SCIENCESOFT CUSTOM QRADAR APPS
QLEAN APP SUITE

REFERENCE GUIDE

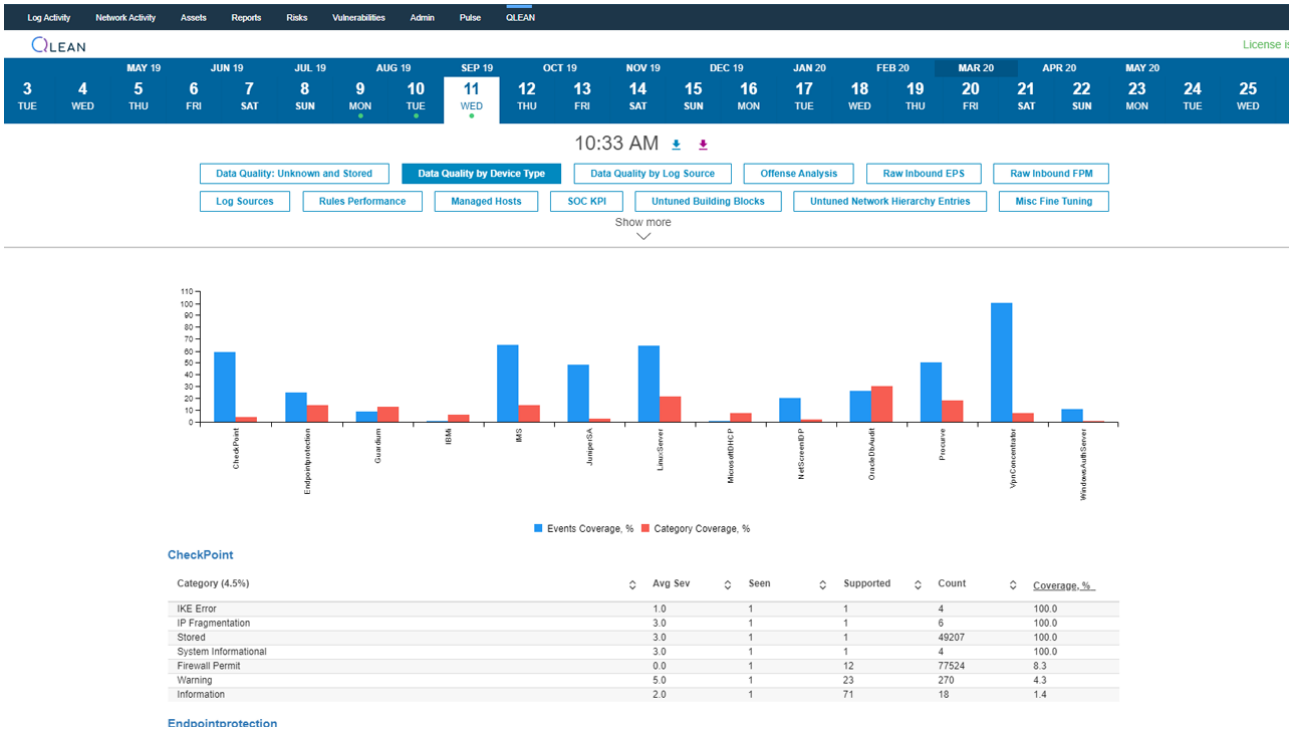
Table of Contents

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

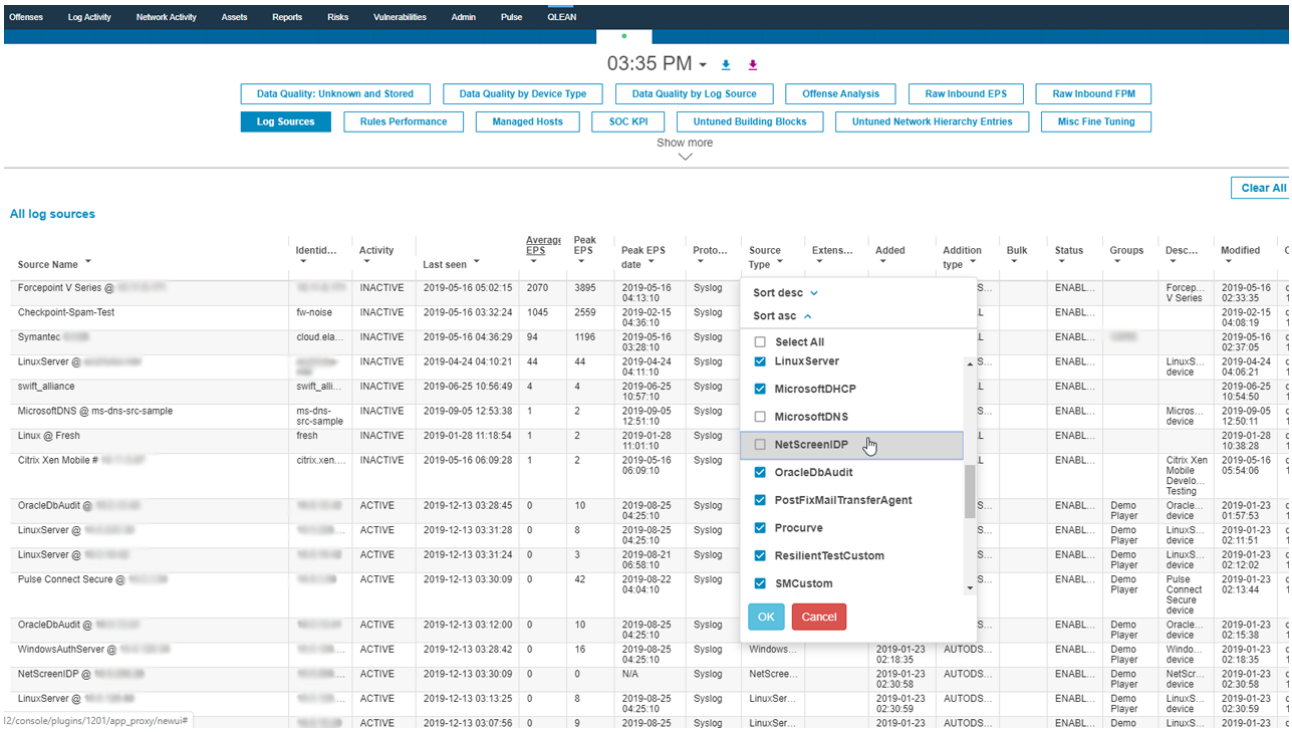
QLEAN has been named finalist as Outstanding Security Solution by IBM 2020 & 2021 Beacon Awards.

QLEAN.io website: LINK

QLEAN interactive online demo: LINK

QLEAN sample report: LINK

QLEAN video: LINK



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

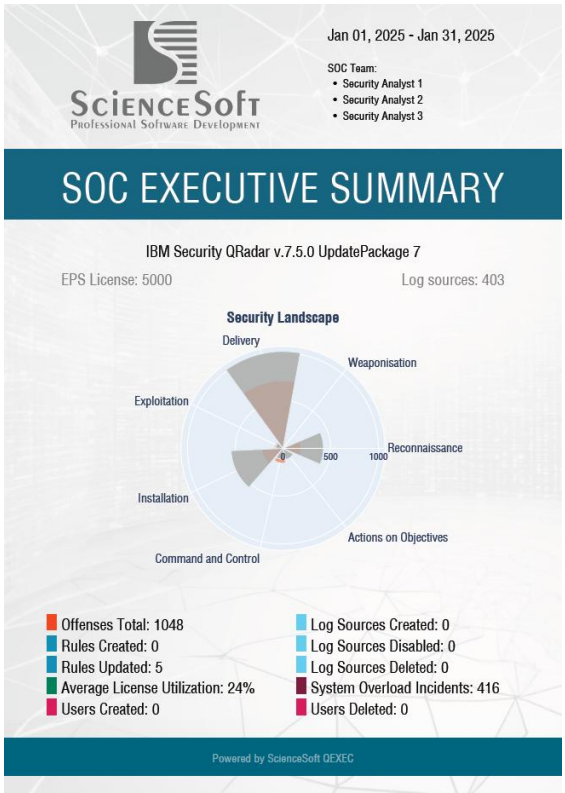
https://apps.xforce.ibmcloud.com/extension/24f7cc75935dd411474001bd175c2d69

