

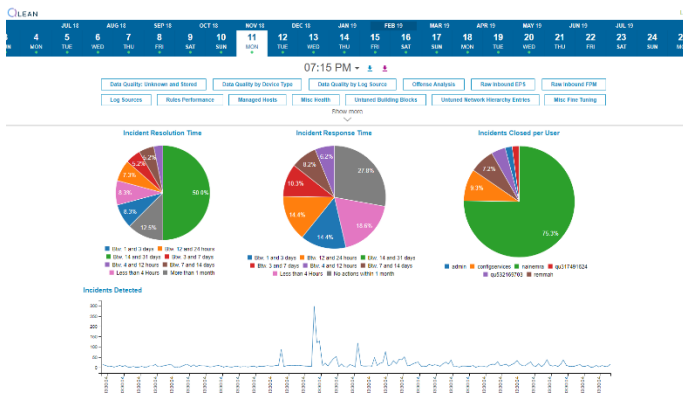


- QLEAN for QRadar health assessment and tuning
- QSM Session Manager
- QWAD WinCollect Assisted Deployment
- QIN Incident Notifier
- QMEA Microsoft Exchange Audit
- QDATA LDAP Reference Data Feed
- QLSI Log Source Inventory
- QOR Offense Reporter
- QSSA Slow Search Alert
- QMLA Missing Logs Alert
- QLED Log Source EPS Details
- QVTI VirusTotal Integration for Hash Verification
- QTOR Darknet Monitoring
- QEFC Exclude from Correlation button
- QFSO Find Similar Offenses button
- QDGA DGA Analyzer

QLEAN for QRadar health assessment, tuning and SOC automation



A tool designed to promptly identify operational deviations in IBM QRadar SIEM performance along with data losses, and helping to troubleshoot them quickly.



Over 50 performance and behavioral metrics

25 health markers

A comprehensive view of QRadar SIEM system state

Available on IBM App Exchange

QLEAN (previously known as Health Check Framework)

Log Activity Network Activity Assets Reports Risks Vulnerabilities Admin Pulse QLEAN License It

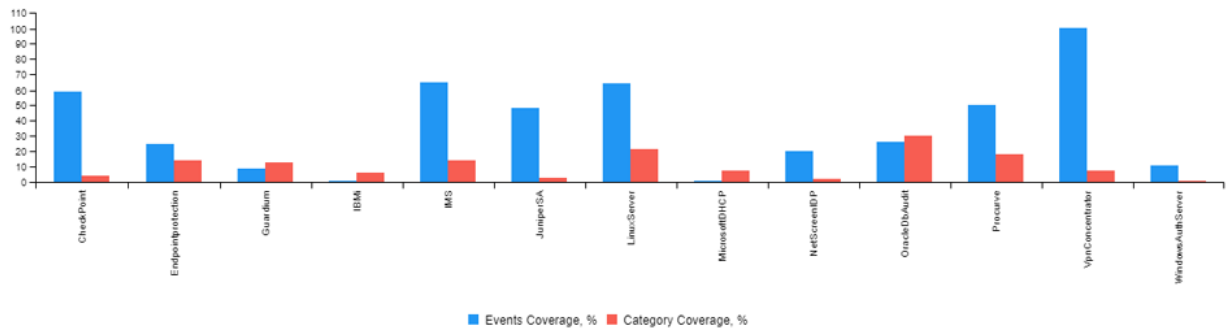
QLEAN

MAY 19 JUN 19 JUL 19 AUG 19 SEP 19 OCT 19 NOV 19 DEC 19 JAN 20 FEB 20 MAR 20 APR 20 MAY 20

3 TUE 4 WED 5 THU 6 FRI 7 SAT 8 SUN 9 MON 10 TUE 11 WED 12 THU 13 FRI 14 SAT 15 SUN 16 MON 17 TUE 18 WED 19 THU 20 FRI 21 SAT 22 SUN 23 MON 24 TUE 25 WED

10:33 AM

Show more



CheckPoint

Category (4.5%)	Avg Sev	Seen	Supported	Count	Coverage, %
IKE Error	1.0	1	1	4	100.0
IP Fragmentation	3.0	1	1	6	100.0
Stored	3.0	1	1	49207	100.0
System Informational	3.0	1	1	4	100.0
Firewall Permit	0.0	1	12	77524	8.3
Warning	5.0	1	23	270	4.3
Information	2.0	1	71	18	1.4

Endpointprotection

QSM Session Manager



QRadar extension for user sessions management and security events investigation through sessions information that allows to easily track user's actions all over the network since initial authentication till the end of session, even when username is not available in log messages, e.g:

Operating Systems logs without username

Web Servers activity

IDS/IPS activity

Firewall activity

Database and business application queries

Session information for specific user or IP address can be accessed via right-click menu in Log Activity tab, or through the QSM tab.

QSM is essential in environments with lots of DHCP endpoints and users, and other scenarios.

