



SCIENCE SOFT CUSTOM QRADAR APPS QLEAN APP SUITE

REFERENCE
GUIDE

Table of Contents

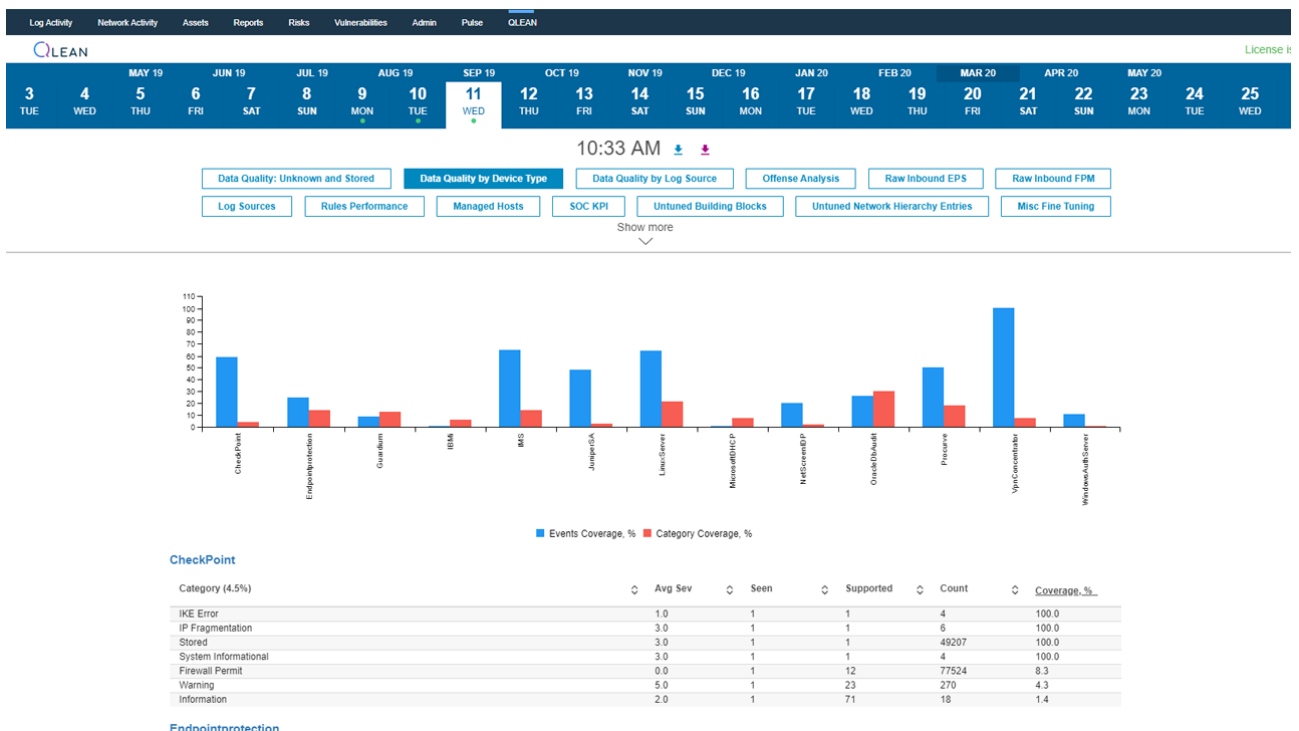
QLean for Tuning & Health Check [commercial]	3
QEXEQ - Executive Reports [commercial]	5
QMEA - Microsoft Exchange Audit [commercial]	6
QDATA - LDAP Data Enrichment [free].....	7
QVTI - VirusTotal Integration for Hash Checking [free]	9
QTOR - TOR Nodes Monitoring [free].....	10
QMLA - Missing Logs Alert [free].....	11
QLSI - Log Source Inventory [free]	12
QSSA - Slow Search Alert [free]	13
QOR - Offense Reporter [free].....	14
QWAD - WinCollect Assisted Deployment [commercial]	15
QLED - Log Source EPS Details [free]	18
QEFC - Exclude From Correlation [free]	19
QFSO - Find Similar Offenses [free]	20
QDGA - DGA Analyzer [free].....	21
QSM Session Manager [free]	22
QIN - Incident Notifier [commercial]	23
QArtifact [commercial]	25
Addon 1: MITRE for QRadar	27
Addon 2: Custom DSM.....	27
Addon 3: Coming Soon	27

QLean for Tuning & Health Check [commercial]

QLEAN (previously known as HCF or Health Check Framework) is the most advanced app for QRadar fine tuning and health check. QLEAN makes QRadar maintenance easy and transparent by optimizing and automating routine SOC processes and a wide range of advanced fine tuning and health check procedures that can free up to 30% QRadar admin time.

QLEAN Unique Value

- Over 50 advanced performance and behavioral metrics including Data Quality, Offense Analysis, Raw EPS and FPI timeline, Rules Performance, SOC KPIs, Fine Tuning and many others
- XLS/JSON reporting, scheduled mode, advanced innovative metrics independent of the QRadar API version
- An instant complete snapshot of the system state and data quality with timeline that makes it easy to investigate security threats & top offenses
- Savings of up to 250 admin hours annually per average deployment
- Helps improve log data coverage
- Helps improve efficiency of SIEM license use and data quality
- A single-component plug & play architecture
- Advanced report delivered via email
- Significantly lower QRadar maintenance costs and improved ROI
- Higher client/operator satisfaction
- User base includes major banks, MSSPs, Fortune 500 companies and government organizations



For a complete list of supported metrics with the detailed description please visit: [LINK](#)

QLEAN has been named finalist as Outstanding Security Solution by IBM 2020 & 2021 Beacon Awards.

QLEAN.io website: [LINK](#)

QLEAN interactive online demo: [LINK](#)

QLEAN sample report: [LINK](#)

QLEAN video: [LINK](#)

The screenshot shows the QLEAN dashboard interface. At the top, there is a navigation bar with tabs for Offenses, Log Activity, Network Activity, Assets, Reports, Risks, Vulnerabilities, Admin, Pulse, and QLEAN. Below this is a header area with a clock showing 03:35 PM and several filter buttons: Data Quality: Unknown and Stored, Data Quality by Device Type, Data Quality by Log Source, Offense Analysis, Raw Inbound EPS, Raw Inbound FPM, Log Sources, Rules Performance, Managed Hosts, SOC KPI, Untuned Building Blocks, Untuned Network Hierarchy Entries, and Misc Fine Tuning. A 'Show more' link is also present.

The main content area is titled 'All log sources' and contains a table with the following columns: Source Name, Identid..., Activity, Last seen, Average EPS, Peak EPS, Peak EPS date, Proto..., Source Type, Extens..., Added, Addition type, Bulk, Status, Groups, Desc..., and Modified. The table lists various log sources such as Forcepoint V Series, Checkpoint-Spam-Test, Symantec, LinuxServer, swift_alliance, MicrosoftDNS, Linux @ Fresh, Citrix Xen Mobile, OracleDbAudit, WindowsAuthServer, NetScreenDP, and LinuxServer. A context menu is open over the 'NetScreenDP' source, showing options like 'Select All', 'LinuxServer', 'MicrosoftDHCP', 'MicrosoftDNS', 'NetScreenDP', 'OracleDbAudit', 'PostFixMailTransferAgent', 'Procurve', 'ResilientTestCustom', and 'SMCustom'. 'OK' and 'Cancel' buttons are at the bottom of the menu.

License

Free QLEAN demo version contains limited functionality available without a license. Some of the metrics are available in the XLS report. To start a free trial of the full version and request professional SIEM services please request a license key by emailing QLEAN tech support at qlean@scnsoft.com

IBM App Exchange

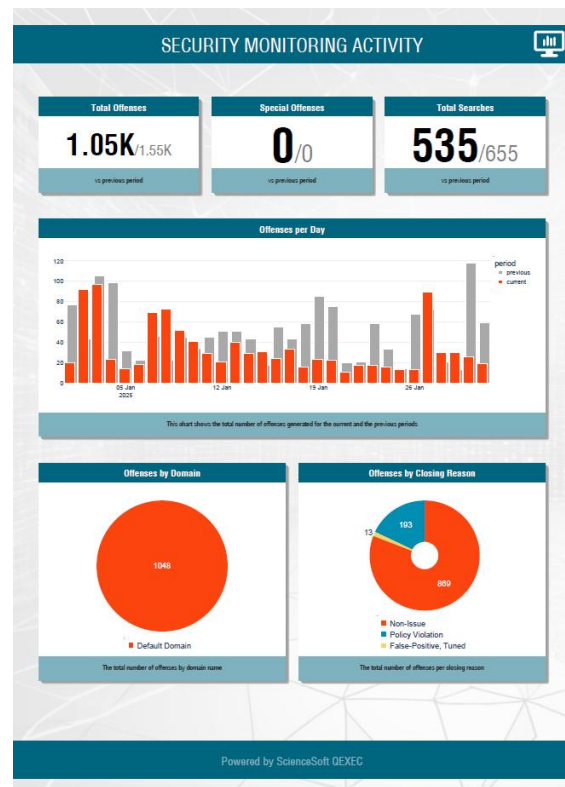
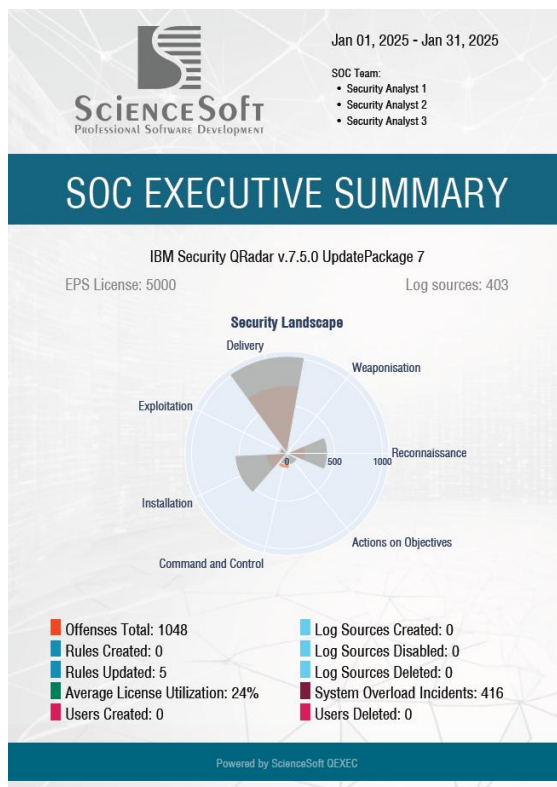
<https://apps.xforce.ibmcloud.com/extension/24f7cc75935dd411474001bd175c2d69>

QEXEQ – Executive Reports [commercial]

QEXEQ is IBM QRadar SIEM add-on developed by ScienceSoft which closes this gap by delivering fully automated, unbiased security insights. This solution pulls rich security intelligence directly from QRadar and presents it to executives without manual intervention, eliminating the risk of human bias and oversight in reporting.

QEXEQ Unique Value

By providing a single source of truth on security for leadership, QEXEQ bridges the gap between the SOC and the C-suite. It turns your existing IBM QRadar deployment into an executive decision-support system, ensuring that the valuable data QRadar collects is translated into actionable intelligence at the highest level. Busy executives can quickly grasp the organization’s security health, track improvements or emerging threats, and steer strategy with confidence. With fully automated, unbiased reporting, there’s no need to rely on overburdened analysts to manually compile updates. The result is stronger governance and faster response: when leaders see the full security picture clearly, they can allocate budget, adjust policies, and initiate security initiatives proactively.