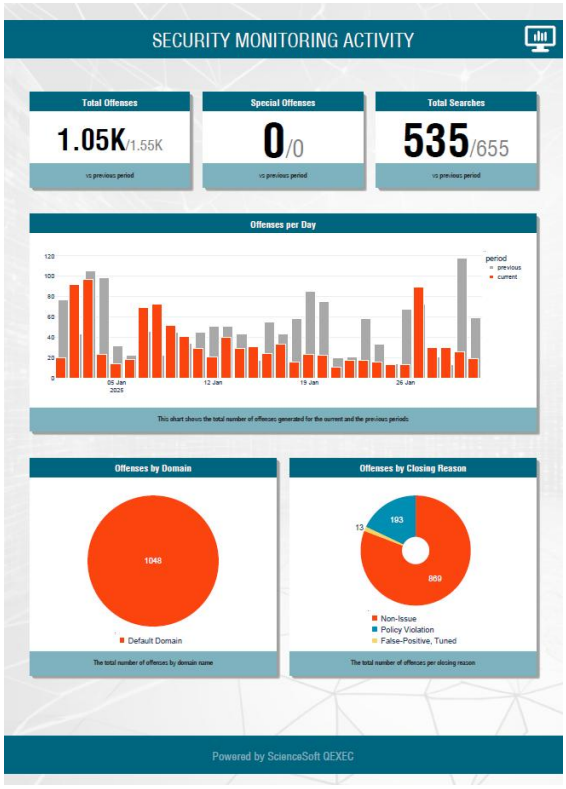
QEXEQ – Executive Reports [commercial]

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.

QXEQ 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

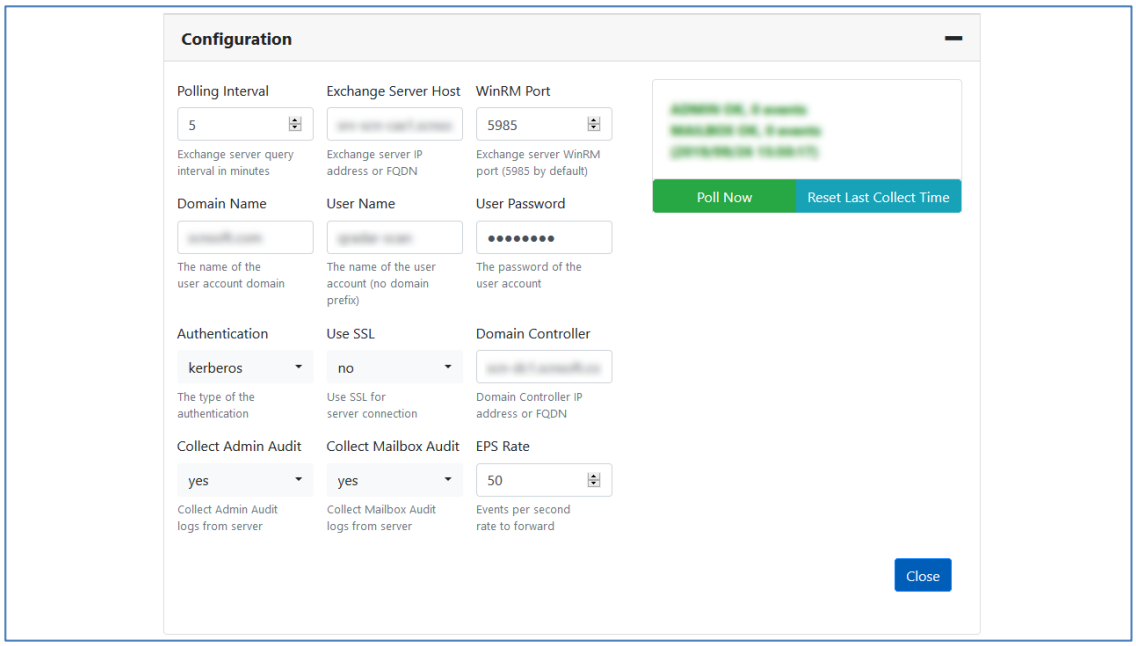
Free QEXEQ demo version contains full functionality with the only limitation of generating reports for 3-day periods only. The full version allows you to generate weekly and monthly reports. To start a free trial of the full version and request professional SIEM services please request a license key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

Link

https://qlean.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.



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]

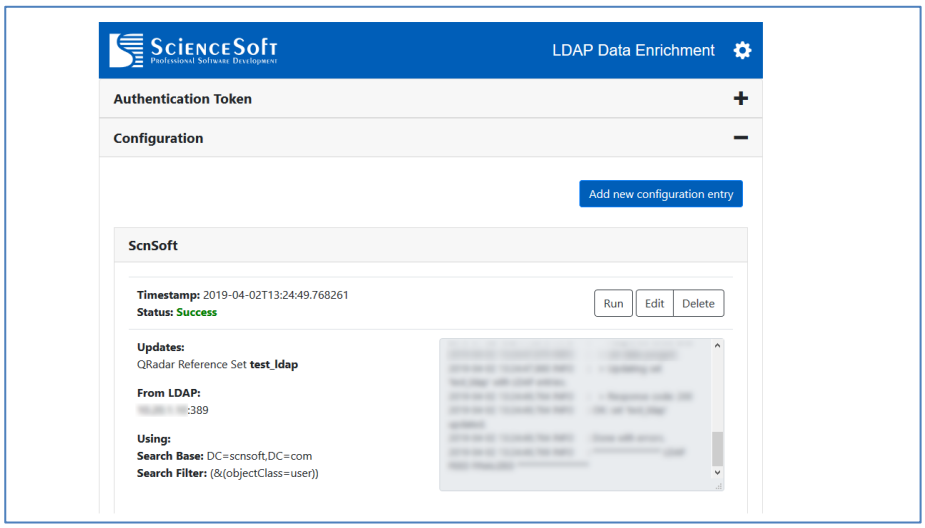
QDATA LDAP Data Enrichment is a free application by ScienceSoft that synchronizes the content of QRadar reference sets and tables with information from Active Directory and other LDAP-based storages.

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. You can also request QRadar Professional Services for assistance.

IBM App Exchange

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

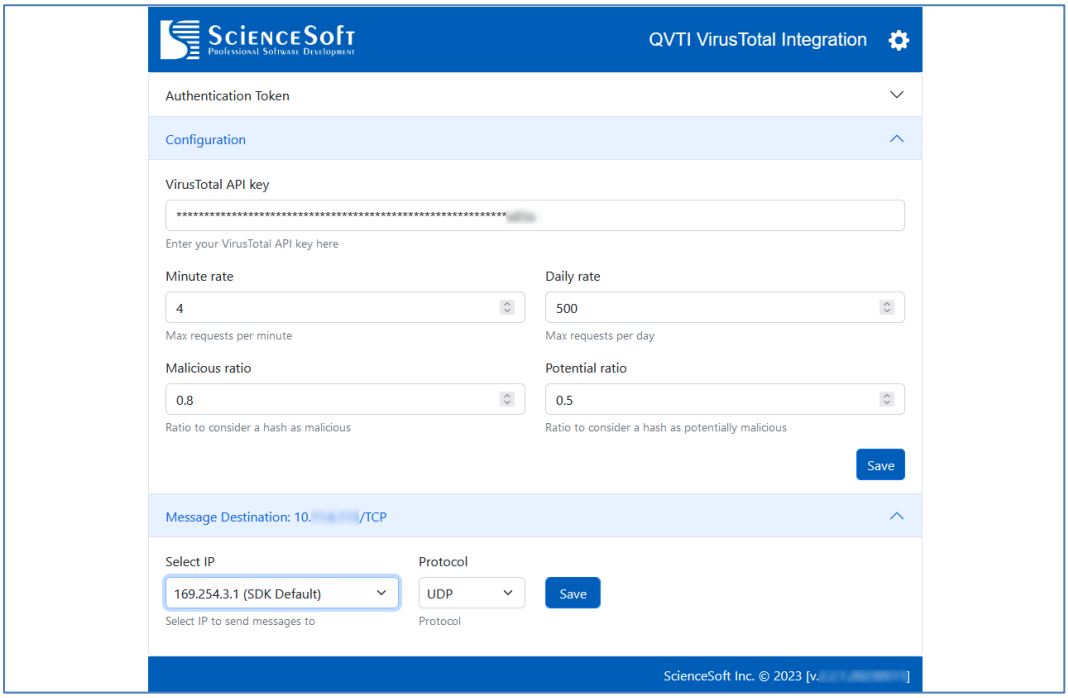
QVTI - VirusTotal Integration for Hash Checking [free]

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).



