

The logo for QLEAN features a stylized 'Q' on the left, composed of two overlapping curved segments in shades of blue and purple. To the right of the 'Q' is the word 'LEAN' in a bold, dark blue, sans-serif font.

QLEAN

Use Cases

USER STORY : DAILY HEALTH CHECK

As a platform administrator, I would like to have a dashboard or a list of steps to be performed in QLEAN App in order to perform a quick health check of the system during daily routines

Task 1. Review Managed Hosts metrics

OBJECTIVES

Identify deployment problems, performance issues, data loss risks

WHERE TO FIND

QRadar UI	Managed Hosts
Excel report	DPT Hosts

The screenshot displays the QLEAN interface for monitoring QRadar hosts. The main table lists host details, and three sub-tables show disk usage for specific hosts.

IP Address	HA IP Address	Hostname	HA host role	Console	Host status	Uptime in days	Avg CPU load, %	Total RAM, Mb	Free RAM, %	Total /store space	Free /store space, %	Disk usage alert	Appliance type
10.100.202.115	10.100.202.115	soce01.acme.com	Primary		Offline								N/A
10.153.101.14	10.153.101.13	socep01-primary.acme.com	Primary		Standby	160	0	64253	62.50%	N/A	N/A		1624
10.153.101.12	10.153.101.13	socep01-secondary.acme.com	Secondary		Active	277	50	64253	30.6%	15.8TB	28.9%		500
10.100.202.36	10.100.202.36	socfp01.acme.com	Primary		Active	277	0	64254	31.4%	15.7TB	69.0%	/var/log:92%	1724
10.100.202.20	10.100.202.20	socmcp.acme.com	Primary	Yes	Active	75	350	64254	5.9%	15.7TB	94.5%		3124
10.100.202.22	10.100.202.22	SOCQN01.acme.com	Primary		Active	276	250	63700	74.9%	82.7GB	80.3%		6300

Disk usage socep01-secondary.acme.com			socfp01.acme.com			socmcp.acme.com		
Mount point	Size	Usage	Mount point	Size	Usage	Mount point	Size	Usage
/	7.3GB	30%	/	7.3GB	30%	/	7.3GB	50%
/dev	31.4GB	0%	/dev	31.4GB	0%	/dev	31.4GB	0%
/dev/shm	31.4GB	0%	/dev/shm	31.4GB	0%	/dev/shm	31.4GB	0%
/run	31.4GB	11%	/run	31.4GB	11%	/run	31.4GB	11%
/sys/fs/cgroup	31.4GB	0%	/sys/fs/cgroup	31.4GB	0%	/sys/fs/cgroup	31.4GB	0%
/boot	1014.0MB	16%	/boot	1014.0MB	16%	/boot	1014.0MB	16%
/boot/efi	99.8MB	16%	/home	597.7MB	6%	/home	597.7MB	32%
/storetmp	9.9GB	62%	/var	2.9GB	5%	/opt	7.3GB	77%
/opt	7.3GB	69%	/storetmp	10.0GB	40%	/var	2.9GB	20%
/tmp	1.8GB	29%	/boot	1014.0MB	16%	/storetmp	10.0GB	56%
/var	2.9GB	6%	/tmp	1.8GB	29%	/recovery	5.1GB	78%
/home	597.7MB	6%	/opt	7.3GB	69%	/tmp	1.8GB	14%
/var/log	8.3GB	15%	/var/log	8.3GB	92%	/var/log	8.3GB	23%
/var/log/audit	1.7GB	5%	/var/log/audit	1.7GB	5%	/var/log/audit	1.7GB	20%
/transient	1.8TB	1%	/store	15.7TB	33%	/store	15.7TB	6%
/store	15.8TB	72%	/run/user/0	6.3GB	0%	/run/user/0	6.3GB	0%
/run/user/0	6.3GB	0%						

ITEMS TO CHECK

- Host status
- CPU load
- /store partition utilization
- Disk space alerts

Task 2. Review System Notifications

OBJECTIVES

Explore alerts automatically generated by the system

WHERE TO FIND

QRadar UI	Last Warnings and Errors from System Notifications
Excel report	DPT Health: Last Warnings and Errors from System Notifications

Last warnings and errors from System Notification		
IP address	Date	Description
10.100.202.20	2018-09-04 20:45:09.765	Unable to determine associated log source for IP address <asmddb2>. Unable to automatically detect the associated log source for IP address.
10.100.202.20	2018-09-04 19:50:26.919	Failed to auto-register WinCollect client on DPSNPS23.
10.100.202.20	2018-09-04 18:49:23.222	System load over 1 minute has an average of 5.7 over the past 1 intervals, and has exceeded the configured threshold of 5.4. To resolve: If your system continues to exhibit th
10.100.202.20	2018-09-04 17:15:33.996	Unable to determine associated log source for IP address <192.168.45.43>. Unable to automatically detect the associated log source for IP address.
10.100.202.20	2018-09-04 15:04:51.237	System load over 15 minutes has an average of 4.0 over the past 1 intervals, and has exceeded the configured threshold of 3.9. To resolve: If your system continues to exhibit
10.100.202.20	2018-09-04 13:03:42.615	Average time in ms for I/O requests for device sdb has an average of 620.2 over the past 1 intervals, and has exceeded the configured threshold of 500.0. To resolve: If your sy
10.100.202.20	2018-09-04 10:49:35.769	License 'QRadar Forensics' is allocated to host 'socmcp' but is expired.
10.100.202.20	2018-09-04 08:32:13.867	Raid Controller Misconfiguration - Hardware Monitoring has determined that a virtual drive is misconfigured and local storage performance may be negatively impacted - Wr
10.100.202.20	2018-09-04 02:37:07.324	Unable to determine associated log source for IP address <172.20.16.50>. Unable to automatically detect the associated log source for IP address.
10.100.202.20	2018-09-04 01:09:23.596	Cancelled 1 TX activities with pid=27009 on host 10.10.250.166 (loop 943)

ITEMS TO CHECK:

- Performance degradation
- Rule parsing issues
- Misconfiguration
- Etc.

