Security Operations Center (SOC)

Last updated 09-25-23

Security Operations Center (SOC) includes monitoring and management of intrusion detection systems, anti-malware and antispam, endpoint protection, and endpoint detection and response, and Cloud Access Security Broker. SOC also provides:

- Access to a team of analysts to resolve alerts, identify and analyze indicators of compromise, indicators of attack and respond to attacks.
- Assistance in optimizing an organization's protection, detection and response capabilities.
- Includes services that typically make up managed detection and response (MDR) solutions and can be considered as an evolution of both Managed Security Service and MDR.

The service benefits of SOC include uninterrupted and comprehensive centralized monitoring and analysis of enterprise systems for suspicious activity; improved incident response times and practices; faster detection of security events; and resolution of all alerts to get maximum value out of existing systems. Other benefits include the consolidation of all security threats, tools and systems into a single point of control to address and resolve alerts, and the ability to evaluate the effectiveness of existing controls for improvement.

The SOC delivers security analytics and threat intelligence, providing a single solution for attack detection, threat visibility, proactive hunting and threat response. The service also aggregates and reports on log data events within the state's information technology environment, and the service is offered with a delegated administration model; customer data and system resources are separate and administered by customer administrators. Managed services staff members provide technical expertise in the use of the platform and are on call 24/7 to resolve any system problems with the production environment. The SOC solution also produces trending reports that allow for the measurement of the effectiveness of activities.

Helpful information

Service category

Security

Service availability

24/7/365

Planned maintenance

Performed as required during non-peak hours.

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

Intended customers

The SOC service is provided to large, medium, small agencies, boards, commissions, and Tribal governments on the State Government Network (SGN) or Public Government Network (PGN).

Options available with this service

- Threat hunting by OCS threat hunters to assist agencies that need proactive help finding indicators of compromise.
- Incident response runbooks and playbooks to bring consistency to common events and incidents.

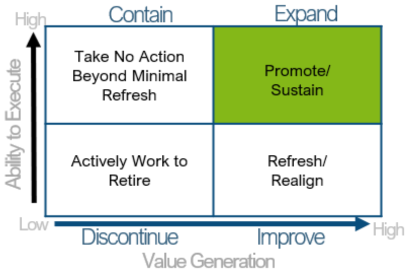
Customer engagement

- 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 Open Office hours are conducted weekly to ensure feedback to the community.

Action plan

Current activity



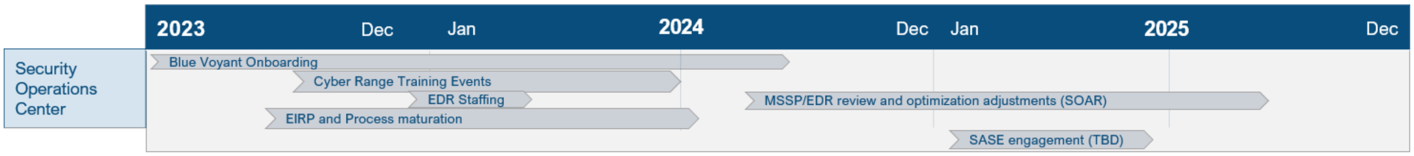
- Deployment, configuration and fine-tuning of SOC has been underway for 12 months.
- Provide Red and Blue Team exercises based on real incident data with runbooks and playbooks by Q4 2023.
- Complete 60% of MSSP onboarding for agencies, anticipating that the third wave will be complete by end of calendar year.
- Recruit a technical staff member to managed EDR tool set.
- Recruit a SOC supervisor who will be responsible for tactical workloads across the operating environment, building capacity to strengthen strategic capabilities across OCS.
- Mature SOC processes and procedures to improve customer engagement and identify capability caps in current service offerings.
- Engage in Security Access Service Edge (SASE) exploration to identify tools sets.
- Identify current WaTech service offerings to ensure appropriate service alignment across infrastructure, operations, and security business offerings to provide best value to enterprise customers.

One- to two-year goals

- Complete onboarding for participating agencies for the MSSP by Q2 CY 2024.
- Offer fully automated and orchestrated functions (i.e., triage and escalation of alerts into incident data) with actionable mitigation and remediation steps by EOY 2024.
- Build out by agency workspaces for MSSP engagement.
- Follow up on training for customers as they are onboarded.
- Build strategic metrics based on maturation of service offering visibility and engagement tracking.
- Leverage metrics based analysis to identify capability gaps and potential solutions to address critical security problem statements.

Three- to five-year goals

- Build decision packages to grow funding, resourcing, and solutions sets to close critical capability gaps.
- Close SSL decrypt and inspection capabilities to maximize return on investment problem statements in current tool sets.
- Integration with "whole of state" SOC functionality, to increase visibility and local government support opportunities.
- Add fully documented efforts via runbooks and playbooks to a repository for information sharing.

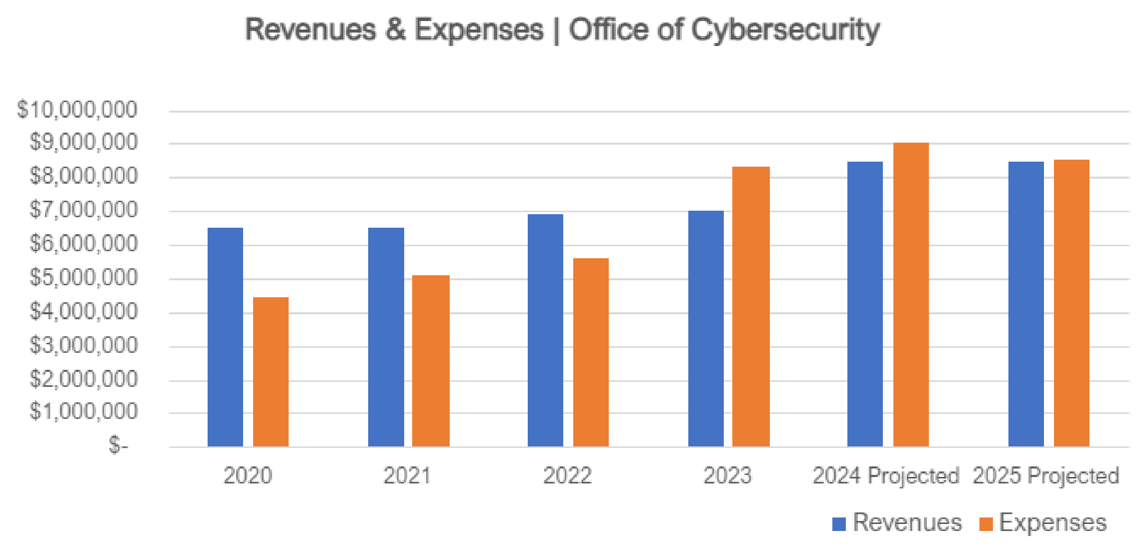


Service review and fully loaded service budget projection

Revenue source

The service is bundled and funded using revenue from the OCS central service model. This was established to ensure consistent funding for cybersecurity policy and technology leadership for state government, as well as to promote cooperation and coordination between regional and national governments, and corporations. Agencies with 50+ FTEs pay a yearly base fee of $2,000. The remaining cost of the office is allocated based on the agency's number of budgeted FTEs. OFM maintains the source data for budgeted FTEs.

Net Profit over time


Revenues & Expenses | Office of Cybersecurity
$10,000,000
$9,000,000
$8,000,000
$7,000,000
$6,000,000
$5,000,000
$4,000,000
$3,000,000
$2,000,000
$1,000,000
$-
2020
2021
2022
2023
2024 Projected
2025 Projected
Revenues
Expenses