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.

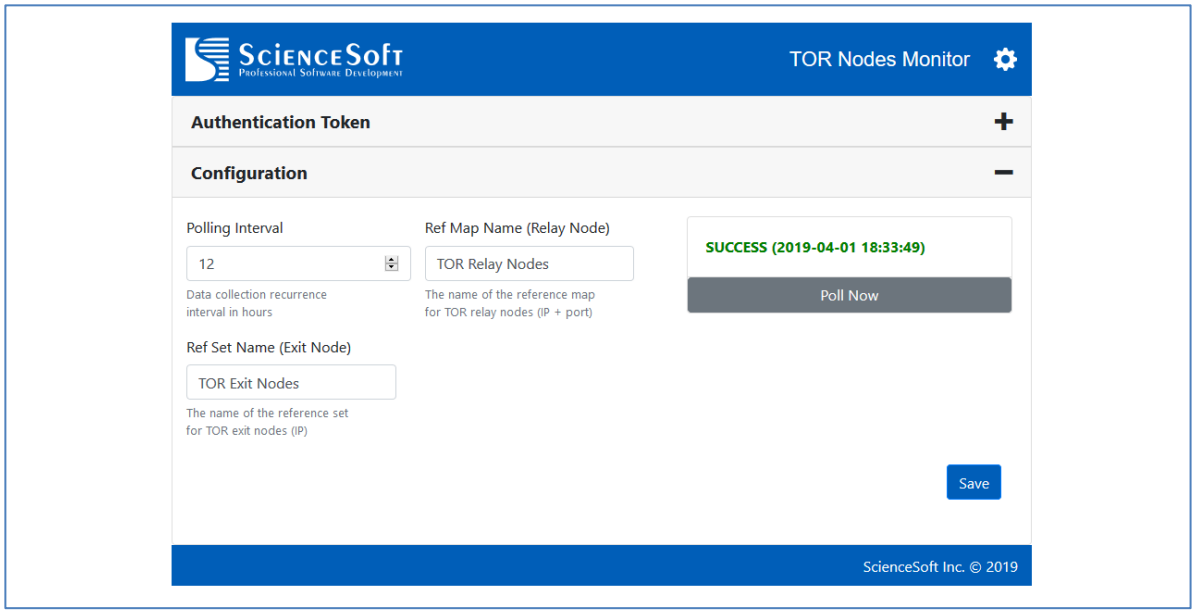
IBM App Exchange

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



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.

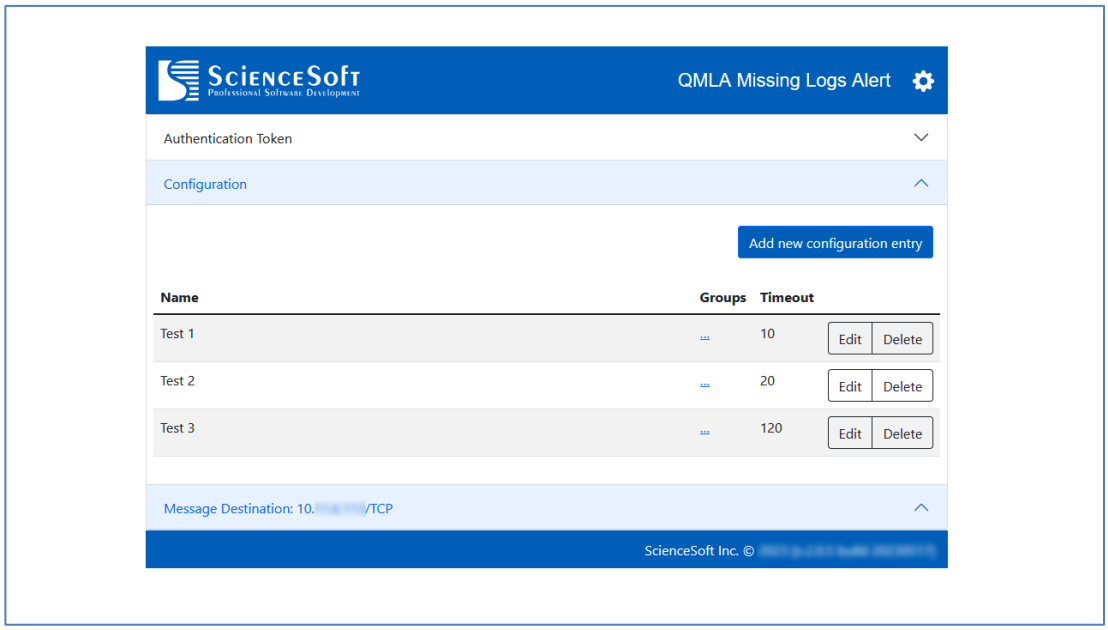
IBM App Exchange

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

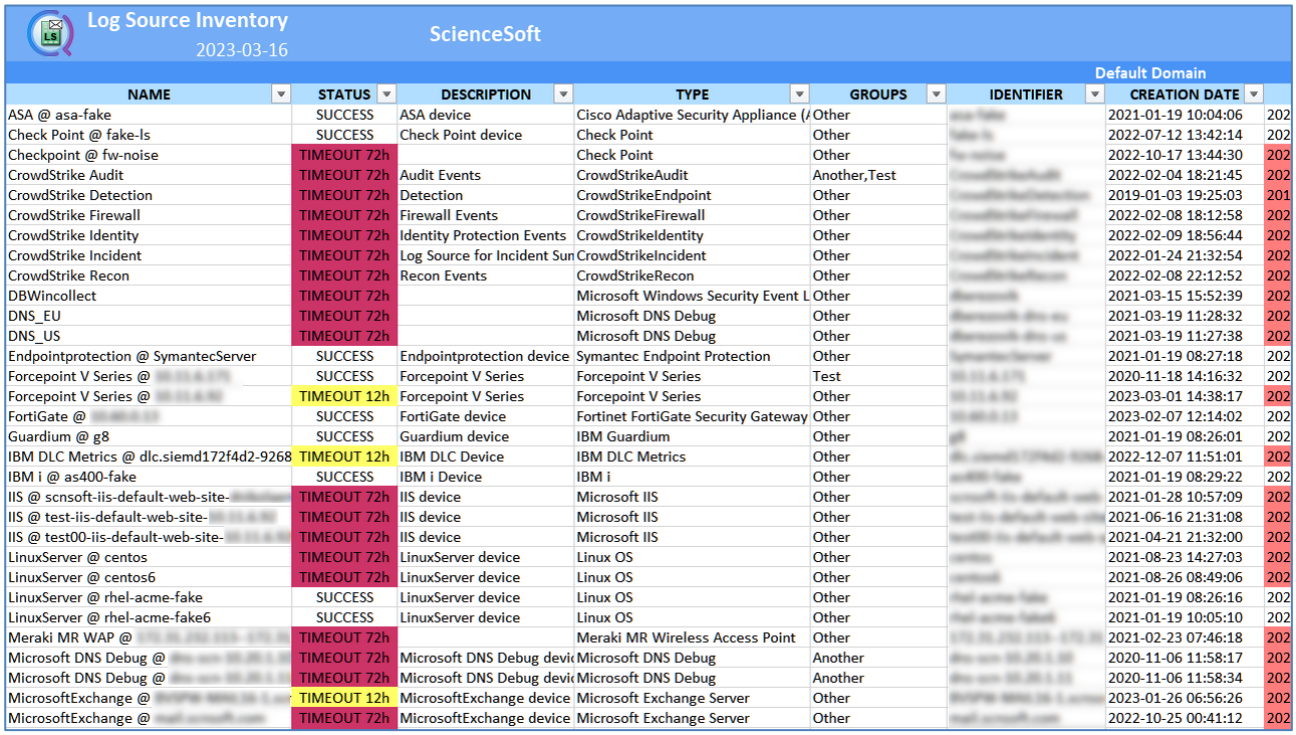
https://exchange.xforce.ibmcloud.com/hub/extension/eec42bd10ed3fed6d7841a41c01cfed9