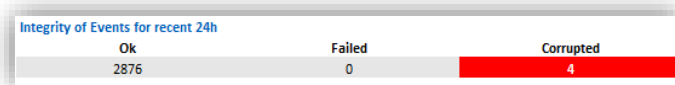
Task 3. Review Data Integrity

OBJECTIVES

Make sure the collected data is intact

WHERE TO FIND

QRadar UI	Misc Health: Integrity of Events/Flows for recent 24h
Excel report	DPT Health: Integrity of Events/Flows for recent 24h



ITEMS TO CHECK:

- Failed or corrupted hashes

Task 4. Review Backup status

OBJECTIVES

Inspect automatic backups state

WHERE TO FIND

QRadar UI	Misc Health: Recent Backups
Excel report	DPT Health: Recent Backups

Date	Hostname	Type	Status	Size, MB
09_09_2018	10.100.202.20	config	SUCCESS	6889
08_09_2018	10.100.202.20	config	SUCCESS	6890
07_09_2018	10.100.202.20	config	SUCCESS	6895
06_09_2018	10.100.202.20	config	SUCCESS	6902
05_09_2018	10.100.202.20	config	SUCCESS	6911

ITEMS TO CHECK:

- Failed backups

Task 5. Review EPS Anomalies

OBJECTIVES

Examine what is causing EPS spikes and events being dropped or sent directly to storage

WHERE TO FIND

QRadar UI	EPS Anomalies
Excel report	ENV EPS ALERTS

Detected anomalies

Date 2023-02-02 14:31:24
Type Spike
Event Processor socep01

Log Source LinuxServer @ infoblox.localdomain

Event Name	EPS	Event Count
Process Created	672	403728
Command Execution - Execve Event	1	882
User space user has logged out	0	2
Process Creation Failed	0	45
User shell command and args	0	1
User space authentication	0	7
Audit Event	0	49
User space authentication failed	0	1
User space session start	0	51
User space user has logged in	0	2
User space session end	0	34

Log Source PaSeries @ SACMEPANDGWY-B

Event Name	EPS	Event Count
Traffic End	417	250795
Reset Both	23	14015
FileType Detected	2	1310
Session Allowed	1	626

ITEMS TO CHECK:

- EPS spikes
- Event drops
- Involved Log Sources
- Top frequent events

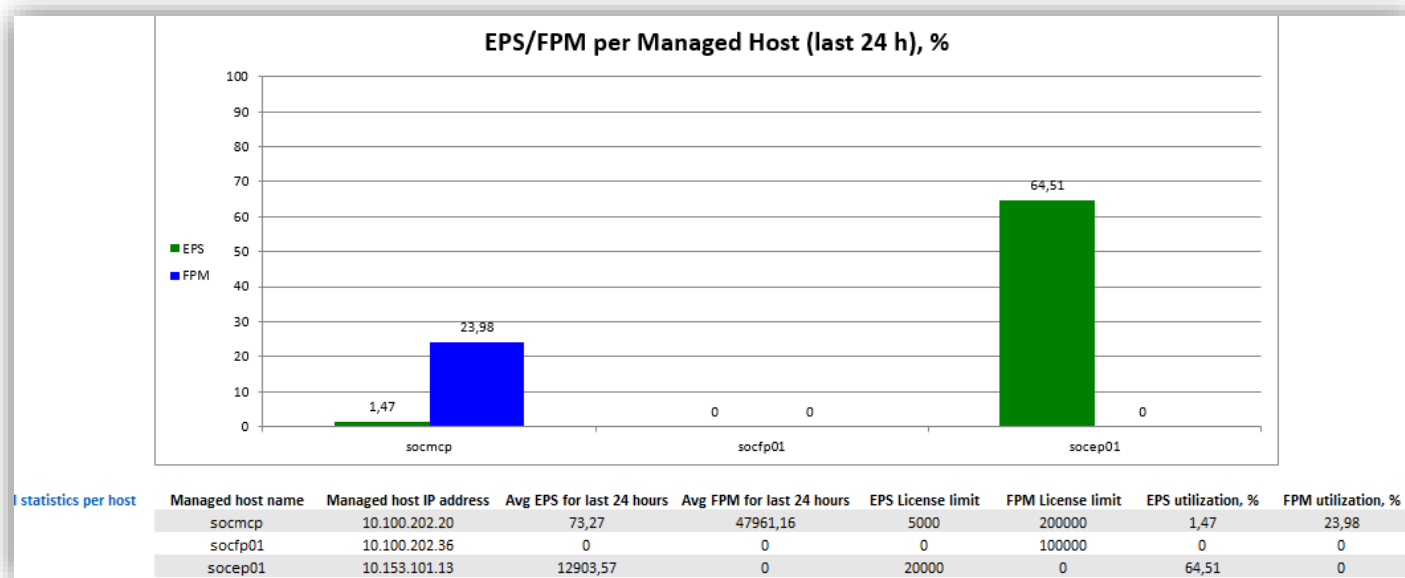
Task 6. Review EPS consumption

OBJECTIVES

Verify EPS/FPM license utilization across the deployment, reconsider license allocation

WHERE TO FIND

QRadar UI	EPS/FPM per Managed Host
Excel report	ENV EPS



ITEMS TO CHECK:

- Average EPS per host
- Average FPM per host
- License utilization

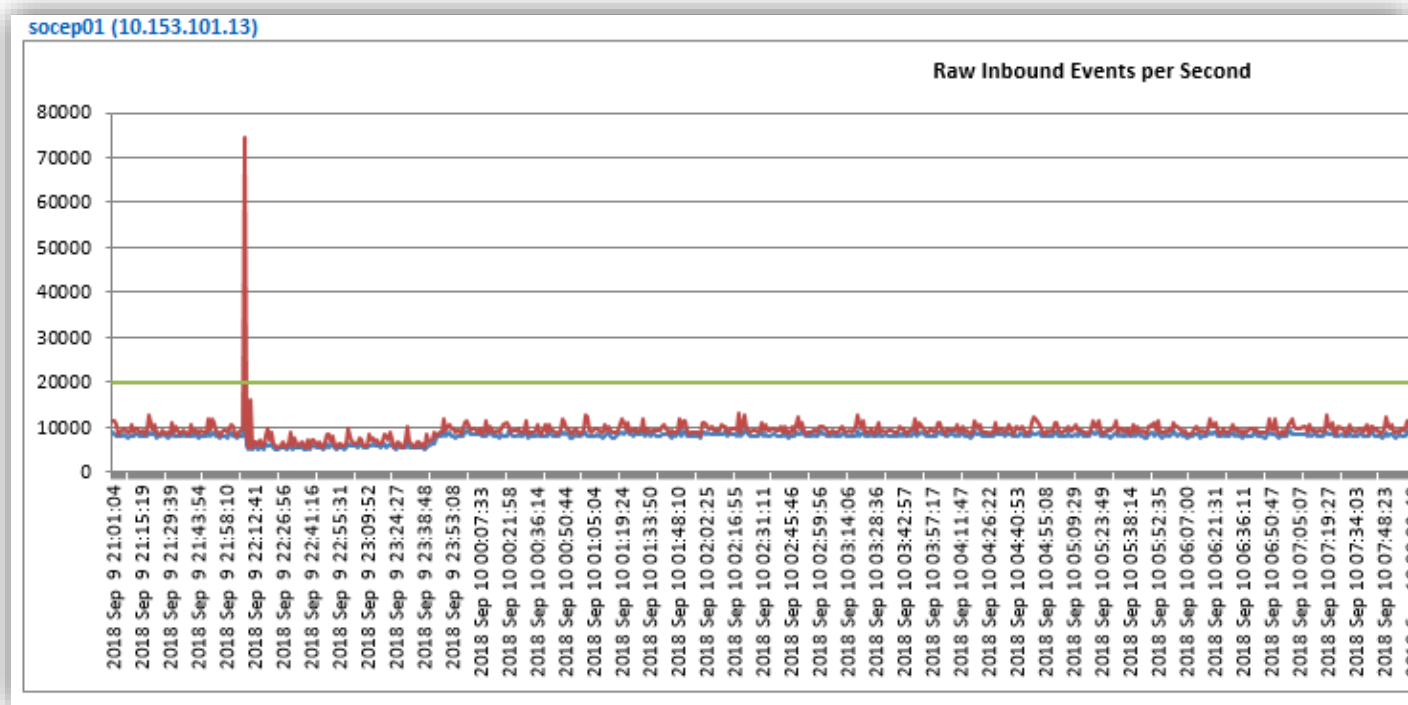
Task 7. Review Raw EPS/FPM charts

OBJECTIVES

Visualize EPS/FPM load throughout the day and detect anomalies

WHERE TO FIND

QRadar UI	Raw Inbound EPS / Raw Inbound FPM
Excel report	ENV Raw EPS / ENV Raw FPM



