EXPOSURE MANAGEMENT SERVICES: VULNERABILITY MANAGEMENT

Service Definition Document

Approved by: Faizal Ashruf, Head of Exposure Management Services, CyberProof

Contents

Service Definition

The Vulnerability Management Service is designed to identify, assess, and assist in the remediation of security vulnerabilities across an organisation's systems and networks. This service encompasses continuous vulnerability scanning, risk-based prioritisation, and the provision of actionable remediation recommendations. The objective is to reduce exposure to cyber threats and enhance the overall security posture of the organisation.

Service Highlights

Service Features

- Seamless Governance Integration and Organisational Alignment

The service adopts a governance model that ensures seamless integration with existing organisational structures. This approach promotes strong alignment between technology initiatives and organisational objectives, enabling efficient coordination across departments and functions.

- Streamlined Threat and Vulnerability Reporting

Reporting mechanisms are optimised for clarity and speed, facilitating systematic communication of identified threats and vulnerabilities. This ensures that relevant stakeholders are kept informed in a timely manner, supporting proactive decision-making and risk mitigation.

- Efficient Remediation Workflows

Well-defined workflows are established for tracking the remediation of vulnerabilities and the execution of management action plans. These workflows support the prompt resolution of identified security gaps and provide clear visibility into the status of remediation efforts.

- Benchmarking and Maturity Analysis

The service incorporates benchmarking and maturity analysis to evaluate security posture across multiple dimensions, including organisational size, industry, geography, technology, and business processes. This enables the organisation to measure its capabilities against industry standards and best practices.

- Technology, People, and Process Integration

Integration efforts extend beyond technology to include people and process dimensions. This holistic approach ensures that security measures are embedded into everyday operations and that staff are actively engaged in supporting the organisation's security objectives.

- Compliance and Audit Support

The governance model supports the organisation's compliance and audit requirements. It provides structured processes and documentation to help demonstrate adherence to regulatory standards and internal policies during audits and assessments.

Service Benefits

- Proactive detection of vulnerabilities for early identification and validation, ensuring weaknesses are detected before exploitation can occur.
- Reduced Cyber Risk - Continuous scanning and prioritisation help organisations address critical vulnerabilities before attackers can exploit them.
- Enhanced Visibility - Provides a clear view of the organisation's security posture across systems, networks, and applications.
- Continuous Improvement - Regular assessments highlight recurring issues and trends, helping organisations strengthen long-term security strategies.
- Identification of Quick Wins – Enables seamless operations by addressing easily remediated vulnerabilities first.
- Provision of 8x5 Support – Dedicated assistance during business hours to ensure timely resolution of issues.

Service Operations

- Automated Vulnerability Scanning: Continuous execution of authenticated and unauthenticated scans across all registered assets to identify software vulnerabilities, leveraging VM platform capabilities for real-time detection.
- Threat-Intelligence Driven Prioritization: Integration of external and platform-native threat intelligence feeds to dynamically rank vulnerabilities by exploitability, severity (CVSS), and business impact. Prioritized vulnerability lists are generated and shared to client stakeholders.
- Patch Correlation and Remediation Mapping: Correlation of detected CVEs with vendor patch repositories and available hotfixes. Host-specific remediation guidance is produced, ensuring actionable recommendations aligned with patch availability and system compatibility.
- Configuration Benchmarking: Continuous assessment of system configurations against CIS Benchmarks and other industry standards. Non-compliant configurations are reported, tracked, and monitored for remediation status.
- Comprehensive Asset Discovery and Inventory: Deployment of supported discovery platforms (e.g., CrowdStrike, Qualys) to enumerate known and unmanaged assets across on-premises infrastructure, cloud workloads, endpoints, mobile devices, and applications. For unsupported platforms, integration with third-party discovery tools is recommended.
- Asset Profiling and Metadata Collection: Collection and correlation of device attributes including hardware identifiers, running services, installed software packages, and versioning. All discovered assets are automatically enrolled into appropriate scanning profiles to maintain coverage integrity.
- Operational Reporting: Generation and distribution of technical reports in accordance with client-defined SLAs, including vulnerability metrics, remediation progress, and compliance status.
- Collaborative Engagements: Active participation in operational review meetings with client teams, providing technical input and remediation guidance.
- System Health and Vulnerability Metrics: Weekly and monthly reporting cycles highlighting system health indicators, vulnerability distribution by asset class, and categorization by severity and exploitability.

- Trend and Lifecycle Analysis: Monthly analytics detailing vulnerability lifecycle metrics, including counts of newly opened, closed, and patched vulnerabilities. Trend analysis is shared to support strategic risk reduction initiatives.