QSM Session Manager

Session Manager Help License is valid

Configuration

Connection Profiles Activity Columns

DEFAULT Connected

Debug Mode[Off]

Set Time Range

Start Time: 2018-08-16 11:12 End Time: 2018-08-16 15:12 Set Current

Hours Ago: 1 4 72

Get Sessions

Username/IP: gregory_durkin Reset Get Sessions

Sessions

user name	ip address	start time	end time	status
<input checked="" type="checkbox"/> gregory_durkin	10.0.5.50	2018-08-16 15:06:29		Active
<input checked="" type="checkbox"/> gregory_durkin	10.0.240.39	2018-08-16 14:05:52		Active
<input checked="" type="checkbox"/> gregory_durkin	10.0.230.173	2018-08-16 12:41:50	2018-08-16 13:01:15	
<input checked="" type="checkbox"/> gregory_durkin	10.0.240.39	2018-08-16 12:34:41	2018-08-16 13:01:28	

Activity

event time	log source	category
2018-08-16 15:10:47	Guardium @ 10.0.3.60	Unauthorized Activity
2018-08-16 15:10:47	Guardium @ 10.0.3.60	Unauthorized Access Atte
2018-08-16 15:10:47	Guardium @ 10.0.3.60	Unauthorized Access Atte

2018-08-16 15:06:29 - Active

Source	Destination	Time	Event	Severity	Count	Source IP	Destination IP	Source Port	Destination Port	User	View
LinuxServer @ nms.ac...	LinuxServer @ nms.ac...	1 Aug 16, 2018, 11:54:39 AM	Session Opened	Info	0	10.0.120.60	10.0.120.60	0	0	gregory_durkin	View
OracleDbAudit @ oracl...	OracleDbAudit @ oracl...	1 Aug 16, 2018, 11:54:38 AM	System Action Allow	Info	32893	10.0.110.120	10.0.10.41	0	0	victor_mangan	View
LinuxServer @ nms.ac...	LinuxServer @ nms.ac...	1 Aug 16, 2018, 11:54:38 AM	Misc Logout	Info	32893	10.0.110.120	10.0.10.41	0	0	victor_mangan	View
linuxycServer @ vasca...	linuxycServer @ vasca...	1 Aug 16, 2018, 11:54:35 AM	Host Login Succeeded	Info	49169	10.0.110.123	10.0.120.70	0	0	jodi_verduzco	View
SM # session_manager	SM # session_manager	1 Aug 16, 2018, 11:54:34 AM	Messages	Info	0	10.0.240.39	169.254.2.35	0	0	gregory_durkin	View
LinuxServer @ nms.ac...	LinuxServer @ nms.ac...	1 Aug 16, 2018, 11:54:34 AM	Host Login Succeeded	Info	58623	10.0.240.39	10.0.120.60	0	0	gregory_durkin	View
SM # session_manager	SM # session_manager	1 Aug 16, 2018, 11:54:33 AM	Messages	Info	0	10.0.100.190	169.254.2.35	0	0	julian_vanasche	View
LinuxServer @ nms.ac...	LinuxServer @ nms.ac...	1 Aug 16, 2018, 11:54:33 AM	SSH Login Failed	Info	58623	10.0.240.39	10.0.120.60	0	0	gregory_durkin	View
linuxycServer @ vasca...	linuxycServer @ vasca...	1 Aug 16, 2018, 11:54:33 AM	SSH Login Failed	Info	49169	10.0.110.123	10.0.120.70	0	0	jodi_verduzco	View
WindowsAuthServer @ ...	WindowsAuthServer @ ...	1 Aug 16, 2018, 11:54:32 AM	Host Login Succeeded	Info	23253	10.0.5.224	10.0.120.30	0	0	jacob_cagle	View
OracleDbAudit @ oracl...	OracleDbAudit @ oracl...	1 Aug 16, 2018, 11:54:32 AM	Misc Login Succeeded	Info	3155	10.0.230.104	10.0.10.41	0	0	dwhight_bird	View
OracleDbAudit @ oracl...	OracleDbAudit @ oracl...	1 Aug 16, 2018, 11:54:32 AM	System Action Allow	Info	3155	10.0.230.104	10.0.10.41	0	0	dwhight_bird	View
WindowsAuthServer @ ...	WindowsAuthServer @ ...	1 Aug 16, 2018, 11:54:32 AM	Host Login Succeeded	Info	5181	10.0.230.25	10.0.110.120	0	0	victor_mangan	View
OracleDbAudit @ oracl...	OracleDbAudit @ oracl...	1 Aug 16, 2018, 11:54:32 AM	System Action Allow	Info	3289	10.0.110.120	10.0.10.41	0	0	victor_mangan	View
OracleDbAudit @ oracl...	OracleDbAudit @ oracl...	1 Aug 16, 2018, 11:54:32 AM	Misc Login Succeeded	Info	3289	10.0.110.120	10.0.10.41	0	0	victor_mangan	View
IBM IMS @ 10.0.3.30	IBM IMS @ 10.0.3.30	1 Aug 16, 2018, 11:54:32 AM	Information	Info	0	10.0.3.30	10.0.3.30	0	0	hoist	View
IBM IMS @ 10.0.3.30	IBM IMS @ 10.0.3.30	1 Aug 16, 2018, 11:54:32 AM	Information	Info	0	10.0.3.30	10.0.3.30	0	0	hoist	View
IBM IMS @ 10.0.3.30	IBM IMS @ 10.0.3.30	1 Aug 16, 2018, 11:54:32 AM	User Account Remo...	Info	0	10.0.3.30	10.0.3.30	0	0	hoist	View
IBM IMS @ 10.0.3.30	IBM IMS @ 10.0.3.30	1 Aug 16, 2018, 11:54:32 AM	Information	Info	0	10.0.3.30	10.0.3.30	0	0	hoist	View
IBM IMS @ 10.0.3.30	IBM IMS @ 10.0.3.30	1 Aug 16, 2018, 11:54:32 AM	Information	Info	0	10.0.3.30	10.0.3.30	0	0	hoist	View
JuniperSA @ 10.0.3.50	JuniperSA @ 10.0.3.50	1 Aug 16, 2018, 11:54:32 AM	Misc Login Succeeded	Info	190	10.0.100.190	10.0.100.190	0	0	bobbi	View
JuniperSA @ 10.0.3.50	JuniperSA @ 10.0.3.50	1 Aug 16, 2018, 11:54:32 AM	Auth Server Session ...	Info	0	10.0.100.190	172.16.15.10	0	0	julian	View
JuniperSA @ 10.0.3.50	JuniperSA @ 10.0.3.50	1 Aug 16, 2018, 11:54:32 AM	Misc Logout	Info	0	10.0.100.190	10.0.3.50	0	0	julian_vanasche	View
SM # session_manager	SM # session_manager	1 Aug 16, 2018, 11:54:32 AM	Messages	Info	0	10.0.110.123	169.254.2.35	0	0	jodi_verduzco	View
LinuxServer @ db.acm...	LinuxServer @ db.acm...	1 Aug 16, 2018, 11:54:32 AM	Host Login Succeeded	Info	10327	10.0.110.123	10.0.220.15	0	0	jodi_verduzco	View
Custom Rule Engine-8...	Custom Rule Engine-8...	1 Aug 16, 2018, 11:54:31 AM	User Privilege	Info	3405	10.0.230.169	10.0.3.40	0	0	travis_tom	View
VpnConcentrator @ vp...	VpnConcentrator @ vp...	1 Aug 16, 2018, 11:54:31 AM	Host Login Succeeded	Info	0	10.0.230.2	10.0.230.2	0	0	sandy_spencer	View
IBMi @ 10.0.3.40	IBMi @ 10.0.3.40	1 Aug 16, 2018, 11:54:31 AM	System Status	Info	0	10.0.3.40	10.0.3.40	0	0	travis_tom	View
IBMi @ 10.0.3.40	IBMi @ 10.0.3.40	1 Aug 16, 2018, 11:54:31 AM	System Status	Info	0	10.0.3.40	10.0.3.40	0	0	travis_tom	View
IBMi @ 10.0.3.40	IBMi @ 10.0.3.40	1 Aug 16, 2018, 11:54:31 AM	User Account Changed	Info	3405	10.0.230.169	10.0.3.40	0	0	travis_tom	View
IBMi @ 10.0.3.40	IBMi @ 10.0.3.40	1 Aug 16, 2018, 11:54:31 AM	System Status	Info	0	10.0.3.40	10.0.3.40	0	0	travis_tom	View
IBMi @ 10.0.3.40	IBMi @ 10.0.3.40	1 Aug 16, 2018, 11:54:31 AM	System Configuration	Info	0	10.0.3.40	10.0.3.40	0	0	travis_tom	View
IBMi @ 10.0.3.40	IBMi @ 10.0.3.40	1 Aug 16, 2018, 11:54:31 AM	System Status	Info	3405	10.0.230.169	10.0.3.40	0	0	travis_tom	View
IBMi @ 10.0.3.40	IBMi @ 10.0.3.40	1 Aug 16, 2018, 11:54:31 AM	System Informational	Info	0	10.0.3.40	10.0.3.40	0	0	travis_tom	View
IBMi @ 10.0.3.40	IBMi @ 10.0.3.40	1 Aug 16, 2018, 11:54:31 AM	System Status	Info	3405	10.0.230.169	10.0.3.40	0	0	travis_tom	View
IBMi @ 10.0.3.40	IBMi @ 10.0.3.40	1 Aug 16, 2018, 11:54:31 AM	Access Denied	Info	0	10.0.3.40	10.0.3.40	0	0	travis_tom	View
IBMi @ 10.0.3.40	IBMi @ 10.0.3.40	1 Aug 16, 2018, 11:54:31 AM	System Status	Info	3405	10.0.230.169	10.0.3.40	0	0	travis_tom	View

