QRadar Health Check Offering with QLEAN by ScienceSoft

www.qlean.io | www.scnsoft.com

ScienceSoft Cybersecurity is a team of **SIEM/SOAR/SOC experts**. Our flagship cybersecurity product called **QLEAN SIEM App Suite** has been named a global Beacon Award finalist for two years in a row (2020, 2021). ScienceSoft engineers bring two decades of expertise & solutions development, deployment, integration, migration, health checks, fine-tuning, optimization, continuous L3 SIEM support & maintenance, remote monitoring services, training, and SOC consulting.

Our **QRadar Health Check offering** deploys a ScienceSoft subject matter expert to conduct a technical and operational review of the QRadar environment based on the QLEAN results, create a findings and recommendations document so improvements can be made, and assists with tuning and other implementation recommendations.

ScienceSoft QRadar experts will use **QLEAN**, an automated tuning & health check tool, to conduct thorough analysis of multiple QRadar deployment parameters including performance metrics, quality of incoming data and system settings. QRadar Health Check will deliver a **360-degree view of your QRadar SIEM** and provide **actionable recommendation** by using both automated and manual approaches. Automated approach assumes installation of QLEAN for QRadar Health Check & Tuning. ScienceSoft will assess your QRadar deployment and prepare a **detailed health check report** and recommendations for any necessary fixes and enhancements. Our Client will have a 30-day license to use the QLEAN product. After 30 days, the client will be able to purchase a QLEAN license and support from ScienceSoft for continuous assessment and service.

Pricing

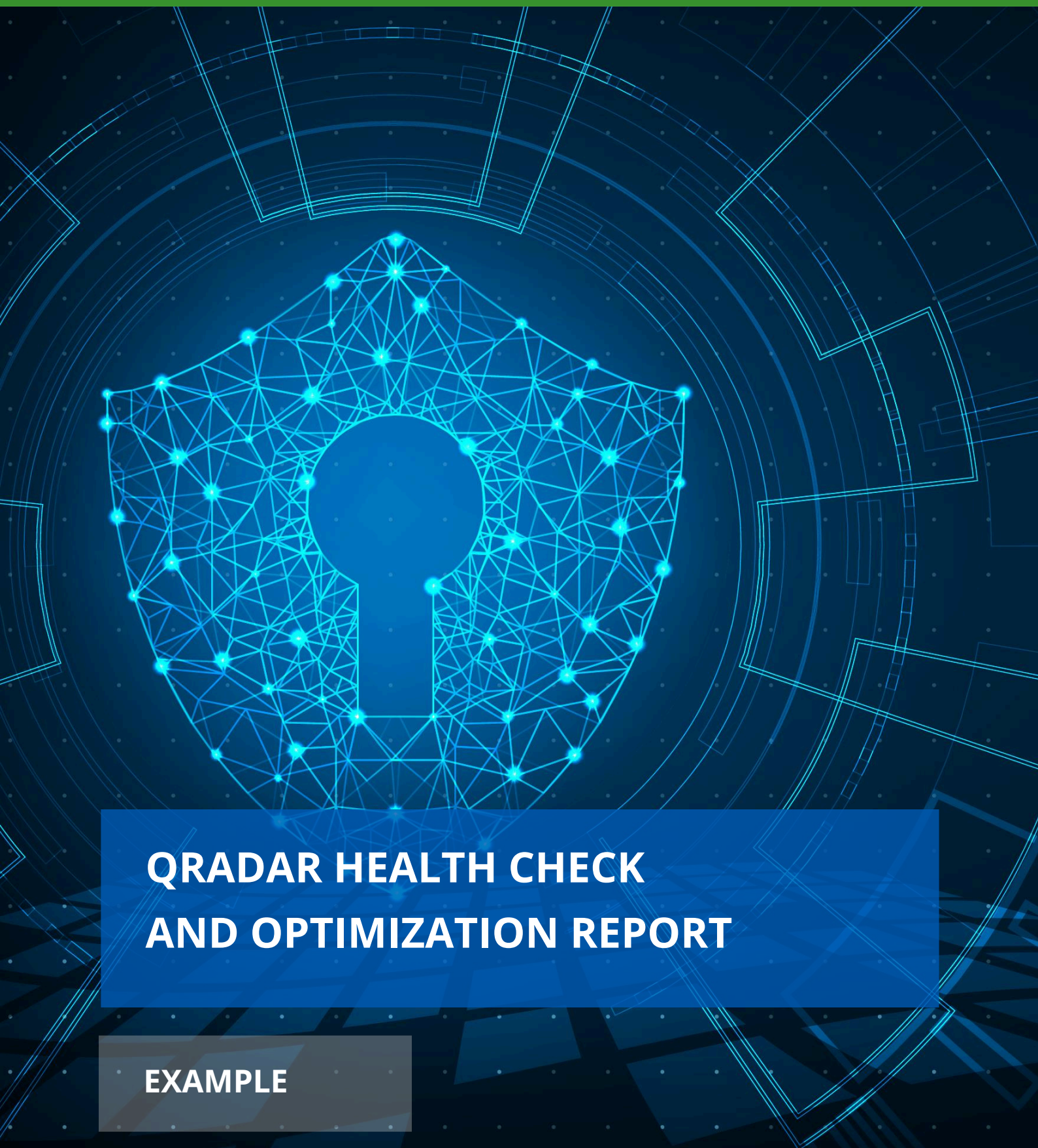
	Client total licensed EPS capacity	Price in USD
✓	Up to 5000 EPS	4000
✓	Up to 50000 EPS	6000
✓	Up to 100000 EPS	8000
✓	From 100000 EPS and more	10000

