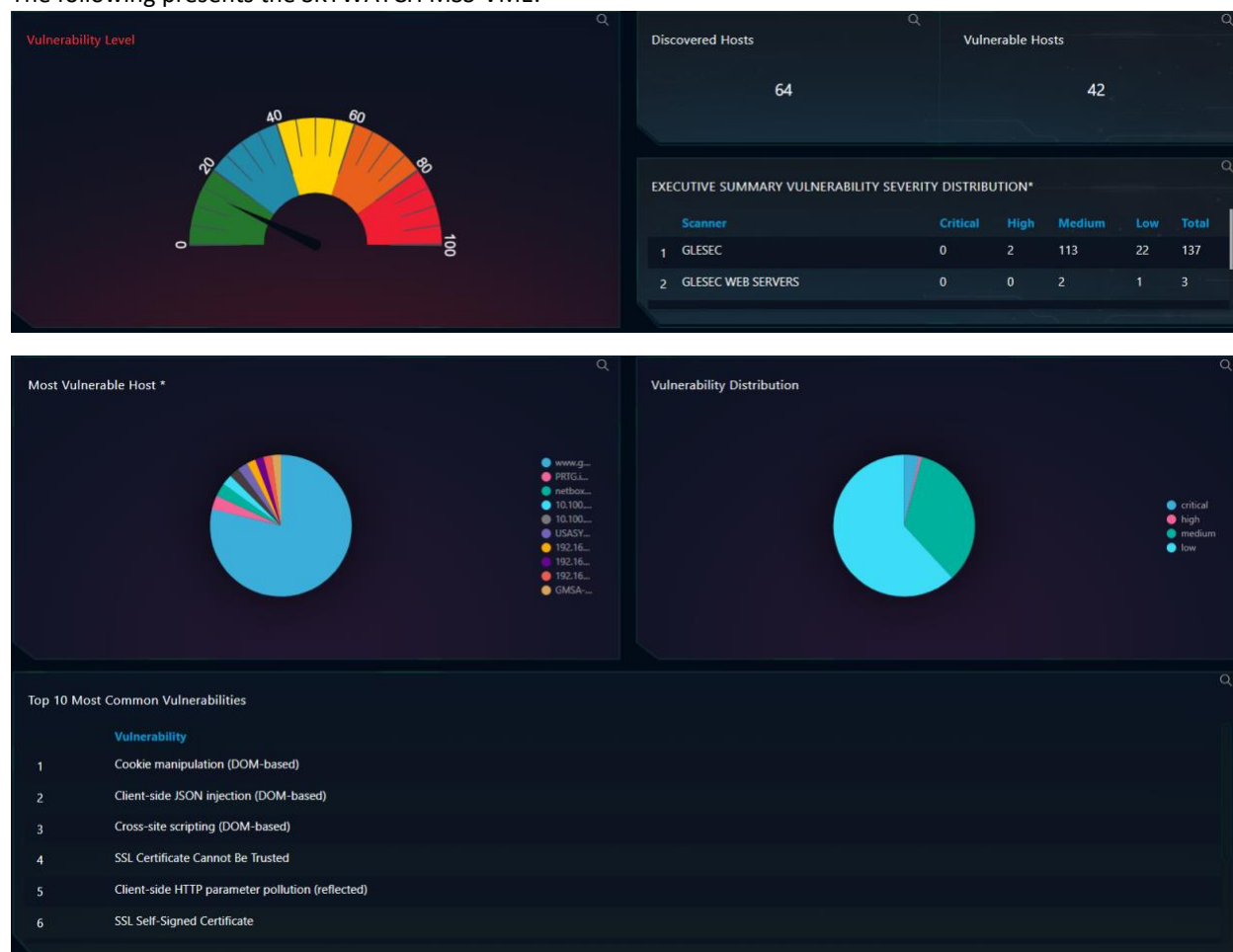# GLESEC
COMPLETELY PERSPECTIVE

EXTERNAL (AND ADVANCED) MANAGED VULNERABILITY SERVICE (MSS-VME)

