Security Information and Event Management (SIEM)

Last updated 8-17-23

Security threat actors attempt to breach enterprise systems and services every day. Security Information and Event Management (SIEM) is a platform that collects and provides analytics to identify, alert and respond to malicious activity.

SIEM is a platform within information security. The correlation of information from IT infrastructure, application systems and threat intelligence provides real-time insight into malicious and anomalous behavior. Alerts are triggered to inform the Security Operations Center (SOC) and Computer Incident Response Team of the severity and related response actions. Automated report generation and data logging are key components of our SIEM service.

Service features

- **Collect data** across all users, devices, applications and infrastructure. Currently the SIEM ingests approx. 250TB of data monthly across 37 unique agency log analytics workspaces.
- **Detect** previously uncovered threats and minimize false positives using analytics and threat intelligence. The SIEM solutions identifies approximately 800,000 potential incidents per month.
- **Investigate** threats and hunt suspicious activities. Potential incidents identified per month, approximately 2,500 are of interest.
- **Respond** to incidents rapidly with built-in orchestration and automation. Automated blocking actions resolve approximately 90%, with approximately 50 alerts actioned per month.

Of the 50 actionable alerts, half of those are resolved by the OCS SOC team, with delegated (agency) actions accounting for the other half.

Helpful information

Service category
Security

Service availability
24/7/365

Planned maintenance
Planned maintenance is performed after hours and coordinated with agency representatives.

Related services
- CIRT Security Assessment
- Vulnerability Management

How to request service
Submit a request for service through our Customer Portal.

Service owner
Deputy CISO Security Operations

The SIEM solution delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for attack detection, threat visibility, proactive hunting and threat response, including the following:

- Aggregates and reports on log data events within the information technology environment.
- Offered as a delegated administration model. Customer data and system resources are separate and administered by customer administrators.
- Managed services staff members provide technical expertise in using the platform and are on call 24/7 to resolve any system problems with the production environment.
- Produces trending reports that allow for effective measurement of activities.

Intended customers

This service is for all executive branch agencies. WaTech's Office of Cybersecurity (OCS) coordinates with a managed security service provider for agencies to outsource analytics functions.

Options available with this service

- Support Syslog and common event format logs for correlation and analysis.
- Real-time monitoring and detection of malicious behavior.
- Threat hunting by OCS threat hunters to assist agencies that need proactive help finding indicators of compromise and indicators of attack.

- Incident response runbooks and playbooks to bring consistency to common events and incidents.

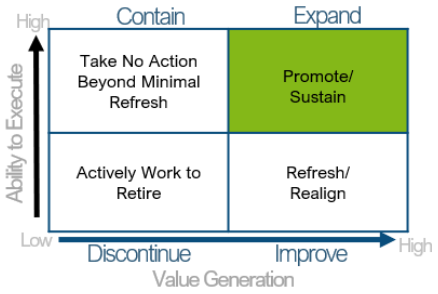
Customer engagement

- OCS holds calls with agency chief information officers (CIOs) and chief information security officers (CISOs) and conducts engagement during onboarding. We will also create sites for knowledge sharing and ad hoc engagements on specific security events.
- Monthly Technology Management Council, Business Management Council, and Enterprise Security Governance meetings for agency CIOs and IT leaders to inform and sponsor enterprise strategy, policy and investments.
- Regularly scheduled meetings between customers and business relationship managers to connect, advise, address concerns, and provide solutions.
- Weekly group calls for state CIOs and CISOs to provide updates on important and immediate issues and actions.
- Regular outreach to solicit feedback, provide updates and inform agencies on emerging projects, initiatives, and services.
- Requests for new consultations and modifications to existing applications.
- OCS is running Office Hours to ensure multiple engagement interfaces.

Action plan

Current activity

- Conducting SIEM installation, onboarding, configuration, and fine-tuning.
- Conducting analytics for cost optimization and logging and monitoring options to ensure maximum efficiency and collection of high-value security logs.
- BlueVoyant project will continue to onboard agencies and provide customer engagement and training.
- Threat hunting capabilities and automation via runbooks and playbooks are in the final stages. Completion is expected by Sept. 30, 2023.
- Create Terms of Service (TOS) and service page.



