

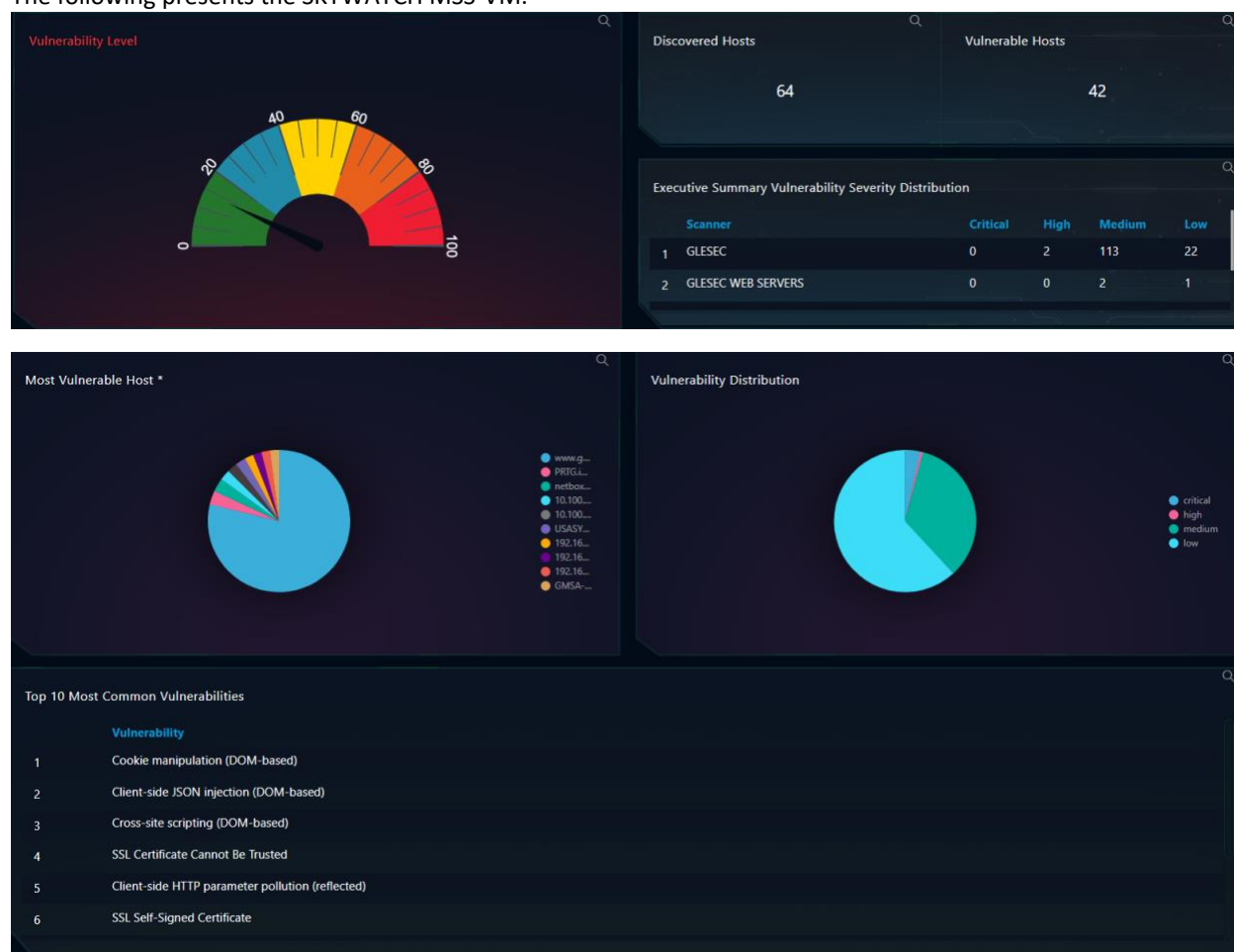
MANAGED VULNERABILITY SERVICE (MSS-VM)

