QLEAN

www.scnsoft.com

IMPROVING OPERABILITY & PERFORMANCE OF SIEM SOLUTIONS:

QLEAN FOR IBM SECURITY QRADAR® SIEM

5900 S. Lake Forest Drive, Suite 300, McKinney, TX , +1 214 306 68 37, contact@scnsoft.com

EXECUTIVE SUMMARY

SIEM adoption is growing, prompted by evolving threats and compliance policies. To stay on top of dynamic environments in which they operate, CISOs must ensure high operability and performance of their SIEM deployments. Routinely, however, security operations teams face complex system maintenance, data quality issues and inefficiencies in the performance of rules and reports, to name just a few challenges.

Focusing on the market leader, IBM Security QRadar SIEM, this white paper introduces a new automated health monitoring tool that improves the situation. Used by some of the world's leading financial and professional services organizations, *QLean* for *IBM® Security QRadar® SIEM (aka Health Check Framework for QRadar)*, offers over 50 operational metrics and 25 Health Markers for dynamic, automated health assessment. The white paper explains how QLean makes maintenance significantly easier, helps to improve data quality and enables operation teams to troubleshoot multiple performance issues.

The white paper targets Information Security executives, SOC and compliance managers.

ON THE ESSENTIAL SIEM HYGIENE

> *"Measuring SIEM health and operations is still an emerging art."*
> *Anton Chuvakin, Research VP at Gartner's GTP Security and Risk Management Group*

Security Information and Event Management (SIEM) is a growing area of Information Security Technology. In the latest Gartner Magic Quadrant report the SIEM market of $1.6 billion was estimated to grow by further 12.4% in 2015 after an 11% increase a year before (the figures driven by the technology's innovative leap as well as its role in compliance reporting for such industries as Public Sector, Financial Services, Healthcare, Retail, Telecommunications and Energy).

As SIEM systems have evolved into powerful security intelligence platforms, there is a growing urge for organizations to maximize the return on their considerable investments into SIEM solutions. That is, getting the most of their SIEM system's operability and performance while keeping the *costs*, *time* and *resources* required for the operation and maintenance stages reasonably down.

SIEM system is at the core of an SOC infrastructure, and its 'health' becomes a key priority. If overlooked, operability and performance issues can affect the system, increasing the possibility of incidents that could compromise an organization's information security and thus expose it to higher risks of breaches. Maximization of operability and performance is subject to ongoing *health monitoring* accompanied by skillful *fine-tuning* and *re-configuration*, and there are a number of pitfalls to it:

COMPLEX AND COSTLY MAINTENANCE

INFERIOR DATA QUALITY

POOR PERFORMANCE

PITFALL 1: COMPLEX AND COSTLY MAINTENANCE

- Constantly evolving security threats
- Misconfigured, unidentified or irrelevant log sources
- Misconfigured custom correlation rules that need to be fine-tuned

PITFALL 2: INFERIOR DATA QUALITY

- Logs that contain incomplete data
- Logs that were not normalized and categorized

PITFALL 3: POOR PERFORMANCE

- Error-prone performance under high loads (e.g. 30,000+ security events per second)
- Time-inefficient reporting and correlation rules execution

The **lack of automation** to monitor the operability and performance of a SIEM deployment makes minimization of resource consumption and timely troubleshooting nearly impossible. This ultimately drives the system's total cost of ownership up and the ROI down. Until recently, the only way for organizations to automate health monitoring as opposed to doing so manually was to create custom add-ons – something that would make their SIEM budget grow beyond its already large figure.

To help organizations increase the ROI from a SIEM deployment by keeping it at its most effective at all times, we introduce **QLean** for *IBM Security QRadar SIEM*, which is now available under a commercial license.

QLEAN: RESPONDING TO THE URGE

MAINTENANCE

QLean is an automated, off-the-shelf tool that helps organizations increase the return on their *IBM Security QRadar SIEM* investments. With **over 50 metrics** and **25 Health Markers**, *QLean* provides all-round visibility into statistical, performance and behavioral parameters of a QRadar environment at any given moment.