ITEMS TO CHECK:

- EPS spikes and gaps over time

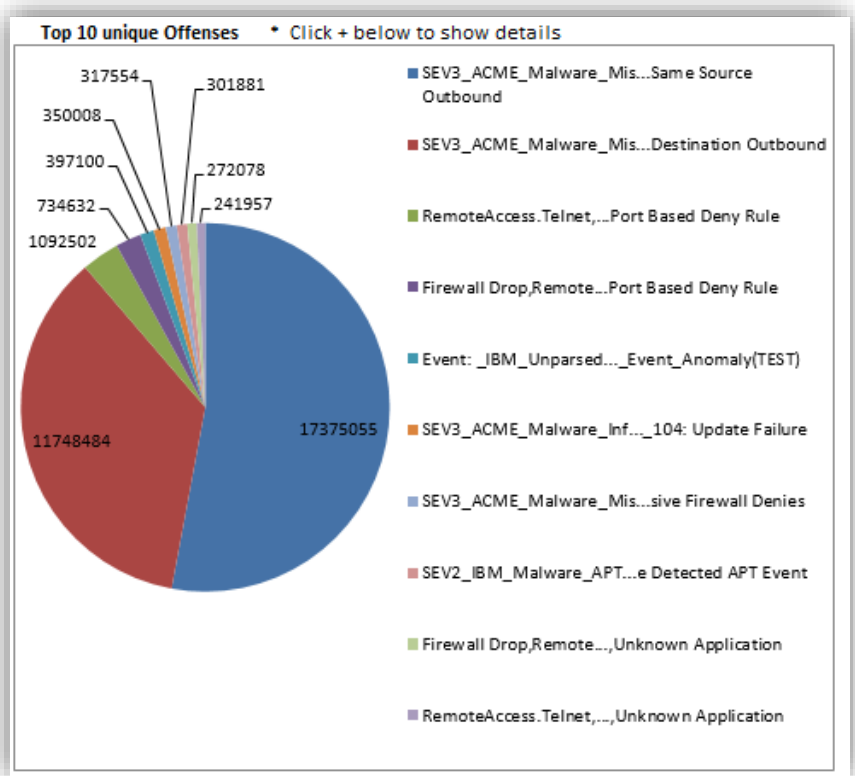
Task 8. Review Top Offenses

OBJECTIVES

Explore correlation trends, find possible False Positives

WHERE TO FIND

QRadar UI	Top Unique Offenses
Excel report	CRL Offenses: Top 10 Unique Offenses



ITEMS TO CHECK:

- Top offenses indicate False Positives or recent incidents

Task 9. Review Offense sources

OBJECTIVES

Identify & fix rules configuration flaws

WHERE TO FIND

QRadar UI	Offense Analysis
Excel report	CRL Offenses: Offense Analysis

_ACME_Malware_Infection_ePO_104: Update Failure
Catch ePO update failures

when the event(s) were detected by one or more of McAfee ePolicy Orchestrator and

when the event QID is one of the following (25250336) Update Failed, (25250124) The update failed; see event log

Offense ID	Source IP	EVENT
180600	10.106.206.186	37695
180116	10.131.40.125	26750
180011	10.131.40.172	24192
180114	10.106.206.47	20323
180445	10.131.40.60	17658
180016	10.106.179.206	16058
180017	10.131.40.205	13754
180012	10.106.213.159	13038
180118	10.106.195.151	12108
180024	10.106.188.139	11950
180023	10.131.40.38	11624
180122	10.131.40.239	11590
180444	10.106.206.66	10249
180025	10.153.70.242	9516
180124	10.106.206.109	8949
180015	10.106.211.118	7508

Offense Analysis

Rules Hit (top 10)

Rule Name	Hit Count
_ACME_Malware_Infection_ePO_104: Update Failure	302
_ACME_Malware_MiscMalware_Firewall_060:...	131
_ACME_Malware_MiscMalware_Firewall_059:...	128
_ACME_PolicyViolation_SuspiciousUserActivity_Cor...	28
_ACME_InformationCompromise_DataLoss_Bluecoa...	20
_ACME_Malware_MiscMalware_Firewall_036:...	18
_ACME_Malware_Botnet_Firewall_040: Direct DNS...	15
_ACME_Malware_Botnet_Correlation_101:...	10
Recon: Local L2L IRC Server Scanner	10
_IBM_TechnicalAttack_NetworkCompromise_Wind...	9

ITEMS TO CHECK:

- Top noisy rules
- Offense indices
- Rules logic
- Number of events/flows

USER STORY : LOG SOURCES

As a platform administrator, I would like to have a dashboard or a list of steps to be performed in QLEAN App in order to perform log source collections checkups

Task 1. Review EPS Anomalies

OBJECTIVES

Examine what is causing EPS spikes and events being dropped or sent directly to storage

WHERE TO FIND

QRadar UI	EPS Anomalies
Excel report	ENV EPS ALERTS

The screenshot displays a table titled "Detected anomalies" with the following data:

Date: 2023-02-02 14:31:24			
Type: Spike			
Event Processor: socep01			
Log Source: LinuxServer @ infoblox.localdomain			
Event Name	EPS	Event Count	
Process Created	672	403728	
Command Execution - Execec Event	1	882	
User space user has logged out	0	2	
Process Creation Failed	0	45	
User shell command and args	0	1	
User space authentication	0	7	
Audit Event	0	49	
User space authentication failed	0	1	
User space session start	0	51	
User space user has logged in	0	2	
User space session end	0	34	
Log Source: PaSeries @ SACMEPANDGWY-B			
Event Name	EPS	Event Count	
Traffic End	417	250795	
Reset Both	23	14015	
FileType Detected	2	1310	
Session Allowed	1	626	

ITEMS TO CHECK:

