ScienceSoft
Professional Software Development

QLEAN METRICS DESCRIPTION

KEY

- **i** **Description**
- **?** **Usage**
- **QRadar integration**
- **⚙** **Configurable**

US, McKinney, TX +1 214 306 68 37
www.scnsoft.com contact@scnsoft.com

Finland, Vantaa +358 (45) 178 48 80

Contents

1. GENERIC

1.1 Console IP address

ℹ IP Address of AiO/Console appliance

? Identify specific deployment when running QLEAN reports on multiple QRadar instances

1.2 Console UUID

ℹ Unique hardware identifier

? Use this value to request QLEAN license

1.3 QRadar software version

ℹ Current version of QRadar deployment

? Use this value to request QLEAN license

1.4 Version History

ℹ List of major releases and patches installed since an initial deployment, including dates of installation and the number of installed or upgraded packages

? Keep track of deployment updates; identify potentially faulty version, if some problem have started on particular date

1.5 Users

ℹ List of QRadar users with their roles

? Track excess permissions, outdated or unwanted accounts

2. DEPLOYMENT: HOSTS

2.1 QRadar hosts

ℹ List of Managed Hosts configured within deployment, including HA IP addresses and roles, performance information, disk usage details, etc.

? Deployment overview, identify hosts in non-operational state, hosts running out of disk space; plan upgrades or migration, etc.

3. DEPLOYMENT: HEALTH

3.1 Recent backups

i List of last automatic configuration and data backups

? Track auto backup’s status, assess disk space requirements, identify backup tasks failures

⚙ The number of displayed records can be adjusted via **Backup number** control in QLEAN Execution parameters

3.2 Integrity of Events / Flows for recent 24h

i Integrity information for events / flows Ariel data files for last 24 hours. Corresponding data hashing must be enabled in QRadar Ariel database settings

? Identify disk failures or malicious corruption of data

3.3 Last Warnings and Errors from System Notification

i List of severe events from System Notification

? Track important notifications that may be omitted or dismissed by mistake when browsing QRadar UI

⚙ The number of displayed records can be adjusted via **Sys Notification Count** control in QLEAN Execution parameters

3.4 Last autoupdate errors

i List of failed automatic updates

? Failed dependencies can be resolved manually by downloading and installing missing packages

⚙ The number of displayed records can be adjusted via **Autoupdate Errors Count** control in QLEAN Execution parameters

3.5 Modified crontab

ℹ List of host with modified crontab tasks

? Track modified, deleted or added crontab tasks on all Managed hosts to detect changes that may cause system malfunction

4. ENVIRONMENT: LOG SOURCES

4.1 Last Inactive Log Sources

ℹ List of Log Sources in N/A or Error state, from which no events were received in more than 12 hours. If particular Log Source has been modified in specific timeframe (24h by default, configurable globally across all metrics via **Time range for Ariel queries** parameter) before the last event was seen, corresponding QRadar user name is displayed. If modification happened beyond SIM Audit retention period, User value will be empty

? Detect idle, faulty or misconfigured Log Sources; identify QRadar users who are responsible for their modification

⚙ The number of displayed records can be adjusted via **Log Source Actions Count** control in QLEAN Execution parameters

4.2 Last Disabled Log Sources

ℹ List of Log Sources in Disabled state. QRadar user name who has disabled the Log Source is displayed if the action was performed within SIM Audit retention period

? Detect disabled Log Sources and QRadar users who are responsible for their disablement

⚙ The number of displayed records can be adjusted via **Log Source Actions Count** control in QLEAN Execution parameters

4.3 Protocol Configuration Errors

ℹ List of Log Sources in WARN state, with corresponding failure reason. If particular Log Source has been modified in specific timeframe (24h by default, configurable globally across all metrics via **Time range for Ariel queries** parameter) before the last event was seen, corresponding QRadar user name is displayed. If modification happened beyond SIM Audit retention period, User value will be empty

? Detect misconfigured Log Sources, that poll data periodically, and QRadar users who are responsible for their modification

⚙ The number of displayed records can be adjusted via **Log Source Actions Count** control in QLEAN Execution parameters

4.4 Last Added Log Sources

ℹ List of recently added and enabled Log Sources. If a Log Source has been added by QRadar user, and the action was performed within SIM Audit retention period, corresponding QRadar user name is displayed

? Track new Log Sources, identify those ones that cause abnormal EPS capacity consumption

⚙ The number of displayed records can be adjusted via **Log Source Actions Count** control in QLEAN Execution parameters

4.5 Last Modified Log Sources

ℹ List of recently modified Log Sources. If a Log Source has been modified by QRadar user, and the action was performed within SIM Audit retention period, corresponding QRadar user name is displayed

? Track Log Sources modification, identify causes of event pipeline changes, normalization failures, etc.