Please find a sample QRadar assessment report on the following page
For more information, kindly email us at qlean@scnsoft.com

ScienceSoft USA Corporation
5900 S. Lake Forest Drive, Suite 300
McKinney, TX 75070, USA
+1 (214) 306-6837
qlean@scnsoft.com
www.scnsoft.com
www.qlean.io

ScienceSoft
Professional Software Development

www.scnsoft.com



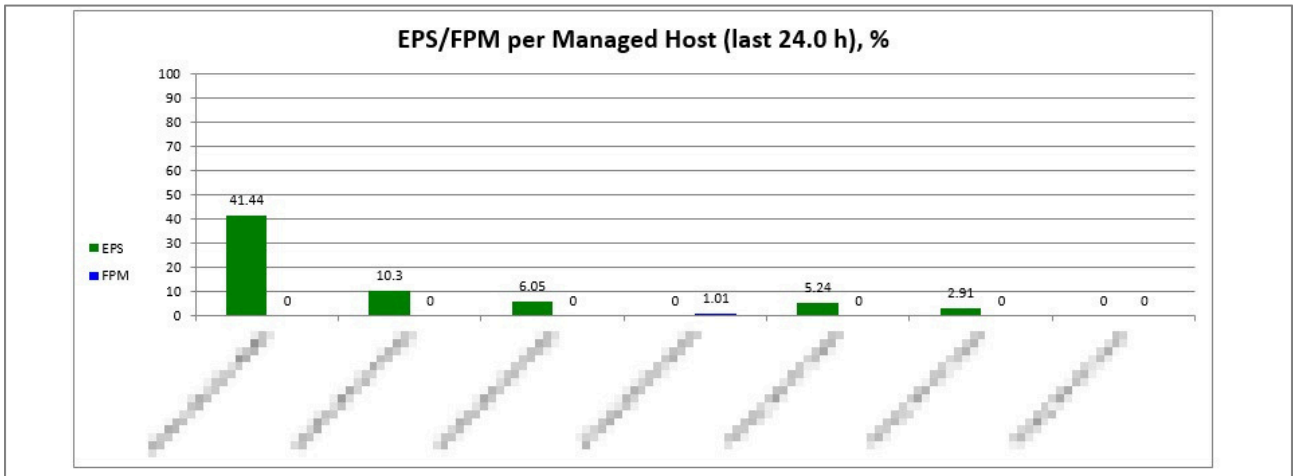
QRADAR HEALTH CHECK AND OPTIMIZATION REPORT

EXAMPLE

Table of Contents

Overview

ScienceSoft SIEM team proudly presents a detailed summary for **Customer** QRadar Health Check status, based on data obtained by QLean software on August 30, 2024.



Managed host name	Managed host IP address	Avg EPS for last 24.0 hours	Avg FPM for last 24.0 hours	EPS License limit	FPM License limit	EPS utilization, %	FPM utilization, %
[redacted]	[redacted]	414	0	1000	0	41.44	0
[redacted]	[redacted]	1545	0	15000	0	10.3	0
[redacted]	[redacted]	907	0	15000	0	6.05	0
[redacted]	[redacted]	**0**	**2011**	**0**	**200000**	**0**	**1.01**
[redacted]	[redacted]	786	0	15000	0	5.24	0
[redacted]	[redacted]	436	0	15000	0	2.91	0
[redacted]	[redacted]	**0**	**0**	**0**	**100000**	**0**	**0**

Please find a quick summary of issues discovered during the Health Check in the next chapter.

Quick Health Check Summary

- **Critical**: Retention policies keeping log data for 3 months only (99% of storage is free). **[link]**
- **Critical**: Missing mission-critical logs: DNS, Authentication/AD, DHCP. **[link]**
- **Critical**: Parsing enhancements required for supported log sources (6 types). **[link]**
- **Critical**: Parsing enhancements required for custom DSMs (6 types). **[link]**
- **Critical**: Business applications and network devices are receiving unprocessed data or data is missing at all (35 log sources of 12 types). **[link]**

- **Medium**: Flow collection potential misconfiguration (low NetFlow data volume). **[link]**
- **Medium**: Auto-update requires manual dependency resolution. **[link]**
- **Medium**: Receive frame errors on interface eno3 on 10.10.10.11. **[link]**
- **Medium**: Tuning of default system BBs (building blocks) is required to minimize false-positives. **[link]**
- **Medium**: Audit settings of several device types need to be adjusted (no important categories). **[link]**
- **Medium**: Offense processing workflow should be established (closing reasons, etc.). **[link]**
- **Medium**: 15 high-load log sources are not auto-discovered (up to 3,000,000 events in 24h each) and need to be configured/parsed. **[link]**
- **Critical**: SIEM solution will require tuning after adding missing log source types (AD, DNS, etc). **[link]**

Non-critical requirements to be fixed:

- Incident Response. **[link]**
- Log Source Grouping. **[link]**

Detailed Report

Retention Policies

Various compliance requirements (NIST 800, ISO 27001, GDPR) are stating that 1 year of storing log data is a bare minimum. Any historical investigation for over than 3 months ago are currently impossible to perform because of retention setting.

