SOCaaS

SOCaaS is a combination of a security operations center, a facility that houses an information security team responsible for ongoing monitoring and analyzation of an organization's cybersecurity, and security information event management or SIEM. SIEM is software used by the SOC team that aggregates, analyzes and collects security data from network devices, such as firewalls, servers, routers, switches, wireless access points, O365, and much more.

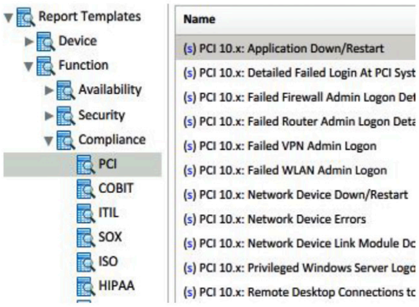
Security operations centers are staffed with Tier 1 SOC analysts, Advanced Security Engineers, Threat Hunters and Threat Intelligence Managers. SOC staff are experts who monitor all the data gathered by SIEM that is used to alert our customer in real-time when abnormal or malicious behavior is detected anywhere in their network.

SIEM is designed to provide organizations real-time analysis of security alerts generated by applications and network hardware without any of the headache or capital investment. The offering is a comprehensive SIEM solution, fully hosted in a secure and compliant cloud to manage and monitor your critical systems regardless of where they may be.

Segra's SIEM solution enables organizations to gain all the benefits of the world's most powerful and flexible SIEM without the hardware or personnel investment for deployment, management, or maintenance of the system. Segra takes care of all the infrastructure, maintenance, upgrades, patches, capacity planning, backups, and security of the system and platform.

FEATURES

- Real-time alerting
- Security and compliance out-of-the-box
- Cloud scale architecture
- Self-Learning Asset Inventory (CMDB)
- Exhaustive device support
- Event source monitoring
- Network, virtualization, and application intelligence
- Identity and location intelligence
- Configuration and configuration change monitoring
- Database security, availability, and anomalous activity monitoring
- Real-time and historical cross-correlation
- Prioritized security incidents with correlated and raw details
- Dynamic dashboards, topology maps, and notifications
- Compliance and standards-based reports
- Compliance automation
- Log management
- Machine Learning



- Report Templates
  - Device
  - Function
    - Availability
    - Security
    - Compliance
      - PCI
      - COBIT
      - ITIL
      - SOX
      - ISO
      - HIPAA

Name
(s) PCI 10.x: Application Down/Restart
(s) PCI 10.x: Detailed Failed Login At PCI Syst
(s) PCI 10.x: Failed Firewall Admin Logon Det
(s) PCI 10.x: Failed Router Admin Logon Deta
(s) PCI 10.x: Failed VPN Admin Logon
(s) PCI 10.x: Failed WLAN Admin Logon
(s) PCI 10.x: Network Device Down/Restart
(s) PCI 10.x: Network Device Errors
(s) PCI 10.x: Network Device Link Module Dc
(s) PCI 10.x: Privileged Windows Server Logo
(s) PCI 10.x: Remote Desktop Connections tc

DISCLAIMER: All information in this proposal is proprietary and is not for general distribution without express permission from Segra.