

VULNERABILITY MANAGEMENT

1. OVERVIEW

Overwatch Vulnerability Management Service is a comprehensive risk management solution that proactively detects and prioritizes the remediation of vulnerabilities based on contextual risk and regulatory standards. This solution includes remediation workflow tracking and an executive dashboard that depicts business risk and the progress in reducing risk. We incorporate a best-in-class vulnerability management, monitoring and risk assessment tool, to provide you with real-time, centralized oversight of all scanned assets and applications in your digital ecosystem.

2. SERVICE DEPLOYMENT

The Overwatch Vulnerability Management service deployment includes:

2.1 VULNERABILITY SCANNING

Overwatch utilizes advanced vulnerability scanning tools to identify potential weaknesses in your systems, applications, and network devices. We cover a wide range of assets, including servers, workstations, firewalls, routers, and web applications discovering and identifying potential vulnerabilities in systems, applications, and network infrastructure.

2.1.1 DEPLOYMENT OPTIONS

There are several ways to deploy this service:

2.1.1.1 AGENT-BASED SCANNING

A deployed agent for Windows (Servers, Workstations, AD) MacOS (Workstation) and Linux (Coming soon) which scans the local machine for application and configuration vulnerabilities. Provides a Network Edge Scan where the primary browser is checked for hardening. Provides OVAL and SCAP for Webserver and specific compliance reporting applications.

2.1.1.2 SUPER-AGENT NETWORK PROBE SCANNING

The agent scanner discussed in section 2.1.1.1 can be deployed as a “Super Agent” which uses Windows Hyper-V virtualization on the host machine to run a containerized network probe scanner. This agent configuration is beneficial for deploying a network probe scanner in an environment that does not have dedicated virtualization hardware already in place yet requires a more powerful machine to operate without disruption to the End-user. 12-core CPU, 24 GB RAM with at least 150 GB of free SSD storage space is recommended, of which at least 2 (up to 4) CPU cores will be allocated during scanning tasks, with the requisite amount of system memory and storage being allocated as well.

2.1.1.3 VM-BASED NETWORK PROBE SCANNER

Scanning of network assets (Firewalls, Switches, APs, Servers, Workstations, etc.) across the attack surface on a partner-specified scan schedule (daily continuous, weekly, monthly). The results of this network layer vulnerability scanning will be aggregated alongside the other scanning methodologies to create a more unified picture of the organizational risk profile and vulnerability feasibility. Requirements for Scanner size and VLAN size as a function of the scan schedule will be shared during onboarding to ensure we have proper compute resources allocated to allow for full advanced network scanning to be completed in the desired scan frequency window.

2.1.1.4 CLOUD-BASED EXTERIOR SCANNER

Exterior scan targets (public-facing Web Server, public-facing static WAN IP or FQDN, WAF, FW, or any other exterior-facing IP addressable interface) will be scanned by an Overwatch-maintained cloud-based scanner that will give you the “outside-In” look at your publicly deployed assets.

2.1.1.5 PUBLIC CLOUD MARKETPLACE SCANNERS

We have native AWS and Azure marketplace-loaded scanner containers available for your extensive cloud deployments. These are the same type of scanners that can be deployed on-premises for network probe scanning, but in your AWS or Azure environment.

2.2 VULNERABILITY ASSESSMENT

Once vulnerabilities are identified, they need to be assessed to understand their potential impact and likelihood of exploitation. This involves analyzing the vulnerabilities to determine their severity, possible attack vectors, and the potential business risks they pose.

By deploying Overwatch Vulnerability Management service, you will significantly enhance your visibility to cyber risk and gain clear guidance on remediation actions you can take to reduce your risk posture.

2.2.1 CONTEXTUAL RISK PRIORITIZATION & CATEGORIZATION

Our contextual risk scoring engine employs machine learning to correlate over 30 vulnerability metrics to accurately score the most relevant vulnerabilities specific to each customer organization. Vulnerabilities that are discovered within the platform are categorized based on organizational risk profiles and business contexts (established by the defined EC technical resource [MSP, vCISO, Internal IT, etc.]). This categorization process yields the top riskiest contextualized vulnerabilities that exist within the platform’s visibility (depending on deployment type). The tool also analyzes the feasibility of a potential vulnerability to be used against the environment (depending on deployment and visibility) in a “Real-Life Exploitation” style detection that pulls in attributes from across the attack surface to present additional detail on mitigation and remediation strategies, all delivered in an easy to understand narrative, with references and links to the weaponized exploit (if available) for use in exploring additional detection and response schema.

2.2.2 BULK ACTION REMEDIATION REPORTING

Gain insight into remediation actions that have the largest net impact on the environment.

3. SERVICE MANAGEMENT

Overwatch Vulnerability Management service management includes:

3.1 24/7/365 US-BASED ANALYSTS AND LAYERED SUBJECT MATTER EXPERTS

Overwatch Vulnerability Management service offers round-the-clock support from our 100% US-Based SOC analysts who are always available to help interpret results from a particular alert or help implement additional detection rules (if a secondary Overwatch service is deployed that has capability to affect the discovered vulnerability).

3.2 REMEDIATION WORKFLOW

Our service includes remediation workflow analysis and patching timelines, giving you an overview of progress in the remediation of vulnerabilities, contextual risk vulnerabilities patched, and any potential areas for improvement.

This involves tracking the application of software patches, implementing security updates, reconfiguring systems, or applying security controls to eliminate or minimize the identified vulnerabilities.

3.3 REGULAR REPORTING & REVIEW

Overwatch services include regular reporting, giving you an overview of your security posture, the threats that have been neutralized, any potential areas for improvement in contextual risk scoring. Regular reviews are conducted to ensure the service evolves with your customer’s organization and continues to provide the most effective protection.

3.4 CONTINUOUS UPDATES & MAINTENANCE

Overwatch Vulnerability Management service is continuously updated to respond to the latest threat trends and vulnerabilities. Regular maintenance ensures the efficiency and effectiveness of the service, minimizing your cybersecurity risks.

3.5 ONGOING MONITORING

Vulnerability management is not a one-time process but an ongoing effort. Regular monitoring is essential to detect new vulnerabilities, track changes in the threat landscape, and ensure that the organization's systems and applications remain secure. This can involve continuous vulnerability scanning, real-time threat intelligence feeds, staying updated with security advisories and patches.

4. BENEFITS

Overwatch Vulnerability Management service offers:

- **Enhanced Security Posture:** By identifying and addressing vulnerabilities before they are exploited, you can significantly reduce the risk of data breaches and cyber-attacks for your organization.
- **Compliance and Auditing:** Our service helps you meet regulatory compliance requirements and provides valuable insights for third-party security audits.
- **Business Continuity:** Strengthening your security measures helps ensure uninterrupted business operations and protects your brand reputation.
- **Peace of mind:** With 24/7 100% US-Based monitoring, and real-time alerts, you can focus on your business knowing that your digital ecosystem is protected.

Overwatch Vulnerability Assessment services equip your organization with the knowledge and tools needed to maintain a robust cybersecurity posture. By leveraging Overwatch expertise, you can confidently defend against emerging threats and protect your critical assets from potential security breaches. Stay one step ahead of cyber threats with our proactive and reliable Vulnerability Assessment Service.