Current retention policies:

Name	Type	Retention, days	Modification Date
Default	events	91	2023-09-03 09:01:00

Percentage of a free space for each host in deployment.

HA IP Address	Appliance Type	Total /store space	Free /store space, %
10.10.7.10	1726	23.5TB	99.9%
10.10.7.11	3126	19.8TB	98.5%
10.10.7.12	1400	23.9TB	98.2%
10.10.7.13	1626	23.5TB	98.2%
10.10.7.14	1400	23.9TB	99.4%
10.10.7.15	1626	23.5TB	99.4%
10.12.12.13	1626	23.5TB	98.5%
10.12.12.14	1626	23.5TB	99.4%
10.12.12.15	1726	23.5TB	99.9%

Missing Mission-Critical Logs

Collecting information from DHCP, DNS, Edge Firewall, and authentication/identity system logs is **mandatory**. This data provides comprehensive visibility into network activity, user authentication, and user activities, enabling the detection of threats that might otherwise go unnoticed. Gathering this information ensures that security teams can identify, prioritize, and respond to potential threats quickly and more effectively.

Following critical log types are missing:

- Authentication (AD, LDAP, VPN, etc.)
- DNS (Windows DNS Debug, etc.)
- DHCP (no active DHCP – minor amount of logs)
- Edge FW (need to verify if we are getting logs of outbound connections)
- Other important security solutions

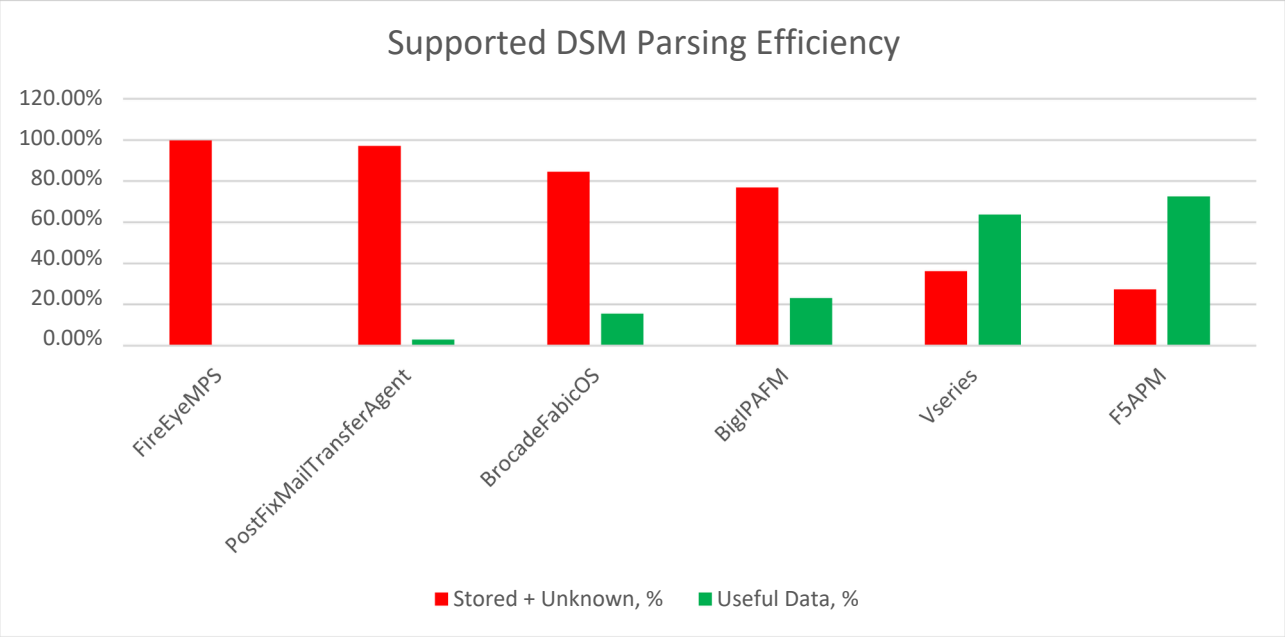
The current appliance contains the following sources of information:

Log Source Type	Type
Anti-malware/anti-virus	McAfee
Cloud Management Software	Gigamon
DNS Servers	**No Data**
DHCP servers	BlueCat Network Adonis, Linux DHCP (**Low Data**)
Network Firewall	F5 Big IP, F5 ASM, F5 APM, F5 TLM, Forcepoint V series, Juniper
WAF (Web Application Firewall)	F5 AFM
Virtualization	VMware V center
Authentication	**No Data**

NOTE: *ScienceSoft has no access to Customer production environment. This analysis is based on QLean report and might need clarification with Customer network/system administrators.

Parsing. Supported DSM

To ensure effective correlation, QRadar processes various types of information using official DSMs (Device Support Modules) developed by IBM. Solution deployment analysis has revealed potential audit misconfigurations and/or parsing issues that need to be addressed. Below, you can find a graph that illustrates how events are recognized.

