 1 1		Search:
Top 10 Remote Hos Hostname	red	tion	11	MD5	II SHA2	Count 3 2 2 2 1 1 1		Search:
Top 10 Remote Hos Hostname	red	tion	11	MD5	11 11 11 SHA2	Count 3 2 2 2 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		Search:
Top 10 Remote Hos Hostname	red	tion	11	MD5	11 11 11 11 11 11 11	Count 3 2 2 2 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		Search:

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

or QHadar											
Time Range	Fadpoint (IP)	i Hisks Vulnerabilitie	Hoet								уато
	Endpoint (IP)		TIOSC								
El cast do minutes +			All				Go				
Top 10 Endpoint Info	ormation										
									Search:		
Device IP	11 Device Name	11 Infected	Mac Address		IT SER	P Installed	11	Last Seen Time		11 Count	
1000 000 h 1100	uni segni i alte							14-14-2010 IV 14-45		17224	
100.000.0.00	101-102-12-000										
10.0 10.01	Manufaction 1							21-12-22-12-12-12-12		-	
100.000.0.00	and applied and									-	
100.000.000	101 (102) (112) (112)							10.00.00.00		10.00	
102 108 108 108	101 - 102 TO 1 + 101									11.00	
1000 - 1000 (1 - 1000)	101 100 101 101							27-02-2019 10-02-07		-	
	and applied whith							10.04.0010.004.00		1000	
100 100 100	101-102/011-010									-	
10.0.00.00	and and										
Top 10 Related Files	3										
									Search:		
Device IP	ce Name 11 Filename			11	MD5 11	SHA2 IT	Username	Action Taken	Threat Na	me 11 Virus	Na
· 102 100 3 100 units	apita atta manada min						LOGIC SERVICE	100			
·	apiti all mercuit analog	Annesistant and Annesis	or a formation of the	and and			1004, 1004	08			
·	apiti at a manufacture	- arritran Transf will ad	and second where the				LOOK NOTION	08			
·	apiti-size increased acceleration	Antering Contract State	and the second sec	-			LOOK NORM	100			
·	aption in the second		ei andra				1008.0054				
·	applied in the state	Marchine's August March	and to				LOOK SERVICE	181			
·	apital meaning		crust and c				1004.0094				
·	applied increase and an alter	Anna briter an area	a anda.				1004, 1094				
·	aption mountained	Server already dependent	an anda				1004, 1004				
· 102 100.2 100 unit	aptivity increasing	Sugar Carthelines	-				LOCAL SERVICE	100			
Showing 1 to 10 of 10 entrie	15										
Top 10 Related Con	nections										
									Search:		
Device IP	Device Name	URL		11	Data Sou	urce Domain	URL	11 Userna	me	11 Count	
1982 1988 2 110	102 102 110	10g-76/hopeoils-serie	and the second second		No. Income	-					
Showing 1 to 1 of 1 entries											
Top 10 Related Three	ats										
									Search:		
Device IP	11 Device Name	11	Threat Name	11	Usern	ame	11	File Count	11	Count	
	100.00713.404		WE Reputation 1		Sector S					-	
100.000.1115			and descentions of		and the	100		-		-	
1982 1988 3 115	VMI SEPTEMB										
1622-1688 (2-115) 1622-1626 (2-116) 1622-1626 (2-116)	Viel SCHLARK Viel SCHLARK		Togan Lan MPE		-			-		-	
1922-002.3.115 1922-002.3.115 1922-002.2.114 1922-012.21	Version and		Trape Sec 1975		-			14		26 26	

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.

