

EPM Configuration

Steps to obtain an integration with QRadar:

1). User id and password to the EPM tenant – this needs to be fill into the xml parameter file.

2). There are 3 log source type:

EPM – EPM aggregated events

EPM-AdminAudit1 – EPM admin audit

EPM-Policy – EPM aggregated policy audits

QRadar Log Source Configuration

To ingest data from the EPM event log using Universal Rest API Protocol, configure a log source on the QRadar® Console using the Workflow provided.

Make sure to install the **EPM DSM Extension** from the IBM App Exchange beforehand. If you don't, you won't find *EPM* in the Log Source Types and will not be able to correctly parse the events.

Also, make sure to have the **QRadar Universal Cloud REST API protocol** available on your QRadar® deployment. This is a Log Source you can obtain from the IBM Fix Central, and it comes in RPM form you need to install and deploy. You can find an updated fix, as the time of writing, for [QRadar 7.4 on this link](#)

1. Log in to QRadar.
2. Go to the admin panel, click on the *QRadar Log Source Management* app icon.
3. Click *New Log Source* > Single Log Source.
4. On the *Select Log Source Type* page, select *EPM*, and go to Step 2.
5. On the *Select Protocol Type* page, select *Universal Cloud REST API*, and go to Step 3.
6. On the Configure the Log Source parameters page, configure the log source parameters:
 - Insert a name for this log source (*EPM Events Log Source*);
 - For the field *Extension*, select *EPMCustom_ext*;
 - Disable *Coalescing Events* to make sure every event is reported each time;
7. On the Configure the Protocol Parameters page, configure:
 - Insert a log source identifier (*epm_events*);
 - Copy the Workflow XML you downloaded from Github and paste it into the *Workflow* field;

Epm-AggregatedEvents.xml – for EPM Events

Epm-AggregatedPolicy.xml – for EPM Policy Audit

Epm-AdminAudits.xml – for Epm Admin Audits

- Copy the EPM-Workflow-Parameter-Values.xml (make sure your username and password are populated) into the *Workflow Parameters Values* field;
- Set *1440M* as the Recurrence for daily - 24 hrs or 60M for hourly

8. In the Test protocol parameters window, click *Start Test*. All tests should pass.

- Test events in this part may or may not be present, based on your activity on the EPM tenant

9. To fix any errors, click *Configure Protocol Parameters*. Configure the parameters and click Test Protocol Parameters.

10. Click *Finish*

11. Do a full configuration deploy (**Deploy Changes -> Advanced -> Deploy Full Configuration**)

12. Repeat this process if you need to add EPM admin audit(EPMAdminAudit1Custom_ext) or EPM aggregated policy audit(EPMPolicyCustom_ext)

Troubleshooting

You can extract the debug run of the workflow from /var/log/qradar.log into a file and share the file with Cyberark support. Each workflow has a specific prefix for logging.

For event workflow:

```
grep "EPM::AggEvent" qradar.log > aggevent.log
```

For policy workflow:

```
grep "EPM:AggPolicy" qradar.log > aggpolicy.log
```

For admin audit workflow:

```
grep "EPM::AdminAudit" qradar.log > aggaudit.log
```

You can also grep on the EPM:: prefix to capture logs for all 3 workflows. Here is a sample where the password was changed in EPM but not reflected in the workflow parameter xml file in Qradar.

```
[root@host-1 log]# grep "EPM::" qradar.log
```

Mar 26 13:50:37 ::ffff:10.0.0.1 [ecs-ec-ingress.ecs-ec-ingress] [Thread-165] com.q1labs.semsources.sources.universalcloudrestapi.v1.workflow.action.LogAction: [INFO] [NOT:0000006000][10.0.0.1/- -] [-/- -]
JEPM::AdminAudit - The EPM Bookmark value was 1679466638733 : 2023-03-22T06:30:38.733Z

Mar 26 13:50:40 ::ffff:10.0.0.1 [ecs-ec-ingress.ecs-ec-ingress] [Thread-165] com.q1labs.semsources.sources.universalcloudrestapi.v1.workflow.action.LogAction: [INFO] [NOT:0000006000][10.0.0.1/- -] [-/- -]
JEPM::AdminAudit - Abort - Login fail, check userid and password.