Automated & Unbiased Reporting: QEXEQ continuously analyzes SIEM data and generates executive-ready reports on a scheduled basis – no spreadsheets or analyst compilation needed. This ensures a complete, unfiltered picture of threats and incidents, so nothing critical gets lost in translation. Leaders gain confidence that they’re seeing the whole story, not a curated subset (addressing the common concern that current security reports often fall short).

Adaptive Baselines: Whether you’re a lean small business or a complex global enterprise, QEXEQ provides a 360° view of your security environment. Like ScienceSoft’s other QRadar tools that add value to deployments “of all sizes”, QEXEQ scales to cover your entire infrastructure, aggregating data across all systems and locations. Executives in even the smallest teams can

leverage the same full- spectrum visibility as those in large enterprises – leveling the playing field in security oversight.

Posture Tracking & Trends: QEXEQ gives executives a dynamic dashboard of security metrics and trends over time. It highlights patterns such as rising incident volumes or improving response times, offering a clear snapshot of your security posture month-by-month. This means the boardroom can quickly identify positive or negative trends and react before small issues grow into serious risks.

License

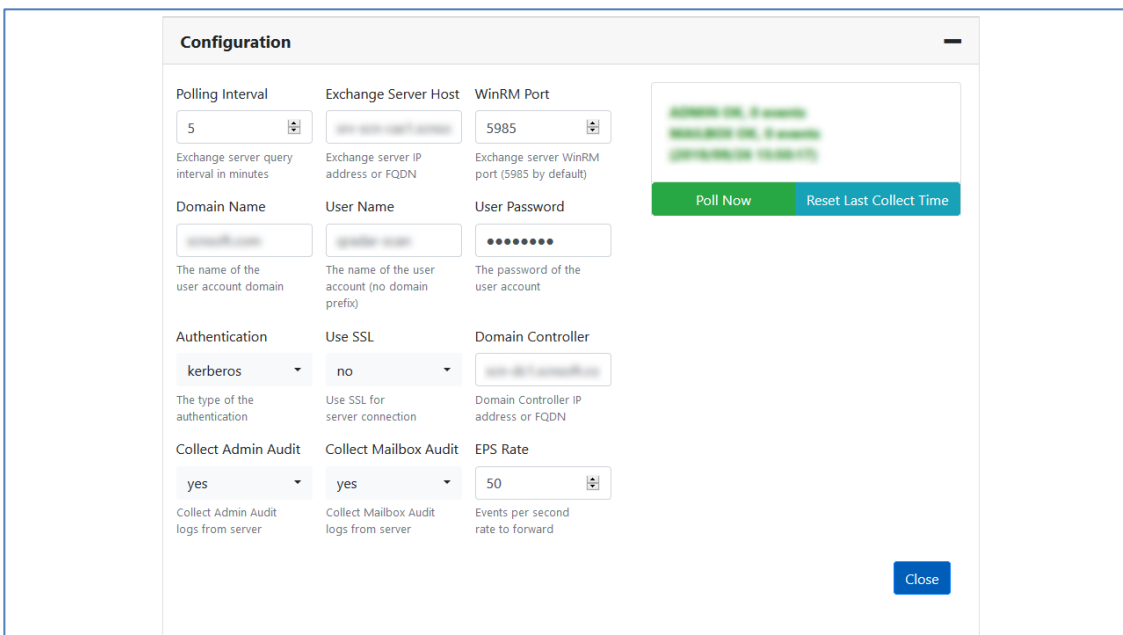
Free QEXEQ demo version contains full functionality with the only limitation of generating reports for 3-day periods only. The full version allows you to generate weekly and monthly reports. To start a free trial of the full version and request professional SIEM services please request a license key by emailing QEXEQ tech support at glean@scnsoft.com

Link

https://glean.io/qexeq.html#download_qexeq

QMEA - Microsoft Exchange Audit [commercial]

QMEA Microsoft Exchange Audit Export Tool for QRadar enables easy export of Microsoft Exchange Admin Audit and Mailbox Audit logs and forwards log records via Syslog protocol (TCP/514) to QRadar SIEM Console IP in near real-time. QMEA's audit log format is automatically recognized by QRadar so there is no need in custom DSM. Supported Microsoft Exchange versions are: 2010 SP1+/2013/2016.



The screenshot displays the 'Configuration' window for QMEA. It contains several sections for setting up the tool:

- Polling Interval:** A dropdown menu set to '5'.
- Exchange Server Host:** A text input field for the Exchange server IP address or FQDN.
- WinRM Port:** A dropdown menu set to '5985'.
- Domain Name:** A text input field for the user account domain.
- User Name:** A text input field for the user account name (no domain prefix).
- User Password:** A password input field with masked characters.
- Authentication:** A dropdown menu set to 'kerberos'.
- Use SSL:** A dropdown menu set to 'no'.
- Domain Controller:** A text input field for the Domain Controller IP address or FQDN.
- Collect Admin Audit:** A dropdown menu set to 'yes'.
- Collect Mailbox Audit:** A dropdown menu set to 'yes'.
- EPS Rate:** A dropdown menu set to '50'.

Additional features include a 'Poll Now' button, a 'Reset Last Collect Time' button, and a 'Close' button at the bottom right.

Logs Collection

Initial collect will get audit data for the last 1 hour. You can reset last collect time to start next collect as initial with respective button in configuration window. To minimize potential performance impact for Exchange Server, if last collect time is more than 24 hours ago, the actual audit logs collection will be performed only for the recent 24 hours.

QRadar Native Alternatives

These logs are not available via standard QRadar protocols. Third-party LogBinderEX solution is much more expensive and requires agent installation on target servers.

License

QMEA is a commercial application with a single limitation: non-licensed mode allows only to perform collect once per 6 hours. Continued near-real-time audit logs collection is available only when the proper license is applied. To unlock continuous near real-time monitoring or request a PoC, please contact us at qlean@scnsoft.com. You can also request [QRadar Professional Services](#) for assistance.

IBM App Exchange

<https://apps.xforce.ibmcloud.com/extension/c14345f935164d5b397f79f10dd93f70>

QDATA - LDAP Data Enrichment [free]

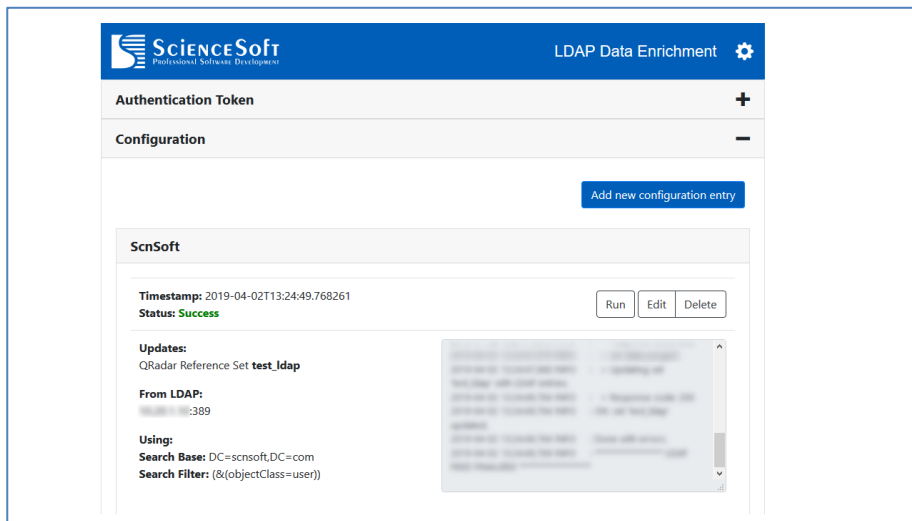
QDATA LDAP Data Enrichment is a free application by [ScienceSoft](#) that synchronizes the content of QRadar reference sets and tables with information from Active Directory and other LDAP-based storages.

QDATA supports:

- Multiple tasks with either periodic or scheduled synchronization
- Complex LDAP queries
- Advanced configuration
- Per-task statistics
- In-app logging

QDATA is vital for developing rules that depend on specific account type or group of users. Use cases include:

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



Using a simple flat list with usernames (reference set), it's just a matter of configuring a proper LDAP query in QDATA and adding e.g. "when any of Username are contained in any of Corp_Admin_Accounts" as a rule test.

QRadar Native Alternatives

The official QRadar LDAP extension provides imported data in a format that cannot be used in correlation rules.

License

Open Source / Apache 2. To start a free trial of any other QLEAN App Suite tools or request a custom application development contact us at qlean@scnsoft.com or [QLEAN App Suite website](http://qlean.scnsoft.com). You can also request [QRadar Professional Services](#) for assistance.

IBM App Exchange

<https://exchange.xforce.ibmcloud.com/hub/extension/8259e5edf13edc14c430d45a19eedb45>

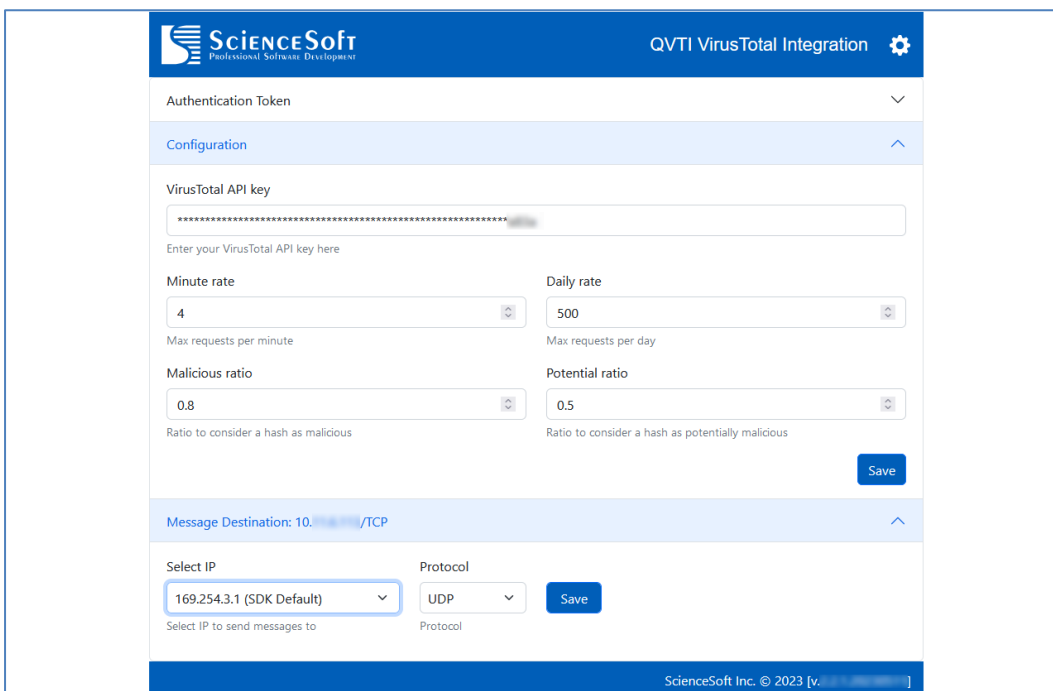
QVTI - VirusTotal Integration for Hash Checking [free]

QVTI Virus Total Integration for IBM Security QRadar SIEM (aka QVTI) is an application for checking software process hashes against VirusTotal DB using VirusTotal public API.