Filter on Username is dwhight_bird
Filter on Username is not dwhight_bird
Quick Filter...
False Positive
View path from 10.0.230.104 to 10.0.10.41
View in DSM Editor
More Options...
View Assets
View Events
Open in Session Manager

QWAD WinCollect Assisted Deployment

Automatically installs and configures IBM WinCollect Agents in unmanaged mode, and includes:



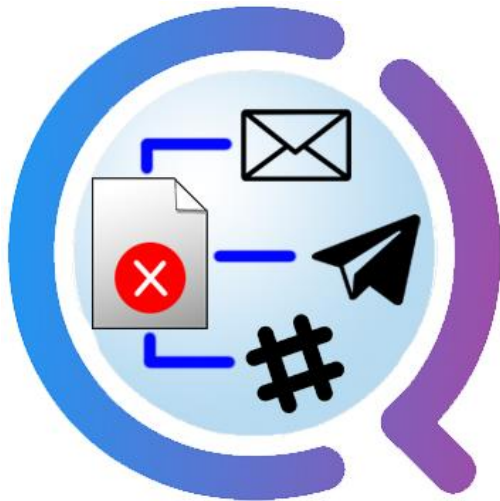
- Auto-detection & configuration of all supported Windows logs: Event Log, MS IIS, MS SQL, DNS Debug, DHCP and MS Exchange
- Detection and configuration of custom logs via File Forwarder
- Sending logs to specific destination (Event Collector) based on subnet the Windows server belongs to
- Sending logs to multiple destinations (Event Collectors) Individual Log Source ID for each configured source
- Eliminates cases of log sources mixture, e.g. when DHCP logs are received in Windows Event log source
- Automatic Sysmon deployment and configuration
- XPath queries support and Integration with VirusTotal

QWAD WinCollect Assisted Deployment

Automatically installs and configures IBM WinCollect Agents in unmanaged mode, and includes:

