Tools created by ScienceSoft

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

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

- Over 50 performance and behavioral metrics
- 25 health markers
- A comprehensive view of QRadar SIEM system state
- Available on IBM App Exchange
QLEAN (previously known as Health Check Framework)

Tools created by ScienceSoft
QSM Session Manager

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

- Operating Systems logs without username
- Web Servers activity
- IDS/IPS activity
- Firewall activity
- Database and business application queries

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

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

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

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

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

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

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

- Offense information
- Correlation rule information
- Affected asset information
- Event information
- Flow information
- HTML tags in custom templates
QIN Incident Notifier

From: QRadar
Sent: Monday, February 8, 2020 5:44 PM
To: QRadar Admin
Subject: Multiple Login Failures for the Same User containing An authentication attempt was unsuccessful - ID:18577

QRadar Offense Information:

<table>
<thead>
<tr>
<th>Offense ID</th>
<th>Offense Name</th>
<th>Offense Category</th>
<th>Start Time</th>
<th>End Time</th>
<th>Cred/Rel/Sev</th>
</tr>
</thead>
<tbody>
<tr>
<td>18577</td>
<td>Multiple Login Failures for the Same User containing An authentication attempt was unsuccessful</td>
<td>General Authentication Failed; User Login Failure</td>
<td>2020-01-16 20:38:48</td>
<td>2020-01-16 20:39:51</td>
<td>4/3/4</td>
</tr>
</tbody>
</table>

Offense Type: Unknown
Offense Source: unknown
N/A

Manage Offense: Close or View

Rules:

<table>
<thead>
<tr>
<th>Rule Type</th>
<th>Rule Name</th>
<th>Rule Description</th>
<th>Rule Tests</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVENT</td>
<td>Multiple Login Failures for Single Username</td>
<td>Reports authentication failures for the same username</td>
<td>when an event matches any of the following BDI Category-Definition Authentication Failures and when at least 10 events are seen with the same Username in 5 minutes</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Device Name</th>
<th>Device Time</th>
<th>Payload</th>
<th>Event Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>Port</td>
<td>Username</td>
<td>Network</td>
<td>IP</td>
<td>Port</td>
</tr>
<tr>
<td>10.0.15.10</td>
<td>0</td>
<td>unknown</td>
<td>Net_10_0_0_0</td>
<td>10.0.15.10</td>
<td>0</td>
</tr>
<tr>
<td>10.0.15.10</td>
<td>0</td>
<td>unknown</td>
<td>Net_10_0_0_0</td>
<td>10.0.15.10</td>
<td>0</td>
</tr>
<tr>
<td>10.0.120.70</td>
<td>0</td>
<td>unknown</td>
<td>Net_10_0_0_0</td>
<td>10.0.120.70</td>
<td>0</td>
</tr>
<tr>
<td>10.0.15.20</td>
<td>0</td>
<td>unknown</td>
<td>Net_10_0_0_0</td>
<td>10.0.15.20</td>
<td>0</td>
</tr>
<tr>
<td>10.0.15.20</td>
<td>0</td>
<td>unknown</td>
<td>Net_10_0_0_0</td>
<td>10.0.15.20</td>
<td>0</td>
</tr>
<tr>
<td>10.0.120.70</td>
<td>0</td>
<td>unknown</td>
<td>Net_10_0_0_0</td>
<td>10.0.120.70</td>
<td>0</td>
</tr>
</tbody>
</table>
QMEA Microsoft Exchange Audit

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

Hints

Microsoft Exchange Audit Export Tool for IBM Security QRadar SIEM is an application for exporting Microsoft Exchange Admin Audit and Mailbox Audit logs and forwarding log records via Syslog protocol (TCP/514) to the QRadar Console in near-real-time. The audit log format generated by this tool is recognized by QRadar log source auto-discovery mechanism (no need to create log source manually). Supported Microsoft Exchange versions are: 2010 SP1, 2013, 2016.

Hints: Initial collect will get audit data for the last one hour. You can reset last collect time to start next collect as initial with respective button.

