MANAGED VULNERABILITY SCANNING - SERVICE GUIDE

Last Modification Date: 05/13/2022
Exported and Shared on: 03/18/2024

For additional information, visit www.intervision.com

CONTENTS

Managed Vulnerability Scanning is a managed service that performs vulnerability scanning to assess internal and Internet-facing servers, workstations and network-attached devices for threats and weaknesses.

As a recurring diagnostic scan, it builds reports that define, identify and classify security risks. When available, information including recommended patches, bug fixes and configuration changes are provided to assist in remediation.

Scanner performs assessments at scheduled intervals with automated ticketing to provide tracking and auditing back to the Security Operations Center (SOC) . It also prioritizes improvements and quickly eliminates security holes that hackers may exploit while also meeting requirements within compliance audits.

1 FEATURES

- Service utilizes recognized leading vulnerability scanning appliance - Qualys Vulnerability Scanner.
- SOC to assist with:
  - Determine acceptable scan time frames and determine escalation process in the event of unintended system impact.
  - Configure vulnerability scanning parameters and targets of evaluation.
  - Perform vulnerability scanning and data collection activities for Internet-accessible systems and services.
  - Perform vulnerability scanning of hosts and endpoints and data collection activities for internal network-accessible systems and services.
  - Host and service discovery.
  - Vulnerability identification and reporting.

2 RESPONSIBILITY MATRIX

	Client	InterVision	
		Managed Service	**Optional ProServices**
Implementation			
Provide Physical or Virtual vulnerability scanning appliance		X	
Install scanner (virtual or physical) for internal scans	X	Remote Support	
Configure scans		X	Advanced
Configure reports		X	Advanced
Provide inputs to Service Runbook	X		

	Client	InterVision	
		Managed Service	Optional ProServices
Establish Service Runbook		X	
Configure with client provided Password Management Server			X
Monitoring and Alerting			
Monitor Scanner Health		X	
Monitor Job Success		X	
Notification of New Critical Vulnerabilities		X*	
Change Management			
Scheduling changes		X	
Scan configuration changes		X	
Add / Remove IP block		X	
Configure scan policies (Exclusions, Scan windows,...)		X	
Adhoc threat or vulnerability hunting			X
Administration			
Troubleshoot Scan Failures		X	
Administer preconfigured regularly schedule scans		X	
Configure and run adhoc scans		X	

	Client	InterVision	
		Managed Service	Optional ProServices
Scanner Updates (automated)		X	
Scanner Move or reconfiguration		X	
Incident Response			
Cancel scan		X	
RCA on failed scans		X	
Troubleshoot scanning network performance impact			X
Security Analysis			
Review report			X
Patch Management Strategy			X
Vulnerability Assessment			X

* Requires Professional service to configure

3 MANAGED VULNERABILITY SCANNING SCANNER APPLIANCE

A physical or virtual vulnerability scanner is placed on the network and is monitoring by the Managed Network Service for performance and availability.

3.1 VIRTUAL SCANNER RESOURCE REQUIREMENTS:

Minimum resource configuration

1 x vCPU | 1.5 GB RAM | 1 x 56GB virtual HDD

Maximum resource configuration

16 x vCPU (recommended maximum of 8) | 16GB RAM

4 SERVICE LEVEL AGREEMENT

This service will adhere to the Managed Services SLA detailed in the Work Order.

5 OPTIONAL PROFESSIONAL SERVICES

Professional services is require for initial and advanced configuration and set up.

Professional service and be added to ongoing operations to provide vulnerability assessments and help designing a vulnerability management program. These engagements will be tailor the client specific needs but may include the following:

- Periodic assessments
- Remediation guidance and advisory
- Network topology and asset scope
- External vulnerability testing
- Internal vulnerability testing
- Review exceptions and reconcile scoped targets of evaluation with actual results.
- Collate report data and publish raw findings for follow-up analysis.
- Security Vulnerability Reporting, Analysis, and Recommendations
- Analyze findings and determine appropriate remediation steps.
- Produce summary of findings and recommendations for mitigation or remediation.
- Present findings, summary, analysis, and recommendations.
- Recommend vulnerability management program (tools, approach, policy best practices, etc.)