- EPS spikes
- Event drops
- Involved Log Sources
- Top frequent events

Task 2. Review Log Source list

OBJECTIVES

Monitor overall Log Sources health & configuration problems

WHERE TO FIND

QRadar UI	Log Sources
Excel report	ENV Log Sources: All log sources

All log sources	Source Name	Identifier	Activity	Last seen	Avg EPS	Peak EPS	Peak EPS date	Protocol	Source Type	Extension	Added	Addition ty	Bulk	Status
	Bind @ csprodallprod.acme.com	csprodallprod.acme.com	INACTIVE	2017-09-15 03:27:32	7759	22784	2017-09-12 07:35:10	Syslog	Bind		2017-06-20 04:49:15	AUTODSCV		ENABLED
	F5 BigIP @ PROSFAMG01a	PROSFAMG01a	ACTIVE	2018-09-10 12:37:37	1213	13426	2018-09-02 11:15:10	Syslog	BigIPAFM	F5_DNS	2017-11-10 11:12:29	MANUAL		ENABLED
	F5 BigIP @ PROSFAMG02a	PROSFAMG02a	ACTIVE	2018-09-10 12:37:37	1199	13430	2018-09-02 11:15:10	Syslog	BigIPAFM	F5_DNS	2017-11-01 11:20:33	AUTODSCV		ENABLED
	LinuxServer @ infoblox.localdomain	infoblox.localdomain	INACTIVE	2017-04-18 08:44:27	588	2943	2017-04-17 11:00:01	Syslog	LinuxServer		2017-03-21 09:47:44	AUTODSCV		ENABLED
	Bind @ csprodslprod.acme.com	csprodslprod.acme.com	INACTIVE	2017-10-25 01:26:43	480	5802	2017-09-29 08:33:10	Syslog	Bind		2017-06-20 04:49:14	AUTODSCV		ENABLED
	PaSeries @ SACMEPANDGWY-B	SACMEPANDGWY-B	ACTIVE	2018-09-10 12:37:37	442	1742	2018-07-10 08:35:10	Syslog	PaSeries		2015-09-29 04:38:27	AUTODSCV		ENABLED
	PaSeries @ GCCPABLUEMIX-P	GCCPABLUEMIX-P	ACTIVE	2018-09-10 12:37:30	364	9372	2018-05-28 04:48:10	Syslog	PaSeries		2018-03-07 12:10:15	AUTODSCV		ENABLED
	FortiGate @ 10.135.51.9	10.135.51.9	ACTIVE	2018-09-10 12:37:37	357	691	2018-07-10 04:32:10	Syslog	FortiGate		2017-11-17 01:20:11	AUTODSCV		ENABLED
	zOS SHC @ shcmp.acme.com	zOS SHC @ shcmp.acme.com	INACTIVE	2017-06-20 12:59:53	317	1215	2017-06-19 01:17:10	LogFileProtocol	IBMTOS		2016-06-06 01:10:52	MANUAL		DISABLED
	PaSeries @ SACMEPALEOF01-P	SACMEPALEOF01-P	ACTIVE	2018-09-10 12:37:37	315	3060	2018-05-04 07:19:10	Syslog	PaSeries		2018-03-20 11:21:17	AUTODSCV		ENABLED
	WindowsAuthServer @ TR220330	TR220330	INACTIVE	2017-11-06 02:37:25	293	581	2017-11-05 01:25:10	Syslog	WindowsAuthServer		2017-09-24 02:03:21	AUTODSCV		ENABLED
	zOS CIS @ 10.102.255.245	zOS CIS @ 10.102.255.245	INACTIVE	2017-06-20 11:33:08	245	1206	2017-06-19 01:17:10	LogFileProtocol	IBMTOS		2016-06-06 01:28:06	MANUAL		DISABLED
	RACF SHC @ shcmp.acme.com	RACF SHC @ shcmp.acme.com	5:22 with excel	2018-02-09 03:16:06	220	562	2017-06-28 11:56:04	LogFileProtocol	RACF		2016-06-06 01:08:28	MANUAL		DISABLED
	RACF CIS @ shcmp.acme.com	RACF CIS @ shcmp.acme.com	5:22 with excel	2018-02-09 03:16:42	209	542	2017-06-28 11:56:04	LogFileProtocol	RACF		2016-06-06 12:10:37	MANUAL		DISABLED
	PaSeries @ SACMEPANSL-P	SACMEPANSL-P	ACTIVE	2018-09-10 12:37:37	190	5688	2018-06-11 10:23:04	Syslog	PaSeries		2015-10-07 04:39:18	AUTODSCV		ENABLED
	CheckPoint @ 10.135.54.34	10.135.54.34	ACTIVE	2018-09-10 12:37:37	186	10127	2017-12-16 01:11:10	LEA	CheckPoint		2015-05-11 01:36:09	AUTODSCV		ENABLED
	LinuxServer @ svomivaas2850	svomivaas2850	INACTIVE	2018-09-09 10:10:20	152	697	2018-08-23 02:16:10	Syslog	LinuxServer		2018-01-23 01:56:23	AUTODSCV		ENABLED
	WindowsAuthServer @ TR258032	TR258032	INACTIVE	2017-11-06 02:37:25	136	401	2017-08-22 09:56:10	Syslog	WindowsAuthServer		2017-07-30 05:15:49	AUTODSCV		ENABLED
	zOS DEV @ 10.102.255.245	zOS DEV @ 10.102.255.245	INACTIVE	2017-06-20 01:39:15	127	1559	2016-06-07 02:04:10	LogFileProtocol	IBMTOS		2016-06-06 12:07:29	MANUAL		DISABLED
	zOS SHC2 @ shcmp.acme.com	zOS SHC2 @ shcmp.acme.com	INACTIVE	2017-06-20 01:36:58	108	1271	2016-11-18 10:19:10	LogFileProtocol	IBMTOS		2016-06-06 01:04:03	MANUAL		DISABLED
	LinuxServer @ svomivaas3473	svomivaas3473	INACTIVE	2018-09-09 10:10:20	107	107	2018-09-09 10:11:10	Syslog	LinuxServer		2018-05-08 11:50:28	AUTODSCV		ENABLED
	Bind @ cssv2.ks.acme.com	cssv2.ks.acme.com	INACTIVE	2017-10-25 01:33:12	104	6600	2017-09-29 08:33:10	Syslog	Bind		2017-08-09 09:33:41	AUTODSCV		ENABLED
	zOS FDB @ 10.102.255.245	zOS FDB @ 10.102.255.245	INACTIVE	2017-06-20 11:36:12	100	2817	2016-06-07 02:10:10	LogFileProtocol	IBMTOS		2016-06-06 01:50:47	MANUAL		DISABLED
	LinuxServer @ svomivaas1791	svomivaas1791	INACTIVE	2018-09-09 10:10:20	98	98	2018-09-09 10:11:10	Syslog	LinuxServer		2017-04-30 04:46:24	AUTODSCV		ENABLED
	WindowsAuthServer @ TR122965	TR122965	INACTIVE	2017-11-06 02:37:25	89	143	2017-10-11 06:38:10	Syslog	WindowsAuthServer		2017-07-30 04:31:38	AUTODSCV		ENABLED
	LinuxServer @ svomivaas1764	svomivaas1764	INACTIVE	2018-09-09 10:10:20	82	336	2018-08-23 03:49:10	Syslog	LinuxServer		2017-04-09 07:07:28	AUTODSCV		ENABLED
	HadoopItronport @ 10.223.134.133	svomivaas133.prod.acme.co	INACTIVE	2018-02-08 11:04:26	71	283	2018-01-21 05:06:10	Syslog	HadoopItronportLogsCustom	HadoopItronport	2017-10-18 02:04:15	MANUAL		ENABLED

