



ATTACK SURFACE MANAGEMENT VULNERABILITY PROCESS ASM-VP

V031623

This document is a briefing that describes the operation and use of the ASM-VP Dashboard, and it is meant for all users of SKYWATCH WEB Platform.

Purpose of this Dashboard

The SYWATCHSM Attack Surface Management Vulnerability Process (ASM-VP) addresses, in the most comprehensive manner, all the components and information flow from testing to remediation of the organization's vulnerabilities.

The ASM-VP aims to reduce the time that it takes an organization to resolve (remediate) its vulnerabilities and provides all the service-modules necessary. It addresses the following issues:

- 1. Takes time and resources to detect and respond.**
- 2. Lack of a unified view for all the parts of information**
- 3. Incomplete asset inventory**
- 4. Inaccurate and inefficient prioritization of vulnerabilities**
- 5. Overwhelming volume of vulnerabilities**
- 6. Management's focus, attention, and communication**

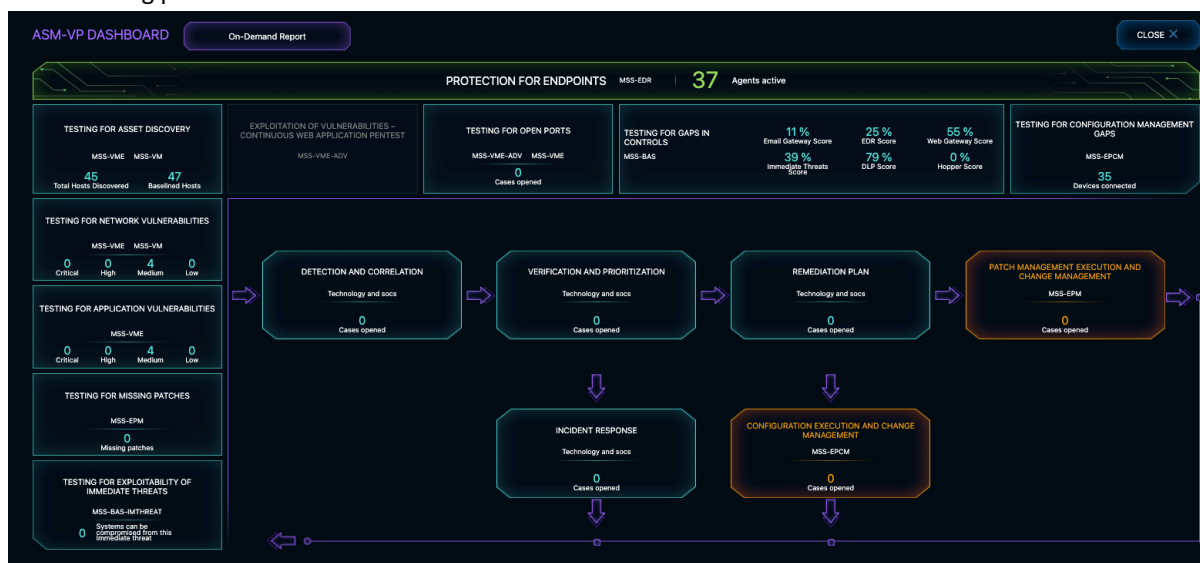
The ASM-VP Dashboard provides the following functionality:

- Presents in graphical form the flow of information and the parameters to measure security and operational information.
- Provides a "door" into more detailed dashboards for each component of services involved and contracted.
- Displays key security and operational indicators of the full process and components (based on the contracted services by the client).
- Shows the number of cases per stage and department/organization.
- Creates a report that is on-demand that combines all the detailed reporting for the complete Vulnerability Process related modules (service dashboards).





The following presents the SYWATCHSM ASM-VP for VISIBILITY and ON-DEMAND REPORT.



# of discovered assets; # of baselined assets	Network Vulnerability counters: # of critical; # of high; # of medium; # of low vulnerabilities	# of missing patches	# of cases of exploitation of vulnerability	# of cases	# of cases open and answered	# of cases open and answered	# of cases open and answered
Testing for Asset Discovery	Testing for Network Vulnerabilities	Testing for Missing Patches	Testing for Exploitability of immediate threats	Testing for Configuration Management GAPS	TESTING	Verification and Prioritization	Configuration Execution and Change Management

Application Vulnerability counters: # of critical; # of high; # of medium; # of low vulnerabilities	% penetration for: (Email Endpoint Web Immediate Threat DLP LM)	# of cases	# of cases of ports that are open and not baselined	# of cases	# of cases open and answered	# of cases open and answered	# of agents active
Testing for Application Vulnerabilities	Testing for gaps in controls	Exploitation of vulnerabilities – continuous Web Application Pentest	Testing for open ports	Testing for Configuration Management GAPS	Detection and Correlation	Remediation Plan	Protection for Endpoints

of cases per stage





The services listed are either lighted with a link to the corresponding service page (for contracted services) or dark (for non-contracted services).

Detailed Description of functionality of the ASM-VP Dashboard

Below the description and use cases of each of the components.

