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.

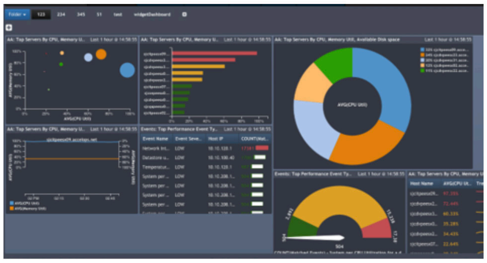
Security operations centers are staffed with Tier 1 SOC analysts, Advanced Security Engineers, Threat Hunters and Threat Intelligence Managers. SOC staff are experts who monitor all the data gathered by SIEM that is used to alert our customer in real-time when abnormal or malicious behavior is detected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

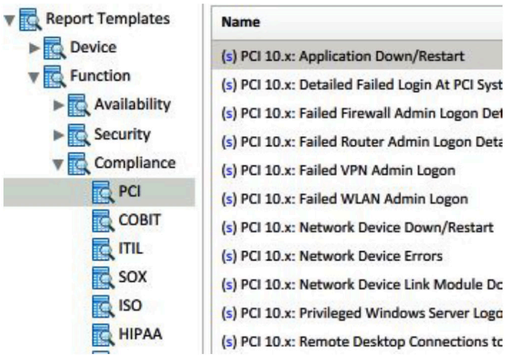
SIEM is designed to provide organizations real-time analysis of security alerts generated by applications and network hardware without any of the headache or capital investment. The offering is a comprehensive SIEM solution, fully hosted in a secure and compliant cloud to manage and monitor your critical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

SOCaaS

Today's cyberattacks are more advanced than ever before, and the old preventative tactics of simply using firewalls and antivirus software are outdated. Attacks are no longer stopped simply by edge devices blocking incoming attacks from the cloud, as attacks can come from inside your network. Malware is now attached in emails, banner ads, pseudo websites, etc., and can gain access to your network through an internal device. Intrusion detection and prevention systems (IDS/IPS) alone won't be able to detect or prevent malware like this.

Most organizations lack the technology or personnel to even detect these emerging cybersecurity threats. Studies show the average time between a data breach and discovery is 205 days – that's over 7 months! Simply implementing security tools such as firewalls or anti-virus isn't enough. This is even more true for organizations that fall under PCI, HIPAA, or FFIEC regulations. For those companies, compliance is absolutely critical to avoid fines or worse consequences.

Today's threats and compliance guidelines require organizations of all sizes to collect, correlate, and analyze security information from all IT systems to enable rapid detection and remediation. Our comprehensive cybersecurity monitoring and compliance solution solves this need by providing continuous monitoring of your entire network to detect and respond to hidden cybersecurity threats.

One of the biggest decisions companies are faced with is whether or not to build, deploy and maintain an in-house security operations center. Companies will quickly come to the understanding that outsourcing this service will not only benefit them in cost savings, but also simplify the need for expertise, ongoing resources and future exposure possibilities.

KEY COMPONENTS

- Network Firewall
- SIEM
- Multiple Security Analyst
- 24/7/365 Support

FORCED REGULATORY COMPLIANCE

- Retail - PCI
- Healthcare - HIPAA
- Financial - FFIEC

OTHER REGULATORY COMPLIANCE

- GLBA
- SOX
- NIST
- ISO

	SEGRA	DIY
COST	Predictable and Economical	Unpredictable and cost prohibitive for small to mid-size with no/limited security staff
STAFFING	Fully managed by Segra	Entire responsibility of recruitment, training, and retention rests with the organization
DEPLOYMENT	Turnkey	Months to potentially years for full deployment
RESILIENCY	Cloud-based design to ensure enterprise-grade service reliability	All factors that could contribute to downtime must be identified and accommodated by the organization
TECHNOLOGY EVOLUTION	Fully Managed by Segra/3rd Party with new features and upgrades offered to all customers following testing and implementation	Timing and frequency dependent on organization's planning, budgeting, and implementation efficacy