This QRadar extension checks new incoming hashes against VirusTotal DB, stores legitimate hashes to 'clean' Reference Set and generates offenses on malicious ones.

QVTI relies on the log data provided by Sysmon forwarded via WinCollect.

Automatic Sysmon/WinCollect installation and configuration is possible with *QWAD - WinCollect Assisted Deployment* application (see below).



The screenshot shows the configuration page for QVTI VirusTotal Integration. At the top, there's a header with the ScienceSoft logo and the title 'QVTI VirusTotal Integration'. Below the header, there are several sections:

- Authentication Token:** A dropdown menu.
- Configuration:** A section with a blue header and an upward arrow.
- VirusTotal API key:** A text input field with a masked key and a placeholder 'Enter your VirusTotal API key here'.
- Minute rate:** A dropdown menu set to '4' with the label 'Max requests per minute'.
- Daily rate:** A dropdown menu set to '500' with the label 'Max requests per day'.
- Malicious ratio:** A dropdown menu set to '0.8' with the label 'Ratio to consider a hash as malicious'.
- Potential ratio:** A dropdown menu set to '0.5' with the label 'Ratio to consider a hash as potentially malicious'.
- Message Destination:** A section with a blue header and an upward arrow, showing '10. /TCP'.
- Select IP:** A dropdown menu set to '169.254.3.1 (SDK Default)' with the label 'Select IP to send messages to'.
- Protocol:** A dropdown menu set to 'UDP' with the label 'Protocol'.
- Save:** A blue button to save the configuration.

At the bottom of the page, there is a footer: 'ScienceSoft Inc. © 2023 [v.]'.

QRadar Native Alternatives

No such functionality in QRadar. Users have to manually extract hashes from payload and upload them to VirusTotal.

License

Open Source / Apache 2. To start a free trial of any other QLEAN App Suite tools or request a custom application development contact us at qlean@scnsoft.com or [QLEAN App Suite website](#). You can also request [QRadar Professional Services](#) for assistance.

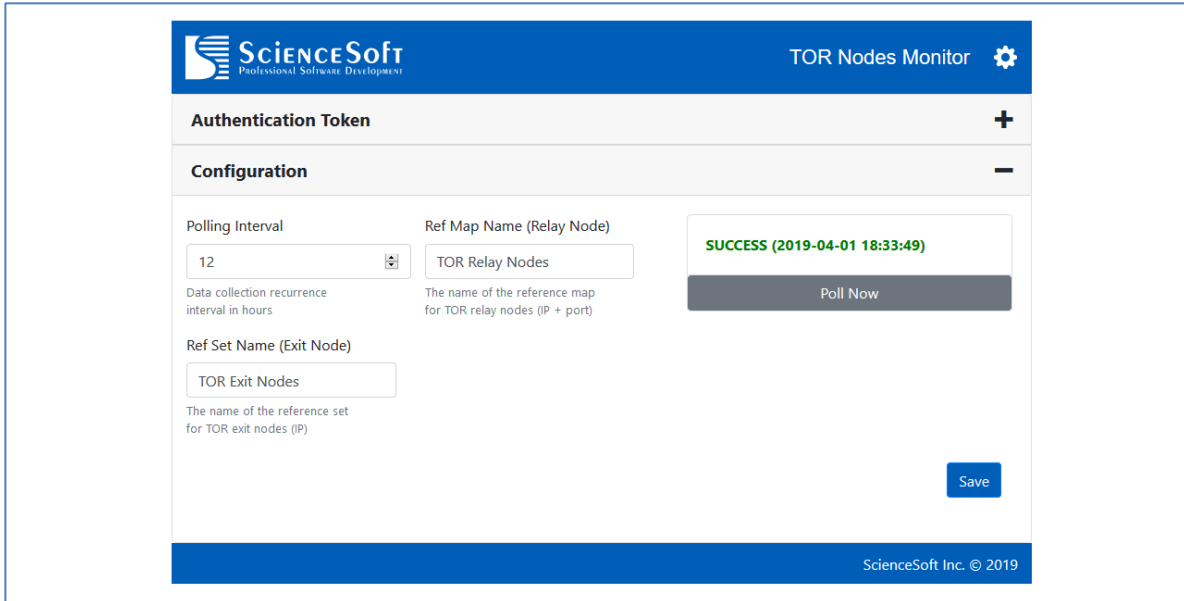
IBM App Exchange

<https://exchange.xforce.ibmcloud.com/hub/extension/db73ab17547d28409303c2c2583a5160>

QTOR – TOR Nodes Monitoring [free]

QTOR TOR Nodes Monitoring is a QRadar app that lets you easily monitor inbound and outbound connection to Darknet via TOR relay and exit nodes.

QTOR requires Internet access to reach <https://onionoo.torproject.org> website which is used to gather information about active relay and exit TOR nodes



The screenshot shows the configuration page for the 'TOR Nodes Monitor' app. At the top, there is a ScienceSoft logo and the app name 'TOR Nodes Monitor' with a settings gear icon. Below this are sections for 'Authentication Token' (with a plus icon) and 'Configuration' (with a minus icon). The configuration section includes:

- Polling Interval:** A text input field containing '12' with a dropdown arrow. Below it, the text reads 'Data collection recurrence interval in hours'.
- Ref Map Name (Relay Node):** A text input field containing 'TOR Relay Nodes'. Below it, the text reads 'The name of the reference map for TOR relay nodes (IP + port)'.
- Ref Set Name (Exit Node):** A text input field containing 'TOR Exit Nodes'. Below it, the text reads 'The name of the reference set for TOR exit nodes (IP)'.

 To the right of these fields, there is a green success message: 'SUCCESS (2019-04-01 18:33:49)' and a grey 'Poll Now' button. At the bottom right of the configuration area is a blue 'Save' button. The footer of the interface reads 'ScienceSoft Inc. © 2019'.

QTOR package contains the following security content:

- QRadar application to poll TOR nodes
- Two custom rules for inbound and outbound TOR connections monitoring (works for both events and flows)

QRadar Native Alternatives

No such functionality in QRadar. Users have to manually extract and search for the required data.

License

Open Source / Apache 2. To start a free trial of any other QLEAN App Suite tools or request a custom application development contact us at qlean@scnsoft.com or [QLEAN App Suite website](#). You can also request [QRadar Professional Services](#) for assistance.

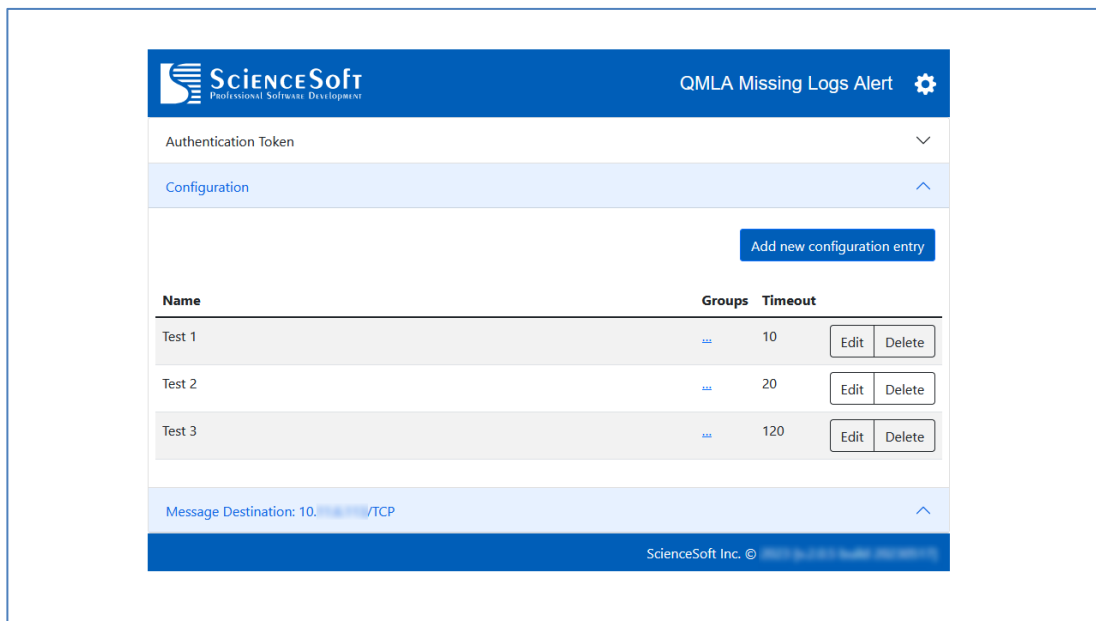
IBM App Exchange

<https://exchange.xforce.ibmcloud.com/hub/extension/a223db85970ba80e85dec70a52a279a3>

QMLA - Missing Logs Alert [free]

QMLA Missing Logs Alert is a QRadar app that allows users to easily monitor Log Sources that stopped sending events.

QMLA works at the log source group level and allows to specify timeout values for each log source group individually. This application provides users with comprehensive information about Log Sources that stopped sending events (that includes: Log Source Name, Log Source Type, Log Source Group, the last time events were seen from this Log Source, etc.)



QRadar Native Alternatives

QRadar does allow to notify for Log Source group not sending logs, but requires separate custom rule to be implemented for each group. QRadar native notifications for idle groups do not contain specific Log Source name, so administrator is unable to identify specific log source(s) which are not sending events any more.

License

Open Source / Apache 2. To start a free trial of any other QLEAN App Suite tools or request a custom application development contact us at qlean@scnsoft.com or [QLEAN App Suite website](#). You can also request [QRadar Professional Services](#) for assistance.

IBM App Exchange

<https://exchange.xforce.ibmcloud.com/hub/extension/eec42bd10ed3fed6d7841a41c01cfed9>

QLSI - Log Source Inventory [free]

QLSI Log Source Inventory is a QRadar app that generates periodical log sources reports in Excel format and sends them by email. QLSI reports are:

- configurable
- include log sources with all possible statuses (OK, in error, warning/timeout, disabled, unknown)
- include all major log source information and a legend
- XLSX formatted - allows sorting and filtering

You can also generate on-demand report and download it from UI. Two timeouts are applicable for each log source: default one (720 minutes) and custom (72h) that will help to differentiate log source inactivity as short-term and long-term.