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
2023-03-16
ScienceSoft

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-ls	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 devic	Microsoft DNS Debug	Another		2020-11-06 11:58:17	202
Microsoft DNS Debug @	TIMEOUT 72h	Microsoft DNS Debug devic	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

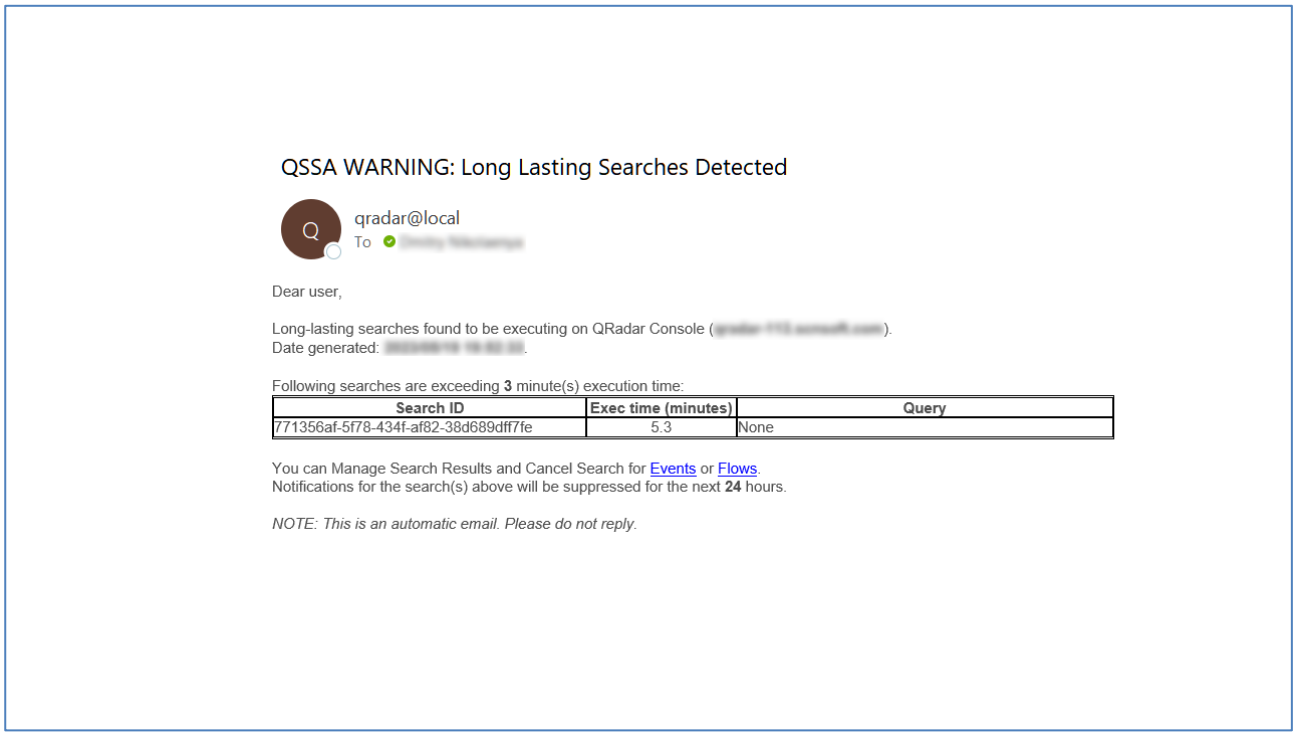
Open Source / Apache 2. To start a free trial of any other QLEAN App Suite tools or request a custom application development contact us at qlean@scnsoft.com or QLEAN App Suite website. You can also request QRadar Professional Services for assistance.

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 ( ).
Date generated: .

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.

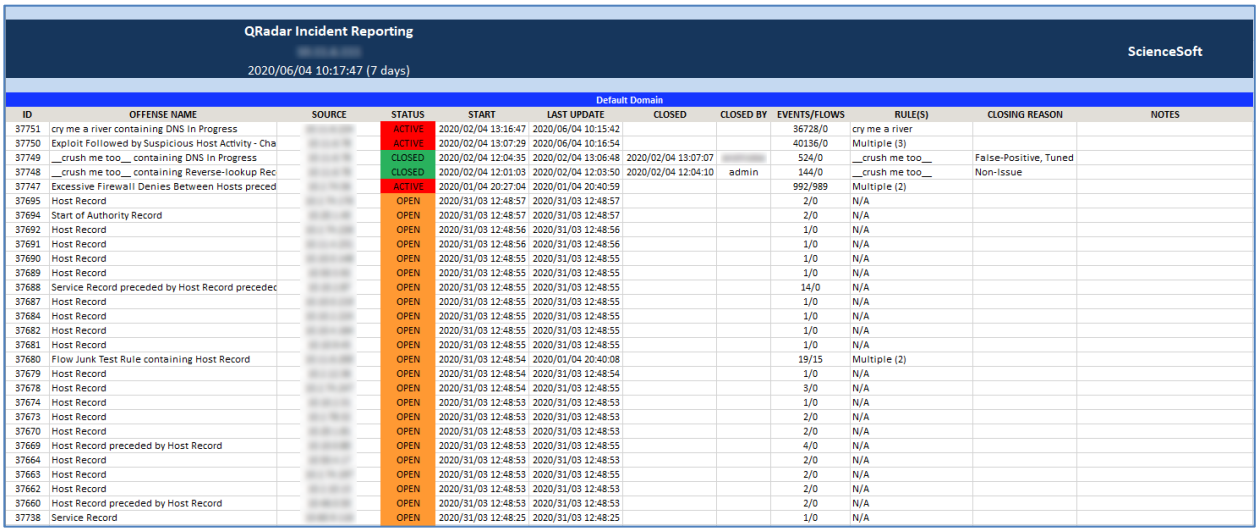
IBM App Exchange

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

Default Domain

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 precedec		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. You can also request QRadar Professional Services for assistance.