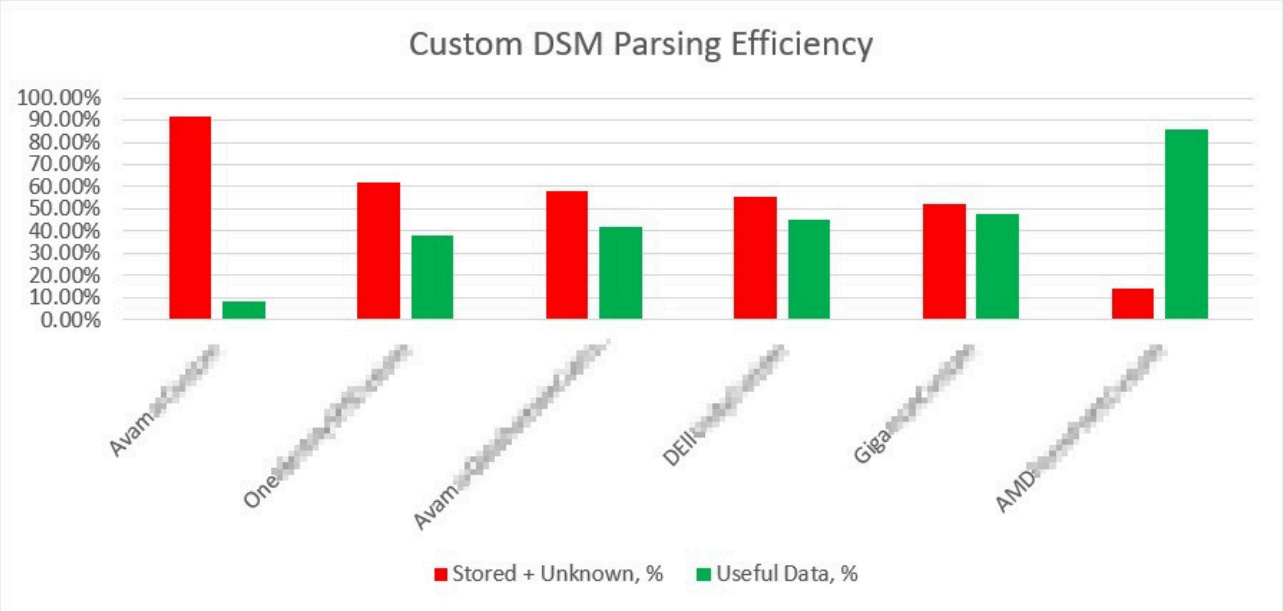


Device Type	Stored + Unknown, %	Useful Data, %
FireEyeMPS	99.8%	0.2%
PostFixMailTransferAgent	97.1%	2.9%
BrocadeFabicOS	84.5%	15.5%
BigIPAFM	76.9%	23.1%
Vseries	36.3%	63.8%
F5APM	27.4%	72.6%

Parsing. Custom DSM

Collected information must be accurately processed (parsed and mapped) for effective correlation in QRadar. Solution deployment analysis has revealed log data processing issues with many Custom DSM that are applied on the system.

Regular review and updates of these DSMs will accommodate new log formats, optimize parsing performance, and ensure precise normalization. Custom DSMs below are required to be updated in order to provide properly normalized data for SIEM solution.



Device Type	Stored + Unknown, %	Useful Data, %
Avam...	91.4%	8.6%
One...	61.8%	38.2%
Avam...	58.2%	41.8%
Dell...	55.2%	44.8%
Giga...	52.6%	47.4%
AMD...	14%	86%

Inactive Log Sources

Log sources must always be active (especially the most critical), and any issues that prevent event collection must be resolved immediately. Below is the list of sources that have stopped sending data and require additional investigation and fix.

Also, ScienceSoft recommends to implement alerting mechanism for most critical log sources, so production team will be alerted when any important log source has stopped sending events.

Source Name	Source Type	Last seen
Avam...	Avam...	2024-05-16 03:21:34
Blue...	Blue...	2023-09-27 06:38:25
Blue...	Blue...	2024-07-17 06:06:17
Blue...	Blue...	2023-09-06 02:39:13
Blue...	Blue...	2024-05-14 01:11:11
Blue...	Blue...	2023-09-27 06:38:06
Blue...	Blue...	2023-09-06 02:23:23
Blue...	Blue...	2024-06-04 02:41:27
Blue...	Blue...	2023-09-06 02:26:45
Blue...	Blue...	2023-09-06 02:27:57
Blue...	Blue...	2023-09-06 02:34:08
Blue...	Blue...	2023-09-06 02:35:30
Blue...	Blue...	2023-09-06 02:24:22
F5...	F5ASM	N/A
F5ASM...	F5ASM	2024-07-04 10:04:41
F5ASM...	F5ASM	2024-07-17 07:07:28
Fireeye...	Fire...	2024-07-31 01:53:37
Force...	Vseries	2024-01-29 12:47:05
Force...	Force...	2024-08-11 04:07:41
Giga...	Giga...	2024-02-19 10:50:28
Mcafee...	Mcafee...	2024-08-04 02:03:41
Mcafee...	Mcafee...	2024-08-04 02:07:58
Nexus...	Nexus	2024-08-05 11:33:26
Post...	Post...	2024-08-02 09:00:35
Pulse...	Jun...	2024-07-14 03:57:38

All of the business applications that are currently connected to the SIEM solution are NOT sending data and most probably require a new device type to be created (other than GenericDSM) and appropriate parsing/categorization applied.