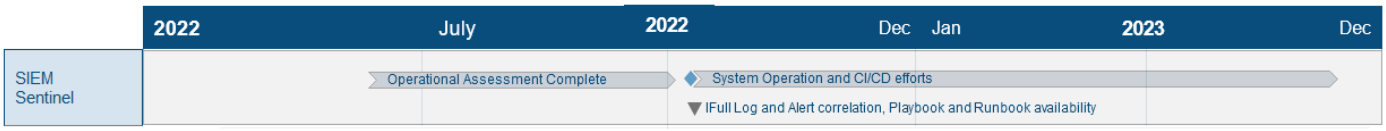
One- to two-year goals

- WaTech OCS currently provides services to 61 agencies. Our goal is to have 95% of agencies integrated and participating in this service by the end of FY 2023 as part of the Blue Voyant project.
- Conduct service offerings analysis and provide additional clarity during the Service Catalog Revamp project.
- Continue service updates and technology improvements throughout the lifespan of the product.
- Begin Security Operations and Automation Response (SOAR) integration during 2023 onboarding activities, with the expectation that SOAR functions are fully integrated with actionable mitigation and remediation steps August 2024.
- Provide technical exercises available based on real incident data with runbooks and playbooks by Q4 2024.
- Identify and ingest additional critical log sources (e.g., cloud logs, service, WAF, etc).

Three- to five-year goals

- Conduct a Return-on-Investment review of current SIEM solution, explore other offerings in the market space, conduct customer engagement on capability gaps that may be emergent needs across the enterprise.
- Select and migration this service as needed based on service assessment and community feedback.
- Develop and maintain technical skill sets across the enterprise by conducting technical workshops for threat hunting tips and tricks, with the intent that 100% of staff across the agency operating environments expected to conduct work in this platform have attended at least one training session.
- Assess current SIEM solution to determine ROI metrics related to SIEM technical platform to ensure best value to the enterprise.

- Improve security visibility, risk management integration, and cost optimization through the development and analytics of metrics.
- Bring real-time threat intelligence and remediation to agencies, which will be documented via runbooks and playbooks that will be added to a repository for information sharing.



Service review and fully loaded service budget projection

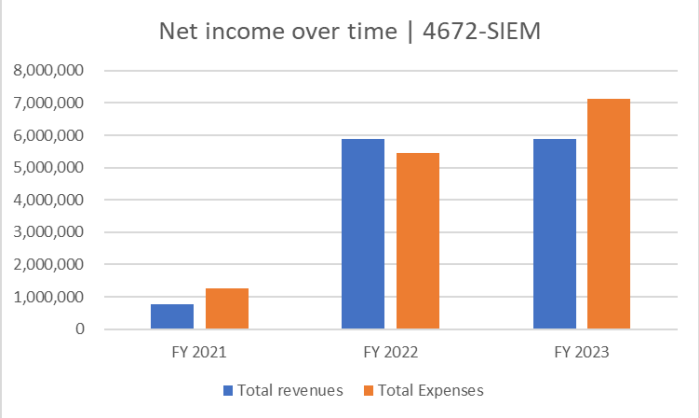
Revenue source

The service is bundled and funded using revenue from the Security Infrastructure central service model. This was established to ensure consistent funding for cybersecurity policy and technology leadership for state government, and promote cooperation and coordination between regional and national governments, and corporations.

The service is funded through the Enterprise Security Infrastructure Central Service Model (CSM). Annually, the Office of Financial Management uses the financial model to allocate funding support from state agencies that use the service.

Net income over time

WaTech OCS incurs expenses to operate and staff the SOC as a service provider. The graph compares these for the next two years.



Decision packages

In the 2021 supplemental budget, WaTech received approximately $10.5 million in biennial funding to support the SIEM.

Expenditures:
SIEM is a subprogram under OCS SOC. Expenses specific to SIEM consist primarily of two security analysts, a Managed Security Service Provider (MSSP), and logs analysis, management, and retention.

Decision Packages:
WaTech submitted a request for additional funding support for the MSSP in the 2024 Supplemental Budget.