Mar 26 13:52:23 ::ffff:10.0.0.1 [ecs-ec-ingress.ecs-ec-ingress] [Thread-170] com.q1labs.semsources.sources.universalcloudrestapi.v1.workflow.action.LogAction: [INFO] [NOT:0000006000][10.0.0.1/- -] [-/- -]
JEPM::AggEvent - The EPM Bookmark value was 1679466723151 : 2023-03-22T06:32:03Z

Mar 26 13:52:23 ::ffff:10.0.0.1 [ecs-ec-ingress.ecs-ec-ingress] [Thread-171] com.q1labs.semsources.sources.universalcloudrestapi.v1.workflow.action.LogAction: [INFO] [NOT:0000006000][10.0.0.1/- -] [-/- -]
JEPM::AggPolicy - The EPM Bookmark value was 1679466723143 : 2023-03-22T06:32:03Z

Mar 26 13:52:25 ::ffff:10.0.0.1 [ecs-ec-ingress.ecs-ec-ingress] [Thread-170] com.q1labs.semsources.sources.universalcloudrestapi.v1.workflow.action.LogAction: [INFO] [NOT:0000006000][10.0.0.1/- -] [-/- -]
JEPM::AggEvent - Abort - Login fail, check userid and password.

Mar 26 13:52:25 ::ffff:10.0.0.1 [ecs-ec-ingress.ecs-ec-ingress] [Thread-171] com.q1labs.semsources.sources.universalcloudrestapi.v1.workflow.action.LogAction: [INFO] [NOT:0000006000][10.0.0.1/- -] [-/- -]
JEPM::AggPolicy - Abort - Login fail, check userid and password.

Known issue and limitation:

1). Once the data is pulled into QRadar, you can write custom search view of the data. Here is a sample arranging the view with specific EPM attributes. Or you can use the out of the box normalized view. Writing custom search is out of the scope of this app and it's the job of the QRadar admin.

IBM QRadar

Dashboard

Offenses

Log Activity

Network Activity

Assets

Reports

Risks

Vulnerabilities

Admin

Pulse

System Time: 5:57 PM

Search...

Quick Searches

Add Filter

Save Criteria

Save Results

Cancel

False Positive

Rules

Actions

Advanced Search

Search

Start Time

3/18/2023

5:56 PM

End Time

3/21/2023

5:56 PM

Update

View:

Select An Option:

Display:

Custom

Results Limit

1,000

Completed

Current Filters:

Log Source Type is EPM-AdminAudit1

Clear Filter

Current Statistics

Total Results

2,329 (775.3KB Total)

Compressed Data Files Searched

0 (0B Total)

Duration

81ms

Data Files Searched

75 (161.2MB Total)

Index File Count

190 (17.9MB Total)

More Details

Records Matched Over Time

Reset Zoom

3/18/23, 5:56 PM - 3/21/23, 5:56 PM

Update Details

(Hide Charts)