⚙ The number of displayed records can be adjusted via **Log Source Actions Count** control in QLEAN Execution parameters

4.6 Last Deleted Log Sources

ℹ List of recently deleted Log Sources. QRadar user name who has deleted the Log Source is displayed if the action was performed within SIM Audit retention period

? Identify whether Log Sources have been deleted for optimization/troubleshooting purposes or maliciously, or mistakenly

⚙ The number of displayed records can be adjusted via **Log Source Actions Count** control in QLEAN Execution parameters

4.7 All Log Sources

ℹ List of all external (not own QRadar services) Log Sources in details

? Quickly sort, filter and search

🛡 Edit a Log Source by clicking on its name

5. ENVIRONMENT: EPS ALERTS

5.1 EPS Anomalies

ℹ List of recent *Max events reached* and *Events were routed directly to storage* warnings from System Notifications, along with Log Sources that generated the most number of events. For each Log Source a list of top event types is provided.

? Keep track of EPS spikes and dropped events. Identify Log Sources and event types that put excessive load on the system

⚙ The minimal amount of generated events for a Log Source to be listed in the report can be adjusted via **EPS Anomalies Threshold** control in QLEAN Execution parameters

6. ENVIRONMENT: EPS

6.1 EPS/FPM per Managed Host

ℹ List of event/flow processing hosts (21xx, 31xx, 16xx, 17xx, 18xx) with their EPS/FPM license limits and actual capacity utilization statistics for last interval (24 hours by default, configurable via **Time range for Ariel queries** parameter)

? Identify overloaded or idle hosts, re-consider licenses allocation or enhancement

6.2 EPS per Log Source Type

ℹ List of the most EPS consuming Log Sources grouped by Type (DSM). Average and peak EPS values are lifetime stats

? Review audit baseline for Log Source Types that produce too many events and disable logging or filter out unwanted messages

⚙ The number of displayed records can be adjusted via **Log Source Types Count** control in QLEAN Execution parameters

7. ENVIRONMENT: RAW EPS

7.1 Raw Inbound Events Per Second

ℹ Real amount of incoming events per Managed Host (including Event Collectors), without considering license limitations. Timeframe is 24 hours by default, configurable via **Time range for Ariel queries** parameter.

❓ Detect spikes and gaps, re-consider license allocation or enhancement

8. ENVIRONMENT: RAW FPM

8.1 Raw Inbound Flows Per Minute

ℹ Real amount of incoming flows per Managed Host (including Flow Collectors), without considering license limitations. Timeframe is 24 hours by default, configurable via **Time range for Ariel queries** parameter.

❓ Detect spikes and gaps, re-consider license allocation or enhancement

9. ENVIRONMENT: DATA QUALITY BY DEVICE TYPE

9.1 Data Quality by Device Type

ℹ List of Device Types (DSMs) in use, each containing:

List of Event Categories for which no events were received in defined timeframe (24 hours by default, configurable globally across all metrics via **Time range for Ariel queries** parameter);

Category coverage: percentage of seen Event Categories against all supported by DSM;

List of seen Event Categories, including average event severity, number of seen Event Types, number of supported Event Types, total number of events seen in Category, and Event Coverage - percentage of seen Event Types against supported ones.

Note: Event Coverage 101% (Types Seen > Types Supported) means that specific DSM utilizes QIDs from other DSMs. E.g. LinuxServer shares many QIDs with OS Services, etc.

Assess quality of audit configuration, when all Log Sources of one type are configured using the same baseline;

Identify important categories missing in event pipeline; detect DSMs that require update or LSX.

Compare several daily reports to identify Categories that are constantly missing

Data Quality metrics run multiple Ariel searches over all collected data, and therefore require notable amount of time to execute. To minimize QLEAN report generation time, either use **Time range for Ariel queries** parameter to narrow down the timeframe, or disable these metrics via **Disable Data Quality Metrics** checkbox.

Drill down to event type's distribution by clicking on Category name

Drill down to normalized or raw events via right-click menu on Category name

10. ENVIRONMENT: DATA QUALITY BY LOG SOURCE

10.1 Data Quality by Log Source

List of Device Types (DSMs) in use, each containing:

List of Log Sources with their event pipeline statistics for defined timeframe (24 hours by default, configurable globally across all metrics via **Time range for Ariel queries** parameter), regardless of Categories; each contains: Device Type (DSM), average event severity, number of seen Event Types, number of supported Event Types by DSM, total number of events, coverage - percentage of seen types against supported ones.

Assess quality of audit configuration per Log Source instance, consider updating DSM or creating LSX/Custom DSM. Attention to Log Sources in the Worst Coverage list, ones with Types Seen =1 and low severity.