Fig. 1 shows an example of the *QLean*'s dashboard that places two of its many metrics on top – *Top 10 Most Risky Assets* and *Top 10 Unique Offenses*. These metrics provide a dynamic view of the system performance and enable stakeholders to respond to asset issues and threatening offense landscapes in close to real time. The tab in the right part of the screen contains categories that encompass all the 60 metrics and make navigation through them quick and easy.

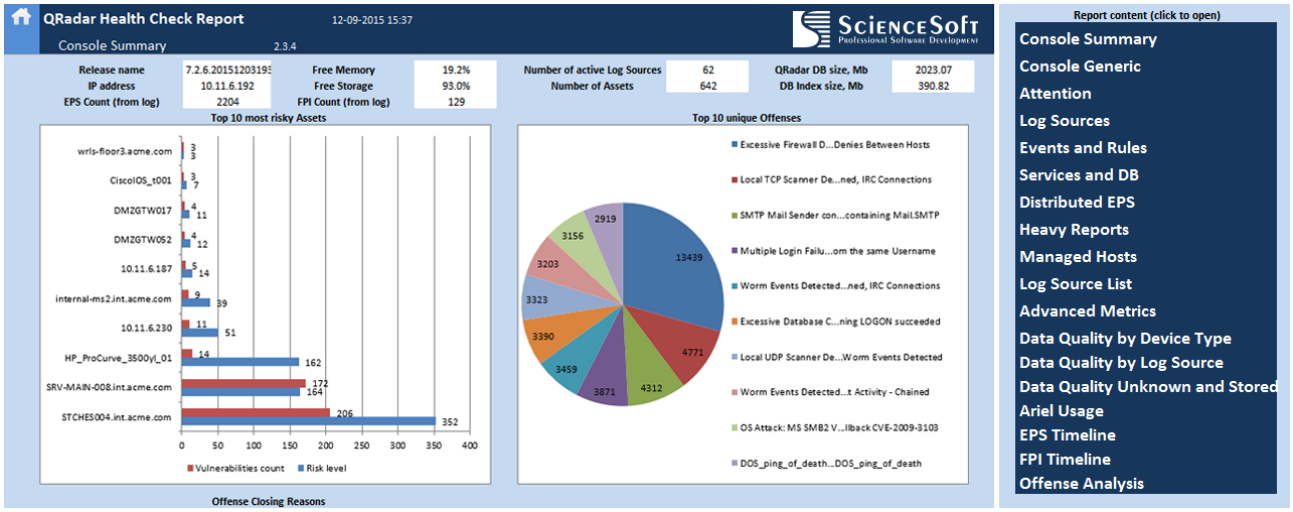

Fig. 1 – A sample QLean Health Check report

As an off-the-shelf product, *QLean* can either reduce or completely eliminate the necessity to create *custom* scripts and reporting tools, with *less time*, *budget* and *resources* required to secure the QRadar operability continuously.

Through its extensive functionality, the tool touches upon the responsibility areas of SOC engineers and analysts, system administrators, compliance managers and business owners.

HIGHER EFFICIENCY, LOWER TCO WITH QLEAN

- Easier maintenance
- Better control of deployments
- Minimized risks of security incidents that result from the system faults
- Improved data quality
- Predictably stable performance
- Preventive, not reactive security intelligence

Section *WHAT'S IN: MITIGATING THREATS WITH ADVANCED ANALYTICS* provides further details on the maintenance aspect of QLean.

DATA INTEGRITY

QLean helps to improve data quality and minimize risks of missing log data despite high loads of the system. Its *Data Quality Framework* evaluates the incoming log data and identifies:

- log sources that need further configuration of their audit settings;
- misconfigured sources that were not automatically identified by the system and go to SIM Generic Log DSM;
- maliciously or otherwise turned-off and misconfigured log sources for a timely restoration of data inflow;
- 'idle' sources that haven't been generating security events for a specified period; • damage to the Ariel database of events and flows.