Log Source Inventory		ScienceSoft		2023-03-16				Default Domain
NAME	STATUS	DESCRIPTION	TYPE	GROUPS	IDENTIFIER	CREATION DATE		
ASA @ asa-fake	SUCCESS	ASA device	Cisco Adaptive Security Appliance (/	Other		2021-01-19 10:04:06	202	
Check Point @ fake-Is	SUCCESS	Check Point device	Check Point	Other		2022-07-12 13:42:14	202	
Checkpoint @ fw-noise	TIMEOUT 72h		Check Point	Other		2022-10-17 13:44:30	202	
CrowdStrike Audit	TIMEOUT 72h	Audit Events	CrowdStrikeAudit	Another,Test		2022-02-04 18:21:45	202	
CrowdStrike Detection	TIMEOUT 72h	Detection	CrowdStrikeEndpoint	Other		2019-01-03 19:25:03	201	
CrowdStrike Firewall	TIMEOUT 72h	Firewall Events	CrowdStrikeFirewall	Other		2022-02-08 18:12:58	202	
CrowdStrike Identity	TIMEOUT 72h	Identity Protection Events	CrowdStrikeIdentity	Other		2022-02-09 18:56:44	202	
CrowdStrike Incident	TIMEOUT 72h	Log Source for Incident Sun	CrowdStrikeIncident	Other		2022-01-24 21:32:54	202	
CrowdStrike Recon	TIMEOUT 72h	Recon Events	CrowdStrikeRecon	Other		2022-02-08 22:12:52	202	
DBWincollect	TIMEOUT 72h		Microsoft Windows Security Event L	Other		2021-03-15 15:52:39	202	
DNS_EU	TIMEOUT 72h		Microsoft DNS Debug	Other		2021-03-19 11:28:32	202	
DNS_US	TIMEOUT 72h		Microsoft DNS Debug	Other		2021-03-19 11:27:38	202	
Endpointprotection @ SymantecServer	SUCCESS	Endpointprotection device	Symantec Endpoint Protection	Other		2021-01-19 08:27:18	202	
Forcepoint V Series @	SUCCESS	Forcepoint V Series	Forcepoint V Series	Test		2020-11-18 14:16:32	202	
Forcepoint V Series @	TIMEOUT 12h	Forcepoint V Series	Forcepoint V Series	Other		2023-03-01 14:38:17	202	
FortiGate @	SUCCESS	FortiGate device	Fortinet FortiGate Security Gateway	Other		2023-02-07 12:14:02	202	
Guardium @ g8	SUCCESS	Guardium device	IBM Guardium	Other		2021-01-19 08:26:01	202	
IBM DLC Metrics @ dlc.siemd172f4d2-9268	TIMEOUT 12h	IBM DLC Device	IBM DLC Metrics	Other		2022-12-07 11:51:01	202	
IBM i @ as400-fake	SUCCESS	IBM i Device	IBM i	Other		2021-01-19 08:29:22	202	
IIS @ scnsoft-iis-default-web-site-	TIMEOUT 72h	IIS device	Microsoft IIS	Other		2021-01-28 10:57:09	202	
IIS @ test-iis-default-web-site-	TIMEOUT 72h	IIS device	Microsoft IIS	Other		2021-06-16 21:31:08	202	
IIS @ test00-iis-default-web-site-	TIMEOUT 72h	IIS device	Microsoft IIS	Other		2021-04-21 21:32:00	202	
LinuxServer @ centos	TIMEOUT 72h	LinuxServer device	Linux OS	Other		2021-08-23 14:27:03	202	
LinuxServer @ centos6	TIMEOUT 72h	LinuxServer device	Linux OS	Other		2021-08-26 08:49:06	202	
LinuxServer @ rhel-acme-fake	SUCCESS	LinuxServer device	Linux OS	Other		2021-01-19 08:26:16	202	
LinuxServer @ rhel-acme-fake6	SUCCESS	LinuxServer device	Linux OS	Other		2021-01-19 10:05:10	202	
Meraki MR WAP @	TIMEOUT 72h		Meraki MR Wireless Access Point	Other		2021-02-23 07:46:18	202	
Microsoft DNS Debug @	TIMEOUT 72h	Microsoft DNS Debug device	Microsoft DNS Debug	Another		2020-11-06 11:58:17	202	
Microsoft DNS Debug @	TIMEOUT 72h	Microsoft DNS Debug device	Microsoft DNS Debug	Another		2020-11-06 11:58:34	202	
MicrosoftExchange @	TIMEOUT 12h	MicrosoftExchange device	Microsoft Exchange Server	Other		2023-01-26 06:56:26	202	
MicrosoftExchange @	TIMEOUT 72h	MicrosoftExchange device	Microsoft Exchange Server	Other		2022-10-25 00:41:12	202	

QRadar Native Alternatives

Log Source Management extension and QRadar reports allows exporting to CSV format which is not quite convenient for analysis and reporting. QLSI report also contains unique information which is not available from standard exports, like EPS values per each log source.

License

Open Source / Apache 2. To start a free trial of any other QLEAN App Suite tools or request a custom application development contact us at qlean@scnsoft.com or [QLEAN App Suite website](https://www.scnsoft.com). You can also request [QRadar Professional Services](#) for assistance.


IBM App Exchange

<https://exchange.xforce.ibmcloud.com/hub/extension/466f0ff55b35e84e634e7b7f1f5c966a>


QSSA - Slow Search Alert [free]

QSSA Slow Search Alert is a QRadar app developed for sending email notifications when long-lasting searches are detected. Helps administrator to monitor system performance.

QSSA WARNING: Long Lasting Searches Detected



qradar@local

To 

Dear user,

Long-lasting searches found to be executing on QRadar Console ([qradar 7.7.0 console.com](#)).
 Date generated: [2020-08-26 10:00:00](#).

Following searches are exceeding **3** minute(s) execution time:

Search ID	Exec time (minutes)	Query
771356af-5f78-434f-af82-38d689dff7fe	5.3	None

You can Manage Search Results and Cancel Search for [Events](#) or [Flows](#).
 Notifications for the search(s) above will be suppressed for the next **24** hours.

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

QRadar Native Alternatives

No such functionality in QRadar.

License

Open Source / Apache 2. To start a free trial of any other QLEAN App Suite tools or request a custom application development contact us at qlean@scnsoft.com or [QLEAN App Suite website](#). You can also request [QRadar Professional Services](#) for assistance.

IBM App Exchange

<https://exchange.xforce.ibmcloud.com/hub/extension/ca87a26373133fc760e44984f2e7520a>

QOR - Offense Reporter [free]

QOR Offense Reporter is a QRadar app that generates periodical offense reports in Excel formats and sends them by email. Incident Reports are:

- configurable
- report data is separated by domains
- includes all offenses (active, inactive, closed)
- includes closing date, reason, notes, closed-by-user, etc.
- XLSX formatted - allows sorting and filtering

QRadar Incident Reporting											
2020/06/04 10:17:47 (7 days)											ScienceSoft
ID	OFFENSE NAME	SOURCE	STATUS	START	LAST UPDATE	CLOSED	CLOSED BY	EVENTS/FLOWS	RULE(S)	CLOSING REASON	NOTES
37751	cry me a river containing DNS in Progress		ACTIVE	2020/02/04 13:16:47	2020/06/04 10:15:42			36728/0	cry me a river		
37750	Exploit Followed by Suspicious Host Activity - Cha		ACTIVE	2020/02/04 13:07:29	2020/06/04 10:16:54			40136/0	Multiple (3)		
37749	__crush me too__ containing DNS in Progress		CLOSED	2020/02/04 12:04:35	2020/02/04 13:06:48	2020/02/04 13:07:07		524/0	__crush me too__	False-Positive, Tuned	
37748	__crush me too__ containing Reverse-lookup Rec		CLOSED	2020/02/04 12:01:03	2020/02/04 12:03:50	2020/02/04 12:04:10	admin	144/0	__crush me too__	Non-issue	
37747	Excessive Firewall Denies Between Hosts preced		ACTIVE	2020/01/04 20:27:04	2020/01/04 20:40:59			992/989	Multiple (2)		
37695	Host Record		OPEN	2020/31/03 12:48:57	2020/31/03 12:48:57			2/0	N/A		
37694	Start of Authority Record		OPEN	2020/31/03 12:48:57	2020/31/03 12:48:57			2/0	N/A		
37692	Host Record		OPEN	2020/31/03 12:48:56	2020/31/03 12:48:56			1/0	N/A		
37691	Host Record		OPEN	2020/31/03 12:48:56	2020/31/03 12:48:56			1/0	N/A		
37690	Host Record		OPEN	2020/31/03 12:48:55	2020/31/03 12:48:55			1/0	N/A		
37689	Host Record		OPEN	2020/31/03 12:48:55	2020/31/03 12:48:55			1/0	N/A		
37688	Service Record preceded by Host Record precede		OPEN	2020/31/03 12:48:55	2020/31/03 12:48:55			14/0	N/A		
37687	Host Record		OPEN	2020/31/03 12:48:55	2020/31/03 12:48:55			1/0	N/A		
37684	Host Record		OPEN	2020/31/03 12:48:55	2020/31/03 12:48:55			1/0	N/A		
37682	Host Record		OPEN	2020/31/03 12:48:55	2020/31/03 12:48:55			1/0	N/A		
37681	Host Record		OPEN	2020/31/03 12:48:55	2020/31/03 12:48:55			1/0	N/A		
37680	Flow Junk Test Rule containing Host Record		OPEN	2020/31/03 12:48:54	2020/01/04 20:40:08			19/15	Multiple (2)		
37679	Host Record		OPEN	2020/31/03 12:48:54	2020/31/03 12:48:54			1/0	N/A		
37678	Host Record		OPEN	2020/31/03 12:48:54	2020/31/03 12:48:55			3/0	N/A		
37674	Host Record		OPEN	2020/31/03 12:48:53	2020/31/03 12:48:53			1/0	N/A		
37673	Host Record		OPEN	2020/31/03 12:48:53	2020/31/03 12:48:53			2/0	N/A		
37670	Host Record		OPEN	2020/31/03 12:48:53	2020/31/03 12:48:53			2/0	N/A		
37669	Host Record preceded by Host Record		OPEN	2020/31/03 12:48:53	2020/31/03 12:48:55			4/0	N/A		
37664	Host Record		OPEN	2020/31/03 12:48:53	2020/31/03 12:48:53			2/0	N/A		
37663	Host Record		OPEN	2020/31/03 12:48:53	2020/31/03 12:48:55			2/0	N/A		
37662	Host Record		OPEN	2020/31/03 12:48:53	2020/31/03 12:48:53			2/0	N/A		
37660	Host Record preceded by Host Record		OPEN	2020/31/03 12:48:53	2020/31/03 12:48:53			2/0	N/A		
37738	Service Record		OPEN	2020/31/03 12:48:25	2020/31/03 12:48:25			1/0	N/A		

QRadar Native Alternatives

QRadar reports allows exporting offenses to CSV format which is not quite convenient for analysis and reporting. QOR report also contains unique information which is not available from standard exports, like notes, closing reasons, offense rule name, etc.

License

Open Source / Apache 2. To start a free trial of any other QLEAN App Suite tools or request a custom application development contact us at qlean@scnsoft.com or [QLEAN App Suite website](https://www.scnsoft.com/qlean). You can also request [QRadar Professional Services](#) for assistance.

IBM App Exchange

<https://exchange.xforce.ibmcloud.com/hub/extension/630f4d6c412e3fcac7d506b84fc31d8e>

QWAD - WinCollect Assisted Deployment [commercial]

QWAD WinCollect Assisted Deployment is designed to automatically install and configure IBM WinCollect Agent in unmanaged mode.

WinCollect is a Syslog event forwarder that administrators can use to forward events from Windows Event Log to QRadar. With either stand-alone or managed deployment scenario WinCollect can provide an efficient and convenient way to feed log data to SIEM solution, not limited with native Windows audit journals but also most of major Windows services like IIS, DHCP, DNS and others.

Many security architects do realize that integration of the third-party agents into corporate network is not an easy process. Even when all the corporate standards of minor performance impact, code sustainability and supportability are passed, agents still have to be deployed and configured all over the infrastructure. This task requires permanent coordination with operating systems admins, automation tools for deployment, monitoring tools integration, manual interaction for specific log sources configuration on each and every target system, troubleshooting and upgrade policies implementation, and a lot more.