ITEMS TO CHECK:

- Activity status
- Peak EPS
- Configuration errors
- Last event time

Task 3. Review Log Source actions

OBJECTIVES

Explore recent Log Sources modifications, find responsible personnel

WHERE TO FIND

QRadar UI	Misc Log Source Stats
Excel report	ENV Log Sources: Last Inactive/Added/Disabled/Deleted/Modified log sources

Last Inactive Log Sources			Last Added Log Sources		
Name	Date	User	Name	Date	User
WindowsAuthServer @ 10.229.220.44	2018-09-10 00:22:01	N/A	WindowsAuthServer @ 10.112.75.183	2018-09-10 11:56:42	N/A
LinuxServer @ 10.107.84.19	2018-09-10 00:13:42	N/A	WindowsAuthServer @ 10.112.75.159	2018-09-10 11:56:31	N/A
WindowsAuthServer @ 10.112.34.118	2018-09-10 00:12:34	N/A	LinuxServer @ adkva60q07	2018-09-10 11:26:34	remmah
WindowsAuthServer @ 10.229.223.59	2018-09-10 00:04:33	N/A	LinuxServer @ adkzkq0t01	2018-09-10 10:40:12	remmah
PostFixMailTransferAgent @ svomivaiaas3072	2018-09-10 00:02:20	N/A	LinuxServer @ asptvkp2	2018-09-10 10:23:14	remmah
PaSeries @ SACMEPANTWS-B	2018-09-10 00:02:10	N/A	LinuxServer @ asptvkp4	2018-09-10 10:22:24	remmah
PostFixMailTransferAgent @ svomivaiaas451	2018-09-09 23:59:21	N/A	WindowsAuthServer @ TRMBDM01	2018-09-10 10:12:02	N/A
WindowsAuthServer @ 10.229.223.64	2018-09-09 23:52:59	N/A	LinuxServer @ 10.112.31.116	2018-09-10 10:08:38	N/A
LinuxServer @ SACMEPANTWS-B	2018-09-09 23:47:36	N/A	LinuxServer @ 10.112.31.103	2018-09-10 10:04:22	N/A
WindowsAuthServer @ 10.112.34.154	2018-09-09 23:44:36	N/A	LinuxServer @ 10.112.31.107	2018-09-10 10:01:08	N/A

Last Disabled Log Sources			Last Modified Log Sources		
Name	Date	User	Name	Date	User
IBMI @ as25r709	2018-09-07 12:05:35	302842859	WindowsAuthServer @ 10.112.75.183	2018-09-10 11:56:42	N/A
LinuxServer @ 10.214.1.31	2018-08-28 18:10:35	532169703	WindowsAuthServer @ 10.112.75.159	2018-09-10 11:56:31	N/A
Hadoop @ 10.223.134.133	2018-08-28 11:24:29	nainemra	LinuxServer @ adkva60q07	2018-09-10 11:26:34	remmah
Guardium @ 10.214.1.32	2018-08-23 22:46:40	302842859	LinuxServer @ adkzkq0t01	2018-09-10 10:40:12	remmah
LinuxServer @ 10.214.1.32	2018-08-22 13:24:07	302842859	LinuxServer @ asptvkp2	2018-09-10 10:23:14	remmah
RACF MCIS @ 10.102.255.245	2018-08-07 10:51:40	302842859	LinuxServer @ asptvkp4	2018-09-10 10:22:24	remmah
RACF TCIS @ shcmp.acme.com	2018-08-07 10:51:40	302842859	WindowsAuthServer @ TRMBDM01	2018-09-10 10:12:02	N/A
RACF DDEV @ shcmp.acme.com	2018-08-07 10:51:40	302842859	LinuxServer @ 10.112.31.116	2018-09-10 10:08:38	N/A
RACF THIS @ shcmp.acme.com	2018-08-07 10:51:40	302842859	LinuxServer @ 10.112.31.103	2018-09-10 10:04:22	N/A
RACF RTG @ 10.102.255.245	2018-08-07 10:51:40	302842859	LinuxServer @ 10.112.31.107	2018-09-10 10:01:08	N/A

Protocol Configuration Errors			Last Deleted Log Sources		
Status	Name	User	Name	Date	User
Unable to download certificate chain from [acme-CloudTrail @ Automation - Noi		N/A	Squid @ 10.27.3.135	2018-07-16 21:42:39	532169703
Unable to download certificate chain from [acme-S CloudTrail @ Automation - P		N/A	Squid @ 10.27.3.133	2018-07-16 21:42:39	532169703
Unable to download certificate chain from [acme-AWS CloudTrail @ IAM Users		N/A	Squid @ 10.27.3.136	2018-07-16 21:42:39	532169703
Unable to download certificate chain from [acme-AWS CloudTrail @ Compliance		N/A	Azure Security Center Dev	2018-06-29 08:02:53	532169703
Unable to download certificate chain from [acme-AWS CloudTrail @ Networking		N/A	Azure Security Center Alerts	2018-06-29 07:44:15	532169703
Unable to download certificate chain from [acme-S CloudTrail @ ACME01 - NonP		N/A	Azure Security Center Alerts	2018-06-28 17:38:32	532169703
Unable to download certificate chain from [acme-IWS CloudTrail @ ACME01 - Pro		N/A	Azure Security Center	2018-06-28 14:29:56	532169703
Unable to download certificate chain from [acme-CloudTrail @ Shared Services -		N/A	Azure Test @ filtered-activity-logs	2018-06-28 11:21:49	532169703
No new files matching the directory prefix and file	AWS Guard	N/A	Azure @ filtered-diagnostic-logs	2018-06-28 11:21:44	532169703
Connection attempt has failed and connection wil	McAfee ePo Gold	N/A	Azure Security Center	2018-05-11 15:36:42	532169703

ITEMS TO CHECK:

- Newly added Log Sources
- Source deleted by mistake
- Harmful modifications
- Protocol errors

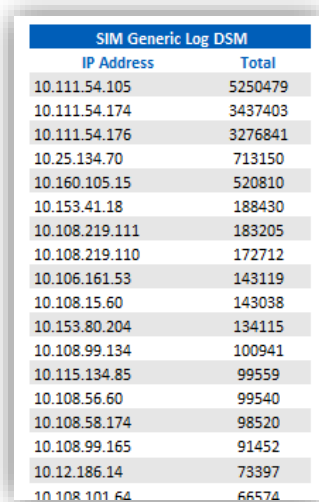
Task 4. Review SIM generic logs

OBJECTIVES

Find neglected data source, misconfigured syslog forwarders, message with excessive length