- Auto-detection & configuration of all supported Windows logs: Event Log, MS IIS, MS SQL, DNS Debug, DHCP and MS Exchange
- Detection and configuration of custom logs via File Forwarder
- Sending logs to specific destination (Event Collector) based on subnet the Windows server belongs to
- Sending logs to multiple destinations (Event Collectors)
- Custom patching mechanism does not require .NET 3.5 to be installed on the system
- No need for manual log source configuration via WinCollect Console in unmanaged mode
- Single executable file without dependencies
- Individual Log Source ID for each configured source (e.g. 'dhcp-hr-10.0.0.3', which is not feasible with managed WinCollect deployments)
- Eliminates cases of log sources mixture, e.g. when DHCP logs are received in Windows Event log source
- Easy to deploy: just a single configuration file to roll out on all required servers via GPO
- Easy to diagnose: provides on-demand debug logs and WinCollect configuration details
- Automatic re-configuration and log sources detection without re-installing the agent
- Automatic Sysmon deployment and configuration
- XPath queries support and Integration with VirusTotal

QIN Incident Notifier



Enhanced notification mechanism designed to notify on triggered offenses via email, Telegram and Slack. Notification emails include:

Offense information

Correlation rule information

Affected asset information

Event information

Flow information

HTML tags in custom templates

QIN Incident Notifier

From: QRadar
Sent: Monday, February 3, 2020 5:44 PM
To: QRadar Admin
Subject: Multiple Login Failures for the Same User containing An authentication attempt was unsuccessful - ID:18577

QRadar Offense Information:

Offense ID	Offense Name	Offense Category	Start Time	End Time	Cred/Rel/Sev
18577	Multiple Login Failures for the Same User containing An authentication attempt was unsuccessful	General Authentication Failed; User Login Failure	2020-01-16 20:36:48	2020-01-31 08:11:51	4 / 3 / 4

Offense Type: Unknown
 Offense Source: unknown

N/A

Manage Offense: [Close](#) or [View](#)

Rules:

Rule Type	Rule Name	Rule Description	Rule Tests
EVENT	Multiple Login Failures for Single Username	Reports authentication failures for the same username	When an event matches any of the following BB:CategoryDefinition: Authentication Failures and when at least 10 events are seen with the same Username in 5 minutes

Events and Flows [Total: 10, Showed: 10]:

Source				Destination				Device Name	Device Time	Payload	Event Count
IP	Port	Username	Network	IP	Port	Username (from RefSet)	Network				
10.0.15.10	0	unknown	Net_10_0_0_0	10.0.15.10	0	john_doe	Net_10_0_0_0	Custom Rule Engine-105 :: qradar-ep01	2020-01-28 14:34	Multiple Login Failures for the Same User Detected multiple (10) authentication failures for the same user name in a 5 minute period.	1
10.0.15.10	0	unknown	Net_10_0_0_0	10.0.15.10	0	john_doe	Net_10_0_0_0	Linux:Server @ 10.0.15.10	2020-01-28 14:33	<182>Jan 28 14:33:16 10.0.15.10 login: pam_unix(remote:auth): check pass; user unknown	1
10.0.120.70	0	unknown	Net_10_0_0_0	10.0.120.70	0	john_doe	Net_10_0_0_0	Linux:Server @ 10.0.120.70	2020-01-28 14:33	<182>Jan 28 14:33:09 10.0.120.70 login: pam_unix(remote:auth): check pass; user unknown	1
10.0.15.20	0	unknown	Net_10_0_0_0	10.0.15.20	0	john_doe	Net_10_0_0_0	Linux:Server @ 10.0.15.20	2020-01-28 14:33	<182>Jan 28 14:33:09 10.0.15.20 login: pam_unix(remote:auth): check pass; user unknown	1
10.0.15.20	0	unknown	Net_10_0_0_0	10.0.15.20	0	john_doe	Net_10_0_0_0	Linux:Server @ 10.0.15.20	2020-01-28 14:33	<182>Jan 28 14:33:02 10.0.15.20 login: pam_unix(remote:auth): check pass; user unknown	1
10.0.120.70	0	unknown	Net_10_0_0_0	10.0.120.70	0	john_doe	Net_10_0_0_0	Linux:Server @ 10.0.120.70	2020-01-28 14:33	<182>Jan 28 14:33:02 10.0.120.70 login: pam_unix(remote:auth): check pass; user unknown	1
10.0.15.10	0	unknown	Net_10_0_0_0	10.0.15.10	0	john_doe	Net_10_0_0_0	Linux:Server @ 10.0.15.10	2020-01-28 14:33	<182>Jan 28 14:33:02 10.0.15.10 login: pam_unix(remote:auth): check pass; user unknown	1

QMEA Microsoft Exchange Audit



QRadar extension designed to collect Admin Audit and Mailbox Audit log entries from MS Exchange servers. Does not require any Custom DSM or third-party solutions.