Note: usually DSMs include QIDs for multiple versions and optional components/features available for an application or appliance, thus 100% coverage is unlikely for most Device Types. Normally, coverage > 20% is supposed to be good enough.

Data Quality metrics run multiple Ariel searches over all collected data, and therefore require notable amount of time to execute. To minimize QLEAN report generation time, either use **Time range for Ariel queries** parameter to narrow down the timeframe, or disable these metrics via **Disable Data Quality Metrics** checkbox

Drill down to event types distribution by clicking on Log Source name

11. ENVIRONMENT: DATA QUALITY: UNKNOWN EVENTS AND SOURCES

11.1 Unknown events

List of Log Sources that have unknown events detected in defined timeframe (24 hours by default, configurable globally across all metrics via **Time range for Ariel queries** parameter), including total number of received events, number of unknown events, and percentage of the latter against the first

Detect Log Sources that produce significant amount of un-parsed data; either to disable noise, or to extract important security information

Data Quality metrics run multiple Ariel searches over all collected data, and therefore require notable amount of time to execute. To minimize QLEAN report generation time, either use **Time range for Ariel queries** parameter to narrow down the timeframe, or disable these metrics via **Disable Data Quality Metrics** checkbox

Drill down to events payload by clicking on Log Source name

11.2 SIM Generic Log Sources

List of IP addresses from which un-identified events were received and not assigned to any existing Log Source in defined timeframe (24 hours by default, configurable globally across all metrics via **Time range for Ariel queries** parameter), including the number of such events

Detect unwanted noise, or important events that cannot be identified as belonging to particular Log Source because of message format, or Log Sources that must be created manually

Drill down to events payload by clicking on source IP Address

12. CORRELATION: OFFENSES

12.1 Top Unique Offenses

ℹ	List of open Offenses involving the greatest number of events or flows, grouped by Offense description
?	Identify false-positives or actual attacks
⚙	The number of displayed records can be adjusted via **Top Offenses Count** control in QLEAN Execution parameters
🛡	Open the list of similar offenses by clicking on Offense name

12.2 Offense Closing Reasons

ℹ	List of reasons and partially notes used to close offenses during the recent 30 days
?	Identify most common incident types; assess the clarity of resolutions made by security team

12.3 Offense Analysis

ℹ	List of enabled correlation rules along with offenses being generated by them, rules logic, and notes. Stats are lifetime and depend on the configured offense retention period (30 days by default). The second column shows the offense type (a property that the offense is indexed by) and appropriate values. The third column header shows the rule type (common, events, flows, offense). Column values represent total number of events and flows involved in the offense. The chart values shows how many times rules have been triggered
?	Identify false-positive offenses, common sources of incidents, fix rules logic accordingly
⚙	Use **Offense Analysis: exclude inactive** and **Offense Analysis: include dismissed** checkboxes in QLEAN Execution parameters to control whether hidden, closed and inactive offenses present in the output
🛡	Drill down to offense details by clicking on its ID Open Rule Wizard by clicking on the pencil icon next to the Rule name Open the list of offenses by clicking on the list icon next to the Rule name

Search for events contributing to the offense by clicking on the index value (Source IP, Username, etc.)

13. CORRELATION: OFFENSES (2)

13.1 Attacker to Target

i Represents links between Attackers networks from Network Hierarchy and specific Destination (Target) IP addresses

? Identify common attack/incident directions

13.2 Top Attackers

i List of top 25 Attackers by their networks from Network Hierarchy

? Identify the most common attacker networks

13.3 Top Targets

i List of top-25 target IP addresses in active offenses

? Identify the most common targets

13.4 Offense per User

i List of top-targeted networks from Network Hierarchy by Users participating in attacks

? Identify the most common usernames attacking internal resources

14. CORRELATION: RULES

14.1 Rules counters

i Includes the number of enabled, disabled, custom (created by user) and modified rules, and the number of Building blocks

? High-level overview of QRadar tuning

14.2 Rules Performance

ℹ Lists of runtime (since the last hostcontext service restart) statistics based on findExpensiveCustomRules support script

? Identify rules that require tuning (add tests to narrow down the amount of data to match, adjust thresholds, replace payload searches with custom properties, fix or disable Custom Action scripts, etc.).

⚙ The number of displayed records can be adjusted via **Rules Performance Count** control in QLEAN Execution parameters.