IMPROVED PERFORMANCE, SIMPLIFIED FINE-TUNING

The following instruments of the QLean functionality assist in fine-tuning and configuration for better performance and reporting:

- *Offense Analysis* revisits registered offenses for a quick identification of correlation rules that need fine-tuning by the new type of reporting based on the correlation rule triggering frequency and the number of affected threat sources.
- *Heavy Reports* identifies the reports that take the longest time to be generated.
- *Events and Rules* evaluates how fast correlation rules are executed, how long it takes for the system to respond to them, how many responses are there per correlation rule. SOC operators can thus optimize the rules consuming the most resources.

WHAT'S IN: MITIGATING THREATS WITH ADVANCED ANALYTICS

QLean minimizes the risk of missing a critical issue within a QRadar solution. With its relevant selection of Health Markers, it alerts to detected issues and offers recommendations for their resolution in each case. An integral, comprehensive health check report further helps to decide on the steps to be taken to recover the full operability of the system, offering an exhaustive description of the identified problems.

What's in a health check report?

Each report generated by QLean contains details of the analyzed QRadar environment(s), including but not limited to the following metrics:

- EPS and FPI statistics tied to applied licenses for all the processors
- Disk, CPU and memory usage on managed hosts
- Log Sources details and recent changes
- Incoming log data quality
- Real inbound Events and Flows timelines for all the processors
- Ariel DB usage statistics for all the processors
- Correlation rules and reports performance
- Console summary
- System warning and errors and more