QMEA Microsoft Exchange Audit

Configuration

<p>Polling Interval</p> <input type="text" value="5"/> <p><small>Exchange server query interval in minutes</small></p>	<p>Exchange Server Host</p> <input type="text" value="192.168.1.100"/> <p><small>Exchange server IP address or FQDN</small></p>	<p>WinRM Port</p> <input type="text" value="5985"/> <p><small>Exchange server WinRM port (5985 by default)</small></p>	<div style="border: 1px solid #ccc; padding: 5px; background-color: #f9f9f9;"> <p style="color: green; font-weight: bold; margin: 0;">Exchange Audit Tool</p> <p style="color: green; font-weight: bold; margin: 0;">Exchange Audit Tool</p> <p style="color: green; font-weight: bold; margin: 0;">Exchange Audit Tool</p> </div> <div style="margin-top: 10px;"> Poll Now Reset Last Collect Time </div>
<p>Domain Name</p> <input type="text" value="example.com"/> <p><small>The name of the user account domain</small></p>	<p>User Name</p> <input type="text" value="admin"/> <p><small>The name of the user account (no domain prefix)</small></p>	<p>User Password</p> <input type="password" value="*****"/> <p><small>The password of the user account</small></p>	
<p>Authentication</p> <input type="text" value="kerberos"/> <p><small>The type of the authentication</small></p>	<p>Use SSL</p> <input type="text" value="no"/> <p><small>Use SSL for server connection</small></p>	<p>Domain Controller</p> <input type="text" value="192.168.1.100"/> <p><small>Domain Controller IP address or FQDN</small></p>	
<p>Collect Admin Audit</p> <input type="text" value="yes"/> <p><small>Collect Admin Audit logs from server</small></p>	<p>Collect Mailbox Audit</p> <input type="text" value="yes"/> <p><small>Collect Mailbox Audit logs from server</small></p>	<p>EPS Rate</p> <input type="text" value="50"/> <p><small>Events per second rate to forward</small></p>	Close

Hints

Microsoft Exchange Audit Export Tool for IBM Security QRadar SIEM is an application for exporting Microsoft Exchange **Admin Audit** and **Mailbox Audit** logs and forwarding log records via Syslog protocol (TCP/514) to the **QRadar Console** in near-real-time. The audit log format generated by this tool is recognized by QRadar log source auto-discovery mechanism (no need to create log source manually). Supported Microsoft Exchange versions are: 2010 SP1+, 2013, 2016. Initial collect will get audit data for the **last one hour**. You can reset last collect time to start next collect as initial with respective button.

Following steps should be completed on **Microsoft Exchange Server** in order to enable audit logs collection:

- o Enable Windows Remoting (WinRM) [\[link\]](#)
- o Enable Admin Audit [\[link\]](#)
- o Enable Mailbox Audit [\[link\]](#)

Following steps should be applied to **user account** to be used for logs collection:

- o Enable 'RemotePowerShellEnabled' privilege [\[link\]](#)
- o Assign 'Discovery Management' role [\[link\]](#)
- o Assign 'Audit Logs' role [\[link\]](#)

License Information

Exchange Server UUID: XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX

Active Mailboxes: 10

Licensed to: example.com

Licensed Mailboxes: 1000

License Expiration: 31/12/2025

QDATA LDAP Data Enrichment



QRadar extension that synchronizes QRadar Reference Sets and Tables content with information from Active Directory and other LDAP-based storages. QDATA App features are:

- multiple tasks can be created
- manual, periodic or scheduled synchronization
- complex LDAP queries
- advanced configuration
- per-task statistics
- in-app logging

QDATA LDAP Data Enrichment

QDATA App allows to store imported LDAP records in Reference Sets, which makes the data easy to utilize in correlation rules. It is vital when developing rules that depend on specific account type or group of users. For example:

- Someone with Windows administrative account is accessing restricted servers;
- Users from HR department are logged in to Sales file server;
- Exchange server admin is accessing another person's mailbox;

Timestamp: 2019-04-02T13:24:49.768261

Status: Success

Run Edit Delete

Updates:

QRadar Reference Set **test_ldap**

From LDAP:

10.10.10.10:389

Using:

Search Base: DC=scnsoft,DC=com

Search Filter: (&(objectClass=user))



Entry Configuration

Entry Name

Configuration Entry Name

LDAP IP <input type="text" value="10.10.10.10"/>	LDAP Port <input type="text" value="389"/>	SSL YES
<small>LDAP Server IP Address</small>	<small>LDAP Server Port Number</small>	<small>Use SSL connection?</small>

Username

LDAP Username

Password

LDAP Password

Search Base

LDAP Search Base

Search Filter

LDAP Search Filter

Search Attributes

LDAP Search Attributes

QLSI Log Source Inventory



QRadar extension that generates periodical log source reports in Excel format and sends them by email.

Log Source Inventory reports are configurable and separated by domains.

They include log sources in all possible states (OK, in error, warning or timeout, disabled, unknown), all important log source information and a legend presented in XLSX format which allows sorting and filtering.

QOR Offense Reporter

QRadar extension that generates periodical offense reports in Excel format and sends them by email. Incident reports are:



Configurable

Separated by domains

Include all offenses (active, inactive, closed)



Include notes, closing date, reason and user, etc.

Presented in XLSX format which allows sorting and filtering

QSSA Slow Search Alert

QRadar app that notifies users via email when QRadar search duration exceeds the configured threshold.



 noreply@qradar.local
WARNING: Long Lasting Searches Detected
To 

Dear user,

Long-lasting searches found to be executing on  QRadar Console host.
Date generated: .

Following searches are exceeding 1 minute(s) execution time:

Search ID	Exec time (minutes)	Query
22f22d79-3adb-4cf6-a0e2-220985eb14bd	2	select * from events last 3 days;

Manage Search Results or Cancel Search for [Events](#) and [Flows](#)
You will not receive notifications for the searches above for next 24 hours.

NOTE: this is an automatic email. Please do not reply.

QMLA Missing Logs Alert



QRadar extension that notifies users about Log Sources that have stopped sending events.



Uses QRadar log source groups and allows to define an individual timeout for each group individually. Notification are generated and sent via a set of rules shipped with the application.

Provides users with comprehensive information about Log Sources that became idle, including: Log Source name, Log Source Type, Log Source Group, the last time events seen from this Log Source, etc.