IBM App Exchange

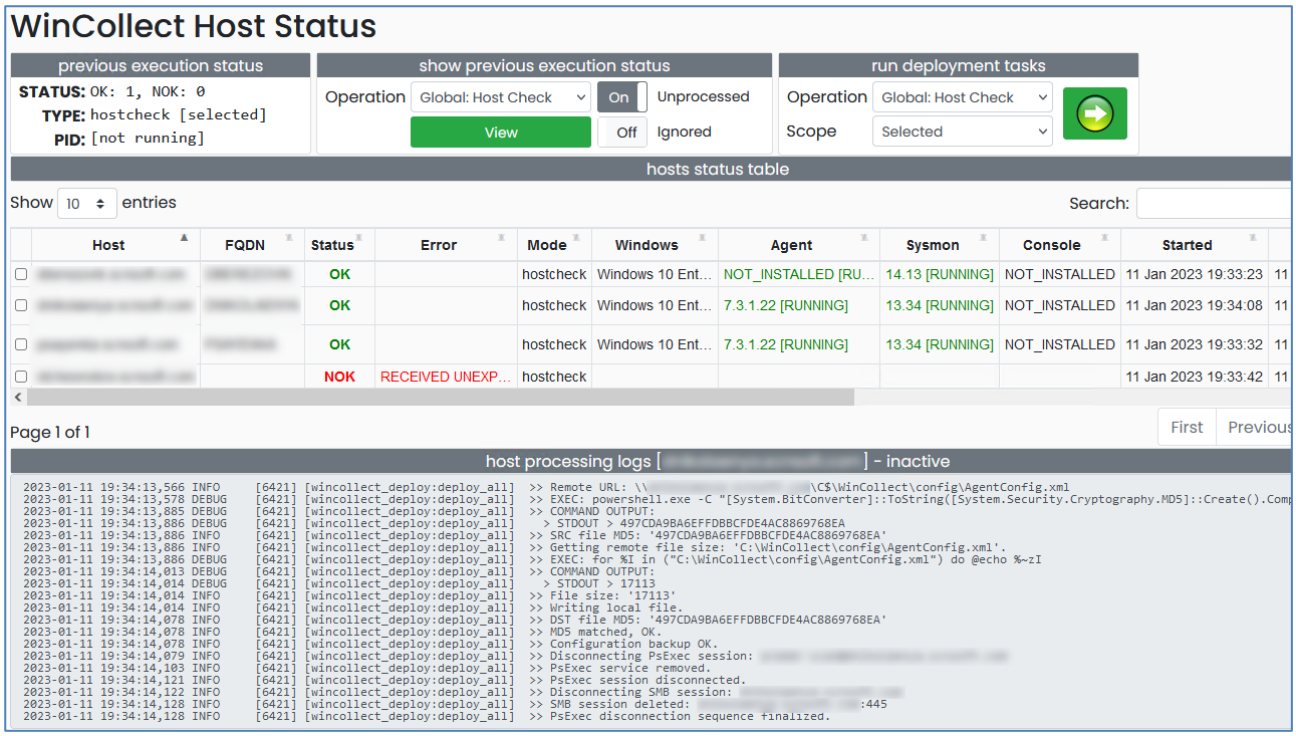
https://exchange.xforce.ibmcloud.com/hub/extension/630f4d6c412e3fcac7d506b84fc31d8e

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.



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.

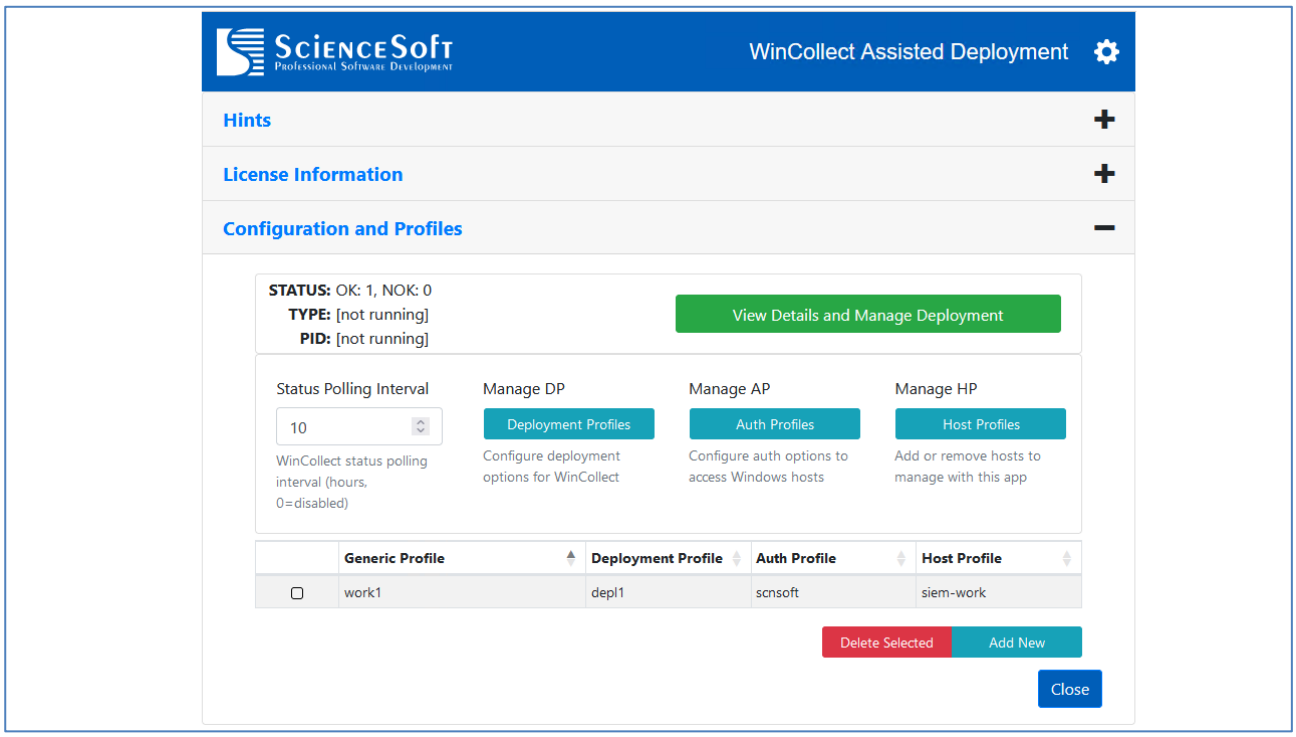
**Operating Systems Supported:*

- *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 qlean@scnsoft.com. You can also request any other QLean App Suite trial licenses and QRadar Professional Services for assistance.

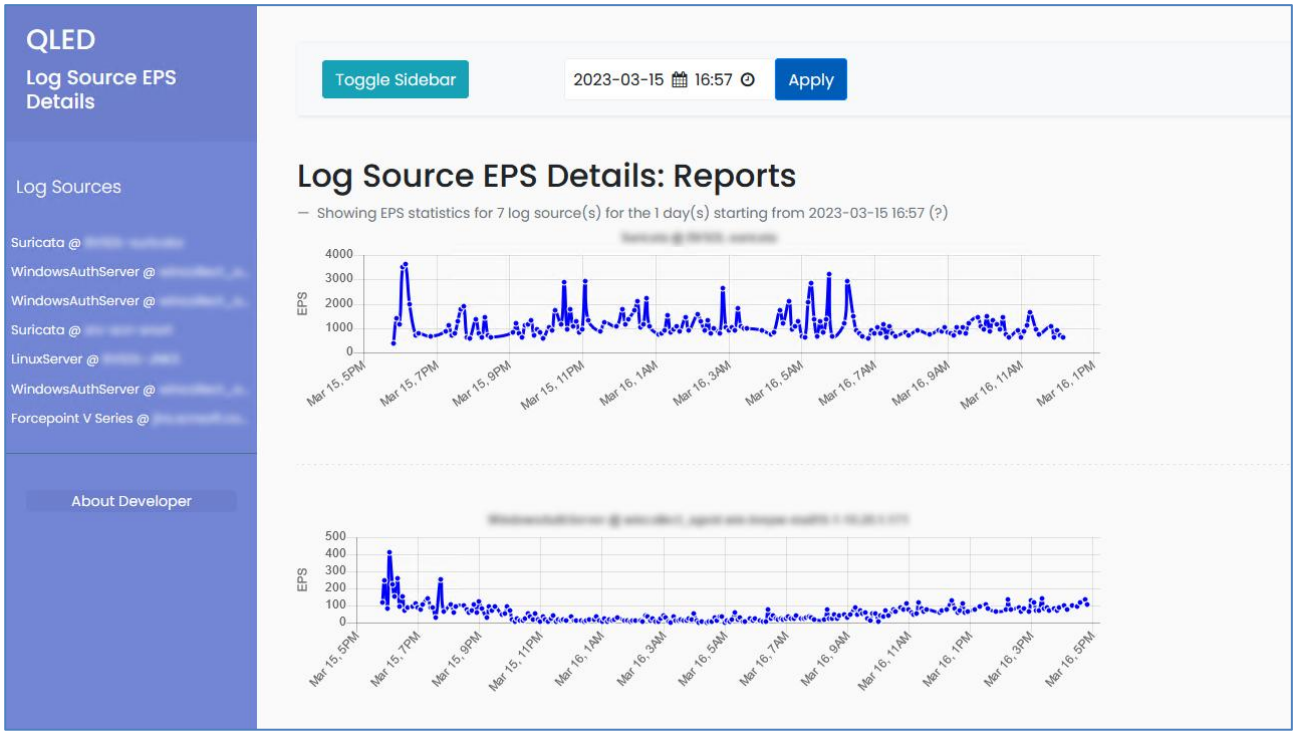
IBM App Exchange

https://exchange.xforce.ibmcloud.com/hub/extension/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. You can also request QRadar Professional Services for assistance.

