ScienceSoft
Professional Software Development

QRadar SIEM Threat Cases Design and Implementation Service

Many SIEM deployments, while serving a good cause, fail to realize the full value of a SIEM solution for the customer. Common issues with SIEM deployments include the misconfiguration of the SIEM system, unconnected log sources from vulnerable business applications and other assets that are not supported out-of-the-box, and a lack of correlation rules that address the right types of assets and/or business context. As a result, many potential security threats relevant to the customer's business often go undetected. This situation does not help in mitigating security risks and keeps the SIEM return on investment (ROI) below its potential.

ScienceSoft assists in addressing these SIEM deployment issues and identifies ways to enhance the ROI of QRadar SIEM by designing and implementing customer-specific Threat Cases through QRadar correlation rules. ScienceSoft Threat Case offering includes:

- Customer infrastructure investigation
- Identification of most business-critical assets
- Clarification for allowed information flow directions for each logical unit
- Identification and recommendations for critical unsupported log sources
- Communicating with asset business owner and creating ACLs (may require additional development to extract information from user repository)
- Recommending threat cases using our common and specific best practices
- Designing threat cases specific for particular environment when necessary
- Implementing threat cases with QRadar correlation rules
- Documenting design and implementation details for further possible reenablement

ScienceSoft has a lot of best practices and appropriate Threat Cases, including both general for network assets and business-specific for different economic sectors. Here are several samples of banking-related best practices and Threat Cases:

- Transactions from the card account with the IP of the country other than the country of the issuing bank
- Transaction from the account for 3 or more different bank accounts at the same time (assuming the existence of a "white list" of current accounts contractors, government funds, tax inspections, etc.)

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 short-time transaction to three or more bank accounts with the same amount
- Debiting funds from account at unusual time (e.g. midnight) above a certain limit
- Bank employee activity in non-working hours
- “Username – UserID” pair change for a bank employee
- Large amount transaction initiated by Call Center operator
- Call Center operator sending access details to the unregistered number

The duration of the Threat Cases implementation procedure depends on several factors, including the number of infrastructure elements that need to be covered, the number of event types available, and log data quality and availability (depending on auditing settings). This implementation can be carried out either onsite or offsite, provided that a VPN connection is enabled and consultation with a customer representative is available.

Some of the preceding steps prior to Threat Cases implementation may include:

- LSX/uDSM development for any information system or network asset, including supporting documentation
- Related automation and development of automation tools
- QRadar SIEM Health Check
- Onsite or remote trainings for security specialists working with QRadar SIEM

About ScienceSoft

ScienceSoft, founded in 1989, employs approximately 800 IT professionals across its global offices. With almost two decades of expertise in the SIEM/SOAR/SOC space, we specialize in the development, testing, implementation, and consulting of SIEM solutions (QRadar, Microsoft Sentinel, Splunk, Palo Alto Cortex XSOAR, Sumo Logic).

ScienceSoft was actively involved in the development of IBM's TSIEM/TSOM from 2006 to 2011. More recently, the company has established itself as one of the leading SIEM implementation experts: https://www.scnsoft.com/security/siem

Our certified QRadar consultants conduct assessments, deployments, testing, and maintenance of SIEM solutions worldwide. Since 2011, our consultants have been engaged in numerous QRadar and TSIEM implementation projects across Europe, the United States, the Middle East, and Africa.

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