QMLA Missing Logs Alert



 **Log Source Group Monitor** 

Entry Configuration


Entry Name: Timeout (minutes):

Configuration Entry Name: Timeout value in minutes:


- Demo Player
- Test Group
- Other



 **Log Source Group Monitor** 

Authentication Token



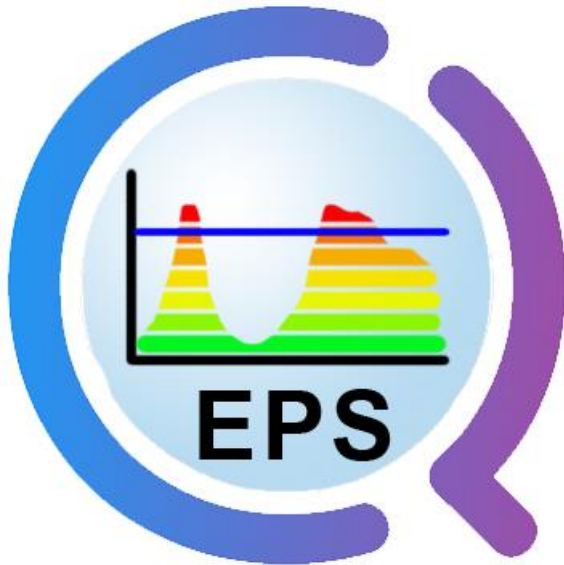
Configuration



Name	Groups	Timeout	
Demo Player		240	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
Test Entry	 <div data-bbox="1275 1099 1468 1242"><p>Group List</p><ul style="list-style-type: none">• Test Group (100074)• Demo Player (100124)• Other (0)</div>	120	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

ScienceSoft Inc. © 2019

QLED Log Source EPS Details



QRadar extension that significantly simplifies monitoring the number of events received by each log source and exceeding configurable EPS threshold.

The application requests data via QRadar API, stores EPS stats in a built-in database and visualizes it via charts in a new QRadar tab.

QLED Log Source EPS Details

EPS per LS

Log Sources

- Snort @ srv-scni-snort
- DC1-DNS-Log
- DC2-DNS-Log
- WindowsAuthServer @ win-scni-dnik
- DC1-Security-log
- WindowsAuthServer @ win-scni-con
- WindowsAuthServer @ win-scni-con
- WindowsAuthServer @ win-scni-con

About

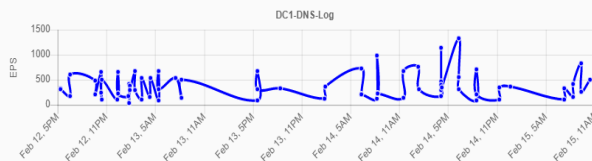
Toggle Sidebar

2019-02-12 📅 17:22 🕒

Apply

EPS per Log Source - Reports

Showing EPS statistics for 8 log source(s) for the 7 day(s) starting from 2019-02-12 17:22



EPS Per LS Configuration ⚙️

Authentication Token +

Configuration -

Polling Interval

1

Data collection recurrence interval in minutes

EPS Limit

1

Minimum EPS value for each log source to get into stats data points

Retention Period

14

Number of days for EPS stats to keep in DB

Show Days Ago

7

Number of days to draw EPS charts for

Show Top X

10

Number of graphs to show

Do Approximate

YES

Do approximation to reduce number of data point for a graph

Approximation Factor

1.5

Deviation, bigger value gives less details. Default is 1.12

Data Query Type

Top X

TopX or specific log source list to display in main app page

Save

QVTI VirusTotal Integration Solution for Hash Verification



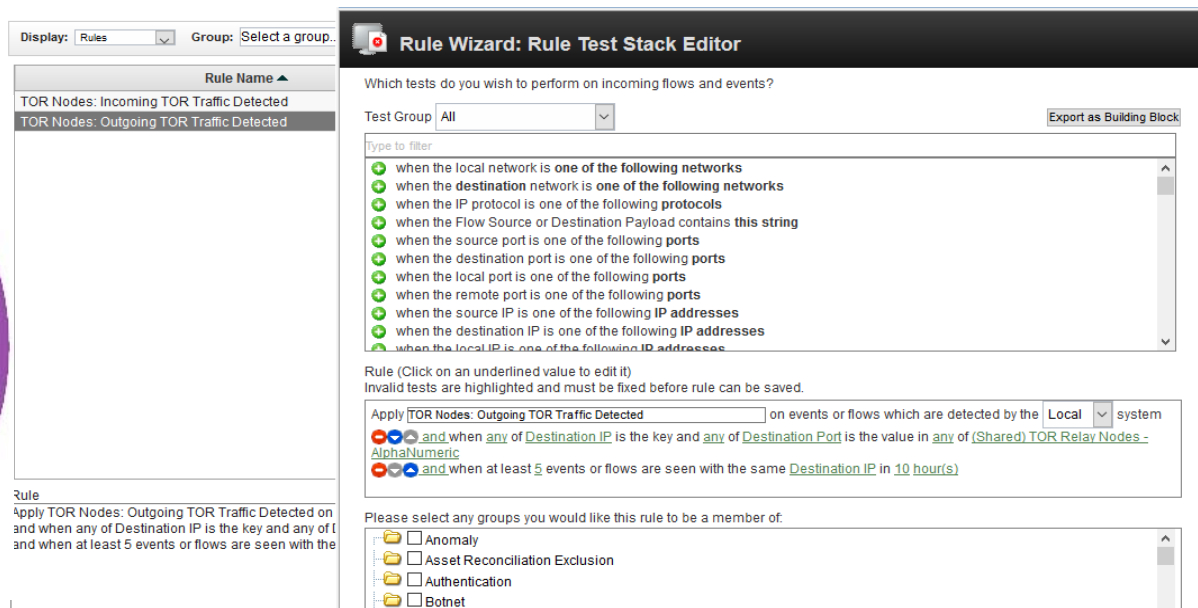
QVTI is an IBM QRadar application for checking software process hashes against VirusTotal database using VirusTotal public API.