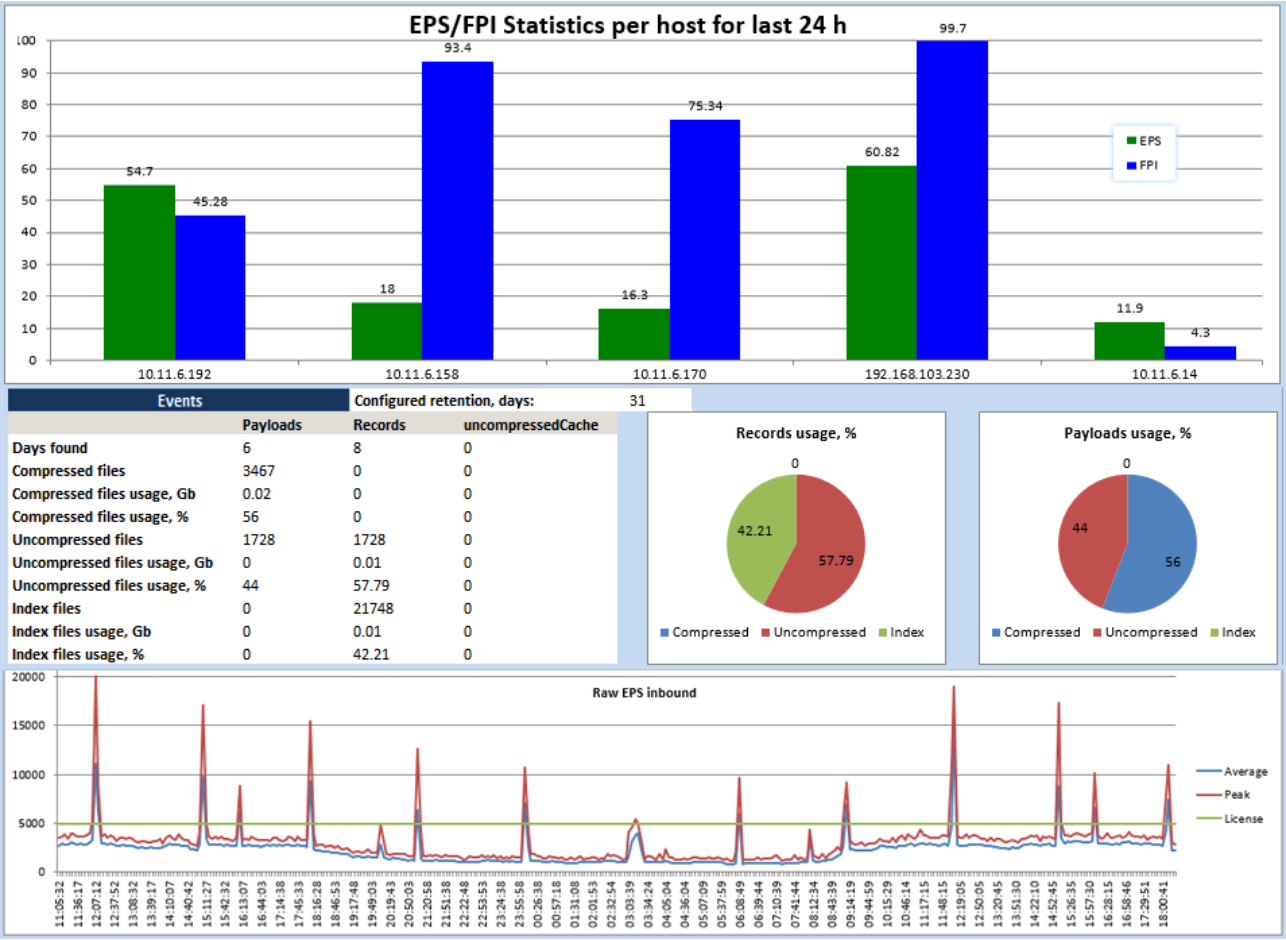

Fig. 2 – Sample analytic dashboards, QLean

What are Health Markers?

QLean summarizes the status of all the important QRadar metrics in the form of 25 OK/Failed Health Markers that are sent in a detailed notification email. In case a marker shows *Failed*, *QLean* subscribers receive an automatic warning with the description and basic recommendations for fixing the issue.

The Health Markers represent a holistic view of the system performance according to the manually specified threshold values that can be configured to fit particular environment requirements. The markers provide a quick snapshot of the system, highlighting such important information as

- availability of all the system components, including cluster elements
- excessive time of correlation rule execution
- excessive amount of security events that are uncategorized or come from unspecified sources and more