Currently, all business applications defined in SIEM are useless and have not provided any logs since initial configuration.
ScienceSoft recommends reviewing the collection protocol issues, restoring events gathering and applying required data normalization.

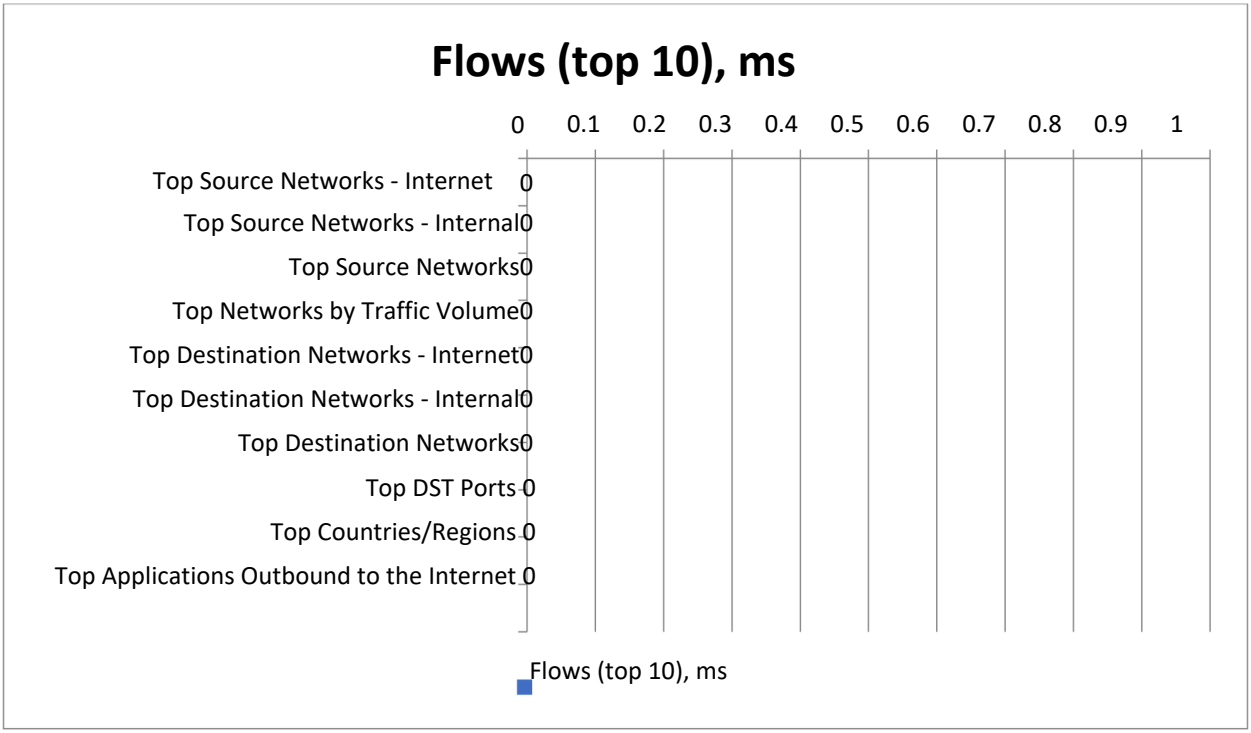
Source Name	Source Type	Last seen
…capacity optimization01	GenericDSM	N/A
…capacity optimization02	GenericDSM	N/A
…DB capacity optimization	GenericDSM	N/A
…DB Vulnerability management	GenericDSM	N/A
…digitalworkplace	GenericDSM	N/A
…capacity optimization01	GenericDSM	N/A
…capacity optimization02	GenericDSM	N/A
…DB capacity optimization	GenericDSM	N/A
…digital workplace	GenericDSM	N/A
…ITSM Vulnerability management	GenericDSM	N/A

Flow Collection Configuration

Flow collection is a valuable source for in-depth inspection of internal network activities. Proper configuration of flow sources is as crucial as event collection. However, due to potential misconfigurations, the system may receive insufficient amount of data.

Managed Host	Managed Host IP	FPM License Limit	Average FPM for 24 h	FPM Utilization, %
QRADAR-HOST-D11	10.10.10.12	200000	2011	1.01
QRADAR-HOST-D21	10.10.12.14	100000	0	0

The data is too limited to yield meaningful statistical insights, system-default flow saved searches are not showing any significant utilization.



ScienceSoft recommends to review NetFlow configuration and potential sources of NetFlow data along with network administrators from the Customer side to resolve this issue.

QRadar Notifications. Auto-Update Error

QRadar notifications are a valuable source of information, which alerts you to maintenance needs. For instance, QRadar is providing error reporting on auto-update issues. Addressing these issues typically requires the manual RPM dependencies resolving.

