Volta

voltainc.com | 888.479.9672 | hello@voltainc.com

SOC as a Service

Reduce the complexity and cost of threat detection.

The strongest security posture requires a 24x7x365 Security Operations Center so that your systems are never left unprotected. Running a 24x7 SOC requires the appropriate staffing and facility. Volta's SOC as Service offering allows an organization to retain continuous monitoring and threat detection without requiring the organization to make a significant investment in security software, hardware, and other infrastructure. At Volta's regionally-based office, we have built a fully equipped central command center for every enterprise infrastructure in our care. Our security operations team monitors, detects, investigates, and responds to cyberthreats around the clock. This protection extends across the many assets of an enterprise, including classified databases, intellectual property, and brand integrity.

THE IMPORTANCE OF A SOC: **24X7 MONITORING** | **CENTRAL VISIBILITY** | **LOWER COSTS**

Continuous monitoring for restful nights.

We know that not every organization needs an all-encompassing cyber security solution. Some organizations simply need after-hours support for their environment. With SOC-as-a-Service from Volta, we monitor all security-related events holistically, from a centralized location, with a team of analysts who investigate, and validate alerts around the clock.

24X7 COVERAGE

- Volta's regionally-based SOC provides a central command center for your entire organization
- Ease the concern of finding skilled security experts to fill every shift in today's tight job market

ALERT PRIORITIZATION

- Develop event severity categories and escalation processes for each category
- Create tooling for the automation of events
- Perform weekly reviews to refine event severity and escalation processes

TRIAGE & ANALYSIS

- Real-time data feeds including:
  - Server & Critical Systems
  - Network
  - Endpoint
- Respond to alerts from identified controls
- Event investigation, consulting, and mitigation as needed

AUTOMATION

- Utilize machine learning monitoring tools to help evolve alongside criminal tactics
- Event correlation and alert ranking
- Reduced risk of error and false positives
- Less time between detection and remediation

We think about your security around the clock, so you don’t have to.

Building and maintaining a SOC in-house is prohibitively expensive for most organizations, and it simply takes an arduous amount of time to obtain the infrastructure, and license and implement the software. Many organizations also don’t have time to consider the ongoing training and professional development costs required to keep up with ever-changing technologies and threats. A significant barrier to launching an in-house SOC is procuring the right talent to run it. Hiring a team of expert security analysts is very costly and the turnover is notoriously high.

With SOC as a Service, organizations can rest easy knowing the entirety of their network environment is under vigilant watch by experts who are trained to search for new and evolving threats. Simply put, choosing a managed SOC solution costs much less than building your own.

STRAIGHTFORWARD SECURITY

24x7 monitoring: Ongoing monitoring is the only way to gain full coverage of the immediate threats on your network.

Correlate suspicious threats: Event correlation through an industry-leading automation tool allows Volta’s SOC team to separate the truly threatening events from the noise on the network.

Detailed remediation steps: We work in partnership with your internal IT teams to remediate detected threats.

COST EFFECTIVE

Managed service: Trade the capital expenditure for a single, simple monthly expense.

No need for experts: Gain the use of a team of cybersecurity experts and analysts that are trained and experienced to monitor for today’s advanced cybersecurity threats.

Reduce repair costs: Utilize a SOC that already exists and relinquish the responsibility to maintain expensive infrastructure.

COMPREHENSIVE FORENSICS

Conduct detailed forensics: Our SOC team gathers relevant evidence on active threats by drawing from different data sources.

Asset inventory: Events are collected from all devices, applications and business resources.

Respond to events faster: Detailed forensics and the integration of past alerts allows us to respond to threats quickly.

ALERT ACTIVITY REPORTING

Holistic perspective: Reduces the complexity of disparate tools, so that all data is visible in one place.

Applicable to compliance frameworks: Maintain best practices to keep your organization in compliance.

Focus on the complex threats: Alert ranking through an industry-leading automation tool.