ScienceSoft SOC Services

Security Operations Centers (SOCs) are responsible for detecting and responding to cyberattacks. The role of a SOC is to limit the damage to an organization by detecting and responding to cyberattacks that successfully bypass your preventative security controls. ScienceSoft team has assisted clients around the globe in establishing and tuning the SOC operations, including but not limited to the examples below:

US Government Agency, South Carolina

- **Duration:** 6 months onsite, 4 months remote
- **Our team:** 3 senior consultants
- **Tasks:** Consolidation of multiple (10+) legacy SIEM platforms into centralized solution, assisting with HW preparation, SW installation and patching, onsite assistance with racking and cabling of new HW in agencies, migrating security content from legacy systems, customized hardware-level IDS solution integration for network traffic analysis for all agencies (incl. iptables customization), reconfiguring existing and adding new security solutions for logging to centralized SIEM, HA configuration for critical SOC infrastructure elements, baselining audit requirements for multiple platforms (Linux, Windows, Cisco, Palo Alto, F5, Barracuda, etc.), implementing and validating different monitoring levels (with different audit requirements) for specific agencies, interviewing new potential team members, new SOC personnel trainings, video-wall SOC dashboards development, creating various SOC documentation templates, solution tuning and troubleshooting, SOC reporting, knowledge transfer sessions. **Custom software development**: automated Windows agents deployment and logs discovery tool, SIEM components mass upgrade script, log sources mass renaming and removal automation tools, customized parsing and mapping for over 50 types of custom/unsupported log types, incoming data quality analysis tool, various SOC automation tools.

National Bank, Middle East

- **Duration:** 4 months
- **Our team:** 1 senior consultant
- **Tasks:** Security monitoring infrastructure implementation from scratch, geo-distributed HA SIEM solution deployment and configuration, assisting with audit policies planning and implementation on various security devices, assisting with establishing security, threat monitoring/analysis and alerting policies, development and integration of threat cases and corresponding correlation logic, SOC dashboards development (incl. dashboards for stakeholders), automating various aspects of SOC operation, customer personnel trainings.

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

Telecom Operator, Europe

- **Duration:** 6 months
- **Our team:** 1 senior consultant
- **Tasks:** Multi-domain distributed MSSP infrastructure and extensible architecture planning and establishment, developing a client-based correlation rules framework that can be easily applied on per-domain basis, applying resource consumption limits per tenant, SAP/ERP and telecom equipment connecting using custom collector scripts and parsers, integrating SAP with ticketing system for alerting purpose, customer personnel training, assisting with MSSP clients onboarding and troubleshooting, performance analysis and troubleshooting.

Managed Security Services Provider, Japan

- **Duration:** 3 months
- **Our team:** 1 senior consultant
- **Tasks:** Initial SOC architecture design, SOC documentation, providing documented audit configuration recommendations and baselines, SIEM solution implementation in Cloud (Amazon), configuration for cross-AWS/production networks, SIEM customization, MSSP clients onboarding documentation preparation, assisting with clients onboarding, implementing parsing and categorization for unsupported devices, assisting with SentinelOne EDR deployment in client's networks and SIEM integration, fundamental security analysts training for L1 team, implementing sandbox environment for personnel training and SOC testing, responsibility matrix for external and internal teams, assistance with solving organizational issues, integrating customer in-house developed hardware security solution with SOC/clients networks, L3 support.

US Community Healthcare Network, California

- **Duration:** ongoing (3.5 years)
- **Our team:** 2 senior consultants
- **Tasks:** SOC L3 support, SIEM solution support and maintenance, security content and data migration, SIEM troubleshooting, optimization and tuning, TI feeds configuration, one-day vulnerabilities monitoring implementation, threat cases design and implementation, complex cyber-security offenses diagnosis, custom security software and tools development, SOC operations automation, extensive periodical reporting for SOC status, collaborating with client personnel tightly, participating in SW/HW provisioning and decommission processes.

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
www.qlean.io