Offenses Log Activity Network Activity Assets Reports Risks Vulnerabilities	Symante	c EDR Overview						<u> </u>				Syste
Time Range File (Name or SHA256 or MD5)	F	lost										
tast 60 minutes ◄		All				• Go						
Top 10 File Information												
									Sear	ch:		
File Name			١ţ	Log Date	11	File Size	11	MD5	SHA256	5	11 Cour	nt
an adjunda				20103-005-10		21007100100					-	
record and/or termptonics, and/or manage*-typedical with						100,0072						
recreased activities are been from all advanced security? All result acts				2010.00.0		100,0072					-	
monadi antiana lamingkanana logitanannyanga "Algoridorgi ada				20100-00-10		100,0072					-	
microsoft annalises, maniplessoft-Appendicent ands				2010.01.10		100,0072					-	
recould address tabuligable's type alread with				2010-00-10		100,0072					-	
recreat and a distinct fragmatical and				2010-02-10		1002072					-	
recread andous insur foller, ap senits with				2010-02-10		100,0072						
recreat and an invariant analysign along and				2010-02-10		100,0072						
racead ardise grappin/stageding eds				2010-02-10		4100400						
Showing 1 to 10 of 10 entries												
Top 10 File Overview												
									Searc	ch:		
Filename	11	Logdate 11	Cynic De	tections	Jî Glob	al First Seen	J† G	lobal Prevalenc	e Band	11 L	ocal First	Seen
a sector a			-				10					_
a count option option load all allocation and build and an			-				1.5			-		
							1.2					
 recreation and sections and section of the section of the 		2010.00.00						and Take				
 monorfit and out-subandige clip*-stoperational only 								and Take				
Recent and an effective disable for persisting and		2010.01.00	-				1.0	and Take		1.1		
Record and an inter titler, apprentix and								in The				
excessificandose lanad sheefs legerational sets		2010.01.0	-					100 T 100				
eccent and an propping "dependent ada		2010.00.00						100 T 100				
Strang 1 is 12 of 12 orbust												
Seen on Top 10 Endpoint												
									Searc	ch:		
Filename	J	Logdate	URL	11 Block	ked 💵	Hostname	lt IP	P Address	Users		lt c	:oun
Filename	J	Logdate	URL	Lî Block	ked Jî	Hostname	lt IF	PAddress	Users	100000	11	:oun
Filename	1)	Logdate	URL	J1 Block	ked 🎝	Hostname	lt iF	P Address	Users		11	Coun
Filename	8	Logdate	URL	J1 Block	ked Ĵ†	Hostname	LT IF	PAddress	Users		tt (Coun
Filename		Logdate	URL	11 Block	ked It	Hostname		PAddress	Users		11 C	Coun
Filename	L:	Logdate	URL	11 Block	ked 11	Hostname	11 16	PAddress	Users		11	Coun
Filename	1:	Logdate	URL	11 Block	ked []	Hostname	11 16	P Address	Users		11 (Coun
Filename	.11	Logdate 1	URL	11 Block	ked I1	Hostname	11 16	PAddress	Users			Coun
Filename	1	Logdate	URL	11 Block	ked 11	Hostname	11 16	P Address	If Users		11	Coun
Filename	1	Logdate 1	URL	11 Block	ked 11	Hostname	11 F	PAddress	IT Users		11	Coun
Filename	1	Logdate	URL	11 Block	ked 11	Hostname	11 8	PAddress	11 Users			Coun
Filename Showing 1 to 10 of 10 entries Top 10 Related Connections on File		Logdate		11 Block	ked 11	Hostname	11 11	PAddress	11 Users		IT (Coun
Filename Showing 1 to 10 of 10 entries Top 10 Related Connections on File		Logdate	I URL	1 Block	ked IT	Hostname	11 11	PAddress	II Users	L		Coun
Filename Showing 1 to 10 of 10 entries Top 10 Related Connections on File Filename I Logdate I Domain I Endpoint Hostname	11	Logdate		URL	ked 11	Hostname	1	PAddress	Searc	ch.	11 C	Cou
Filename Showing 1 to 10 of 10 entries Top 10 Related Connections on File Filename 1 Logdate 1 Domain 1 Endpoint Hostname	11	Logdate 4	T URL	URL	ked 11	Hostname	17 19	P Address	Searce	sh:	11 C	Cou
Filename Filename Showing 1 to 10 of 10 entries Top 10 Related Connections on File Filename 1 Logdate 11 Domain 11 Endpoint Hostname	11	Logdate 4	T URL	URL	ked 11	Hostname	1 1	PAddress	II Users	h	11 C	Cou
Filename Filename Showing 1 to 10 of 10 entries Top 10 Related Connections on File Filename I Logdate II Domain II Endpoint Hostname	11 	Logdate 4	URL 4	URL	ked 11	Hostname		PAddress	III Users	h: ⊥⊺ Us	11 C	Cou
Filename Showing 1 to 10 of 10 entries Top 10 Related Connections on File Filename 11 Endpoint Hostname	11	Indpoint IP Addre	T URL 4	URL	ked 1	Hostname		PAddress	III Users	ch:	ors it	Cou

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.