WinCollect Host Status

previous execution status

STATUS: OK: 1, NOK: 0

TYPE: hostcheck [selected]

PID: [not running]

show previous execution status

Operation: Global: Host Check On Unprocessed

View Off Ignored

run deployment tasks

Operation: Global: Host Check ▶

Scope: Selected ▶

hosts status table										
Host	FQDN	Status	Error	Mode	Windows	Agent	Sysmon	Console	Started	
██████████	██████████	OK		hostcheck	Windows 10 Ent...	NOT_INSTALLED [RU...	14.13 [RUNNING]	NOT_INSTALLED	11 Jan 2023 19:33:23	11
██████████	██████████	OK		hostcheck	Windows 10 Ent...	7.3.1.22 [RUNNING]	13.34 [RUNNING]	NOT_INSTALLED	11 Jan 2023 19:34:08	11
██████████	██████████	OK		hostcheck	Windows 10 Ent...	7.3.1.22 [RUNNING]	13.34 [RUNNING]	NOT_INSTALLED	11 Jan 2023 19:33:32	11
██████████	██████████	NOK	RECEIVED UNEXP...	hostcheck					11 Jan 2023 19:33:42	11

Page 1 of 1 First Previous

host processing logs [] - inactive

```

2023-01-11 19:34:13,566 INFO [6421] [wincollect_deploy:deploy_all] >> Remote URL: \\
2023-01-11 19:34:13,578 DEBUG [6421] [wincollect_deploy:deploy_all] >> EXEC: powershell.exe -C "[System.BitConverter]::ToString([System.Security.Cryptography.MD5]::Create()).Com
2023-01-11 19:34:13,585 DEBUG [6421] [wincollect_deploy:deploy_all] >> COMMAND OUTPUT:
2023-01-11 19:34:13,586 DEBUG [6421] [wincollect_deploy:deploy_all] >> STDOUT > 497CDA9BAGEFFDBBCFDE4AC8869768EA
2023-01-11 19:34:13,586 INFO [6421] [wincollect_deploy:deploy_all] >> SRC file MD5: '497CDA9BAGEFFDBBCFDE4AC8869768EA'
2023-01-11 19:34:13,886 INFO [6421] [wincollect_deploy:deploy_all] >> Getting remote file size: 'C:\WinCollect\config\AgentConfig.xml'.
2023-01-11 19:34:13,886 DEBUG [6421] [wincollect_deploy:deploy_all] >> EXEC: for %I in ("C:\WinCollect\config\AgentConfig.xml") do @echo %~zI
2023-01-11 19:34:14,013 DEBUG [6421] [wincollect_deploy:deploy_all] >> COMMAND OUTPUT:
2023-01-11 19:34:14,014 DEBUG [6421] [wincollect_deploy:deploy_all] >> STDOUT > 17113
2023-01-11 19:34:14,014 INFO [6421] [wincollect_deploy:deploy_all] >> File size: '17113'
2023-01-11 19:34:14,014 INFO [6421] [wincollect_deploy:deploy_all] >> Writing local file.
2023-01-11 19:34:14,078 INFO [6421] [wincollect_deploy:deploy_all] >> DST file MD5: '497CDA9BAGEFFDBBCFDE4AC8869768EA'
2023-01-11 19:34:14,078 INFO [6421] [wincollect_deploy:deploy_all] >> MD5 matched, OK.
2023-01-11 19:34:14,078 INFO [6421] [wincollect_deploy:deploy_all] >> Configuration backup OK.
2023-01-11 19:34:14,079 INFO [6421] [wincollect_deploy:deploy_all] >> Disconnecting PsExec session:
2023-01-11 19:34:14,103 INFO [6421] [wincollect_deploy:deploy_all] >> PsExec service removed.
2023-01-11 19:34:14,121 INFO [6421] [wincollect_deploy:deploy_all] >> PsExec session disconnected.
2023-01-11 19:34:14,122 INFO [6421] [wincollect_deploy:deploy_all] >> Disconnecting SMB session:
2023-01-11 19:34:14,128 INFO [6421] [wincollect_deploy:deploy_all] >> SMB session deleted:
2023-01-11 19:34:14,128 INFO [6421] [wincollect_deploy:deploy_all] >> PsExec disconnection sequence finalized.
                
```

Once installed, IBM WinCollect Assisted Deployment can easily cover following scenarios with this application:

- Deploy WinCollect agent all over the infrastructure*, utilizing different deployment, authentication and host profiles for maximum flexibility;
- Automatically configure all the log source types supported by WinCollect**, and configure custom logs polling;
- Filter out unnecessary events with X-Path;
- Deploy and configure Sysmon along with WinCollect, *easily integrate with VirusTotal*;

- Monitor for agent's status, download remote agent logs for troubleshooting;
- Perform remote upgrade, re-configure agents (detect new Windows services) without re-installation;
- Avoid manual log sources addition to QRadar, all the auto-configured log sources will be auto-detected and appear in QRadar automatically;
- Plan and organize security-related infrastructure separately from operating systems infrastructure;

IBM WinCollect Deployment Assistant App Can be used without any limitations in licensed mode. Non-licensed mode is limited with three (3) target Windows hosts only.

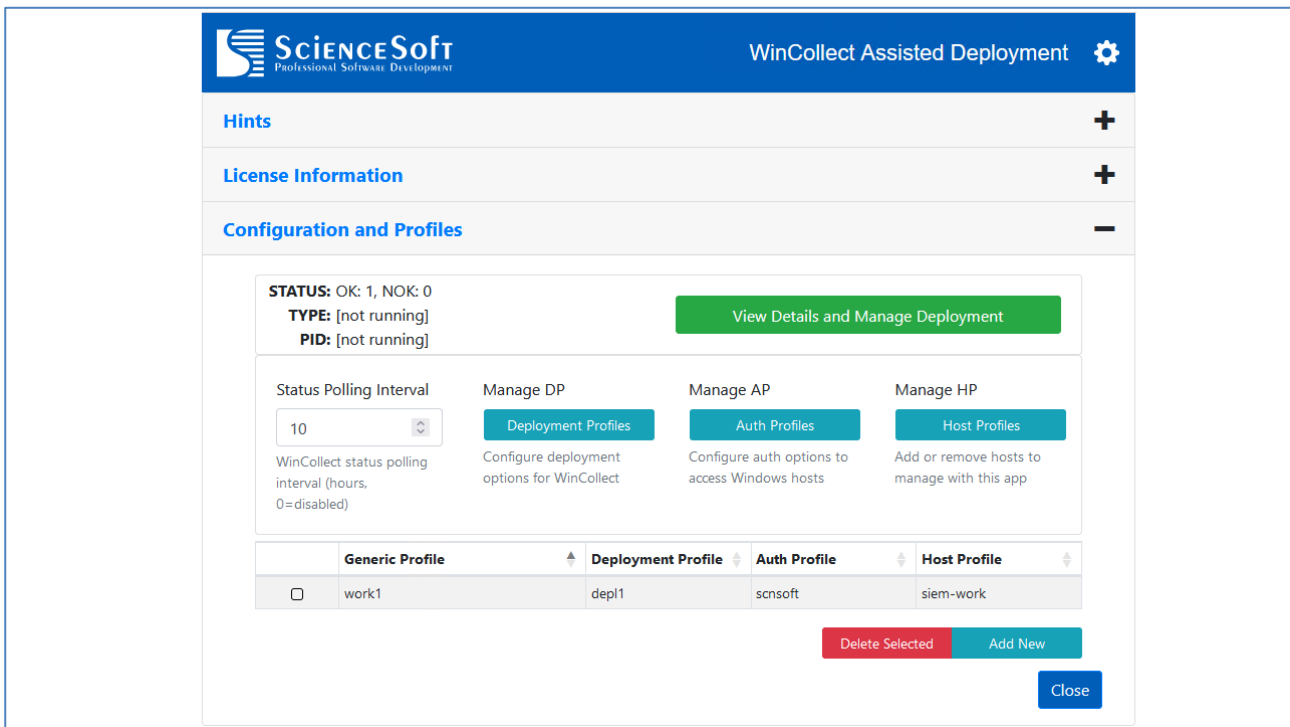
**Operating Systems Supported:*

- *Microsoft Windows 7*
- *Microsoft Windows 10*
- *Microsoft Windows 2003 Server*
- *Microsoft Windows 2008 Server*
- *Microsoft Windows 2008R2 Server*
- *Microsoft Windows 2012 Server*
- *Microsoft Windows 2012R2 Server*
- *Microsoft Windows 2016 Server*
- *Microsoft Windows 2019 Server*
- *Microsoft Windows 2022 Server*

***Auto-configured Log Source Types:*

- *Microsoft Windows Security Log*
- *Microsoft Windows Application Log*
- *Microsoft Windows System Log*
- *Microsoft Directory Service Log*
- *Microsoft File Replication Service Log*
- *Microsoft Forwarded Event Log*
- *Microsoft SQL Log*
- *Microsoft IIS Log*
- *Microsoft DHCP Logs*
- *Microsoft Exchange: Outlook Web Access events (OWA)*
- *Microsoft Exchange: Simple Mail Transfer Protocol events (SMTP)*
- *Microsoft Exchange: Message Tracking Protocol events (MSGTRK)*
- *Microsoft DNS Debug Logs*
- *XPath Query and Sysmon Logs*
- *Custom Plain-Text Logs*
- *Custom IIS-Formatted Logs*
-

NOTE: QWAD can be installed as a QRadar extension, and you can also request a stand-alone MSI package for installation on a Windows server.



QRadar Native Alternatives

No such functionality in QRadar. All steps must be performed manually which is extremely time consuming.

License

QWAD WinCollect Assisted Deployment is a commercial application available for free with one limitation: non-licensed mode allows to verify status of WinCollect instances and perform deployment actions for three (3) Windows hosts only. In order to obtain a quote for the license or request a PoC, please contact us at clean@scnsoft.com. You can also request any other QLean App Suite trial licenses and [QRadar Professional Services](#) for assistance.