Following steps should be completed on Microsoft Exchange Server in order to enable audit logs collection:
- Enable Windows Remoting (WinRM) [link]
- Enable Admin Audit [link]
- Enable Mailbox Audit [link]

Following steps should be applied to user account to be used for logs collection:
- Enable ‘RemotePowerShellEnabled’ privilege [link]
- Assign ‘Discovery Management’ role [link]
- Assign ‘Audit Logs’ role [link]

License Information

Exchange Server UUID: 12345678901234567890123456789012
Active Mailboxes: 50
Licensed to: [redacted]
Licensed Mailboxes: [redacted]
License Expiration: [redacted]
QDATA LDAP Data Enrichment

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

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

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

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

Updates:
QRadar Reference Set test ldap
From LDAP: 10.10.10.10:389
Using:
Search Base: DC=sci,DC=com
Search Filters: (&(objectClass=user))
Search Attributes: sAMAccountName
LDAP Search Attributes
QLSI Log Source Inventory

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

Log Source Inventory reports are configurable and separated by domains.

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

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

- Configurable
- Separated by domains
- Include all offenses (active, inactive, closed)
- Include notes, closing date, reason and user, etc.
- Presented in XLSX format which allows sorting and filtering
Tools created by ScienceSoft

QSSA Slow Search Alert

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

To: noreply@qradar.local

Subject: WARNING: Long Lasting Searches Detected

Dear user,

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

Date generated: ...

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

<table>
<thead>
<tr>
<th>Search ID</th>
<th>Search Time (minutes)</th>
<th>Query</th>
</tr>
</thead>
<tbody>
<tr>
<td>2222222222222222222</td>
<td>2</td>
<td>select * from events last 3 days;</td>
</tr>
</tbody>
</table>

Manage Search Results or Cancel Search for Events and Flows.

You will not receive notifications for the searches above for next 24 hours.

NOTE: This is an automatic email. Please Do not reply.
QMLA Missing Logs Alert

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

- Uses QRadar log source groups and allows to define an individual timeout for each group individually.
- Notification are generated and sent via a set of rules shipped with the application.
- Provides users with comprehensive information about Log Sources that became idle, including: Log Source name, Log Source Type, Log Source Group, the last time events seen from this Log Source, etc.
QMLA Missing Logs Alert

Entry Configuration

<table>
<thead>
<tr>
<th>Entry Name</th>
<th>Timeout (minutes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test Entry</td>
<td>240</td>
</tr>
</tbody>
</table>

Configuration

<table>
<thead>
<tr>
<th>Name</th>
<th>Groups</th>
<th>Timeout</th>
</tr>
</thead>
<tbody>
<tr>
<td>Demo Player</td>
<td></td>
<td>240</td>
</tr>
<tr>
<td>Test Entry</td>
<td></td>
<td>120</td>
</tr>
</tbody>
</table>
QRadar extension that significantly simplifies monitoring the number of events received by each log source and exceeding configurable EPS threshold.

The application requests data via QRadar API, stores EPS stats in a built-in database and visualizes it via charts in a new QRadar tab.
QVTI VirusTotal Integration Solution for Hash Verification

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

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

QVTI relies on Sysmon log data collected with WinCollect agents.
QVTI VirusTotal Integration Solution for Hash Verification

Authentication Token

- Auth Token
  
  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
  
  Authentication Token is set and valid

VirusTotal API Keys

VirusTotal API Keys (one key per line)

Submit

Advanced Settings

Max Hashes

Rate Limit

Max number of hashes to check in a single request

Max number of requests per minute

Submit

ScienceSoft Inc. © 2020
QTOR Darknet/TOR Nodes Monitoring

Helps users easily monitor inbound and outbound connections to DarkNet via TOR relay and exit nodes.
QEFC Exclude from Correlation button

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

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

INFO: In order to make this solution work please add OFFENSE.WHITELISTING: Event Marked False Positive rule to the rule test.

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

QRadar extension that adds a new button on the Offense details page. By clicking it user gets a list of all offenses generated by the same rule.

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

The extension is useful to speed up offense investigation and rules tuning.
QFSO Find Similar Offenses button
QDGA DGA Analyzer

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