Offenses Log Activity Network A	ctivity Assets Reports Ri	sks Vulnerabilities	Symantec EDR	Overview								s
Time Range	Domain (IP or URL or	Domain)	Host									
m⊥ast 60 minutes -		Dornany	All					Go				
Top 10 Domain Information	on											
										Search		
Data Source URL Domain	Data Source IP Address	URL				.lt	Log Date	First Acces	sed Internally	11 Late	st Access	ed Intern
Introprotion		Mg. No hopests	ariaar gidhad a				2010-04-10	10.04.2016	10.10	-	s 2010 20	-
175 108 104 104							2110-01-22	22-03-22198	- 50 102	10.0	0.2010 11.0	a
🗋 at region con							2010/06/05	11-11-2219	0.00	-	6.00% 38	
🔹 est add com							2010/06/05	10.05.0718			6.2019-38	11.04
angle syncarity can		Mg. Sample sym	onine contrary	-			2710-25-22	22 43 20 10		10.0		-
· Interaction							2010/01/20	26-12-2016	10.00	10.0	1.2010-081	
🗧 een segénmege om							219.05.03	10.01.001	10.00			
	100.1108.004	Mg-1011108.0	and the set of	Address of the	period and	-	2212.04.10	10.04.0110	10.00			
										Search		
Data Source URL Domain	□↑ Data Source URL			ţ	Î Logdate lî	Device	e Name 👫	Last IP Associ	ated with Dom	Search nain 1	Users	lî C
Data Source URL Domain	Data Source URL	1 ⁻¹ 104		ł	Î Logdate lî	Device	e Name ⊔î	Last IP Associ	ated with Dom	Search nain 4	Users	lt c
Data Source URL Domain	Data Source URL	e'i see		1	↑ Logdate ↓↑	Device	e Name 👫	Last IP Associ	ated with Dom	Search	Users	lt c
Data Source URL Domain	1 Data Source URL	ti' ana ind ana il pi fallati umipi	234m.m	1	f Logdate Jf	Device	e Name 🛛 🏌	Last IP Associ	ated with Dom	Search nain 1	Users	tt c
Data Source URL Domain	11 Data Source URL	ert and had and dige talkets compo		1	1 Logdate 11	Device	e Name 👫	Last IP Associ	ated with Dom	Search nain 1	Users	ţt c
Data Source URL Domain	1 Data Source URL	tif see Ind see San Salah serije Gangle thangle se			Logdate	Device	e Name 👫	Last IP Associ	ated with Dom	Search	Users	ţt c
Data Source URL Domain Data Source URL Domain Showing 1 to 4 of 4 entries Top 10 Files Downloaded	11 Data Source URL	tif and ind and dig tablet angle tangle thangle an	-7-2-4, m		Logdate 1	Device	e Name 1	Last IP Associ	ated with Dom	Search	Users	lt c
Data Source URL Domain Data Source URL Domain Showing 1 to 4 of 4 entries Top 10 Files Downloaded	1 Data Source URL	tif and ind and al products on the complection photon			Logdate 1	Device	e Name 🛛 1	Last IP Associ	ated with Dom	Search	Users	tt c
Data Source URL Domain Data Source URL Domain Top 10 Files Downloaded Data Source URL Domain	It Data Source URL	1	Logdate	It Comp	Logdate If	Devic	e Name 💵	Last IP Associ	ated with Dom	Search	Users	It c
Data Source URL Domain Showing 1 to 4 of 4 entries Top 10 Files Downloaded Data Source URL Domain	11 Data Source URL		Logdate	it Comp	t Logdate If	Device	e Name 1	Last IP Associ	ated with Dom	Search	Users	II C
Data Source URL Domain Showing 1 to 4 of 4 entries Top 10 Files Downloaded Data Source URL Domain	11 Data Source URL	11	Logdate	1 1 Comp	Logdate I	Device	e Name	Last IP Associ	ated with Dom	Search	Users	lî C
Data Source URL Domain Showing 1 to 4 of 4 entries Top 10 Files Downloaded Data Source URL Domain	11 Data Source URL		Logdate	1 It Comp	Logdate I	Device	e Name	Last IP Associ	ated with Dom	Search	Users	II C
Data Source URL Domain Showing 1 to 4 of 4 entries Top 10 Files Downloaded Data Source URL Domain	Image: state		Logdate	it Comp	Logdate If	Devic	e Name	Last IP Associ	MD5	Search	Users	11 C
Data Source URL Domain Showing 1 to 4 of 4 entries Top 10 Files Downloaded Data Source URL Domain	Image: state		Logdate	it Comp	Logdate If	Device	e Name	Last IP Associ	ated with Dom	Search	Users	II C
Data Source URL Domain Showing 1 to 4 of 4 entries Top 10 Files Downloaded Data Source URL Domain	11 Data Source URL 11 Data Source URL 11 File Name		Logdate	it Comp	Logdate If	Device	e Name	Last IP Associ	Ated with Dom	Search	Users	II C
Data Source URL Domain Showing 1 to 4 of 4 entries Top 10 Files Downloaded Data Source URL Domain	11 Data Source URL 11 Image: Second Sec		Logdate	1 Comp	Logdate If	Device	e Name	Last IP Associ	MD5	Search	Users	II C
Data Source URL Domain Showing 1 to 4 of 4 entries Top 10 Files Downloaded Data Source URL Domain	11 Data Source URL		Logdate	1 It Comp	Logdate I	Devici	e Name	Last IP Associ	MD5	Search	Users	II C.