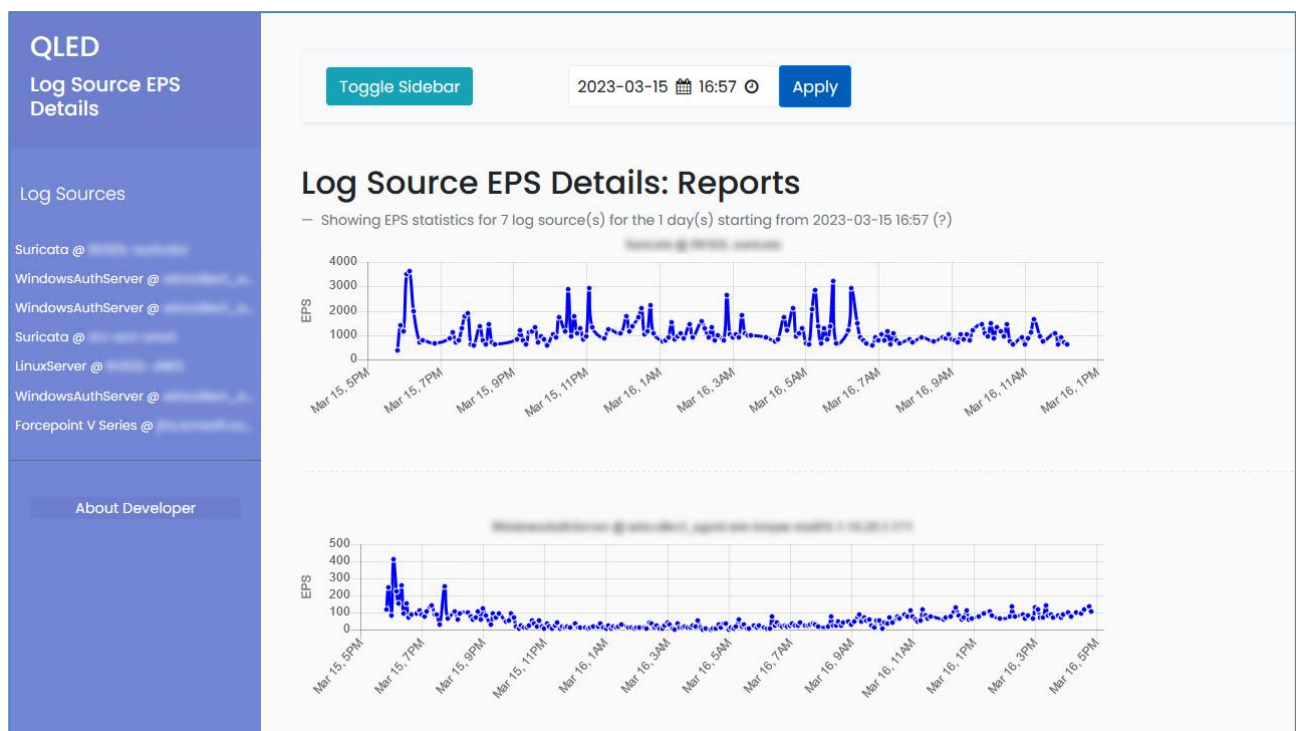
IBM App Exchange

<https://exchange.xforce.ibmcloud.com/hub/extension/0cebfe2f0019efc70d565ca75a20e80a>

QLED - Log Source EPS Details [free]

QLED Log Source EPS Details is a QRadar app that allow to monitor the number of events (EPS) received by each individual log source and drill-down for details.

QLED does not utilize heavy AQL queries, but requests information from QRadar API, stores EPS statistics data in the local SQLite database and visualizes charts in a new QRadar tab. You can configure the app to store statistics only for the log sources exceeding specific number of EPS. You can also use drill-down functionality to investigate the real cause of EPS spike by clicking any data point on the chart.



QRadar Native Alternatives

The native Top Log Sources dashboard shows the number of events instead of EPS (conversion/calculation is needed), doesn't allow drilling down to details of specific event types – manual searching is required, and utilizes heavy AQL queries.

License

Free / Closed Sources. To start a free trial of any other QLEAN App Suite tools or request a custom application development contact us at qlean@scnsoft.com or [QLEAN App Suite website](https://www.scnsoft.com/qlean-app-suite). You can also request [QRadar Professional Services](#) for assistance.

IBM App Exchange

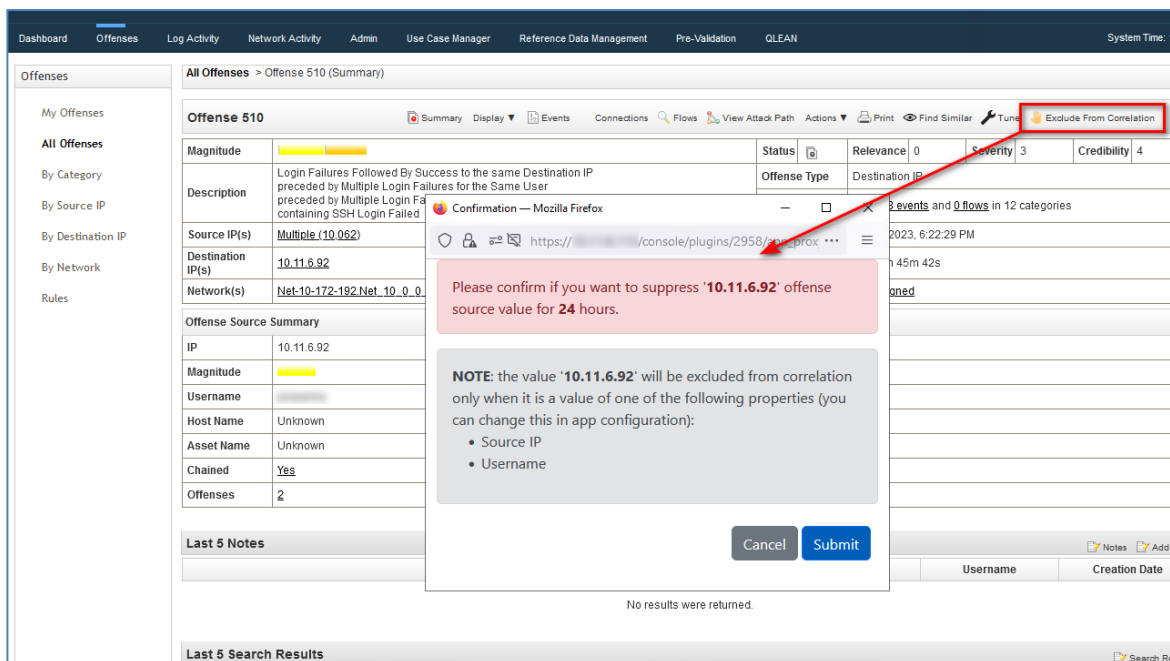
<https://apps.xforce.ibmcloud.com/extension/88ecf797cb7d3084d201dc1c145cdf5b>

QEFC - Exclude From Correlation [free]

QEFC Exclude From Correlation is a QRadar app that adds a new button for offense details page that allows you to *temporary whitelist* offense source value (send it to special reference set) with a single click. Once added to the reference set, this particular offense source value (IP address, username, custom property, etc.) will be whitelisted for configurable amount of time (24 hours by default).

One of the possible usage scenarios is when security response team is already identified a compromised host or username, and want to avoid further notifications from this source till the asset is not fully recovered.

In order to make this solution work you will need to manually add 'OFFENSE.WHITELISTING: Event Marked False Positive' rule to the 'FalsePositive: False Positive Rules and Building Blocks' rule test. Detailed explanation of required configuration steps is available in app configuration page (check Admin tab after QEFC installation).



QRadar Native Alternatives

No such functionality. Analysts must manually change all rules that might trigger on the required property.

License

Open Source / Apache 2. To start a free trial of any other QLEAN App Suite tools or request a custom application development contact us at qlean@scnsoft.com or [QLEAN App Suite website](https://www.scnsoft.com/qlean-app-suite). You can also request [QRadar Professional Services](#) for assistance.

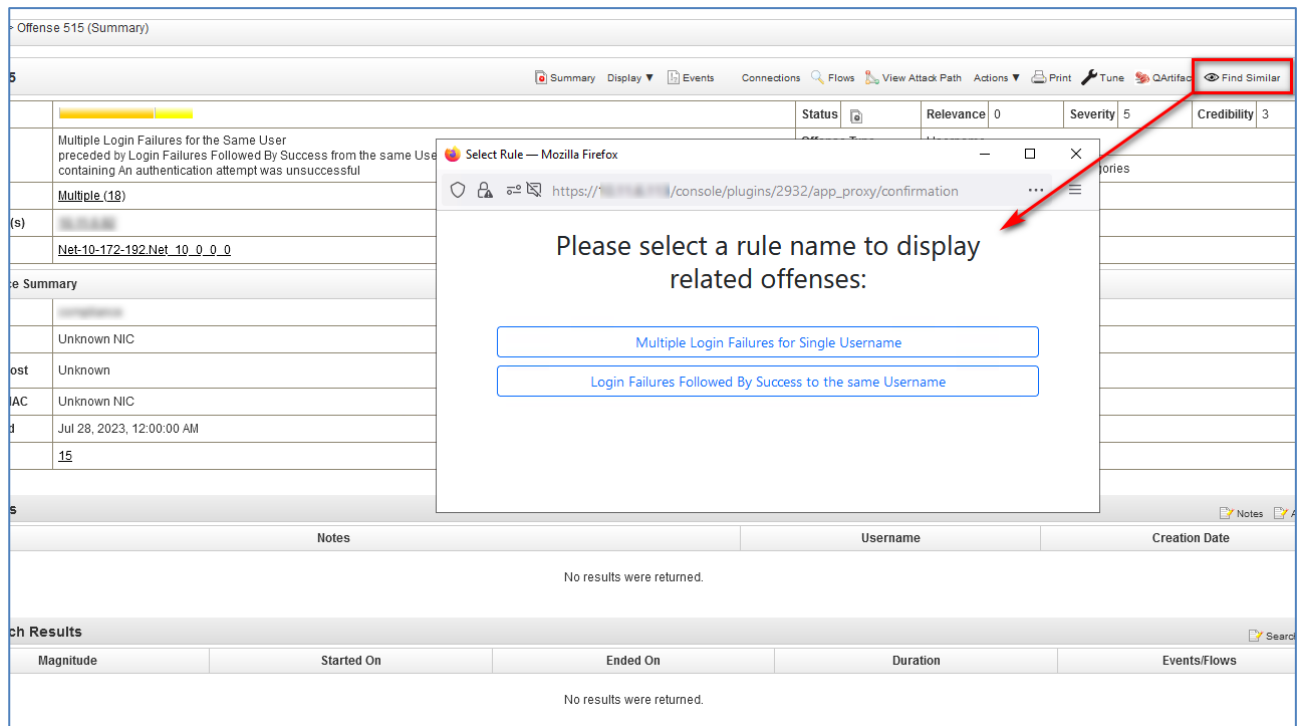
IBM App Exchange

<https://apps.xforce.ibmcloud.com/extension/05d39156d3ed07d21faaf6f23968d109>

QFSO - Find Similar Offenses [free]

QFSO Find Similar Offenses is a QRadar app that adds a new button for offense details page that will open a new window with all similar offenses (generated by the same rule). When several rules are contributed to the offense, user will be given an option to select specific rule.

Such a solution can be useful to speed-up investigations and tuning.



The screenshot shows the QRadar interface for an offense summary. The 'Find Similar' button is highlighted in red. A modal window titled 'Select Rule' is open, displaying two options: 'Multiple Login Failures for Single Username' and 'Login Failures Followed By Success to the same Username'.

Status	Relevance	Severity	Credibility
	0	5	3

Multiple Login Failures for the Same User preceded by Login Failures Followed By Success from the same User containing An authentication attempt was unsuccessful

Multiple (19)

Net-10-172-192.Net_10_0_0_0

Summary

Host	IP	MAC	Date
Unknown NIC	Unknown	Unknown NIC	Jul 28, 2023, 12:00:00 AM

Notes

Notes	Username	Creation Date
No results were returned.		

Search Results

Magnitude	Started On	Ended On	Duration	Events/Flows
No results were returned.				

QRadar Native Alternatives

No such functionality. Analysts have to manually search for similar offenses.