ITEM	SERVICE	INDICATOR	DESCRIPTION
Testing for Asset Discovery	MSS-VM; MSS-VME	# of Discovered assets and # of Baselined assets	What is it? Displays a # on how many patch deployments have occurred, regardless of success or failure. Operation For the SKYWATCH WEB the refresh rate is once every 2-3 days. The information represents data from the last 30 days. Use case. This information can be used to track whether patches have been deployed.
Testing for Network Vulnerabilities	MSS-VM; MSS-VME	# of critical; # of high; # of medium; #low	What is it? Displays a # on how many patch deployments have occurred, regardless of success or failure. Operation For the SKYWATCH WEB the refresh rate is once every 2-3 days. The information represents data from the last 30 days. Use case. This information can be used to track whether patches have been deployed.
Testing for Application Vulnerabilities	MSS-VME	# of critical; # of high; # of medium; #low	What is it? Displays a # on how many patch deployments have occurred, regardless of success or failure. Operation For the SKYWATCH WEB the refresh rate is once every 2-3 days. The information represents data from the last 30 days. Use case. This information can be used to track whether patches have been deployed.
Testing for Missing Patches	MSS-EPM	# of missing patches	What is it? Displays a # on how many patch deployments have occurred, regardless of success or failure. Operation For the SKYWATCH WEB the refresh rate is once every 2-3 days. The information represents data from the last 30 days. Use case. This information can be used to track whether patches have been deployed.
Testing for gaps in controls	MSS-BAS	% penetration for: (Email Endpoint Web Immediate Threat DLP LM)	What is it? Displays a # on how many patch deployments have occurred, regardless of success or failure. Operation For the SKYWATCH WEB the refresh rate is once every 2-3 days. The information represents data from the last 30 days. Use case. This information can be used to track whether patches have been deployed.
Testing for Exploitability of immediate threats	MSS-BAS	# of systems can be compromised from this Immediate threat	What is it? Displays a # on how many patch deployments have occurred, regardless of success or failure. Operation For the SKYWATCH WEB the refresh rate is once every 2-3 days. The information represents data from the last 30 days. Use case. This information can be used to track whether patches have been deployed.
Exploitation of vulnerabilities – continuous Web Application Pentest	MSS-VME-ADV	# of cases of this type	What is it? Displays a # on how many patch deployments have occurred, regardless of success or failure. Operation For the SKYWATCH WEB the refresh rate is once every 2-3 days. The information represents data from the last 30 days. Use case. This information can be used to track whether patches have been deployed.





Testing for open ports	MSS-VME-ADV	# of cases of ports that are open and not baselined	<p>What is it? Displays a # on how many patch deployments have occurred, regardless of success or failure.</p> <p>Operation For the SKYWATCH WEB the refresh rate is once every 2-3 days. The information represents data from the last 30 days.</p> <p>Use case. This information can be used to track whether patches have been deployed.</p>
Testing for Configuration Management GAPS	MSS-EPCM	# of cases opened	<p>What is it? Displays a # on how many patch deployments have occurred, regardless of success or failure.</p> <p>Operation For the SKYWATCH WEB the refresh rate is once every 2-3 days. The information represents data from the last 30 days.</p> <p>Use case. This information can be used to track whether patches have been deployed.</p>
TESTING		# OF CASES OPEN AND ANSWERED	<p>What is it? Displays a # on how many patch deployments have occurred, regardless of success or failure.</p> <p>Operation For the SKYWATCH WEB the refresh rate is once every 2-3 days. The information represents data from the last 30 days.</p> <p>Use case. This information can be used to track whether patches have been deployed.</p>
Detection and Correlation		# OF CASES OPEN AND ANSWERED	<p>What is it? Displays a # on how many patch deployments have occurred, regardless of success or failure.</p> <p>Operation For the SKYWATCH WEB the refresh rate is once every 2-3 days. The information represents data from the last 30 days.</p> <p>Use case. This information can be used to track whether patches have been deployed.</p>
Verification and Prioritization		# OF CASES OPEN AND ANSWERED	<p>What is it? Displays a # on how many patch deployments have occurred, regardless of success or failure.</p> <p>Operation For the SKYWATCH WEB the refresh rate is once every 2-3 days. The information represents data from the last 30 days.</p> <p>Use case. This information can be used to track whether patches have been deployed.</p>
Remediation Plan		# OF CASES OPEN AND ANSWERED	<p>What is it? Displays a # on how many patch deployments have occurred, regardless of success or failure.</p> <p>Operation For the SKYWATCH WEB the refresh rate is once every 2-3 days. The information represents data from the last 30 days.</p> <p>Use case. This information can be used to track whether patches have been deployed.</p>
Incident Response		# of cases opened and answered	<p>What is it? Displays a # on how many patch deployments have occurred, regardless of success or failure.</p> <p>Operation For the SKYWATCH WEB the refresh rate is once every 2-3 days. The information represents data from the last 30 days.</p> <p>Use case. This information can be used to track whether patches have been deployed.</p>
Patch Management Execution and Change Management	MSS-EPM	# of cases opened and answered	<p>What is it? Displays a # on how many patch deployments have occurred, regardless of success or failure.</p> <p>Operation For the SKYWATCH WEB the refresh rate is once every 2-3 days. The information represents data from the last 30 days.</p> <p>Use case. This information can be used to track whether patches have been deployed.</p>
Configuration Execution and	MSS-EPCM	# of cases opened and answered	<p>What is it? Displays a # on how many patch deployments have occurred, regardless of success or failure.</p>





Change Management			Operation For the SKYWATCH WEB the refresh rate is once every 2-3 days. The information represents data from the last 30 days. Use case. This information can be used to track whether patches have been deployed.
Re-testing	# of cases opened and answered		What is it? Displays a # on how many patch deployments have occurred, regardless of success or failure. Operation For the SKYWATCH WEB the refresh rate is once every 2-3 days. The information represents data from the last 30 days. Use case. This information can be used to track whether patches have been deployed.
Protection for Endpoints	MSS-EDR	# of agents active	What is it? Displays a # on how many patch deployments have occurred, regardless of success or failure. Operation For the SKYWATCH WEB the refresh rate is once every 2-3 days. The information represents data from the last 30 days. Use case. This information can be used to track whether patches have been deployed.
Generate on-Demand Report			This action button will generate the ASM-VP REPORT based on the data of the dashboard with the corresponding TLP AMBER designation.
How to use this Dashboard			This document will be presented when this item is selected.