This document is a briefing that describes the operation and use of the MSS-VME and MSS-VME-ADV 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-VME** and **MSS-VME-ADV** 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.
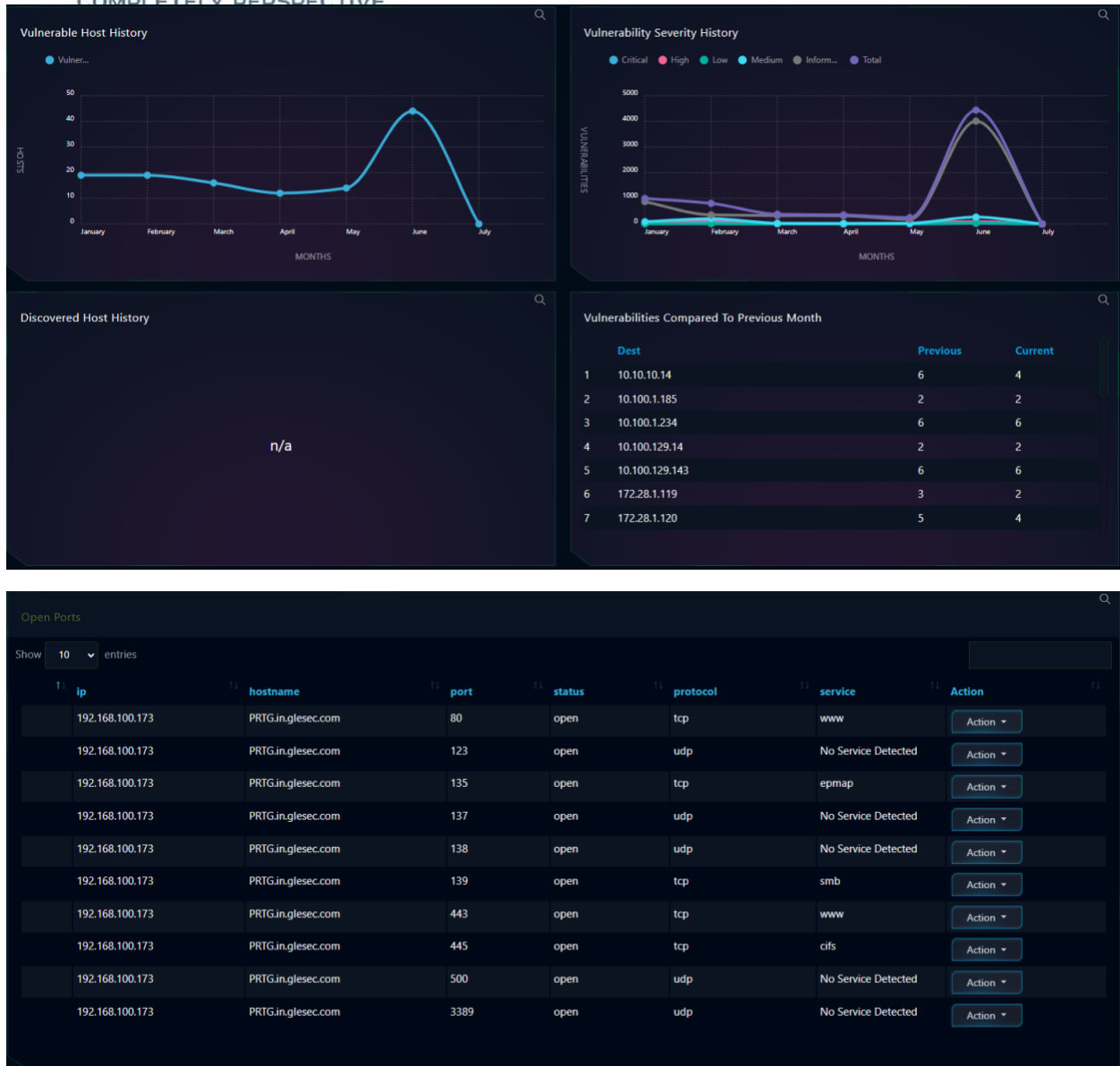
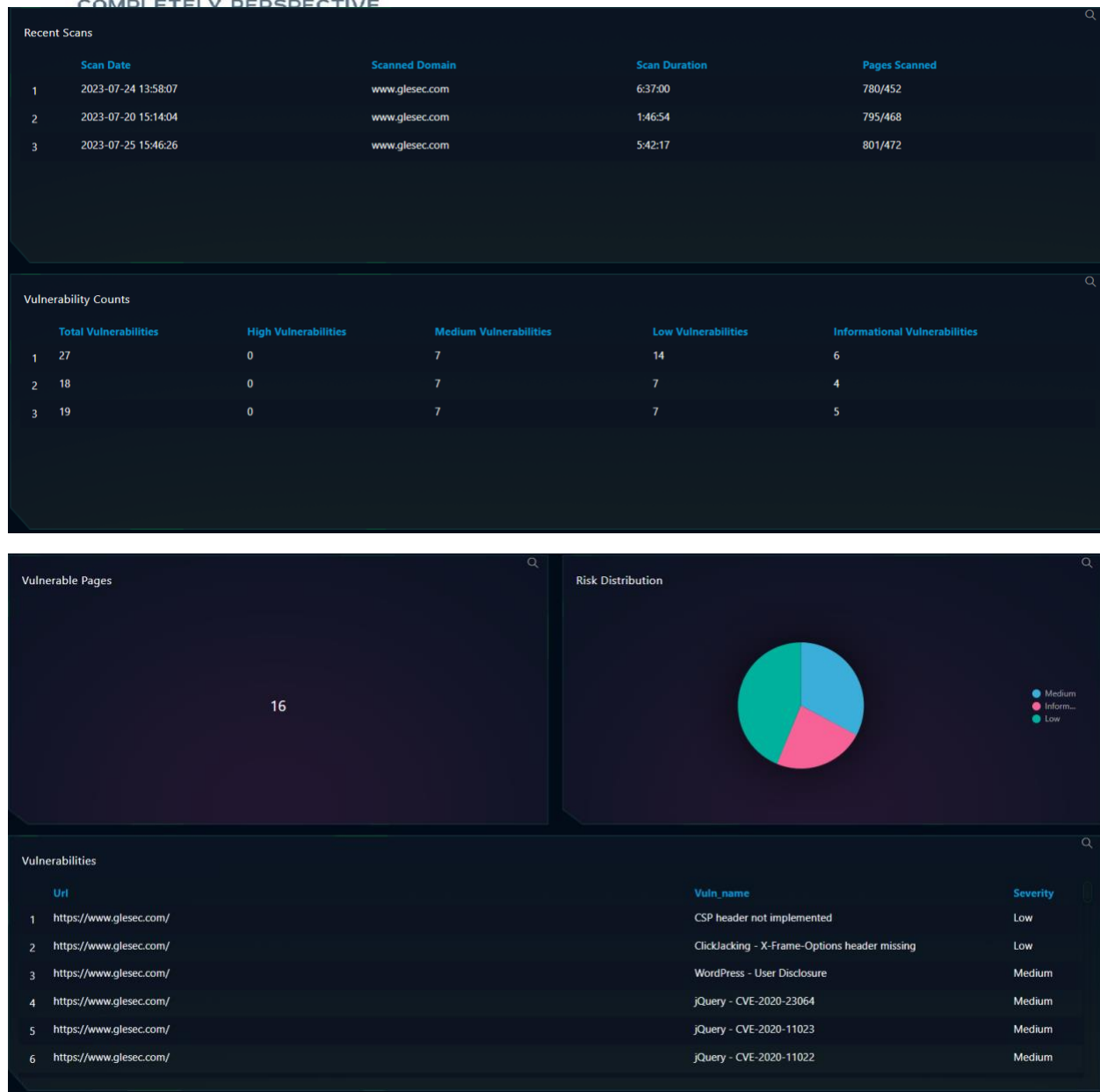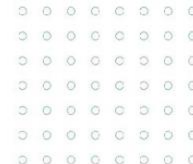The following presents the SKYWATCH MSS-VME.