QRadar solution is an appliance with specific requirement of RPM packages versions for each specific QRadar release. ScienceSoft recommends to resolve all dependency issues for RPM packages very carefully to not affect other solution components.

Date	Package	Description
2024-08-06 18:34:45	DSM-AlibabaActionTrail-7.5-20240417095430.noarch.rpm	PROTOCOL-AlibabaCloudObjectStorageService-7.5-20230922062508.noarch.rpm is not scheduled to install
2024-08-06 18:17:23	DSM-AWSConfig-7.57.5	PROTOCOL-AmazonAWSRESTAPI doesn't exist in AU package
2024-08-06 18:16:05	AlibabaCloudObjectStorageService-7.5-20230922062508.noarch.rpm	PROTOCOL-AmazonAWSRESTAPI doesn't exist in AU package

QRadar Notifications. Network Adapter Error

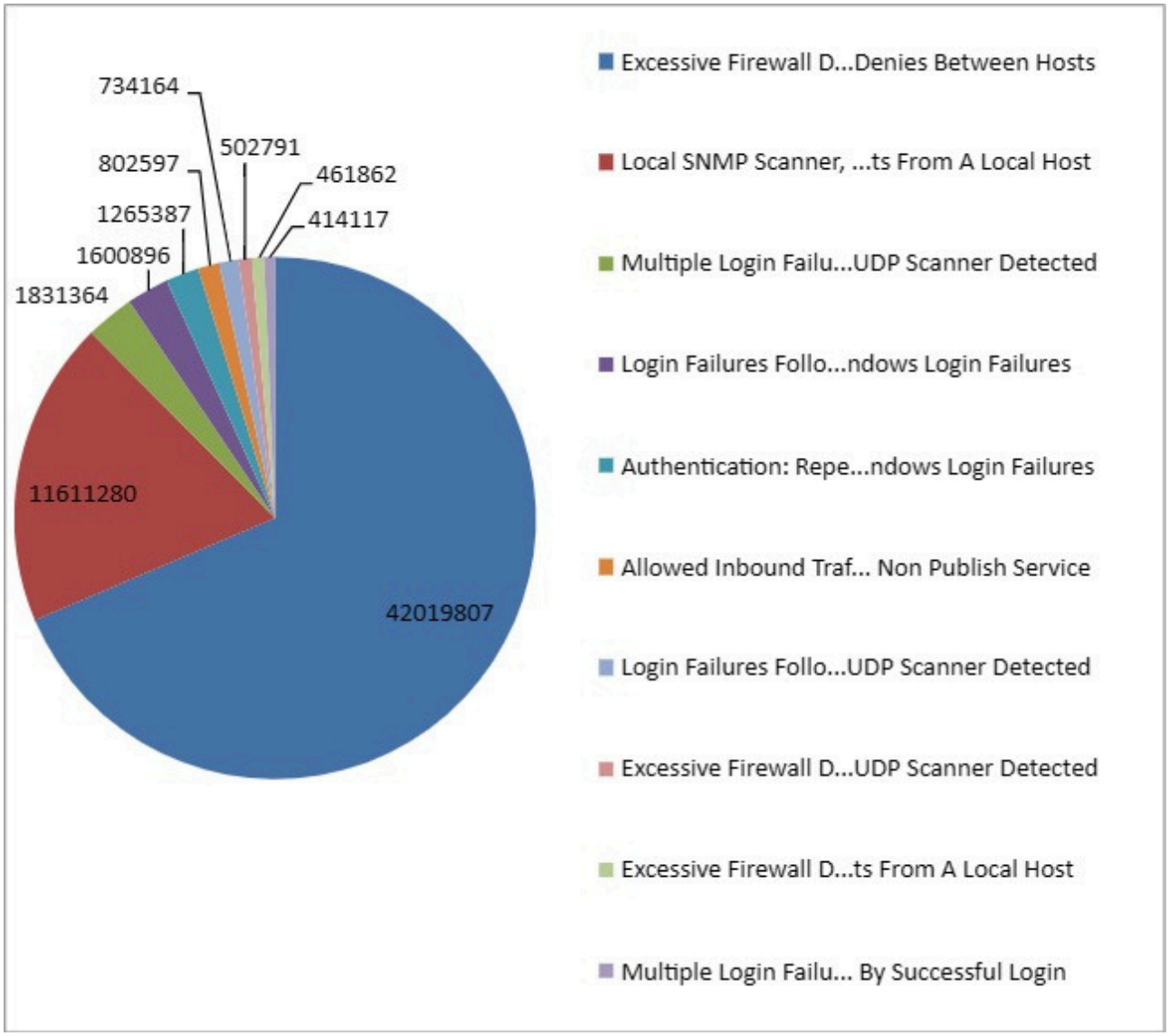
Another alert that requires maintenance pertains to the network adapter. This issue might be related to the current problems with flow collection.

IP Address	Date	Description
10.10.10.11	2024-08-12 09:56:37.169	Receive frame errors on interface eno3 on 10.10.10.11

ScienceSoft recommends to review SIEM solution hardware components status and platform logs to investigate and resolve the issue.

Building Blocks Tuning

High count of events triggered by rules is related to scanner operations. This issue shows that QRadar strongly requires building block tuning and changes in reference sets and assets to exclude scanners from correlation, if they exist in the network.