Event Name	Description (custom)	LoggedAt (custom)	LoggedFrom (custom)	Log Source	Event Count	Start Time	Source IP	Username	Magnitude	Role (custom)
API Get	API Get Admin audit data /API/Sets/...	2023-03-21T07:08:20.907Z	...	Z-EPMADMINAUDIT1-LOG	1	Mar 21, 2023, 4:08:29 AM	...	epmdev@gmail.com	...	SetAdmin
API Get	API Get Admin audit data /API/Sets/...	2023-03-21T07:08:20.907Z	...	Z-EPMADMINAUDIT1-LOG	1	Mar 21, 2023, 4:08:29 AM	...	epmdev@gmail.com	...	SetAdmin
API Get	API Get Policy Audit Aggregations /...	2023-03-21T07:08:55.53Z	...	Z-EPMADMINAUDIT1-LOG	1	Mar 21, 2023, 4:08:29 AM	...	epmdev@gmail.com	...	SetAdmin
API Get	API Get Events Aggregations /API/S...	2023-03-21T07:08:54.92Z	...	Z-EPMADMINAUDIT1-LOG	1	Mar 21, 2023, 4:08:29 AM	...	epmdev@gmail.com	...	SetAdmin
API Get	API Get events raw details /API/Set...	2023-03-21T07:31:37.1Z	...	Z-EPMADMINAUDIT1-LOG	1	Mar 21, 2023, 4:08:29 AM	...	epmdev@gmail.com	...	SetAdmin
API Get	API Get events raw details /API/Set...	2023-03-21T08:01:36.95Z	...	Z-EPMADMINAUDIT1-LOG	1	Mar 21, 2023, 4:08:29 AM	...	epmdev@gmail.com	...	SetAdmin
API Get	API Get events raw details /API/Set...	2023-03-21T07:46:37.44Z	...	Z-EPMADMINAUDIT1-LOG	1	Mar 21, 2023, 4:08:29 AM	...	epmdev@gmail.com	...	SetAdmin
API Get	API Get events raw details /API/Set...	2023-03-21T07:16:37.24Z	...	Z-EPMADMINAUDIT1-LOG	1	Mar 21, 2023, 4:08:29 AM	...	epmdev@gmail.com	...	SetAdmin
API Get	API Get Events Aggregations /API/S...	2023-03-21T07:08:54.92Z	...	Z-EPMADMINAUDIT1-LOG	1	Mar 21, 2023, 4:08:29 AM	...	epmdev@gmail.com	...	SetAdmin
API Get	API Get Events Aggregations /API/S...	2023-03-21T07:08:54.92Z	...	Z-EPMADMINAUDIT1-LOG	1	Mar 21, 2023, 4:08:28 AM	...	epmdev@gmail.com	...	SetAdmin
API Get	API Get Admin audit data /API/Sets/...	2023-03-21T07:08:20.907Z	...	Z-EPMADMINAUDIT1-LOG	1	Mar 21, 2023, 4:08:28 AM	...	epmdev@gmail.com	...	SetAdmin
API Get	API Get Policy Audit Aggregations /...	2023-03-21T07:08:55.53Z	...	Z-EPMADMINAUDIT1-LOG	1	Mar 21, 2023, 4:08:28 AM	...	epmdev@gmail.com	...	SetAdmin
API Get	API Get Admin audit data /API/Sets/...	2023-03-21T07:08:20.907Z	...	Z-EPMADMINAUDIT1-LOG	1	Mar 21, 2023, 4:08:28 AM	...	epmdev@gmail.com	...	SetAdmin

Displaying 1 to 40 of 1000 items (Elapsed time: 0:00:00.096)

Page: 1

1 2 3 ... 25

Page 4 of 7

761 words

Accessibility: Unavailable

Focus

Search... Quick Searches Add Filter Save Criteria Save Results Cancel False Positive Rules Actions

Advanced Search

Search

Start Time 3/19/2023 2:15 PM End Time 3/26/2023 2:15 PM Update

View: Select An Option Display: Custom Results Limit 1,000

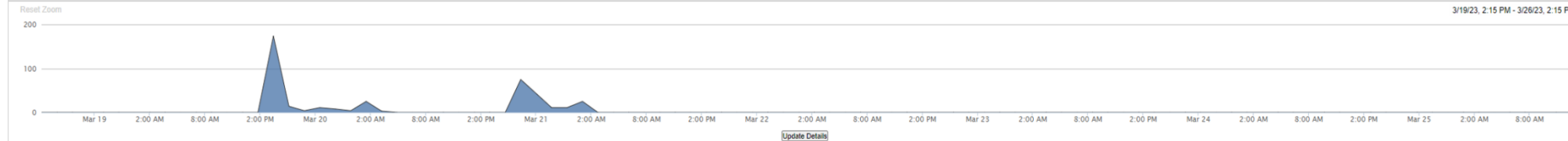
Using Search: EventView1

Current Filters: Log Source Type is EPM (Clear Filter)