Service Delivery and Engagement Model

CyberProof primarily delivers services remotely, with onsite support provided only when necessary and mutually agreed upon. The engagement includes 8x5 support, vulnerability scanning, and scheduled cadence calls. The Customer is responsible for providing all required access and supporting information to ensure effective service delivery.

The scope includes Planning, Current State Analysis, and Target State Development, all based on discussions with the Customer. Business-as-usual (BAU) activities will commence only after both parties have agreed on the engagement cadence, frequency, KPIs, and other relevant performance metrics.

CyberProof VM team collaborates with the client to identify network architecture and gather information necessary for scanner deployment, including types and locations. Scanning profiles are mapped by asset type, and relevant schedules are created and updated to ensure continuous scanning of known assets

A designated Point of Contact will be appointed to serve as the Technical Account Manager (TAM) for the engagement. Small delivery teams, comprising dedicated analysts, will be formed as required, aligned to the defined scope and estimated duration. In the event of high or critical threats or risks in the customer environment, analyst validates, triages and informs relevant teams within 1-2 business hours.

Deliverables

The onboarding process involves mapping the client's topology and connecting to the output of the client's VM tool, or installing and deploying these tools as required. The client must provide technical credentials for the VM tool, such as service accounts and API keys, to facilitate system connections for data collection or process automation. The onboarding process can be categorized as 3 phases: Standardization Phase, Transition Phase and Operationalization Phase.

The standardization phase focuses on establishing a unified global Vulnerability Management (VM) baseline. Project governance will be defined, with sessions conducted to assess the current execution state and align expectations across stakeholders. Policies, processes, and stakeholder inputs will be captured to build a cohesive VM framework. Standardized KPIs, based on CyberProof best practices, will be introduced to measure effectiveness and maturity. Regional requirements will be aligned with global standards to ensure scalability and consistency, while playbooks will be developed to enable uniform and repeatable vulnerability management processes across the enterprise.

The transition phase centres on validating the framework through a pilot implementation in a mutually agreed-upon group of assets/ region. This pilot will be executed in collaboration with the client to test processes and identify areas for improvement. Stakeholder feedback will be systematically collected

to refine KPIs, operational standards, and reporting mechanisms. Lessons learned from the pilot will be incorporated into updated playbooks and enhanced processes, ensuring that subsequent rollouts benefit from improved efficiency and consistency across the complete scope.

The operationalization phase involves the actual BAU activities, culminating in full enterprise-wide implementation of the Vulnerability Management Program. Governance frameworks will be tailored to meet regulatory and compliance requirements, ensuring sustainability and risk mitigation. Scalable deployment strategies will be applied to minimize operational disruptions while maintaining consistent performance across geographies. The final deliverables will include an operationalized VM Program, reinforced by robust governance structures and continuous compliance readiness.

Once the operation transitions to BAU, the following key operational deliverables will be provided:

Weekly Report

A concise summary of weekly activities, including:

- Issues identified and resolutions implemented
- Open action items and ongoing investigations

(Purpose: Ensures transparency and timely follow-up on pending concerns.)

Monthly Report

An overview of monthly activities, highlighting:

- Trends and patterns observed during the reporting period
- Progress updates on key metrics and initiatives
- Summary of recurring or escalated issues

(Purpose: Supports proactive decision-making and early detection of systemic challenges.)

Quarterly Business Review (QBR)

A strategic summary of services delivered over the quarter, covering:

- Improvements in Security and Compliance Posture
- Key performance indicators and service highlights
- Recommendations and roadmap for the upcoming quarter

(Purpose: Aligns business objectives with security and compliance outcomes, fostering continuous improvement.)

Service Governance

CyberProof team is responsible for developing and maintaining policies governing the VM service. These policies define the scope, objectives, and rules for conducting vulnerability assessments, risk prioritisation, and remediation activities.

Comprehensive documentation is provided to clients, covering processes, configuration, and detected infrastructure.

Weekly reviews of scan data are conducted, blockers are addressed, and reports are shared through presentations. Clients are encouraged to provide feedback via email.

For additional requests, the acknowledgement response time is defined to be 8 business hours. Standard service requests may include information requests (such as CVE inquiries), running scans on assets or asset groups, and generating pre-defined reports. Standard change requests can involve configuration changes such as creating new scan profiles, scheduling scans, changing asset categories, or modifying virtual scanners. Complex change requests may encompass scanner agent software upgrades, create new virtual scanners, or deploy new scan agents in the cloud. The resolution time varies depending upon the type of request, and its priority.