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.

IBM QRadar							Ļ	2
Dashboard Offensea	Log Activity Network Activity Assets Reports Risks V	uherabilities Syma	ntec ATP Overview				System Time:	11:07 AM
Return to Event List	ense 🥝 Map Event 🤸 False Positive 🔀 Extract Property 🛛 😡 Previous 🔮 Neo	it 📇 Print 🔒 Obfus	cation 🔻 🧿 Isolate Endpoint 🧔 Rejoin Endpoint 💿 Delete File Hash 💿 Action Status					
Event Information								i î
Event Name	Reputation Request							
Low Level Category	Information							
Event Description								
Magnitude	(3)	Relevance	1 S	everity	3	Credibility	5	
Username	Administrator							_
Start Time	Jun 28, 2018, 7:53:50 PM	Storage Time	Jun 28, 2018, 7:53:50 PM	og Source Time	Jun 28, 20	018, 7:53:50 PM		
Event Summary (custom)	N/A							
Filename (custom)	wuaueng.dll							
Hostname (custom)	N/A							
MD5 Hash (custom)								
URL (custom)	N/A							
VirusName (custom)	N/A							
action_id (custom)	N/A							
atp_host (custom)								
atp_incident_id (custom)	N/A							
data_source_ip (custom)	N/A							
data_source_url_domain (custom)	N/A							
device_ip (custom)								
a								

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

Installation

This chapter includes the following topics:

- Pre-requisites
- Upgrading the App from previous Installation
- Installing App for the First Time
- Configuration
- User Roles/Capabilities
- Uninstalling the Application
- QRadar Cloud Support

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

Symantec EDR App for QRadar

🗋 Add 🕞 Edit 🔁 Cargo 🔛 Enable Clisade 🙋 Delette domain												
Property Name	Delete the selecte	d property Description	Log Source Type	Log Source	Event Name	Category	Expression	Username	Enabled	Creation Date	Modification D	
AccountDomain	Regex	Default custom ex	Microsoft Window.	N/A	N/A	N/A	Target Domain: (.*?)	admin	True	Sep 13, 2008, 6:2	Sep 13, 2008, 6	
Domain	Regex	Default custom ex	Symantec ATP	N/A	N/A	N/A	"domain name" "	admin	True	Jul 3, 2018, 7 45	Jul 4, 2018, 10.3	
data_source_url_domain	Regex	The domain from	Symantec ATP	N/A	N/A	N/A	"data_source_url	admin	True	Jul 2, 2018, 5:50	Jul 4, 2018, 10:3	
domainid	Regex	A list of domains	Symantec ATP	N/A	N/A	N/A	"domainId".\s*(\[[\"	admin	False	May 24, 2017, 1:0	Jul 4, 2018, 10:3	
recommended_action	Regex	Recommended a	Symantec ATP	N/A	Symantec Incidents	N/A	"recommended_a	admin	False	Jul 2, 2018, 6:36	Jul 4, 2018, 10:3	

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.

Symantec EDR App for QRadar

Extensions Management	Search by extension name Q		IBM Securi	ty App Exchange
ALL ITEMS INSTALLED NOT INSTALLED				Add
Name		Status	Author	Added O
Symantec EDR App For QRadar Symantec Endpoint Datection and Response(EDR) helps you uncover, prioritize, investigate, ren and network from one conside. Symantec EDR App provides you an aggregated as well as indivi- collecting data from Symantec EDR. Uninstall Contents: Regex Properties (122) Application Packages (1) Custom Applications (1) Custom Applications (15) Custom Applications (15) Custom Extensions (1) Log Source Extensions (1) Log Source Categories (1) Custome Extensions (1) Custome Extensions (1) Custome Categories (2) Condo Source Categories (3) Group Links (38) Group Links (38) Group Types (1)	nediale complex attacks across endpoint, email, dual visualizations for Network and Endpoint by Installed By: admin Installed Date: May 16, 2019 Version: 1.3.0 rted Languages: unp.US Signed: Signed: Signed: Contact the extension's author (support@symantec.com)	Installed	Symantec Support	May 16, 2
fotal: 6	< 1 ►			0 25 50 Al