IBM App Exchange

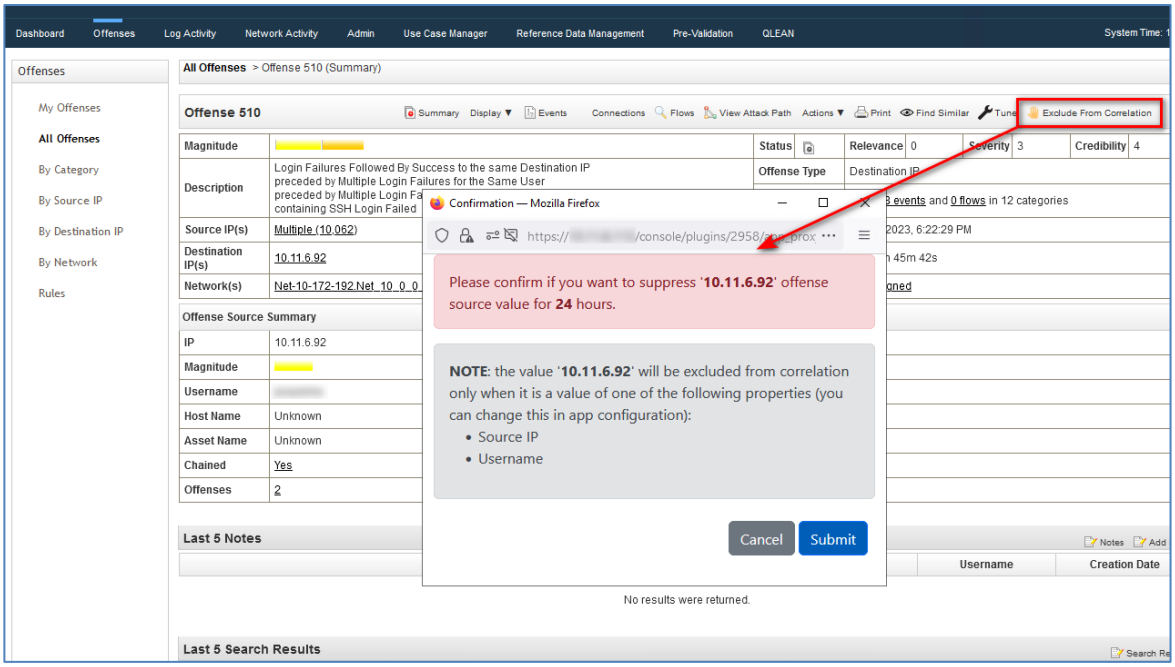
https://apps.xforce.ibmcloud.com/extension/88ecf797cb7d3084d201dc1c145cdf5b

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. You can also request QRadar Professional Services for assistance.

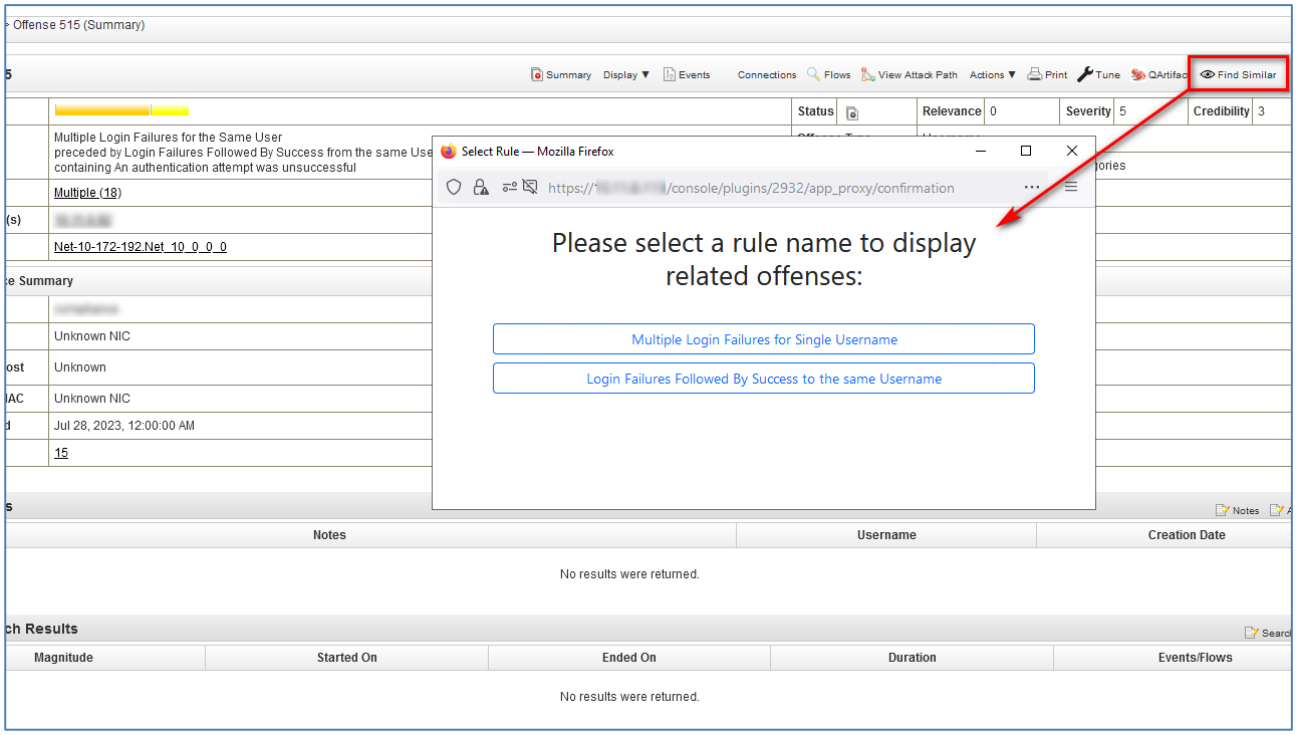
IBM App Exchange

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.



QRadar Native Alternatives

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

License

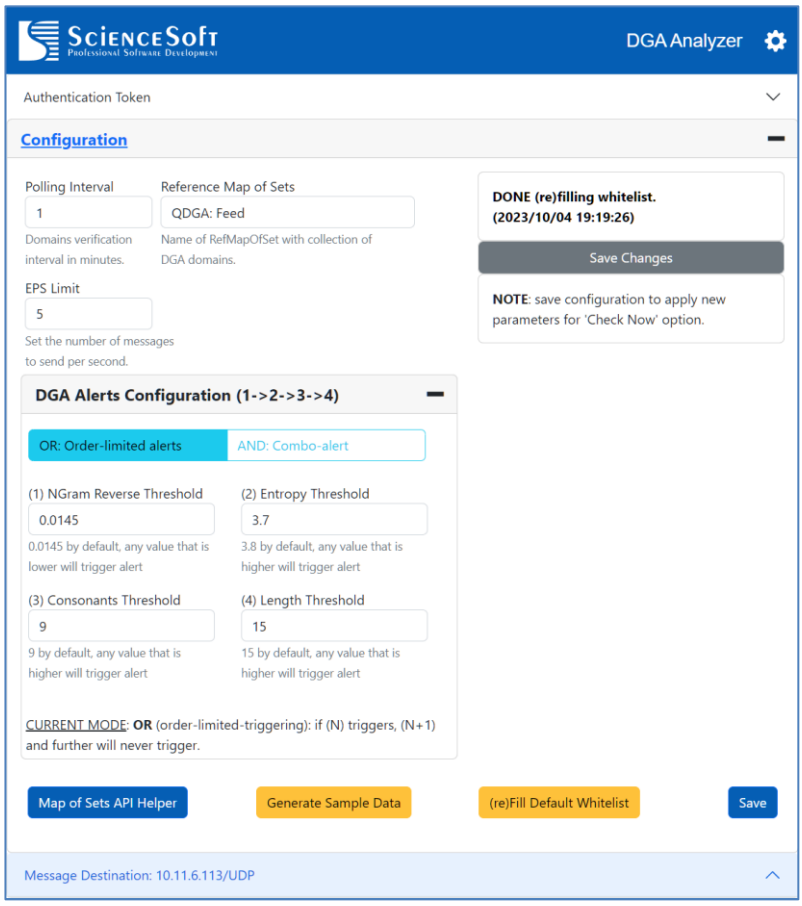
Open Source / Apache 2. To start a free trial of any other QLEAN App Suite tools or request a custom application development contact us at qlean@scnsoft.com or QLEAN App Suite website. You can also request QRadar Professional Services for assistance.