WHERE TO FIND

QRadar UI	Data Quality: Unknown and Stored: SIM Generic Log DSM
Excel report	ENV DQ Unknown: SIM Generic Log DSM



SIM Generic Log DSM	
IP Address	Total
10.111.54.105	5250479
10.111.54.174	3437403
10.111.54.176	3276841
10.25.134.70	713150
10.160.105.15	520810
10.153.41.18	188430
10.108.219.111	183205
10.108.219.110	172712
10.106.161.53	143119
10.108.15.60	143038
10.153.80.204	134115
10.108.99.134	100941
10.115.134.85	99559
10.108.56.60	99540
10.108.58.174	98520
10.108.99.165	91452
10.12.186.14	73397
10.108.101.64	66574

ITEMS TO CHECK:

- Noisy IPs with no Log Source assigned

USER STORY : PARSERS & RULES

As a platform administrator, I would like to have a dashboard or a list of steps to be performed in QLEAN App in order to perform check of the Parsers per Log Source type coverage, Regex issues, expensive rules and building blocks

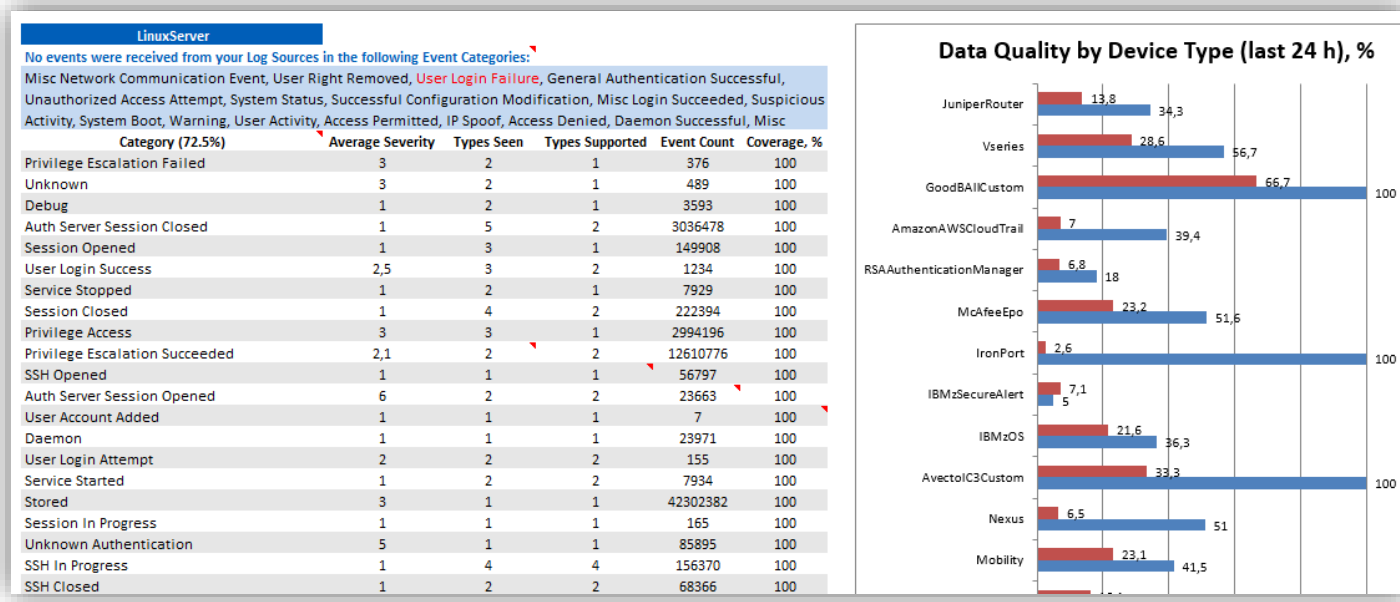
Task 1. Review Data Quality per DSM

OBJECTIVES

Identify potential audit misconfiguration, improperly assigned DSMs, unsupported software versions, redundant filtering, etc

WHERE TO FIND

QRadar UI	Data Quality by Device Type
Excel report	ENV DQ Device Type



ITEMS TO CHECK:

- Missing categories
- Low Coverage % combined with high Event Count
- Low Coverage & for high Severity categories
- Massive events in Unknown & Stored categories
- Massive events in generic categories (Information, Debug, Messages, etc.)
- DSMs with a few (1..3) event categories (low Category coverage %)

Task 2. Review Data Quality per Log Source

OBJECTIVES

Identify audit misconfiguration, unnecessary sources, audit baseline deviations

WHERE TO FIND

QRadar UI	Data Quality by Log Source
Excel report	ENV DQ Log Source

Device Type	Log Source Name	Average Severity	Types Seen	Types Supported	Event Count	Coverage, %
IBMzSecureAlert	zSecure Alert NG	1,7	2	6254	28	0
IBMzSecureAlert	zSecure Alert DEV	5	1	6254	24	0
IBMzSecureAlert	zSecure Alert CX	1,6	2	6254	30	0
JuniperRouter	Juniper JunOS Platform @ 10.106.245.240	3	1	3334	22282	0
JuniperRouter	Juniper JunOS Platform @ 10.107.100.113	1	1	3334	2420	0
JuniperRouter	Juniper JunOS Platform @ 10.107.100.114	1	1	3334	884	0
PaSeries	PaSeries @ CABPAN7050	2,2	4	12749	1519	0
PaSeries	PaSeries @ GCCPABLUEMIX-B	1,8	5	12749	412	0
PaSeries	PaSeries @ SACMEPANMGMT2	2,2	6	12749	855	0
PaSeries	PaSeries @ SACMEPANDM2	3,1	5	12749	615	0
PaSeries	PaSeries @ SACMEPANSC2-B	3,4	6	12749	598	0
PaSeries	PaSeries @ SACMEPANTWS-B	3	2	12749	142	0
PaSeries	PaSeries @ SACMEPANTWS-P	0	4	12749	1481941	0
PaSeries	PaSeries @ SACMEBRDPRX-B	3,6	3	12749	225	0
PaSeries	PaSeries @ SACMEBRDPRX-P	0,1	6	12749	149993	0
PaSeries	PaSeries @ SACMEPATESTBOX-B	2,8	3	12749	185	0
PaSeries	PaSeries @ SACMEPATESTBOX-P	2,5	3	12749	268	0
Vseries	Websense V-Series appliances @ PRDTRS1U	2,2	3	11957	14707	0
Vseries	Websense V-Series appliances @ PRDTRS1U	1,2	5	11957	9326	0
Vseries	Websense V-Series appliances @ PRDTRS1U	1,1	2	11957	6133	0
Vseries	Websense V-Series appliances @ DEVTRAN/	1,1	2	11957	5695	0
WindowsAuthServer	WindowsAuthServer @ 10.115.1.32	3	1	2029	160976	0
WindowsAuthServer	WindowsAuthServer @ 10.115.133.42	3	1	2029	90879	0
WindowsAuthServer	WindowsAuthServer @ 10.115.138.130	3	1	2029	86390	0