License

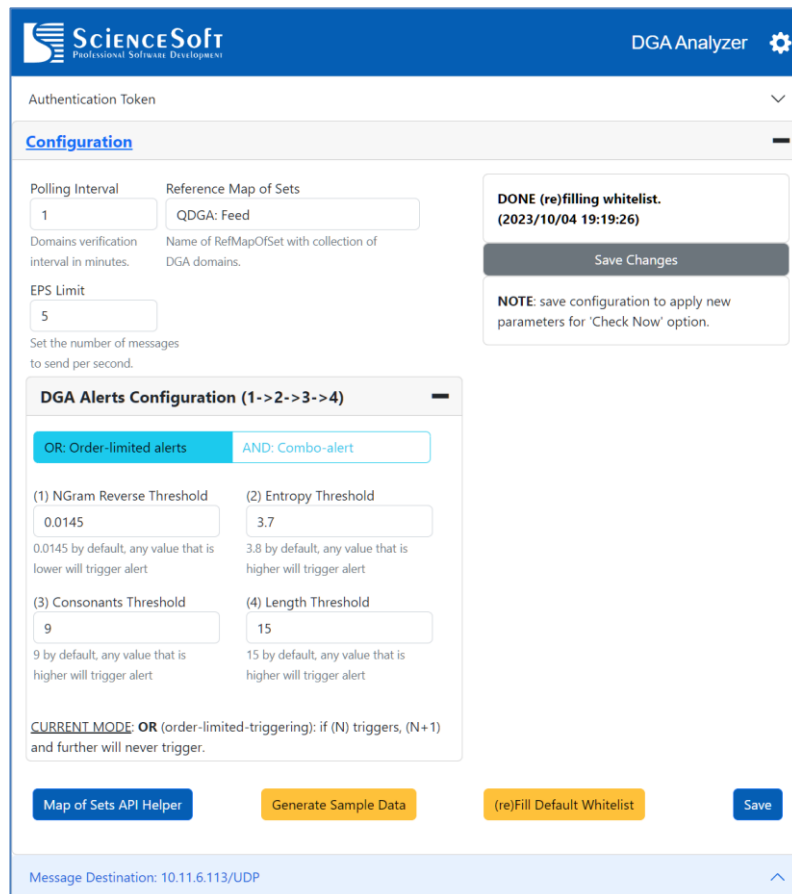
Open Source / Apache 2. To start a free trial of any other QLEAN App Suite tools or request a custom application development contact us at qlean@scnsoft.com or [QLEAN App Suite website](https://www.scnsoft.com/qlean-app-suite). You can also request [QRadar Professional Services](#) for assistance.

IBM App Exchange

<https://exchange.xforce.ibmcloud.com/hub/extension/17d11f13e5d7aee9c84b2d2898d08989>

QDGA - DGA Analyzer [free]

QDGA DGA Analyzer is a QRadar app that includes rules and reference sets and serves as a collector of "bad" domains that were created by Domain Generation Algorithms. Using a special rule, domains will be put to a selected Reference Set from the specified log sources. Then, QDGA processes and filters collected domains by a trained neural network and, in cases DGA is detected, will mark it and alert users by Offense.



SCIENCESoft Professional Software Development DGA Analyzer ⚙️

Authentication Token ⌵

Configuration —

Polling Interval: Reference Map of Sets:
Domains verification interval in minutes. Name of RefMapOfSet with collection of DGA domains.

EPS Limit:
Set the number of messages to send per second.

DONE (re)filling whitelist. (2023/10/04 19:19:26)

Save Changes

NOTE: save configuration to apply new parameters for 'Check Now' option.

DGA Alerts Configuration (1->2->3->4) —

OR: Order-limited alerts AND: Combo-alert

<p>(1) N-Gram Reverse Threshold: <input type="text" value="0.0145"/> <small>0.0145 by default, any value that is lower will trigger alert</small></p> <p>(3) Consonants Threshold: <input type="text" value="9"/> <small>9 by default, any value that is higher will trigger alert</small></p>	<p>(2) Entropy Threshold: <input type="text" value="3.7"/> <small>3.8 by default, any value that is higher will trigger alert</small></p> <p>(4) Length Threshold: <input type="text" value="15"/> <small>15 by default, any value that is higher will trigger alert</small></p>
--	--

CURRENT MODE: OR (order-limited-triggering): if (N) triggers, (N+1) and further will never trigger.

Map of Sets API Helper
Generate Sample Data
(re)Fill Default Whitelist
Save

Message Destination: 10.11.6.113/UDP ⌵

QRadar Native Alternatives

DGA processing is available in QRadar DNS Analyzer application. QDGA is a lightweight alternative to that application.

License

Open Source / Apache 2. To start a free trial of any other QLEAN App Suite tools or request a custom application development contact us at qlean@scnsoft.com or [QLEAN App Suite website](#). You can also request [QRadar Professional Services](#) for assistance.

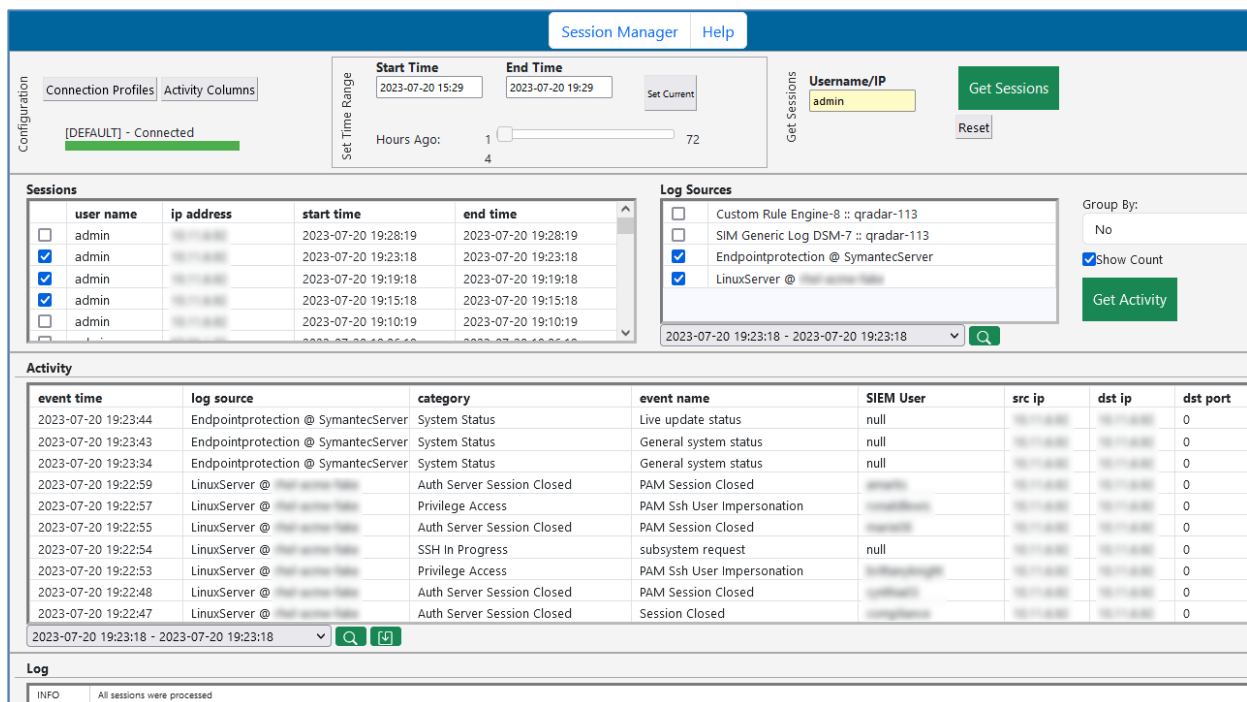
IBM App Exchange

<https://apps.xforce.ibmcloud.com/extension/e5543c93ceebfda932e12e69ae04568e>

QSM Session Manager [free]

QSM QRadar Session Manager makes it easy to track user sessions (username + sourceIP + timeframe combinations) and investigate security events using session information even when a user name is not available in log messages e.g.:

- Firewall activity
- IDS/IPS activity
- Web Servers activity
- Operating Systems logs missing username
- Database and business application queries
- Others



The screenshot displays the QSM Session Manager interface. At the top, there are navigation tabs for 'Session Manager' and 'Help'. Below this, there are configuration options for 'Connection Profiles' and 'Activity Columns'. The main interface is divided into several sections:

- Configuration:** Includes 'Start Time' (2023-07-20 15:29) and 'End Time' (2023-07-20 19:29) fields, a 'Set Current' button, and a 'Hours Ago' slider set to 1.
- Get Sessions:** A section with a 'Username/IP' field containing 'admin', a 'Get Sessions' button, and a 'Reset' button.
- Sessions Table:** A table with columns for 'user name', 'ip address', 'start time', and 'end time'. It lists several sessions for the user 'admin'.
- Log Sources:** A section with checkboxes for 'Custom Rule Engine-8 :: qradar-113', 'SIM Generic Log DSM-7 :: qradar-113', 'Endpointprotection @ SymantecServer', and 'LinuxServer @ ...'. A 'Get Activity' button is present.
- Activity Table:** A table with columns for 'event time', 'log source', 'category', 'event name', 'SIEM User', 'src ip', 'dst ip', and 'dst port'. It shows various system status and session-related events.
- Log:** A section at the bottom with a status message: 'INFO All sessions were processed'.

QRadar Native Alternatives

There's no such functionality available in native QRadar interface. Every search in a series must be created and processed manually. QSM saves up to 3 working hours daily for an analyst who's performing such investigations.

License

Open Source / Apache 2. To start a free trial of any other QLEAN App Suite tools or request a custom application development contact us at qlean@scnsoft.com or [QLEAN App Suite website](https://www.scnsoft.com/qlean). You can also request [QRadar Professional Services](#) for assistance.

IBM AppExchange

<https://exchange.xforce.ibmcloud.com/hub/extension/aad351d53a7c87c76523d1215cf329ed>

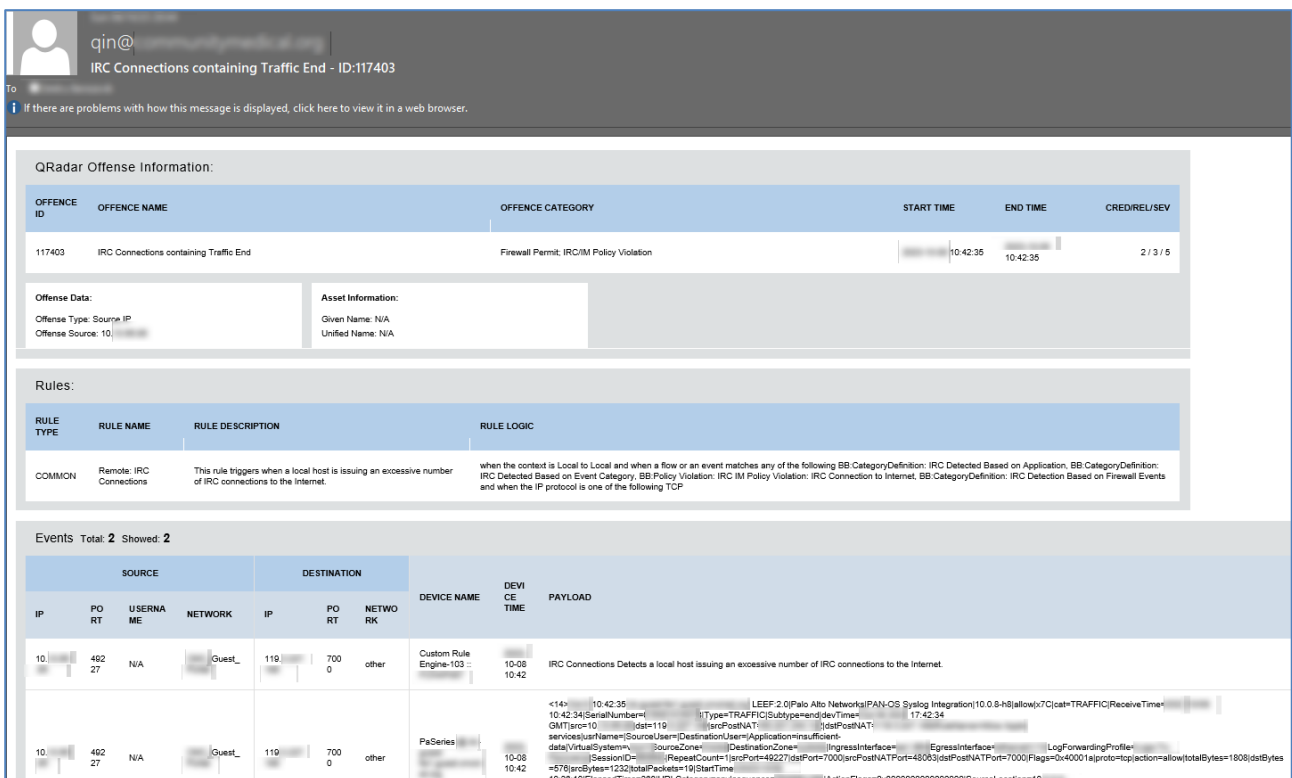
QIN - Incident Notifier [commercial]