Current Statistics

Total Results 400 (731.2KB Total) Compressed Data Files Searched 0 (0B Total) Duration 59ms
Data Files Searched 82 (167.7MB Total) Index File Count 191 (177MB Total) More Details

Records Matched Over Time



Update Details

(Hide Charts)

arrivalTime (custom)	Event Name	lastEventDisplayName (custom)	Log Source	Event Count	Start Time	publisher (custom)	Username	Magnitude	applicationType (custom)	lastEventSourceName (custom)	hash (custom)
2023-03-20T14:35:06.452Z	Access restricte...	update-apps ps1	Z-1...	1	Mar 20, 2023, 11:32:04 AM	Amazon.com, Inc.	NT AUTHORITY\SYSTEM		Script	Windows PowerShell (powershell.exe)	SHA1#...
2023-03-20T09:17:27.576Z	Launch	Microsoft Malware Protection Command Line Utility (MpCmdRun.exe)	Z-1...	1	Mar 20, 2023, 11:32:04 AM	Microsoft Windows Publisher	NT AUTHORITY\SYSTEM		Executable	Updater (Windows Update)	SHA1#...
2023-03-20T13:43:18.466Z	Launch	ptUpdate (ptUpdate.exe)	Z-1...	1	Mar 20, 2023, 11:32:04 AM	Cisco WebEx LLC	CYBERARKLAB\ran		Executable	Old Application	SHA1#...
2023-03-20T13:43:23.954Z	Access restricte...	ptUpdate (ptUpdate.exe)	Z-1...	1	Mar 20, 2023, 11:32:04 AM	Cisco WebEx LLC	CYBERARKLAB\ran		Executable	Old Application	SHA1#...
2023-03-20T13:17:48.823Z	Launch	Google Crash Handler (GoogleCrashHandler64.exe)	Z-1...	1	Mar 20, 2023, 11:32:04 AM	Google LLC	NT AUTHORITY\SYSTEM		Executable	Updater (Google Updater)	SHA1#...
2023-03-20T09:17:57.538Z	Launch	Google Installer (GoogleUpdate.exe)	Z-1...	1	Mar 20, 2023, 11:32:04 AM	Google LLC	NT AUTHORITY\SYSTEM		Executable	Old Application	SHA1#...
2023-03-20T13:17:48.855Z	Launch	Google Crash Handler (GoogleCrashHandler.exe)	Z-1...	1	Mar 20, 2023, 11:32:04 AM	Google LLC	NT AUTHORITY\SYSTEM		Executable	Updater (Google Updater)	SHA1#...
2023-03-20T08:19:10.316Z	Launch	Microsoft Office Click-to-Run (SxS) (OfficeClickToRun.exe)	Z-1...	1	Mar 20, 2023, 11:32:04 AM	Microsoft Corporation	CYBERARKLAB\ran		Executable	ClickToRunSvc - Microsoft Office Click-t...	SHA1#...
2023-03-20T08:18:39.72Z	Launch	Microsoft Office Click-to-Run (SxS) (OfficeClickToRun.exe)	Z-1...	1	Mar 20, 2023, 11:32:04 AM	Microsoft Corporation	NT AUTHORITY\SYSTEM		Executable	ClickToRunSvc - Microsoft Office Click-t...	SHA1#...
2023-03-20T13:43:23.957Z	Access to the m...	ptUpdate (ptUpdate.exe)	Z-1...	1	Mar 20, 2023, 11:32:04 AM	Cisco WebEx LLC	CYBERARKLAB\ran		Executable	Old Application	SHA1#...
2023-03-20T05:47:04.064Z	Launch	XProtect (XProtectRemediatorPrint)	Z-1...	1	Mar 20, 2023, 11:31:36 AM	Software Signing	.peter		MacExecutable	/Library/Apple/System/Library/CoreServ...	SHA1#...
2023-03-20T05:47:04.064Z	Launch	XProtect (XProtectRemediatorDubRobber)	Z-1...	1	Mar 20, 2023, 11:31:36 AM	Software Signing	.peter		MacExecutable	/Library/Apple/System/Library/CoreServ...	SHA1#...