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.



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.

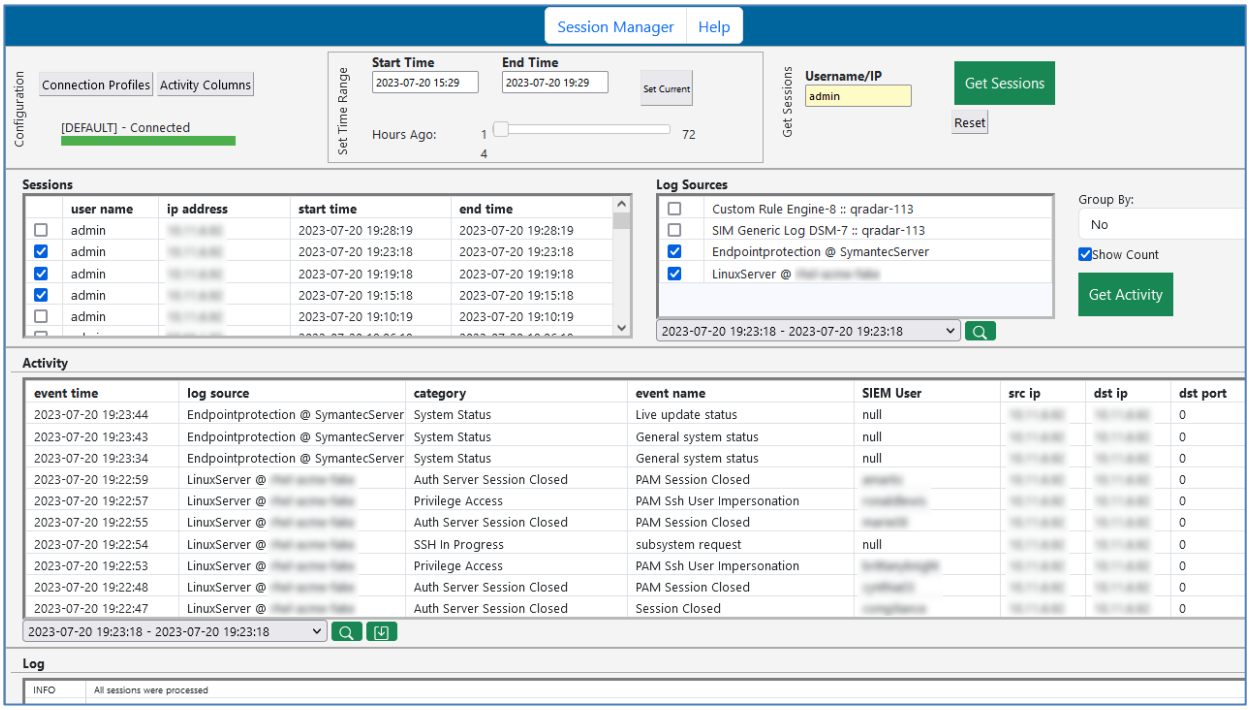
IBM App Exchange

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



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. You can also request QRadar Professional Services for assistance.

IBM AppExchange

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

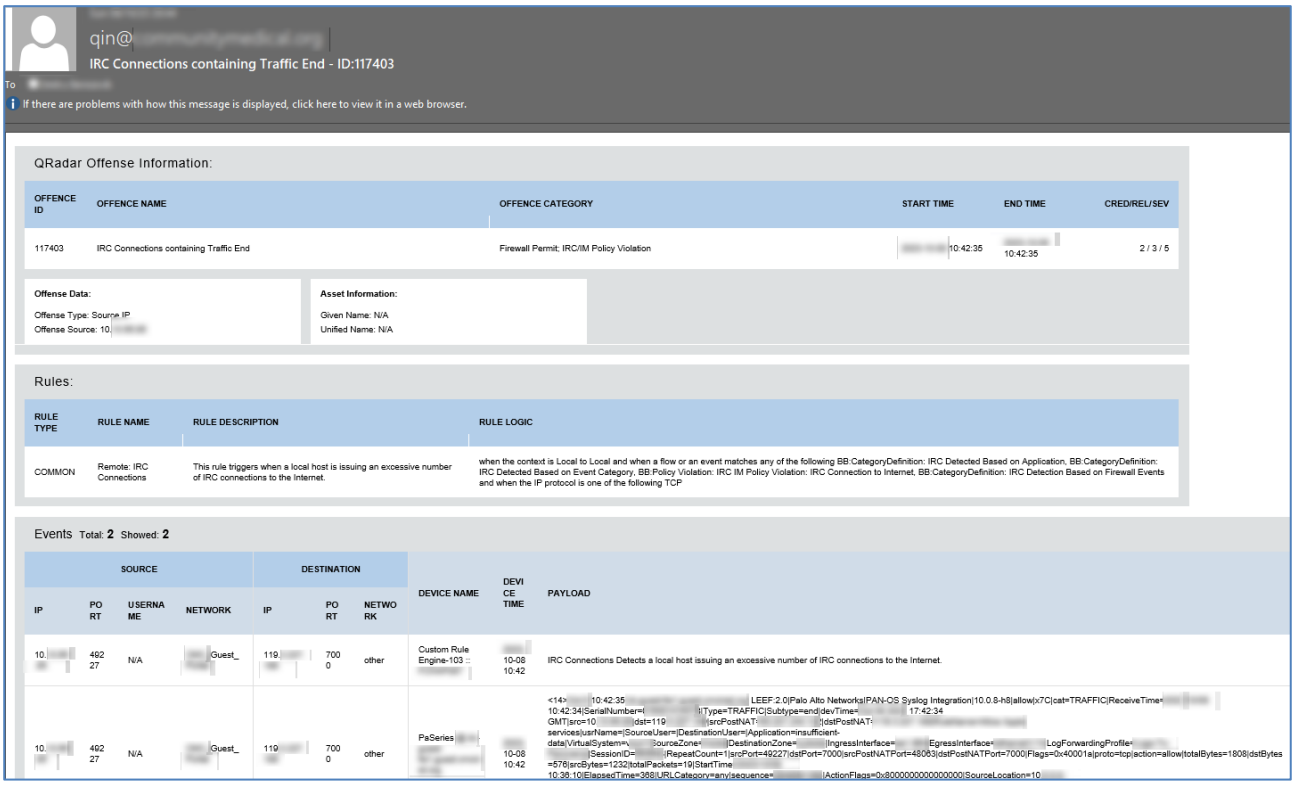
QIN - Incident Notifier [commercial]