ScienceSoft recommends to update related system BBs to reduce the number of potential false positives.

Device Type Category Coverage

Several log source types are discovered to have insufficient event variety to cover auditing of main functionality of the device (e.g. SIEM is getting *Login Success* events, but not getting *Login Failure*). To increase coverage, it is necessary to reconfigure auditing on the devices.

Below is the list of sources with the worst event coverage.

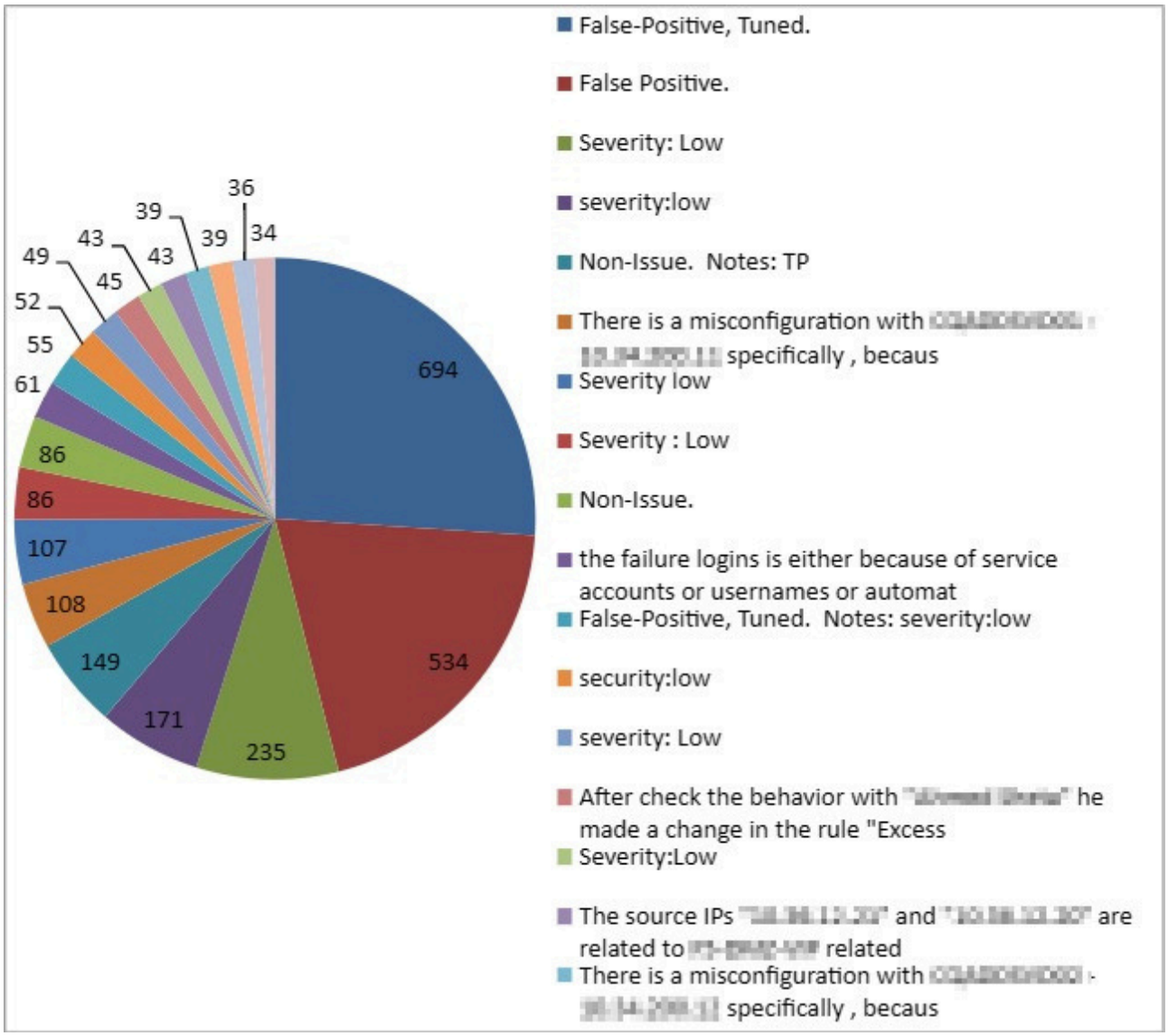
Device Type	Coverage, %
Blue...	57%
F5ASM	33%
LinuxDHCP	26%
Nexus	7%
NetScreenFirewall	2%

ScienceSoft recommends to increase this coverage by reviewing and reconfiguring auditing on each specific device type.

Offense Review

The reasons for closing offenses are currently unstructured and need to be refined to enhance visibility into SOC actual performance and KPIs.

ScienceSoft team of security professionals is happy to offer a detailed overview of best practices and a training for processing and analyzing QRadar offenses.



Generic events

Deployment has 15 high-load sources that have not been auto-discovered, and all the log data from these systems is NOT parsed/categorized, being completely useless for security monitoring and consuming EPS licenses with no actual benefits. These sources need reconfiguration to ensure they receive meaningful data and process it properly.