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

■ IBM QRadar		Ļ	
Admin System Configuration Admin System Configuration Data Sources Remote Networks and Services Configuration YApp Risk Manager Ophida Adsistant Adminger Proofpoint OnDemand Email Security TruSTAR Application Symantec EDR	y Cetting Techol Activity Jose Papers Techol Violations Product Use Data Synamics EDI University Synamics EDR Synamics App Settings Synamics App Settings	-yuun ire	

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: <u>https://help.symantec.com/cs/symantecedr 4.1/EDR/v118551314 v130949130/Generating-an-OAuth-client?locale=EN_US</u>

Symenlec EDR	Configurations		
New			
	EDR Server URL		×
	L'assword	Provide in client_accel remain	
	Seve		

Figure 11: EDR Configurations

Figure 12: EDR Instance Details

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

vice Name:	Symantec ATP		
r Role:	Admin 🔻		
urity Profile:	Admin 🔻		
oiry Date:	8/20/2018	r / INo Expiry	
			Cancel Create Service

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

	Enable	Start Time(in UTC)		Interva
Events		16-05-2019 13:56:26	(dd-mm-yyyy HH:MM:SS)	5 min
Incidents	0	16-05-2019 13:56:26	(dd-mm-yyyy HH:MM:SS)	5 min
Incident Events		16-05-2019 13:56:26	(dd-mm-yyyy HH:MM:SS)	5 min
Authorization To	ken			
Go to Admin> Auti	horized Serv	ices to generate new token		

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

Troubleshooting

This chapter includes the following topics:

<u>Troubleshooting</u>

o <u>Case #1 – Symantec EDR events are shown up as SymantecATPCustom</u> events

- <u>Case #2</u> <u>Symantec EDR App configuration fails with various error messages</u>
- <u>Case #3</u> <u>Symantec EDR events are coming as unknown</u>
- <u>Case #4</u> <u>–</u> <u>Symantec EDR data is not getting</u>

collected

- o Case #5 Symantec EDR UI related issues
- Case #6 Re installation of the app
- <u>Case #7</u> <u>All other issues which are not part of the document</u>

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

SymantecATPCustom Message Symantec ATP SymantecATPCustom Message Symantec ATP
SymantecATPCustom Message Symantec ATP
SymantecATPCustom Message Symantec ATP
SymantecATPCustom Message Symantec ATP

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:

the Collinson	 System Settings 			
stem Settings	Administrative Email Address	root@localhost		
atabase Settings	Alert Email From Address	QRADAR@localhost.localdoma	QRADAR@localhost.localdomain	
iel Database Settings	Email Locale	English	*	
ansaction Sentry Settings	Max Email Attachment Size (KB)	15,360	-	
	Delete Root Mail	Yes	-	
MP Settings	Temporary Files Retention Period	6 hours	-	
nbedded SNMP Daemon	Asset Profile Query Period	1 day(default)	-	
aungs	Coalescing Events	Yes	Ψ.	
MAP Client/Server Settings	Store Event Payload	Yes	*	
set Profile Settings	Global Iptables Access (comma separated)			
onsole Settings	Syslog Event Timeout (minutes)	720	-	
ansore octaings	Partition Testers Timeout (seconds)	30	-	
uthentication Settings	Max UDP Syslog Payload Length	1,024	-	
NS Settings	Max TCP Syslog Payload Length	4096	-	
INS Settings	Max Number of TCP Syslog Connections	2,500	÷	
	Max TCP Syslog Connections Per Host	10	*	
eporting Settings	Timeout for Idle TCP Syslog Connections (seconds)	900	-	
ata Export Settings	Log and Network Activity Data Export Temporary Directory	/store/exports		
Flow Settings	Display Country/Region Flags	Yes	*	
shuark Incidete Cattinge	 Display Embedded Maps in IP Address Tooltips 	Yes	*	
	Enable X-Force Threat Intelligence Feed	No	*	
Switch to:	Database Settings			
Basic	User Data Files	/store/users/		
	Accumulator Retention - Minute-by-Minute	1 week (default)	*	
	Accumulator Retention - Hourly	33 days (default)	*	

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.

Fail: API server is alre	ady configured				
Symantec EDR	Configurations				
New					
EDR Servers					
delete					

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

Fail: API URL/Password is invalid or connection issue					
Symantec EDR Configurations					
New					
EDR Servers					
delete					
	_				

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