2023-03-20T05:47:04.058Z	Launch	TVCacheExtension (TVCacheExtension)	Z-1...	1	Mar 20, 2023, 11:31:36 AM	Software Signing	.peter		MacExecutable	/System/Applications/TV app/Contents/...	SHA1#...
2023-03-20T05:47:04.057Z	Launch	MailCacheDelete (MailCacheDelete)	Z-1...	1	Mar 20, 2023, 11:31:36 AM	Software Signing	.peter		MacExecutable	/System/Applications/Mail.app/Contents...	SHA1#...
2023-03-20T05:47:04.06Z	Launch	XProtect (XProtectRemediatorTrov)	Z-1...	1	Mar 20, 2023, 11:31:36 AM	Software Signing	.peter		MacExecutable	/Library/Apple/System/Library/CoreServ...	SHA1#...
2023-03-20T05:47:04.057Z	Launch	XProtect (XProtectRemediatorGreenAcre)	Z-1...	1	Mar 20, 2023, 11:31:36 AM	Software Signing	.peter		MacExecutable	/Library/Apple/System/Library/CoreServ...	SHA1#...
2023-03-20T05:47:34.031Z	Launch	XProtect (XProtectRemediatorVatenNet)	Z-1...	1	Mar 20, 2023, 11:31:36 AM	Software Signing	.peter		MacExecutable	/Library/Apple/System/Library/CoreServ...	SHA1#...
2023-03-20T05:46:34.515Z	Launch	XProtect (XProtectRemediatorEicar)	Z-1...	1	Mar 20, 2023, 11:31:36 AM	Software Signing	.peter		MacExecutable	/Library/Apple/System/Library/CoreServ...	SHA1#...
2023-03-20T05:47:04.061Z	Launch	CacheDeleteExtension (CacheDeleteExtension)	Z-1...	1	Mar 20, 2023, 11:31:36 AM	Software Signing	.peter		MacExecutable	/System/Volumes/Preboot/Cryptexes/Ap...	SHA1#...
2023-03-20T05:47:04.057Z	Launch	MusicCacheExtension (MusicCacheExtension)	Z-1...	1	Mar 20, 2023, 11:31:36 AM	Software Signing	.peter		MacExecutable	/System/Applications/Music.app/Conten...	SHA1#...
2023-03-20T15:30:58.318Z	Launch	Skype	Z-1...	1	Mar 20, 2023, 11:31:36 AM	Skype	CYBRJohn		Win8App	Windows App	SHA1#...
2023-03-20T14:28:56.192Z	Launch	COM Surrogate (dlhost.exe)	Z-1...	1	Mar 20, 2023, 11:31:36 AM	Microsoft Windows	NT AUTHORITY\NETWORK SERVICE		Executable	Microsoft Windows	SHA1#...
2023-03-20T14:28:56.186Z	Launch	Notepad++ (notepad++.exe)	Z-1...	1	Mar 20, 2023, 11:31:36 AM	Notepad++	CYBRJohn		Executable	Notepad++ (npp.8.4.8.Installer.x64.exe)	SHA1#...
2023-03-20T12:45:22.719Z	Installation	Rmepg.exe	Z-1...	1	Mar 20, 2023, 11:31:36 AM	N/A	CYBRJohn		Executable	Internet (CamStudio Portable)	SHA1#...
2023-03-20T12:45:22.71Z	Installation	CamStudio Player Classic (Player.exe)	Z-1...	1	Mar 20, 2023, 11:31:36 AM	N/A	CYBRJohn		Executable	Internet (CamStudio Portable)	SHA1#...
2023-03-20T12:45:22.719Z	Installation	CamStudio PlayerPlus (PlayerPlus.exe)	Z-1...	1	Mar 20, 2023, 11:31:36 AM	N/A	CYBRJohn		Executable	Internet (CamStudio Portable)	SHA1#...
2023-03-20T12:45:22.704Z	Installation	CamCommandLine.exe	Z-1...	1	Mar 20, 2023, 11:31:36 AM	N/A	CYBRJohn		Executable	Internet (CamStudio Portable)	SHA1#...
2023-03-20T12:44:52.483Z	Ransomware	CamStudio Portable (CamStudioPortable_2.7.4_English.pat.exe)	Z-1...	1	Mar 20, 2023, 11:31:36 AM	Rare Ideas LLC	CYBRJohn		Executable	https://download2.portableapps.com/por...	SHA1#...