ITEMS TO CHECK:

- Single Event Type Seen combined with large Event Count: audit or parsing issues
- Log Sources with behavior significantly different from others of the same type: doesn't follow audit baselines
- Single Event Type Seen combined with low Severity: candidates for removal

Task 3. Review Unknown events

OBJECTIVES

Analyze log source misconfiguration and improperly assigned DSMs

WHERE TO FIND

QRadar UI	Data Quality Unknown and Stored: Unknown and Stored Events
Excel report	ENV DQ Unknown

Source IP	Log Source Name	Device Type	Total	Unknown Count	Unknowns, %
10.160.61.61	WindowsAuthServer @ 10.160.61.61	Microsoft Windows Security Event Log	221023	221023	100
10.108.52.13	WindowsAuthServer @ 10.108.52.13	Microsoft Windows Security Event Log	215007	215007	100
10.153.74.213	WindowsAuthServer @ 10.153.74.213	Microsoft Windows Security Event Log	186546	186546	100
10.160.21.70	WindowsAuthServer @ 10.160.21.70	Microsoft Windows Security Event Log	145	145	100
10.106.184.98	WindowsAuthServer @ 10.106.184.98	Microsoft Windows Security Event Log	141	141	100
10.25.132.230	PostFixMailTransferAgent @ svomivaiaas11:	PostFix MailTransferAgent	121	121	100
10.25.4.131	WindowsAuthServer @ 10.25.4.131	Microsoft Windows Security Event Log	98	98	100
10.25.130.163	PostFixMailTransferAgent @ svomivaiaas61:	PostFix MailTransferAgent	85	85	100
172.31.156.231	F5FirePass @ brjlik0t01	F5 Networks FirePass	53	53	100
10.27.2.126	WebProxy @ prd-10-113-2-126	Squid Web Proxy	30	30	100
10.160.35.50	EMC @ 10.160.35.50	Linux OS	30	30	100
10.27.3.243	WebProxy @ prd-10-113-3-243	Squid Web Proxy	29	29	100
10.27.3.151	WebProxy @ prd-10-113-3-151	Squid Web Proxy	28	28	100
10.27.3.185	WebProxy @ prd-10-113-3-185	Squid Web Proxy	28	28	100
10.153.39.33	PostFixMailTransferAgent @ dmrldpdp014	PostFix MailTransferAgent	17	17	100
10.160.21.173	WindowsAuthServer @ 10.160.21.173	Microsoft Windows Security Event Log	17	17	100
10.153.39.28	PostFixMailTransferAgent @ dmrldpdp005	PostFix MailTransferAgent	15	15	100
10.108.181.122	F5FirePass @ brjlbidd1	F5 Networks FirePass	13	13	100
10.153.39.31	PostFixMailTransferAgent @ dmrldpdp012	PostFix MailTransferAgent	10	10	100
10.153.39.25	PostFixMailTransferAgent @ dmrldpdp006	PostFix MailTransferAgent	8	8	100
10.106.172.226	LinuxServer @ bdskipt10	Linux OS	3	3	100
10.106.131.131	F5FirePass @ brjlitrq3	F5 Networks FirePass	3	3	100
10.27.3.78	WebProxy @ prd-10-113-3-78	Squid Web Proxy	2	2	100
172.31.156.243	F5FirePass @ brjliz0t01	F5 Networks FirePass	2	2	100
10.106.139.122	F5FirePass @ brjlxvq02	F5 Networks FirePass	2	2	100

ITEMS TO CHECK:

- Total = Unknown count (Unknowns 100%): wrong DSM, unsupported format, etc.
- All others: require DSM customization or source audit/format tuning
- Large Total count: first candidates for tuning

Task 4. Review Rules Performance

OBJECTIVES

Identify slow and nonoptimal rules

WHERE TO FIND

QRadar UI	Rules Performance
Excel report	CRL Rules: Rules Performance

Fired count		Top Average Actions Time	
Rule name	Count	Rule name	Time, sec
BB:CategoryDefinition: Regular Office Hours	3032782	UBA : User Volume of Activity Anomaly - Traffic Found	0,02634
BB:NetworkDefinition: Client Networks	3017744	UBA : User Behavior, Session Anomaly by Destination Found	0,01987
BB:CategoryDefinition: Any Flow	2562376	UBA : User Event Frequency Anomaly - Categories Found	0,01574
BB:PortDefinition: Authorized L2R Ports	2004214	System: Flow Source Stopped Sending Flows	0,01498
BB:PortDefinition: Web Ports	1592509	_MSS: Device Stopped Sending Events- Firewall	0,01248
BB:CategoryDefinition: Successful Communication	1004020	System: Device Stopped Sending Events	0,00875
BB:NetworkDefinition: Inbound Communication from	861725	Test Ping 10.10.10.10	0,00673
BB:NetworkDefinition: Untrusted Network Segment	861483	X-Force Risky URL	0,00561
BB:CategoryDefinition: Suspicious Events	707097	_ACME_Current_Campaign_214: Match against IOC	0,00529
BB:CategoryDefinition: Unidirectional Flow	675648	_IBM_PolicyViolation_UnauthorizedAccess_VPN_113: Login Attempts fro	0,00529
Top Average Execution Time		Top Average Response Time	
Rule name	Time, sec	Rule name	Time, sec
BB:CategoryDefinition: Unidirectional Flow DST	0,016393443	X-Force Risky IP, Dynamic	0,01579
X-Force Risky IP, Dynamic	0,010582011	FalsePositive: False Positive Rules and Building Blocks	0,00971
BB:Flowshape: Outbound Only	0,008547009	_BB:ACME_APIPA_IP_Addresses	0,00169
BB:Threats: Suspicious IP Protocol Usage:Unidirectio	0,000708215	BB:Threats: Suspicious IP Protocol Usage:Unidirectional UDP and Misc F	0,00071
System: Load Building Blocks	0,000594059	BB:NetworkDefinition: Darknet Addresses	0,0003
BB:NetworkDefinition: Honeypot like Addresses	0,000315259	BB:Flowshape: Inbound Only	0,00026
BB:HostDefinition: Servers	0,000314961	BB:CategoryDefinition: Unidirectional Flow SRC	0,00025
BB:NetworkDefinition: Darknet Addresses	0,00028547	System: Load Building Blocks	0,0002
BB:CategoryDefinition: Any Flow	0,000199223	BB:CategoryDefinition: Unidirectional Flow	0,00016
BB:CategoryDefinition: Unidirectional Flow SRC	0,00016503	BB:CategoryDefinition: Suspicious Events	0,00016

ITEMS TO CHECK:

- Execution Time: tune conditions, remove plain text searches, etc.
- Response Time: verify email settings, reference data size, custom actions, etc.

