Maryland
DEPARTMENT OF
INFORMATION TECHNOLOGY

Larry Hogan | Governor
Boyd K. Rutherford | Lt. Governor
Michael G. Leahy | Secretary
Lance Schine | Deputy Secretary

SERVICE AGREEMENT

Between

The Maryland Department of Information Technology and Subscribing Entity

For

Cyber Security Service - Vulnerability Management (FY2021)

This Service Agreement forms a part of the Memorandum of Understanding between the Maryland Department of Information Technology ("DoIT") and subscribing entity ("Customer"). The parties agree as follows:

1 Services Covered

Maryland considers vulnerability management a foundational and essential component of security Information Technology (IT) and Operational Technology (OT) systems. The Maryland IT Security Manual and DoIT IT Policy requires units to use this service to identify vulnerabilities in their environments. The service includes the following features and components:

1. Agent-Based Scanning (Most Operating Systems)
2. Credentialed Scanning (Most Operating Systems)
3. Uncredentialed Scanning (Any IP Connected Asset)
4. External Scanning (Internet View)
5. External Scanning (SwGI View)
6. Web Application Scanning

2 Parties Responsibilities

The following contains a non-exhaustive list that describes the responsibilities for both DoIT and the customer and may be updated periodically. Updates will be considered effective 14 calendar days from the posting date of the new service agreement.

2.1 Service Initiation and Onboarding

The parties agree to the following delineation of activities during the onboarding and implementation of the managed firewall service:

2.2 Ongoing Operations

2.2.1 DoIT will:

1. Manage Hardware Platform and Software for:
    a. Security Center Server
    b. Internet Scanner
    c. SwGI Scanner

    d. Datacenter Scanners

2. Manage System
    a. Availability
    b. Capacity
    c. Security
    d. License Capacity
3. Manage user accounts through the Statewide directory
    a. Provide Rules of Behavior to system users
4. Manage customer Hosted Components
    a. Nessus Managers and Remote Scanners
        i. Software and application updates
5. Vendor
    a. Support tickets for plugin issues and system issues.
6. Maintain System Security Plan for the system

2.2.2 The Customer will:

1. Manage Customer Hosted Components
    a. Nessus Managers and Remote Scanners
        i. Physical Security of Hardware (Virtual)
        ii. Hardware (Virtual) availability
        iii. Network Connectivity
2. Report system issues to the Security Operations Center (SOC)
3. Follow system Rules of Behavior
4. Report suspected false-positives and false-negatives through the ticketing system

3 Service Level Agreements

The following describes the SLAs for this service, which DoIT classifies as “Business Operational.” The Security Operations Center monitors system components 24x7x365 for availability, security, and capacity.

3.1 Availability

1. Security Center - System Availability
    a. System Availability Target is 99.9% for 24x7x365
    b. Regularly planned maintenance occurs Thursday from 15:00EST until 18:00EST, when required.
    c. Planned maintenance announcements are sent at least 24 hours in advance of the event.
2. Other components - System Availability
    a. System Availability Target is 99.9% for 24x7x365

        i. Regularly planned maintenance occurs Thursday from 14:00EST until 17:00EST, when required.
        ii. Plugin update checks occur at least daily and may cause the user interface of the Nessus Manager to be unavailable.
    b. Availability problems hosted on customer platforms resulting from issues are excluded from SLA calculations

3.1.1 Availability Target: 99.9%, measured monthly

The availability target excludes planned maintenance windows.

3.2 Incident Handling

- P1 – Service Outage
    - Four (4) Hour Response
    - One (1) Business-Day Resolution
- P2 – Service Degraded
    - Two (2) Business-Day Response
    - Four (4) Day Resolution
- P3 – Service Questions
    - One (1) Business-Day Response
    - Five (5) Business-Day Resolution
- Maximum permissible data loss: 72 hours
- Maximum recovery times: 7 days

4 Maintenance Schedules

Except in instances where an emergency/unplanned outage is required, DOIT will endeavor to provide notice at least one business days before the outage and make every effort to leverage the redundancy of the service to limit any service outage.

5 Support and Service Outages

System users that require support may open a service ticket in the ServiceNow self-service portal or email soc@maryland.gov to request assistance.

6 Costs for Services

The service is charged on a per-unit basis, with a minimum quantity of 500 units for agent-based and scanner-based vulnerability and compliance management (Vulnerability Service) and 1 unit of web-application scanning.

1. Vulnerability: $7.00/Asset
2. Web Application Scanning: $500.00/Web Application

Assistance resolving vulnerabilities on system components that DoIT does not manage will incur T&M charges.

7 Termination of Services

The subscribing entity must provide 90 days advance written notice to terminate services.

8 Warranty

While DoIT strives to provide a secure service, no service can guarantee that all network and system intrusions, compromises, or other unauthorized activity will be detected and prevented.