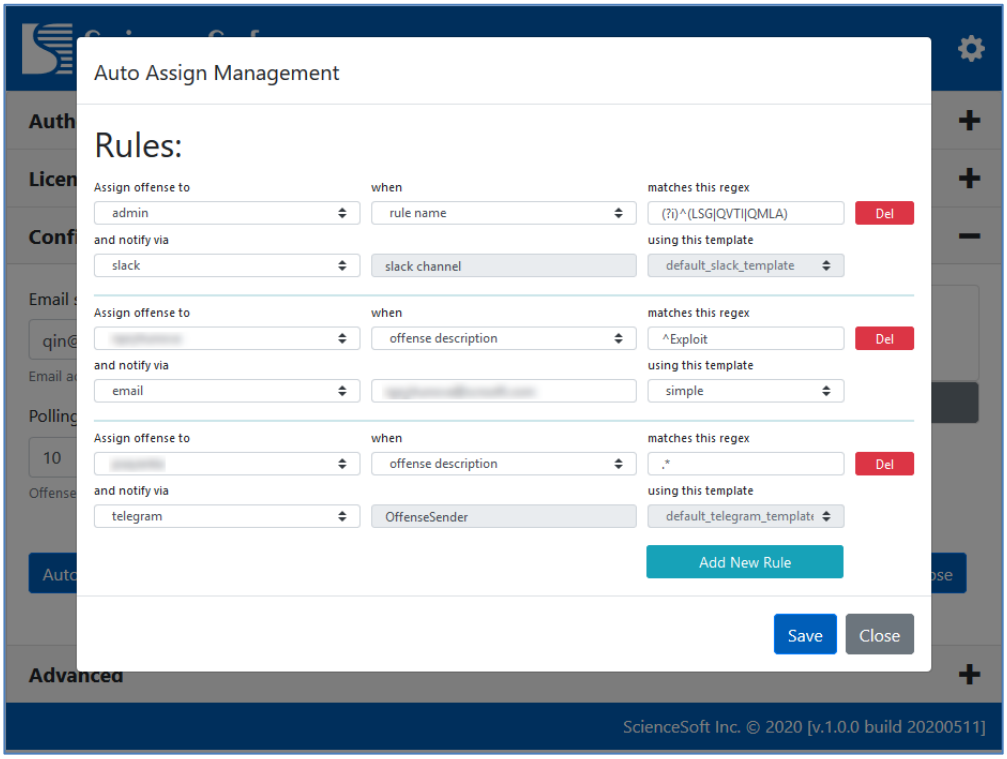
The main purpose of any SIEM systems is to be aware of any security incidents that have just happened as soon as possible. IBM QRadar SIEM does its best parsing and correlating events from all kind of sources and creating offenses whenever any security incident happens. There are out-of-the-box mechanisms, 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.





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

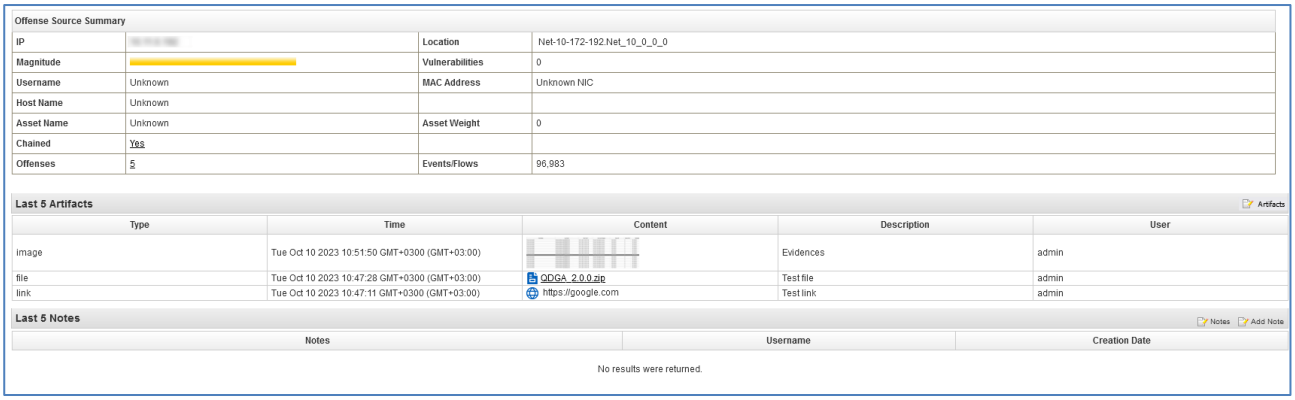
QIN is a commercial application and requires a license to operate. In order to obtain a quote for the license or request a PoC, please contact us at qlean@scnsoft.com. You can also request any other QLean App Suite trial licenses and QRadar Professional Services for assistance.

IBM App Exchange

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

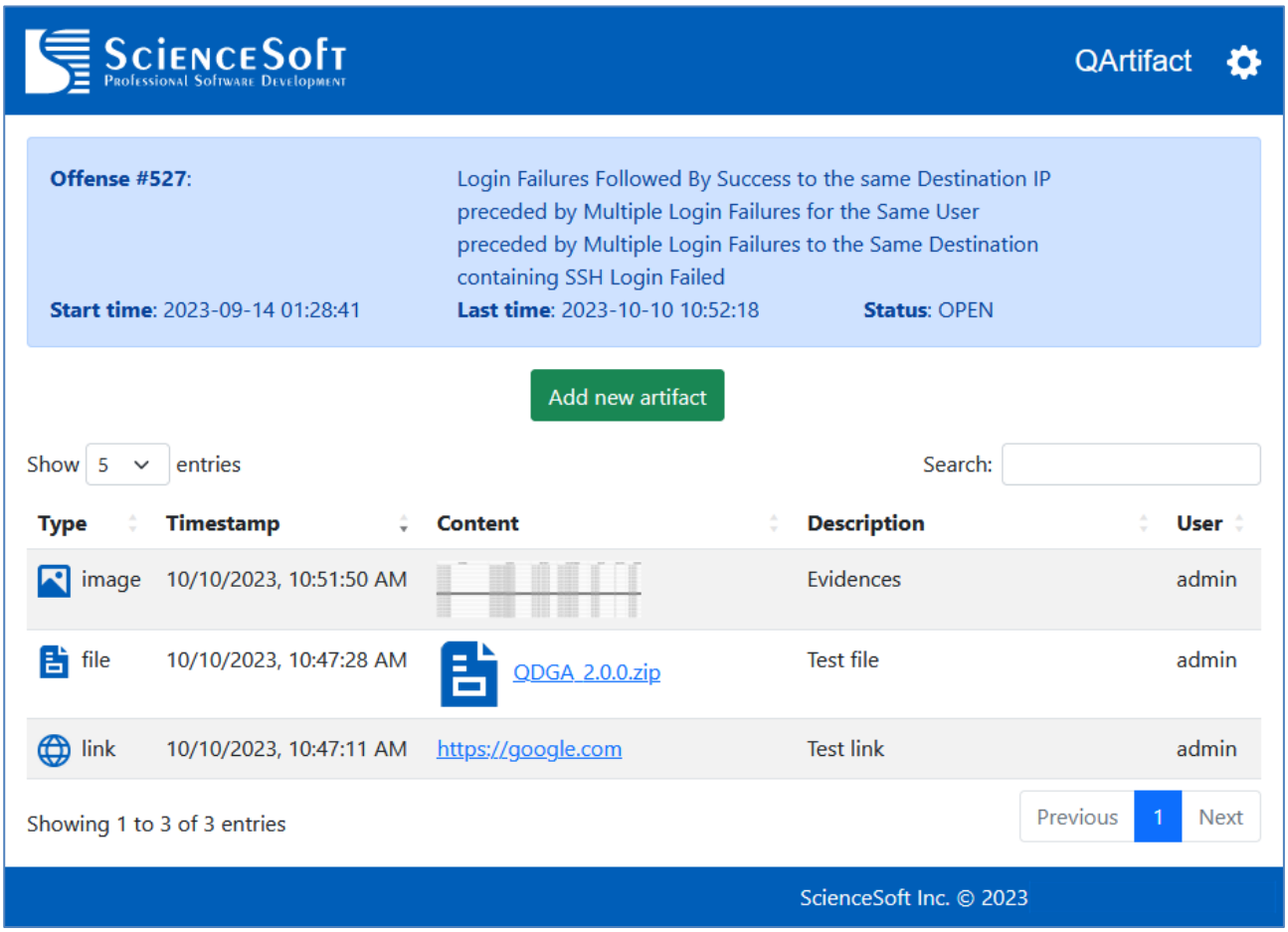
QArtifact [commercial]

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



QRadar Native Alternatives

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



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