Search... Quick Searches Add Filter Save Criteria Save Results Cancel False Positive Rules Actions

Advanced Search

Start Time 3/19/2023 2:15 PM End Time 3/26/2023 2:15 PM Update

View: Select An Option: Display: Username Results Limit 1,000

Grouping By:

Username

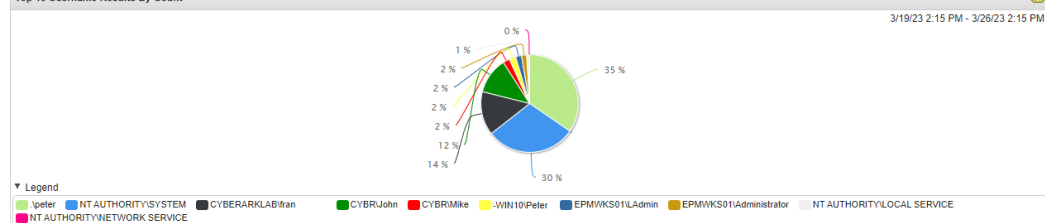
Original Filters:

Log Source Type is EPM (Clear Filter)

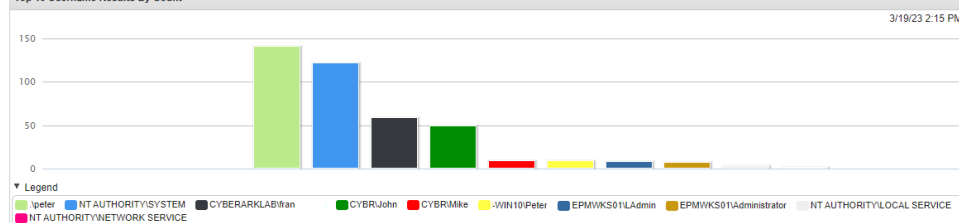
Current Statistics

Total Results 408 (9928 Total) Compressed Data Files Searched Subsearch (No Compressed Data Files) Duration 954ms
Data Files Searched Subsearch (No Data Files) Index File Count Subsearch (No Index Files) More Details

Top 10 Username Results By Count



Top 10 Username Results By Count



(Hide Charts)