The main purpose of any SIEM systems is to be aware of any security incidents that have just happened as soon as possible. IBM QRadar SIEM does its best parsing and correlating events from all kind of sources and creating offenses whenever any security incident happens. There are out-of-the-box mechanisms, such as GUI and email notifications, that allow QRadar to notify security analysts about offenses. While out-of-the-box email notifications work fine, they still lack some flexibility and require some technical knowledge to create or edit an email template. In addition, using vanilla QRadar, you can't assign an offense to a specific analyst based on its type or content.

QRadar Incident Notifier allows you to perform these tasks in a simple way and moreover it allows you to configure notifications to be send not only via email, but also using:

- Twilio SMS
- Telegram
- Slack
- MS Teams
- Jira

QRadar Incident Notifier uses rules to make decisions on where and how to send notifications and to assign offenses to analysts, as well as templates to determine the amount of information to be included into the message. Every rule is based on a regex that can be applied to offense description, name of the rule that has triggered the offense, offense category or the actual payload of related events and/or flows. Integrated Rule Manager and Template Editor make it really easy to configure the app.



The screenshot displays the QRadar Incident Notifier interface. At the top, it shows the user profile 'qin@' and the title 'IRC Connections containing Traffic End - ID:117403'. Below this, there is a message notification: 'If there are problems with how this message is displayed, click here to view it in a web browser.'

The main content area is titled 'QRadar Offense Information:' and contains a table with the following data:

OFFENSE ID	OFFENSE NAME	OFFENSE CATEGORY	START TIME	END TIME	CRED/REL/SEV
117403	IRC Connections containing Traffic End	Firewall Permt. IRC/IM Policy Violation	10:42:35	10:42:35	2 / 3 / 5

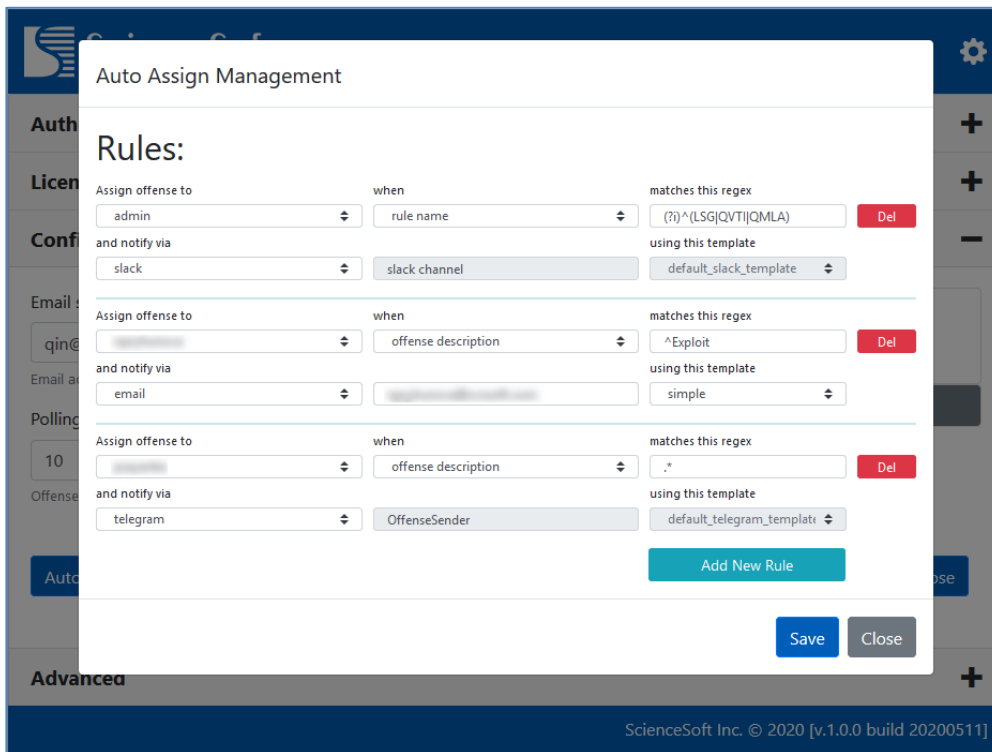
Below the table, there are two sections: 'Offense Data:' and 'Asset Information:'. 'Offense Data:' shows 'Offense Type: Source IP' and 'Offense Source: 10.'. 'Asset Information:' shows 'Given Name: N/A' and 'Unified Name: N/A'.

The 'Rules:' section contains a table with the following data:

RULE TYPE	RULE NAME	RULE DESCRIPTION	RULE LOGIC
COMMON	Remote: IRC Connections	This rule triggers when a local host is issuing an excessive number of IRC connections to the Internet.	when the context is Local to Local and when a flow or an event matches any of the following BB Category:Definition: IRC Detected Based on Application, BB Category:Definition: IRC Detected Based on Event Category, BB Policy Violation: IRC IM Policy Violation: IRC Connection to Internet, BB Category:Definition: IRC Detection Based on Firewall Events and when the IP protocol is one of the following TCP

The 'Events' section shows 'Total: 2' and 'Shown: 2'. It contains a table with the following data:

SOURCE				DESTINATION			DEVI CE NAME	DEVI CE TIME	PAYLOAD
IP	PO RT	USERN AME	NETWO RK	IP	PO RT	NETWO RK			
10.10.10.10	462 27	N/A	Guest_L	119.119.119.119	700 0	other	Custom Rule Engine-103	10-08 10:42	IRC Connections Detects a local host issuing an excessive number of IRC connections to the Internet.
10.10.10.10	462 27	N/A	Guest_L	119.119.119.119	700 0	other	PaSeries	10-08 10:42	<14> 10.42.35 LEEF 2.0/Palo Alto Networks/PAN-OS Syslog Integration 10.0.8.8 allow(x7C)cat=TRAFFIC ReceiveTime=10:42:34 SerialNumber= Type=TRAFFIC Subtype=and devTime= 17:42:34 GMT src=10 dst=119 srcPostNAT: dstPostNAT: services userName= sourceUser= destinationUser= ApplicationInsufficient- data VirtualSystem= SourceZone= DestinationZone= IngressInterface= EgressInterface= LogForwardingProfile= SessionID= RepeatCount= srcPort=46227 dstPort=7000 srcPostNATPort=4803 dstPostNATPort=7000 Flags=0x40001 iprot= action=allow totalBytes=1808 dstBytes=576 srcBytes=1232 totalPackets=19 StartTime=10:39:10 ElapsedTime=368 URLCategory= in sequence= ActionFlags=0x8000000000000000 SourceLocation=10



QRadar Native Alternatives

Out-of-the-box QRadar offense notification mechanism is limited and does not allow to assign offenses; email template modification requires root access and does not support HTML tags. Native email notification can't send offense ID and event details at the same notification, no option to include several related events/flows, rule(s) details and asset information.

License

QIN is a commercial application and requires a license to operate. In order to obtain a quote for the license or request a PoC, please contact us at qlean@scnsoft.com. You can also request any other QLean App Suite trial licenses and [QRadar Professional Services](#) for assistance.

IBM App Exchange

<https://exchange.xforce.ibmcloud.com/hub/extension/8cfc0deb14bb99bcc8e1d8289a948efd>

QArtifact [commercial]

QArtifact is a QRadar extension that enhances offense investigations by allowing security analyst to attach evidences (artifacts) like files, images and links to offenses.



Offense Source Summary			
IP	10.10.10.10	Location	Net-10-172-192.Net_10_0_0_0
Magnitude	High	Vulnerabilities	0
Username	Unknown	MAC Address	Unknown NIC
Host Name	Unknown		
Asset Name	Unknown	Asset Weight	0
Chained	Yes		
Offenses	5	Events/Flows	96,983

Last 5 Artifacts				
Type	Time	Content	Description	User
image	Tue Oct 10 2023 10:51:50 GMT+0300 (GMT+03:00)		Evidences	admin
file	Tue Oct 10 2023 10:47:28 GMT+0300 (GMT+03:00)	QDGA_2.0.0.zip	Test file	admin
link	Tue Oct 10 2023 10:47:11 GMT+0300 (GMT+03:00)	https://google.com	Test link	admin

Last 5 Notes		
Notes	Username	Creation Date
No results were returned.		

QRadar Native Alternatives

No such functionality – only text notes can be attached to offenses.


QArtifact 

Offense #527: Login Failures Followed By Success to the same Destination IP preceded by Multiple Login Failures for the Same User preceded by Multiple Login Failures to the Same Destination containing SSH Login Failed

Start time: 2023-09-14 01:28:41 **Last time:** 2023-10-10 10:52:18 **Status:** OPEN

[Add new artifact](#)

Show 5 entries Search:

Type	Timestamp	Content	Description	User
image	10/10/2023, 10:51:50 AM		Evidences	admin
file	10/10/2023, 10:47:28 AM	QDGA_2.0.0.zip	Test file	admin
link	10/10/2023, 10:47:11 AM	https://google.com	Test link	admin

Showing 1 to 3 of 3 entries
Previous
1
Next

ScienceSoft Inc. © 2023

License

QArtifact is a commercial application and requires a license to operate. In order to obtain a quote for the license or request a PoC, please contact us at qlean@scnsoft.com. You can also request any other QLean App Suite trial licenses and [QRadar Professional Services](#) for assistance.

IBM App Exchange

<https://apps.xforce.ibmcloud.com/extension/5ffbc79a67392e6b80104c7f5761ae78>

Addon 1: MITRE for QRadar

- MITRE ATT&CK for Windows:
<https://exchange.xforce.ibmcloud.com/hub/extension/54490632a4d2b3053330da0a7a079e12>
- MITRE ATT&CK for Linux:
<https://apps.xforce.ibmcloud.com/extension/9cc47a3a2cb6c6cc162e0ba24021f6ec>

Addon 2: Custom DSM

- Kubernetes Integrity Monitoring:
<https://exchange.xforce.ibmcloud.com/hub/extension/b861d171bb69cbf483af1dabd50c23ef>

Addon 3: Coming Soon

- QDLA Dynamic License Allocator
- WarnApp QRadar warning app

<https://qlean.io/#appsuite>

For more information please contact: qlean@scnsoft.com