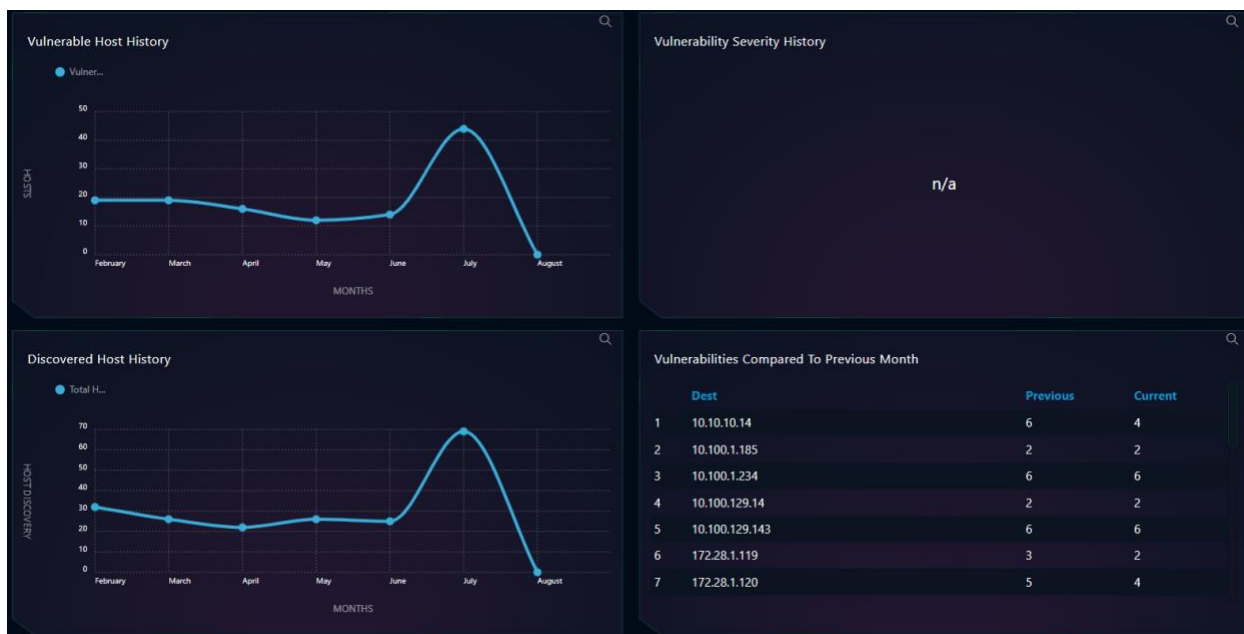
This document is a briefing that describes the operation and use of the MSS-VM Service, and it is meant for all users of SKYWATCH WEB Platform.

Purpose of this Dashboard

This SKYWATCH Dashboard(s) provides **visibility** to the technical and executive users of SKYWATCH about the **MSS-VM** Service and an on-demand **report** for this service (with the information of the dashboard). These are two of the deliverables for this service. There are more consolidated reports that combine the information of this service with other contracted services. Also certain of the parameters defined on this Dashboard are used as indicators to trigger SKYWATCH automations (GLESEC NOTABLE EVENTS – GNE) and this activates the GLESEC OPERATION CENTER(s) (GOC) into action to further investigate and for incident-response.

The following presents the SKYWATCH MSS-VM.





Vulnerability Database

Filter: Location and/or Division

Any Any Filter Group

25 entries per page Search...

	Priority	Severity	IP	OS	Hostname	Division	Location	Vulnerability	Vulnerability ID	Available Exploit	Vulnerability Publication	Since Last Seen	Last Seen On	Action
1	Medium	Medium	172.28.2.65	FreeBSD 12.3-STABLE (arm)	Unknown	GOC	Not Set	Network Time Protocol (NTP) Mode 6 Scanner	97861	n/a	n/a	03 day(s)	2023/07/31 13:59:30+0000	Action - Create Case WHITELIST
2	Medium	Medium	172.28.1.120	Microsoft Windows 10 Pro Build 19045	Unknown	GOC	Not Set	SSL Certificate Cannot Be Trusted	51192	n/a	n/a	02 day(s)	2023/07/31 16:58:58+0000	Action -
3	Medium	Medium	172.28.1.120	Microsoft Windows 10 Pro Build 19045	Unknown	GOC	Not Set	Curl Arbitrary File Write 7.x >= 7.84.0 / 8.x <= 8.1.2 (CVE-2023-32001)	178813	n/a	2023/07/19	02 day(s)	2023/07/31 16:58:58+0000	Action -
4	Medium	Medium	172.28.1.120	Microsoft Windows 10 Pro Build 19045	Unknown	GOC	Not Set	SSL Self-Signed Certificate	57582	n/a	n/a	02 day(s)	2023/07/31 16:58:58+0000	Action -
5	Medium	Medium	172.28.1.120	Microsoft Windows 10 Pro	Unknown	GOC	Not Set	Intel® PROSet/Wireless WiFi Software x <	136670	n/a	n/a	02 day(s)	2023/07/31 16:58:58+0000	Action -