Stats gathering interval can be set via **Rules Performance Interval** control. This value affects execution time of QLEAN report

🛡 Open Rule Wizard by clicking on the rule name

15. CORRELATION: REPORTS

15.1 Top heavy reports

ℹ List of the most time consuming reports, along with their expected and actual execution time

? Identify reports that take longer than usual to generate, refer to Last modified searches metric to check whether any search changes caused reports to slow down

⚙ The number of displayed records can be adjusted via **Top Reports** control in QLEAN Execution parameters

🛡 Open report properties by clicking on its name

15.2 Last 10 recently modified searches

ℹ List of 10 saved searches that were recently modified

? Identify a responsible person, if search modification caused incorrect sampling, increased report execution time, system overload, or affects correlation rules logic

16. SOC KPI

16.1 Incident Resolution Time

ℹ Distribution of offenses closed within 4h, 12h, 1d, 3d, 7d, 14d, 1m timeframes during the last 31 days or within a custom time frame

? Track analyst activities, assess SOC performance

⚙ Define a custom time range via **SOC KPI Data Range** control in QLEAN Execution parameters. If not defined, or **Reset time range** button was pressed, data will be collected for the recent 31 days

16.2 Incident Response Time

ℹ Distribution of assigned or protected offenses within 4h, 12h, 1d, 3d, 7d, 14d, 1m timeframes during the last 31 days or within a custom time frame

? Track analyst activities, assess SOC performance

⚙ Define a custom time range via **SOC KPI Data Range** control in QLEAN Execution parameters. If not defined, or **Reset time range** button was pressed, data will be collected for the recent 31 days

16.3 Incidents Closed per User

ℹ Distribution of offenses closed by analysts during the last 31 days or within a custom time frame

? Track analyst activities, assess SOC performance

⚙ Define a custom time range via **SOC KPI Data Range** control in QLEAN Execution parameters. If not defined, or **Reset time range** button was pressed, data will be collected for the recent 31 days

16.4 Incidents Detected

ℹ Number of new offenses for the last 31 days or within a custom time frame

? Assess quality of correlation tuning

⚙ Define a custom time range via **SOC KPI Data Range** control in QLEAN Execution parameters. If not defined, or **Reset time range** button was pressed, data will be collected for the recent 31 days

16.5 Incident Severity

ℹ Offense severity levels for the last 31 days or within a custom time frame

? Assess quality of correlation tuning

⚙ Define a custom time range via **SOC KPI Data Range** control in QLEAN Execution parameters. If not defined, or **Reset time range** button was pressed, data will be collected for the recent 31 days

16.6 System Tuning Actions

ℹ Number of modifications (reference sets, rules, log sources, etc.) performed during the last 31 days or within a custom time frame

? Track analyst activities, assess SOC performance

⚙ Define a custom time range via **SOC KPI Data Range** control in QLEAN Execution parameters. If not defined, or **Reset time range** button was pressed, data will be collected for the recent 31 days

17. FINE TUNING

17.1 Untuned Building Blocks

ℹ List of active system (not modified) Building Blocks, mostly *HostDefinitions*, containing default IP address placeholders (127.0.0.2)

? Identify default BBs to update with proper values

🛡 Open Rule Wizard by clicking on a Building Block name

17.2 Retention Buckets less than 6 months

ℹ List of active Event and Flow Retention Buckets that store data for less than 6 months

? Identify short-term storage settings to avoid unexpected data loss

17.3 Untuned Network Hierarchy Elements

i List of system networks containing default CIDRs

? Identify default networks to update with proper values

🛡 Open network Hierarchy interface by clicking on an entry name

17.4 Untuned Network Hierarchy Correlation Rules

i List of correlation rules that utilize default Network Hierarchy elements

? Refer to the list to either change rules filters or update corresponding Network Hierarchy entries to avoid false-positives or missed incidents

17.5 Disabled Custom Properties

i List of Custom Properties that were disabled by QRadar automatically and the rules that use these properties

? Refer to the list to enable inactive Custom Properties

17.6 Custom DSM Unknown Events

i Shows the amount of unknown events received from Custom DSM Log Sources

? Custom DSMs are assumed to recognize all events and therefore should not have any Unknowns. Identify event types that weren’t seen before and may contain important security information; and create matchers for them via DSM Editor

17.7 Flow Sources

i Inbound flows statistics per Flow Source for last 24 hours

? Identify most loaded flow capturing interfaces for balancing and tuning

17.8 Unassigned Log Sources

i List of Log Sources that are not assigned to any Log Source Group

? Check the list to make sure that rules utilizing Log Source Groups in their logic capture all required data

18. PERFORMANCE

18.1 Global Views Performance

ℹ Output of collectGvStats support script, showing speed of saved searches and reports for log data and network activity

? Identify and optimize searches that take too long to execute

18.2 Regex Relative Performance

ℹ Assesses regular expressions speed by performing multiple matches against payload. Properties without a payload (Test Field in Custom Properties) are omitted

? Identify and fix custom properties that slow down events processing