IP Address	Events in 24h
10.14.10.42	3057722
10.22.10.67	331990
10.24.23.17	175875
10.24.23.108	26517
10.14.65.42	25159
10.10.71.42	22820
10.24.95.12	18216
10.22.10.53	17803
10.24.37.5	17265
10.24.37.4	17263
10.24.97.10	10857
10.10.10.134	7969
10.15.110.4	7871
10.10.10.203	7711
10.14.11.3	7479

Additional Fine-Tuning

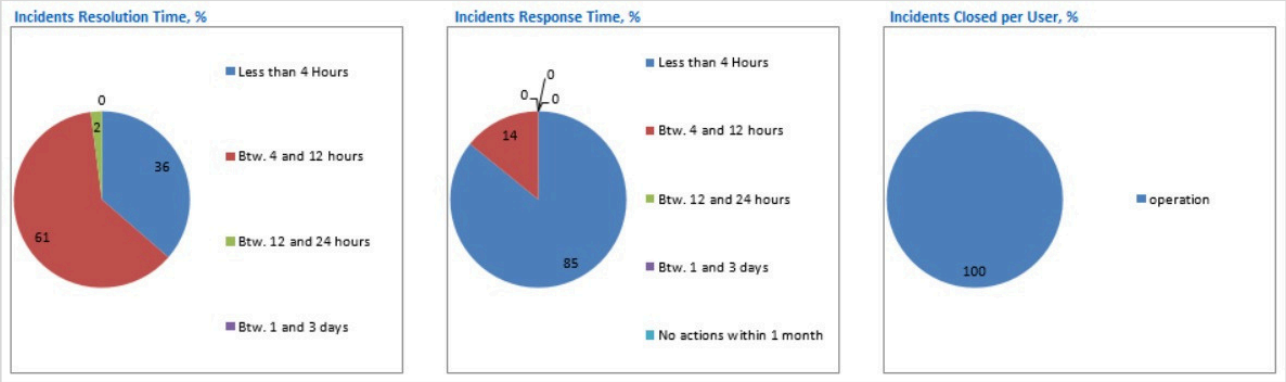
The activities mentioned earlier will lead to a surge of new events once the fixes are applied. This will necessitate additional measures to address potential issues related to data quality, correlation, and system health.

ScienceSoft recommends to perform deep solution Fine Tuning after all the major log source types are connected. This will allow to get rid of false-positives after new massive data addition.

Non-Critical Issues

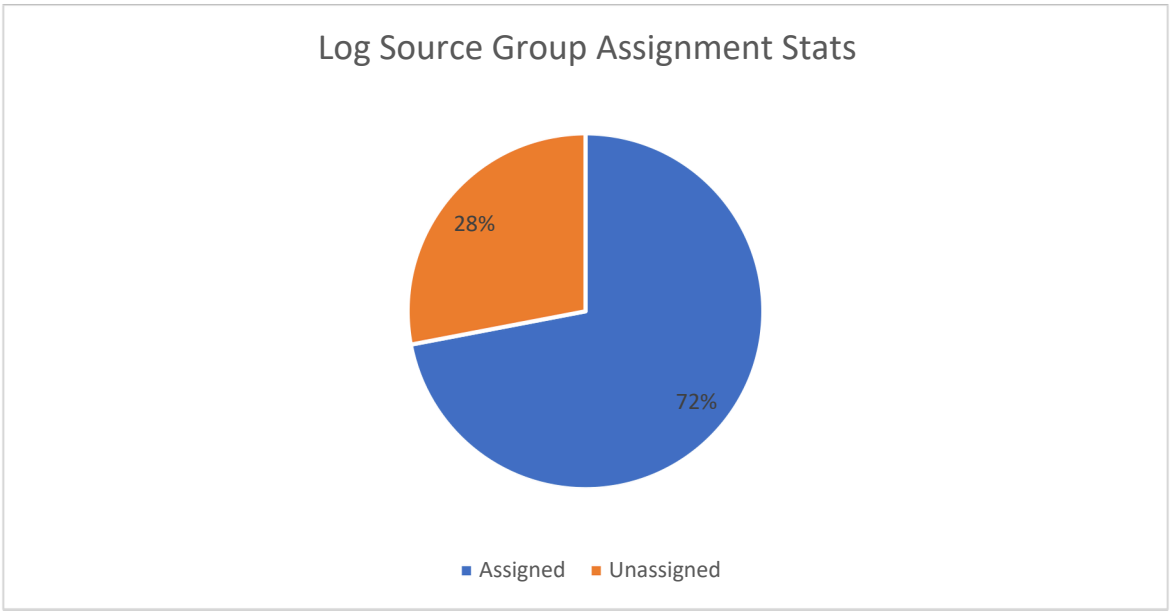
Incident Response

The incident response time is quite low, which is excellent. However, only one user is handling incident response, and it is possible that multiple users are sharing the same account. It is not advisable to use a single account among multiple users.



Log Source Grouping

To improve visibility, it is essential to group every log source. Currently, out of 675 connected log sources, 289 remain ungrouped.



Conclusion

ScienceSoft recommends at least **Critical** and **Medium** items to be resolved as soon as possible, those issues are preventing system to operate properly and cause inability to cover most critical correlation scenarios because of missing log data from particular types of the systems (Authentication/AD and DNS mostly).