The application checks file hashes from incoming events against VirusTotal DB and generates offenses for malicious ones.

QVTI relies on Sysmon log data collected with WinCollect agents.

QTOR Darknet/TOR Nodes Monitoring

Helps users easily monitor inbound and outbound connections to DarkNet via TOR relay and exit nodes.



The screenshot shows the 'Rule Wizard: Rule Test Stack Editor' interface. On the left, a list of rules is displayed under the heading 'Rule Name ▲'. The selected rule is 'TOR Nodes: Outgoing TOR Traffic Detected'. Below this list, a 'Rule' section contains the text: 'Apply TOR Nodes: Outgoing TOR Traffic Detected on and when any of Destination IP is the key and any of l and when at least 5 events or flows are seen with the'. The main area of the wizard is titled 'Which tests do you wish to perform on incoming flows and events?'. It features a 'Test Group' dropdown set to 'All' and an 'Export as Building Block' button. A list of tests is shown, each with a green plus icon and a description: 'when the local network is one of the following networks', 'when the destination network is one of the following networks', 'when the IP protocol is one of the following protocols', 'when the Flow Source or Destination Payload contains this string', 'when the source port is one of the following ports', 'when the destination port is one of the following ports', 'when the local port is one of the following ports', 'when the remote port is one of the following ports', 'when the source IP is one of the following IP addresses', 'when the destination IP is one of the following IP addresses', and 'when the local IP is one of the following IP addresses'. Below the tests, a 'Rule' section allows for configuration: 'Apply TOR Nodes: Outgoing TOR Traffic Detected on events or flows which are detected by the Local system and when any of Destination IP is the key and any of Destination Port is the value in any of (Shared) TOR Relay Nodes - AlphaNumeric and when at least 5 events or flows are seen with the same Destination IP in 10 hour(s)'. At the bottom, a section titled 'Please select any groups you would like this rule to be a member of' includes checkboxes for 'Anomaly', 'Asset Reconciliation Exclusion', 'Authentication', and 'Botnet'.


QEFC Exclude from Correlation button





QRadar extension that allows users to temporarily prevent rules from generating new offenses for specific offense sources (username, IP address, etc.).

The application is useful when incident response team has already identified a compromised host or username and don't need further notifications for the same source until the asset is fully recovered.


QEFC Exclude from Correlation button

SCIENCESoft PROFESSIONAL SOFTWARE DEVELOPMENT Offense WhiteList Button Configuration 

Authentication Token 

Configuration 

INFO: In order to make this solution work please add `OFFENSE.WHITELISTING: Event Marked False Positive` rule to the `FalsePositive: False Positive Rules and Building Blocks` rule test.

Offense Whitelisting TTL 
Number of hours to whitelist offense source

NOTE: you will need to update whitelisting rule(s) when default reference set name is changed.

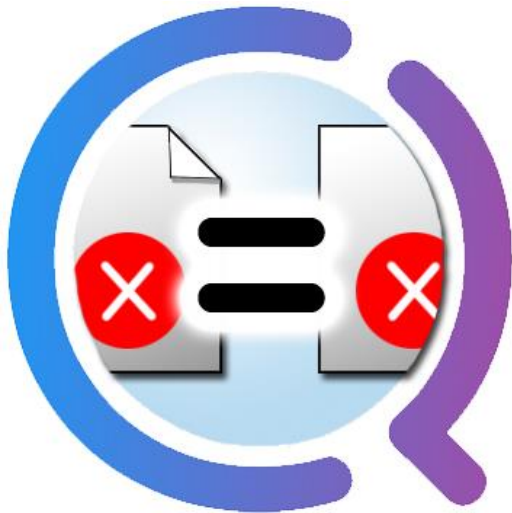
RefSet Name
The name of the ALNIC reference set for whitelisted offense indices

ScienceSoft Inc. © 2019 [v.1.0.0.20190709]

QFSO Find Similar Offenses button

QRadar extension that adds a new button on the Offense details page.