Username	Source IP (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Event Name (Unique Count)	Log Source (Unique Count)	Low Level Category (Unique Count)	Proto (Unique Count)	Magnitude (Maximum)	Event Count (Sum)	Count
.jpeter	10.0.0.1	10.0.0.1	0	Launch	Z - IBM QRADAR EPM Events Plugin	Misc Application Action Allowed	Other	5	141	
NT AUTHORITY\SYSTEM	10.0.0.1	10.0.0.1	0	Multiple (5)	Z - IBM QRADAR EPM Events Plugin	Multiple (4)	Other	6	122	
CYBERARKLAB\fran	10.0.0.1	10.0.0.1	0	Multiple (4)	Z - IBM QRADAR EPM Events Plugin	Multiple (3)	Other	6	59	
CYBRJohn	10.0.0.1	10.0.0.1	0	Multiple (5)	Z - IBM QRADAR EPM Events Plugin	Multiple (5)	Other	6	49	
CYBRMike	10.0.0.1	10.0.0.1	0	Multiple (4)	Z - IBM QRADAR EPM Events Plugin	Multiple (4)	Other	6	9	
WIN10\Peter	10.0.0.1	10.0.0.1	0	Multiple (7)	Z - IBM QRADAR EPM Events Plugin	Multiple (6)	Other	7	9	
EPMWKS01\Admin	10.0.0.1	10.0.0.1	0	Multiple (3)	Z - IBM QRADAR EPM Events Plugin	Multiple (3)	Other	6	8	
EPMWKS01\Administrator	10.0.0.1	10.0.0.1	0	Launch	Z - IBM QRADAR EPM Events Plugin	Misc Application Action Allowed	Other	5	7	
NT AUTHORITY\LOCAL SERVICE	10.0.0.1	10.0.0.1	0	Launch	Z - IBM QRADAR EPM Events Plugin	Misc Application Action Allowed	Other	5	3	
NT AUTHORITY\NETWORK SERVICE	10.0.0.1	10.0.0.1	0	Launch	Z - IBM QRADAR EPM Events Plugin	Misc Application Action Allowed	Other	5	1	

2). Unknown data payload – sometimes the data is not parsed correctly due to DSM parser didn't categorize the data properly. This is not normal. Please double click on the unknown event and copy out the payload and report it to CyberArk support team so it can corrected.

Search... Quick Searches Add Filter Save Criteria Save Results Cancel False Positive Rules Actions

Advanced Search

Start Time 3/18/2023 5:56 PM End Time 3/21/2023 5:56 PM Update

View: Select An Option Display: Event Name Results Limit 1,000

Grouping By:
Event Name

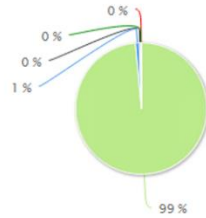
Original Filters:
Log Source Type is EPM-AdminAudit1 (Clear Filter)

Current Statistics

Total Results 1,000 (5266 Total) Compressed Data Files Searched Subsearch (No Compressed Data Files) Duration 14ms
Data Files Searched Subsearch (No Data Files) Index File Count Subsearch (No Index Files) More Details

Top 10 Event Name Results By Count

3/18/23 5:56 PM - 3/21/23 5:56 PM



Legend

API Get View WebPage Agent Action Unknown Policy action

Top 10 Event Name Results By Count

3/18/23 5:56 PM - 3/21/23 5:56 PM



Legend

API Get View WebPage Agent Action Unknown Policy action

(Hide Charts)

Event Name	Source IP (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Log Source (Unique Count)	Low Level Category (Unique Count)	Protocol (Unique Count)	Username (Unique Count)	Magnitude (Maximum)	Event Count (Sum)	Count
API Get	Multiple (3)	10.0.0.1	0	Z-EPMADMINAUDIT1-LOG	Command Execution Success	Other	Multiple (2)	4	986	
View WebPage	10.0.0.1	10.0.0.1	0	Z-EPMADMINAUDIT1-LOG	Command Execution Success	Other		3	9	
Agent Action	10.0.0.1	10.0.0.1	0	Z-EPMADMINAUDIT1-LOG	Command Execution Success	Other		5	3	
Unknown	10.0.0.1	10.0.0.1	0	Z-EPMADMINAUDIT1-LOG	Unknown	Other		3	1	
Policy action	10.0.0.1	10.0.0.1	0	Z-EPMADMINAUDIT1-LOG	Command Execution Success	Other		5	1	