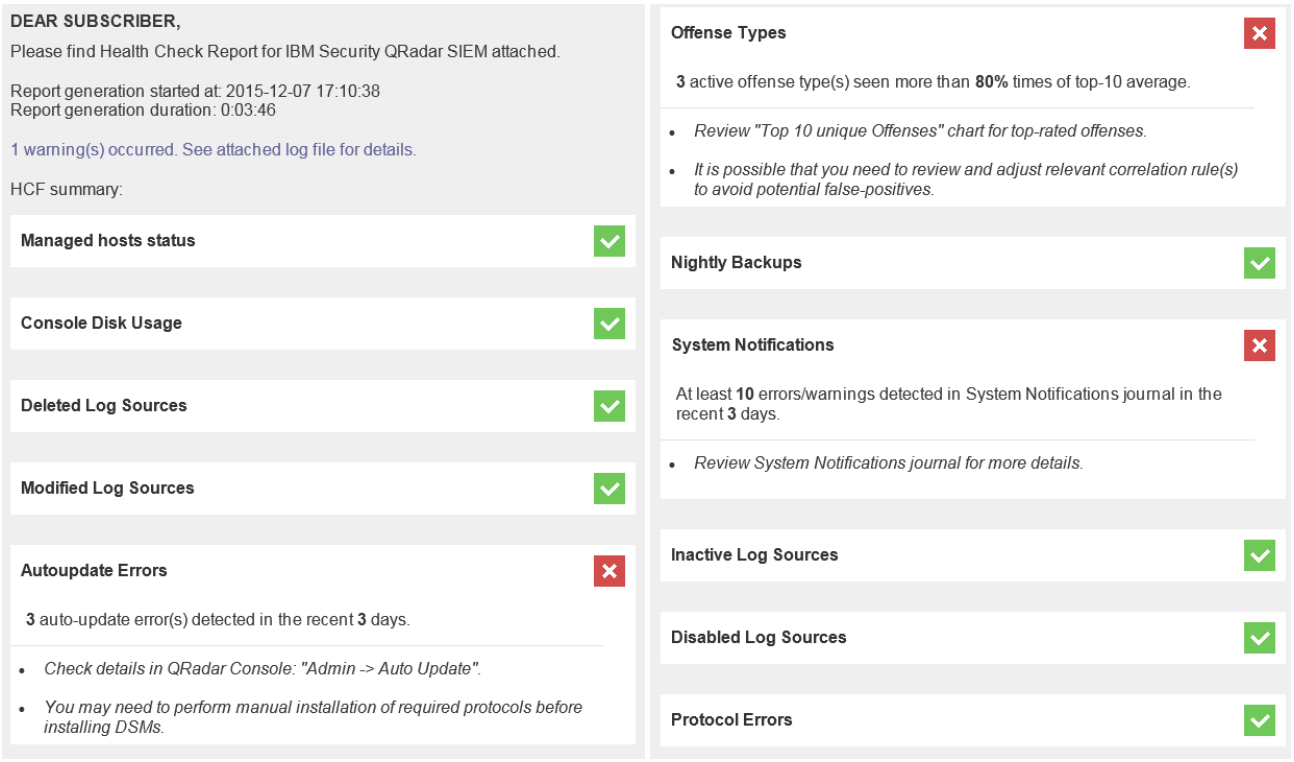

Fig. 3 – A sample QLean notification email containing Health Markers

To download **your free demo**, please follow the link.

CONCLUSION

Deployment of a SIEM platform is a strategic decision that takes considerable in-house resources to continuously monitor and sustain the platform's operability. The lack of automation for performing such tasks poses challenges to SOC managers as it raises the solution's total cost of ownership and reduces the return on SIEM investments.

ScienceSoft's *QLean* for *IBM Security QRadar SIEM* deployments bridges the automation gap in SIEM health monitoring. Through its advanced operational analytics, *QLean* enables proactive security intelligence with easier maintenance, improved data quality and stable, error-free performance of *QRadar* deployments, which spares organizations time, budget and resources required for high-level maintenance.

With its 50+ statistical, performance and behavioral metrics and 25 Health Markers for a quick audit of QRadar operability, the tool offers an all-round view of an organization's SIEM environment at any given moment, alerting system users to operational inconsistencies and data losses as well as helping to fix them with apt recommendations.

To learn more about enterprise solutions in Information Security or to get a personalized information on *QLean* for your business, please contact our SIEM Department consultants at contact@scnsoft.com.

ABOUT SCIENCESOFT

ScienceSoft, an established IT services provider with operations in North America, Western and Eastern Europe and South-Eastern Asia, has been working in Security Intelligence since 2006. We have expertise in SIEM solutions development, testing, implementation and consulting for enterprises in Public Sector, Financial Services, Healthcare and Retail, among other industries. One of IBM Advanced Partners, ScienceSoft holds a Silver Accreditation in IBM Security QRadar SIEM. Our certified QRadar consultants carry out assessments, deployments, testing and maintenance of SIEM solutions. Since 2011, they have been involved in QRadar and TSIEM implementations in the US, Europe, Middle East and Africa.

With 450 experienced professionals and over 28 years of IT business experience, ScienceSoft is a recognized partner of IBM, Microsoft and Oracle. Our business achievements are recognized by prestigious awards, including a national 2014 Fastest-growing company award by Ernst & Young (EY).