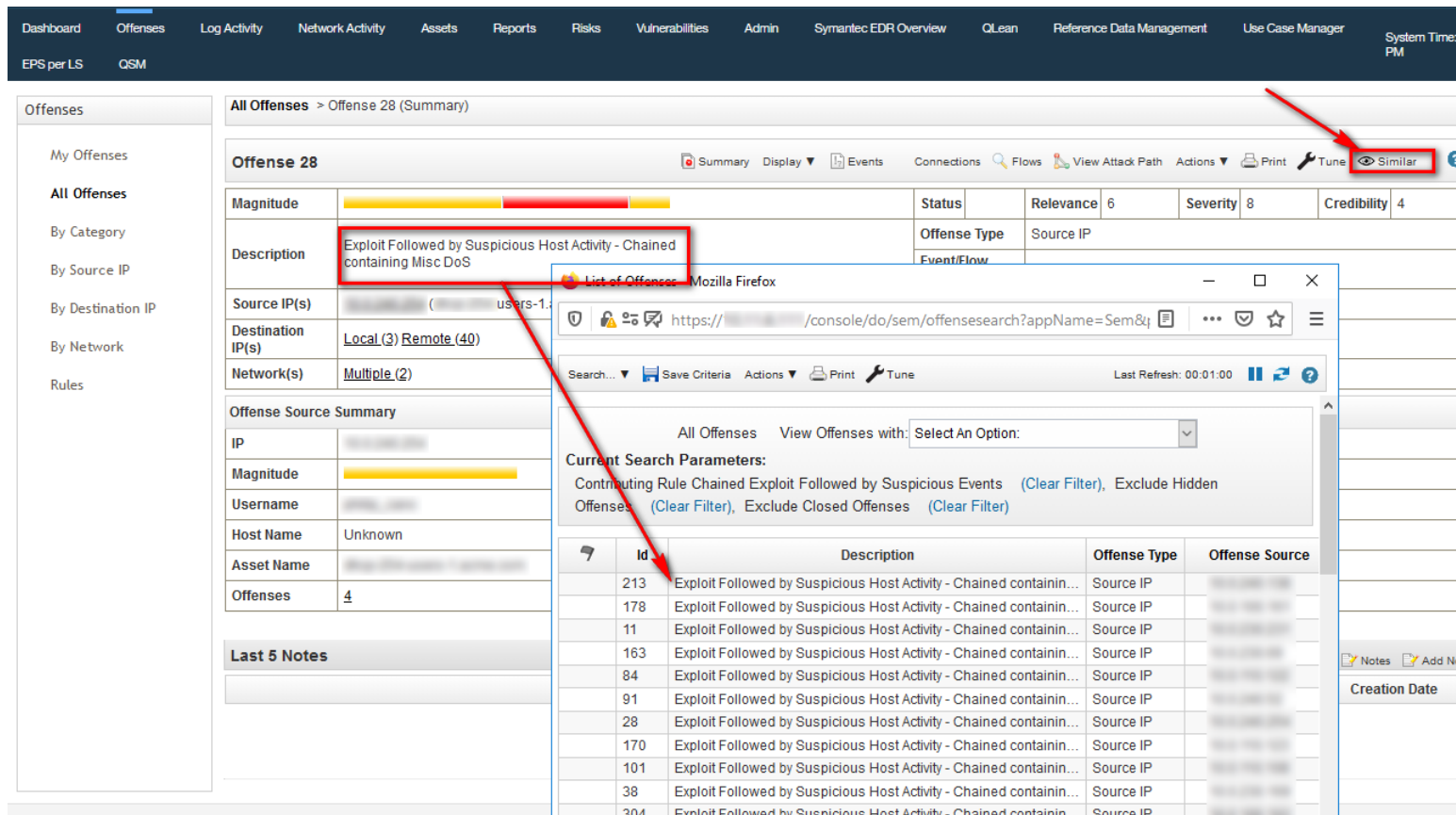
By clicking it user gets a list of all offenses generated by the same rule.



If multiple rules contribute to the offense, the user will be asked to select a specific rule.

The extension is useful to speed up offense investigation and rules tuning.

QFSO Find Similar Offenses button



The screenshot displays the QFSO interface with the 'Find Similar Offenses' button highlighted in a red box. A red arrow points to this button. Below the main interface, a search results window is open, showing a list of offenses with columns for ID, Description, Offense Type, and Offense Source. A red arrow points to the 'Id' column header in the search results table.

Offense 28 Summary:

Magnitude	<div style="width: 100%; height: 10px; background: linear-gradient(to right, yellow, orange, red);"></div>	Status	Relevance	6	Severity	8	Credibility	4
Description	Exploit Followed by Suspicious Host Activity - Chained containing Misc DoS		Offense Type	Source IP				
Source IP(s)	[redacted] (users-1.)		Event/Flow					
Destination IP(s)	Local (3) Remote (40)							
Network(s)	Multiple (2)							

Offense Source Summary:

IP	[redacted]
Magnitude	<div style="width: 100%; height: 10px; background: linear-gradient(to right, yellow, orange, red);"></div>
Username	[redacted]
Host Name	Unknown
Asset Name	[redacted]
Offenses	4

Search Results Table:

ID	Description	Offense Type	Offense Source
213	Exploit Followed by Suspicious Host Activity - Chained containin...	Source IP	[redacted]
178	Exploit Followed by Suspicious Host Activity - Chained containin...	Source IP	[redacted]
11	Exploit Followed by Suspicious Host Activity - Chained containin...	Source IP	[redacted]
163	Exploit Followed by Suspicious Host Activity - Chained containin...	Source IP	[redacted]
84	Exploit Followed by Suspicious Host Activity - Chained containin...	Source IP	[redacted]
91	Exploit Followed by Suspicious Host Activity - Chained containin...	Source IP	[redacted]
28	Exploit Followed by Suspicious Host Activity - Chained containin...	Source IP	[redacted]
170	Exploit Followed by Suspicious Host Activity - Chained containin...	Source IP	[redacted]
101	Exploit Followed by Suspicious Host Activity - Chained containin...	Source IP	[redacted]
38	Exploit Followed by Suspicious Host Activity - Chained containin...	Source IP	[redacted]
304	Exploit Followed by Suspicious Host Activity - Chained containin...	Source IP	[redacted]

QDGA DGA Analyzer

QRadar extension that analyzes domain names using a trained neural network to identify those created by Domain Generation Algorithms (DGA) and notifies security analyst via offenses.



The screenshot displays the ScienceSoft DGA Analyzer web interface. At the top, the ScienceSoft logo and 'DGA Analyzer' title are visible. Below the title bar, there are sections for 'Authentication Token' (with a plus icon) and 'Configuration' (with a minus icon). The configuration section includes a 'Polling Interval' dropdown set to '1', a 'Reference Map of Sets' dropdown set to 'ScienceSoft: DGA Feed', and an 'EPS Limit' dropdown set to '20'. A status message box on the right indicates 'OK - 197 domains has been processed (2020/01/28 17:08:23)' with a 'Check Now' button. At the bottom, there are 'Maps of Set API' and 'Close' buttons. The footer contains the text 'ScienceSoft Inc. © 2020 [v.1.0.0 build 20200128]'.