Detailed Description of functionality of the MSS-VM Dashboard

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

ITEM	DESCRIPTION
Vulnerability Level	<p>Displays a risk chart that shows the total vulnerability level.</p> <p>For the SKYWATCH WEB the refresh rate is once every day. The information represents data from the last 30 days.</p> <p>This information can be used to see what the overall vulnerability risk is.</p>
Discovered Hosts	<p>Displays all the discovered hosts.</p> <p>For the SKYWATCH WEB the refresh rate is once every day. The information represents data from the last 30 days.</p> <p>This information can be used to monitor how many hosts are discovered on your internal network.</p>
Vulnerable Hosts	<p>Displays from the discovered hosts how many have vulnerabilities.</p> <p>For the SKYWATCH WEB the refresh rate is once every day. The information represents data from the last 30 days.</p> <p>This information can be used to monitor how many discovered hosts are vulnerable on your internal network.</p>
Executive Summary Vulnerability Severity Distribution	<p>Displays groups that are being scanned and how many total vulnerabilities they have broken up into varying levels.</p> <p>For the SKYWATCH WEB the refresh rate is once every day. The information represents data from the last 30 days.</p> <p>This information can be used to monitor the amount of vulnerabilities on your network and if they are increasing or decreasing.</p>
Most Vulnerable Host	<p>Displays the top 10 most vulnerable hosts on your network.</p> <p>For the SKYWATCH WEB the refresh rate is once every day. The information represents data from the last 30 days.</p> <p>This information can be used to see which hosts are the weakest and should be addressed first.</p>
Vulnerability Distribution	<p>Displays how many vulnerabilities and in what risk category they belong to on a pie chart.</p> <p>For the SKYWATCH WEB the refresh rate is once every day. The information represents data from the last 30 days.</p> <p>This information can be used to see how many high level vulnerabilities are present on a pie chart.</p>
Top 10 Most Common Vulnerabilities	<p>Displays the top 10 vulnerabilities on your network.</p> <p>For the SKYWATCH WEB the refresh rate is once every day. The information represents data from the last 30 days.</p> <p>This information can be used to see which vulnerabilities are most common and should be addressed first.</p>



Vulnerable Host History	<p>Displays how many vulnerable hosts a network has on a graph over the span of 6 months.</p> <p>For the SKYWATCH WEB the refresh rate is once every day. The information represents data from the last 6 months.</p> <p>This information can be used to see what your network history is with your vulnerable devices.</p>
Vulnerability Severity History	<p>Displays the history of the different levels of the vulnerabilities over the span of 6 months.</p> <p>For the SKYWATCH WEB the refresh rate is once every day. The information represents data from the last 6 months.</p> <p>This information can be used to see what your network history is with your vulnerable devices and their levels of vulnerabilities.</p>
Discovered Host History	<p>Displays the history of the discovered hosts in the network over the span of 6 months.</p> <p>For the SKYWATCH WEB the refresh rate is once every day. The information represents data from the last 6 months.</p> <p>This information can be used to see what your network history is with your discovered devices.</p>
Vulnerabilities Compared To Previous Month	<p>Displays the amount of vulnerabilities on a device currently to how many it had in the previous month.</p> <p>For the SKYWATCH WEB the refresh rate is once every day. The information represents data from the last 60 days.</p> <p>This information can be used to see if your device's vulnerability count is improving.</p>
Vulnerability Database	<p>Displays a table that gives an extensive breakdown of the vulnerabilities on devices.</p> <p>For the SKYWATCH WEB the refresh rate is once every day. The information represents data from the last 30 days.</p> <p>This information can be used to show in great detail how severe the vulnerabilities are and what machine these vulnerabilities exist on. You can also click on action to create a case on the intranet or whitelist the vulnerability.</p>
REPORT	<p>This action button will generate a MSS-VM REPORT based on the data of the dashboard with the corresponding TLP AMBER designation.</p>