Task 5. Review Rule Actions and Responses

OBJECTIVES

Find improperly configured rules

WHERE TO FIND

QRadar UI	Rule Actions and Responses
Excel report	CRL Rules (2)

Rule Name	Action: Offense Index	Response: Dispatched Event Name	Response: Offense Index	Has Response Limiter	RefSet to Add Property to	Property to Add to RefSet	RefSet to Remove Property from	Property to Remove from RefSet	Add to RefData	Remove from RefData	Include Next Events	Change Magnitude	Drop Event	Send Email	Send to Forwarding Destination	Run Custom Action
A Command Shell or Powershell Has been Launched From a Remote System	Source IP	A Command Shell or Powershell Has been Launched From a Remote System	Source IP	NO	Compromised Hosts	sourceIP	N/A	N/A	N/A	N/A	YES	YES	NO	NO	NO	NO
A Hidden Network Share Has Been Added	Source IP	A Hidden Network Share Has Been Added	Source IP	NO	N/A	N/A	N/A	N/A	N/A	N/A	YES	YES	NO	NO	NO	NO
A Malicious Service Has Been Installed in a System	Source IP	A Malicious Service Has Been Installed in a System	Source IP	YES	Compromised Hosts	sourceIP	N/A	N/A	N/A	N/A	YES	YES	NO	NO	NO	NO
A Network Share Has Been Accessed From a Compromised Host	Source IP	A Network Share Has Been Accessed From a Compromised Host	Source IP	YES	N/A	N/A	N/A	N/A	N/A	N/A	YES	NO	NO	NO	NO	NO
A Network Share Has Been Added In a Compromised Host	Source IP	A Network Share Has Been Added In a Compromised Host	Source IP	YES	N/A	N/A	N/A	N/A	N/A	N/A	YES	NO	NO	NO	NO	NO
A Pipe Has Been Created Followed by Updating Service Binary Path to Connect to The Created Pipe	Source IP	A Pipe Has Been Created Followed by Updating Service Binary Path to Connect to The Created Pipe	Source IP	NO	N/A	N/A	N/A	N/A	N/A	N/A	YES	YES	NO	NO	NO	NO
A Scheduled Task Has Been Created in a Compromised Host	Source IP	A Scheduled Task Has Been Created in a Compromised Host	Source IP	NO	N/A	N/A	N/A	N/A	N/A	N/A	YES	NO	NO	NO	NO	NO
A Service Has Been Installed in a Compromised Host	Source IP	A Service Has Been Installed in a Compromised Host	Source IP	NO	N/A	N/A	N/A	N/A	N/A	N/A	YES	NO	NO	NO	NO	NO
Abnormal Parent for a System Process	Source IP	Abnormal Parent for a System Process	Source IP	YES	N/A	N/A	N/A	N/A	N/A	N/A	YES	YES	NO	NO	NO	NO
All Exploits Become Offenses	Source IP	N/A	N/A	NO	N/A	N/A	N/A	N/A	N/A	N/A	YES	NO	NO	NO	NO	NO
An Administrative share Has Been Accessed	Source IP	An Administrative share Has Been Accessed	Source IP	YES	N/A	N/A	N/A	N/A	N/A	N/A	YES	NO	NO	NO	NO	NO
An Administrative share Has Been Accessed From a Compromised Machine	Source IP	An Administrative share Has Been Accessed From a Compromised Machine	Source IP	NO	N/A	N/A	N/A	N/A	N/A	N/A	YES	NO	NO	NO	NO	NO
Anomaly: Excessive Firewall Accepts Across Multiple Hosts	Source IP	Excessive Firewall Accepts Across Multiple Hosts	Source IP	NO	N/A	N/A	N/A	N/A	N/A	N/A	YES	NO	NO	NO	NO	NO
AssetExclusion: Exclude DNS Name By IP	N/A	N/A	N/A	NO	Asset Reconciliation DNS Blacklist	identityHostName	N/A	N/A	N/A	N/A	NO	NO	NO	NO	NO	NO
AssetExclusion: Exclude DNS Name By MAC Address	N/A	N/A	N/A	NO	Asset Reconciliation DNS Blacklist	identityHostName	N/A	N/A	N/A	N/A	NO	NO	NO	NO	NO	NO
AssetExclusion: Exclude DNS Name By NetBIOS Name	N/A	N/A	N/A	NO	Asset Reconciliation	identityHostName	N/A	N/A	N/A	N/A	NO	NO	NO	NO	NO	NO

ITEMS TO CHECK:

- Identify rules that:
 - affect Reference Data
 - affect Event flow (drop/forward)
 - don't have a Response Limit
 - accumulate too many events
 - don't generate alerts
 - etc.

Task 6. Review Disabled Custom Properties

OBJECTIVES

Explore automatically and manually disabled Custom Properties

WHERE TO FIND

QRadar UI	Misc Fine Tuning: Disabled Custom Properties
Excel report	Fine Tuning: Disabled Custom Properties

Disabled Custom Properties	
Property name	Correlation rules
Microsoft DNS - Remote IP	ACME: Risky IP
Microsoft DNS - Domain	ACME: Risky URL

ITEMS TO CHECK:

- Disabled items that may affect rules, searches and reports

Task 7. Review Custom Properties performance

OBJECTIVES

Assess regular expressions performance that may affect event processing pipeline

WHERE TO FIND

QRadar UI	Regex Relative Performance
Excel report	Performance: Regex Relative Performance

Relative performance gap	Custom Property Name	Regex	User	Update time
3196	BytesReceived	.*\scs-bytes=(\d{1,})\ssc-bytes=(\d{1,})\scs-p	admin	2017-08-16 14:24:29
103	ePO Filename	([^\ "]+)"\sThreatCategory:	738806884	2017-04-10 12:08:40
37	CRE Name	(.+?)\t(.+)	admin	2017-08-16 14:24:48
33	expensiverules	(com.q1labs.semsources.cre.CRE:)(.*)\s(Expens	admin	2018-05-18 13:02:08
29	Windows Event ID Count	(\d+)\s+\w{3,4}\s+\w+\s+\d+	805573581	2018-03-16 16:36:48
29	UrlHost	(?:[?cs-host\s*=\s*])?(?:[0-9-]+\s[0-9-]+\s[0-9-	admin	2017-01-23 16:47:48
29	Avecto Username	UserName:[\s]{\}(\.)*[\s]{\}UserID:	309049336	2018-07-31 14:19:35
25	CRE Description	(.+?)\t(.+)	admin	2010-08-04 10:45:36
25	SMTP HELO	[H] [E] [H] [L] O [s] (.+?) \x0d \x0a	admin	2010-08-11 10:01:25
25	Avecto_commandline	CommandLine:\s(.*)\s((ProcessGUID:) Uniq	309049336	2018-08-03 12:05:18

ITEMS TO CHECK:

- Large Relative performance gap value compared to others:
requires regex optimization