Vulnerability Management

Last updated 07-26-23

Vulnerabilities are defined as weaknesses in technical systems. Such weaknesses must be addressed before a threat actor takes advantage of the opportunity. WaTech operates a platform that enables agencies to identify vulnerabilities on technical platforms such as network appliances, servers and workstation endpoints and installed custom developed and commercial-off-the-shelf software (COTS).

The Vulnerability Management service is meant to provide asset scanning to agencies that do not have organic scanning capabilities. For agencies with organic scanning capabilities, agency scans are uploaded to the vulnerability management platform for analytics. Whether agencies conduct their own organic scan or leverage this service, agencies have a responsibility to ensure that all assets are scanned and assessed for vulnerabilities.

The Vulnerability Management service provides agency and enterprise visibility on vulnerabilities across the operating environment, prioritization analytics, and visibility of key risk-based focused areas.

Intended customers

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

Options available with this service

- Scans of assets will be performed on a regular (monthly) basis in coordination with agencies who leverage the scanning service.
- Ad Hoc on-demand scanning capability on request.
- Reports are generated with each scan and report reviews are conducted with OCS personnel.

Customer engagement

- WaTech and Securin hosts monthly status meetings with approximately 30 agencies per month.
- Monthly Enterprise Security Governance meetings for agency CISOs and security professionals to discuss enterprise security issues.
- Monthly Technology Management Council meeting for agency CIOs and IT leaders to inform and sponsor enterprise strategy, policy and investments.
- 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 service support.
- OCS conduct weekly open office hours for customer engagement.

Helpful information

Service category

Security

Service availability

24/7/365

Planned maintenance

Performed as required during non-peak hours.

Related services

- Security Operations Center
- Consulting services

How to request service

Submit a request for service through our Customer Portal.

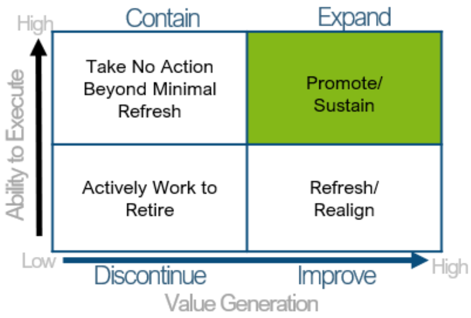
Service owner

Deputy CISO Security Operations

Action plan

Current Activity

We have added Attack Surface Management to this service. Attack Surface Management provides a view of our public-facing infrastructure for analysis of vulnerabilities that threat actors can exploit. This addition was made available on May 1, 2022. Attack surface scans are conducted monthly across the wa.gov operating space, and agencies can request ad hoc scanning via CIRT@watech.wa.gov.



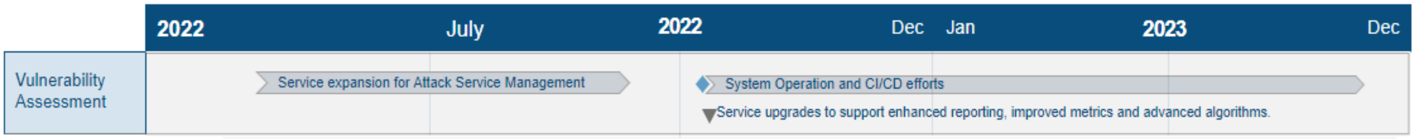
- Engaging with current customers to evaluate service satisfaction and areas for improvement.
- Improving customer knowledge related to all supported vulnerability management systems and platforms.
- Recruiting a technical owner for this service.

One to two-year goals

- Incorporation of all agency Microsoft Defender telemetry within the platform.
- WaTech/OCS will adopt a Continuous Improvement Continuous Development (CI/CD) program for this service.
- This will enable advanced reporting, real-time updates to the vulnerability database and current research on attack techniques and remediation steps. To accomplish the “real-time” update capability OCS will conduct an assessment of the existing scanning platform with consideration towards an agent-based vulnerability reporting tool.
- Mature metrics visibility, focus on improving priority of effort communication cycles to support a more robust risk management vulnerability and risk management cycle for vulnerability and attack surface management.
- Review scanning and patching capability gaps for operational improvement opportunities.

Three to five-year goals

- Engage with the enterprise community for the adoption and service transition to more robust cloud-based patch management solutions.
- Explore, assess, and request funding for solutions, resources, and transition opportunities.
- Submit decision packages for critical capability gap funding, specifically as it relates to scanning of “off SGN” endpoints and services e.g., telework endpoints, cloud resources, and SAAS service vulnerability and attack surface management.
- Engage and deconflict infrastructure, operational, and security service offering alignment, compliance needs, and support models for this service i.e. improving vulnerability and attack surface management of enterprise service offerings.
- Evaluate an integrated vulnerability and patch management platform with “one-click” remediation capabilities.
- Evaluate and implement a threat and vulnerability management solution for mobile devices (mobile phones and tablets, specifically iOS and Android platforms).



Service review and fully loaded service budget projection

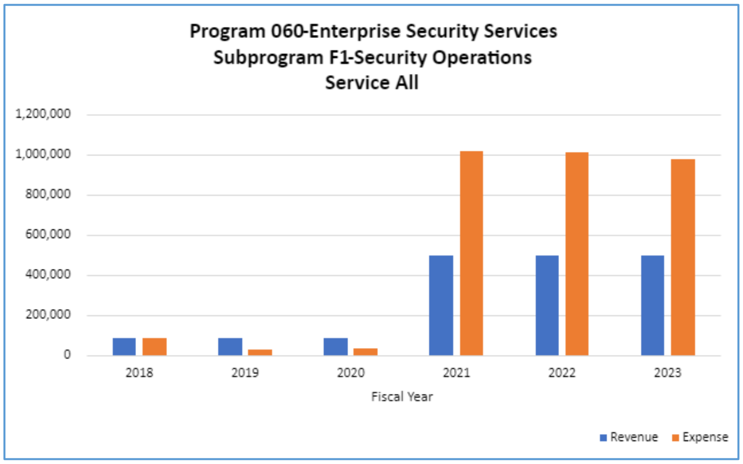
Revenue source:

The Vulnerability Assessment service receives revenues from the Enterprise Security Infrastructure central service model. The Security Infrastructure Allocation funds the hardware and software vulnerability scanning platform service that enables agency security teams to identify where vulnerabilities reside across their environment of network components, servers, workstations, databases, and installed Commercial off the Shelf Software (COTS) programs.

The allocation funding is based on the agency's number of budgeted FTEs and the number of applications each agency has using the gateway. OFM maintains the source data for budgeted FTEs and WaTech tracks the number of applications. Additionally, agencies with 50+ FTEs pay a yearly base fee of $1,500.

Net Income over time:

Investment in equipment was made in FY 2016, and in the following three years, expenses consisted of licenses, support, and annual renewal. In FY 2021, new software and support were purchased to meet the needs of the enterprise.



Decision packages

2023-25 Biennial Budget: A maintenance level request for 650k to support the attack surface management is submitted under the A6 Provide IT Security Essentials decision package request.