QRadar SIEM Health Check Services

Many SIEM deployments, while serving a good cause, do not realize the full value of a SIEM solution for the customer and fail to address Advanced Targeted Threats.

Most typical issues with SIEM deployments include misconfiguration of the SIEM system; missing critical log sources of vulnerable business applications and other assets not supported out-of-the box; incorrect audit settings for connected devices that lead to missed security context; lack of correlation rules that address the right type of assets and/or the business context.

As a result, many potential security threats relevant to customer's business pass unnoticed. This does not help mitigate security risks and leaves the SIEM ROI below its potential level.

ScienceSoft helps address SIEM deployment issues and identify ways to increase QRadar SIEM ROI by carrying out a Health Check of existing deployments.

The Health Check includes:

- Assessment of QRadar SIEM configuration against best practices for various platforms
- Review of the coverage of network assets and business applications by QRadar SIEM
- Implementation of audit configuration best practices for various platforms
- Review of implemented threat cases and correlation rules for the customer environment
- Fine-tuning of the solution (enhance data quality, decrease false positives)
- Quick troubleshooting and performance improvement recommendations
- A written report of the Health Check results and recommendations for improvement

When configured and fine-tuned properly, QRadar correlation rules allow minimizing the possibility of Advanced Targeted Threats to be missed by security professionals.

QRadar SIEM will help its users to identify high-risk threats with near real-time correlation and behavioral anomaly detection, detect vulnerabilities and high-priority incidents among billions of data points and gain full visibility into network, application and user activity.

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

A standard Health Check procedure can be performed onsite as well as offsite.
Some of the steps following the Health Check may include (as a separate contract):

- Threat cases design and correlation rules implementation for the specific customer environment
- Custom DSM development for business systems or network assets
- Automation solutions design and and development of automation tools
- Security monitoring services
- Yearly support for any kind of security services (fixed number of hours can be used for any related task)
- Onsite or remote trainings for security specialists working with QRadar SIEM

About ScienceSoft

ScienceSoft is an international IT consulting company with HQ in McKinney, TX, EU offices in Finland, Lithuania, Latvia and Poland, and Gulf office in UAE. With more than 770 employees and 35 years in business, we bring custom and platform-based solutions to large and midsize companies in Government, Retail, Manufacturing, Telecom, Healthcare, Banking, Oil, Education, and other industries. ScienceSoft has the right experience, skillset and commitment and is perfectly suited to successfully launch and lay the foundation for a successful project completion. In the area of Security Intelligence, we bring 16 years of expertise in SIEM/SOAR solutions development, testing, implementation, and consulting. ScienceSoft was involved in the development IBM's TSIEM/TSOM in 2006-2011. More recently (2011 – 2022) ScienceSoft has become one of IBM's leading implementation partners for the QRadar Security Intelligence platform. Our certified QRadar consultants carry out assessments, deployments, testing and maintenance of SIEM and SOAR solutions.

ScienceSoft consultants have are all mandatory technical skills that might be required for any kind of consulting and development, including:

- Deep information security background
- Hands-on experience with the leading security solutions
- Software Development (Python, JavaScript, SQL, Shell&Batch, Regex, other)
- System administration (Linux, UNIX, Windows, VMware ESXi)
- Network and networking devices troubleshooting
- SIEM/SOAR deployment, upgrade, and fine-tuning
- SIEM customization (custom DSMs, reports, threat cases and correlation rules, automated integration solutions, AQL queries, etc.)
- SOAR customization (playbooks planning, design and development, workflow implementation, automation, custom functions, etc.)
- Proven expertise (participated in creation of several IBM QRadar SIEM certification exams as invited experts: C2150-195 and C2150-214)

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

Over the past 15 years, ScienceSoft has built solid expertise with IBM TSIEM, IBM TSOM, IBM QRadar and IBM Resilient solutions. ScienceSoft has performed more than 100+ SIEM and SOAR implementations and fine-tuning projects worldwide for the customers of banking, finance, government, oil and telecom industry sectors.

ScienceSoft SIEM team have implemented more than 20 unique extensions (free and paid) for QRadar functionality, including:

- QLEAN: formerly known as “Health Check Framework”; allows to perform periodical monitoring of a range of statistical, performance and behavioral metrics of a live IBM QRadar SIEM deployment (including distributed environments)
- QWAD: automated WinCollect agents deployment solution with auto-configuration for different log source types
- QIN: extended notification solution that allows to sent SMS, create tickets in Jira, alert through Teams, and included many other offense notification options; can also automatically assign offenses to specific persons
- QMEA: MS Exchange Admin and Mailbox Audit export via Syslog
- QArtifact: Enables analysts to attach evidence (artifacts) such as files, images, URLs to offenses
- QEXEQ: Executive QRadar SOC reporting app

ScienceSoft applications are available at:

https://exchange.xforce.ibmcloud.com/hub/?q=sciencesoft

https://qlean.io/#appsuite

Our team will work with you hand in hand to ensure that all expectations are not just met but exceeded. We will be available every day, all the way, and provide all the tools and guidance for the implementation of your project.

For more information, please 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