Vulnerable Host History

Vulner...

HOSTS

50
40
30
20
10
0

January February March April May June July

MONTHS

Vulnerability Severity History

● Critical ● High ● Low ● Medium ● Inform... ● Total

VULNERABILITIES

5000
4000
3000
2000
1000
0

January February March April May June July

MONTHS

Discovered Host History

n/a

Vulnerabilities Compared To Previous Month

	Dest	Previous	Current
1	10.10.10.14	6	4
2	10.100.1.185	2	2
3	10.100.1.234	6	6
4	10.100.129.14	2	2
5	10.100.129.143	6	6
6	172.28.1.119	3	2
7	172.28.1.120	5	4

Open Ports

Show 10 entries

ip	hostname	port	status	protocol	service	Action
192.168.100.173	PRTG.in.glesec.com	80	open	tcp	www	Action ▾
192.168.100.173	PRTG.in.glesec.com	123	open	udp	No Service Detected	Action ▾
192.168.100.173	PRTG.in.glesec.com	135	open	tcp	epmap	Action ▾
192.168.100.173	PRTG.in.glesec.com	137	open	udp	No Service Detected	Action ▾
192.168.100.173	PRTG.in.glesec.com	138	open	udp	No Service Detected	Action ▾
192.168.100.173	PRTG.in.glesec.com	139	open	tcp	smb	Action ▾
192.168.100.173	PRTG.in.glesec.com	443	open	tcp	www	Action ▾
192.168.100.173	PRTG.in.glesec.com	445	open	tcp	cifs	Action ▾
192.168.100.173	PRTG.in.glesec.com	500	open	udp	No Service Detected	Action ▾
192.168.100.173	PRTG.in.glesec.com	3389	open	udp	No Service Detected	Action ▾

Recent Scans

	Scan Date	Scanned Domain	Scan Duration	Pages Scanned
1	2023-07-24 13:58:07	www.glesec.com	6:37:00	780/452
2	2023-07-20 15:14:04	www.glesec.com	1:46:54	795/468
3	2023-07-25 15:46:26	www.glesec.com	5:42:17	801/472

Vulnerability Counts

	Total Vulnerabilities	High Vulnerabilities	Medium Vulnerabilities	Low Vulnerabilities	Informational Vulnerabilities
1	27	0	7	14	6
2	18	0	7	7	4
3	19	0	7	7	5

Vulnerable Pages

16

Risk Distribution

● Medium
● Inform...
● Low

Vulnerabilities

	Url	Vuln_name	Severity
1	https://www.glesec.com/	CSP header not implemented	Low
2	https://www.glesec.com/	ClickJacking - X-Frame-Options header missing	Low
3	https://www.glesec.com/	WordPress - User Disclosure	Medium
4	https://www.glesec.com/	jQuery - CVE-2020-23064	Medium
5	https://www.glesec.com/	jQuery - CVE-2020-11023	Medium
6	https://www.glesec.com/	jQuery - CVE-2020-11022	Medium

Detailed Description of functionality of the MSS-VME Dashboard

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

ITEM	DESCRIPTION
Vulnerability Level	Displays a risk chart that shows the total vulnerability level. For the SKYWATCH WEB the refresh rate is once every day. The information represents data from the last 30 days. This information can be used to see what the overall vulnerability risk is.

Discovered Hosts	Displays all the discovered hosts. For the SKYWATCH WEB the refresh rate is once every day. The information represents data from the last 30 days. This information can be used to monitor how many hosts are discovered on your internal network.
Vulnerable Hosts	Displays from the discovered hosts how many have vulnerabilities. For the SKYWATCH WEB the refresh rate is once every day. The information represents data from the last 30 days. This information can be used to monitor how many discovered hosts are vulnerable on your internal network.
Executive Summary Vulnerability Severity Distribution	Displays groups that are being scanned and how many total vulnerabilities they have broken up into varying levels. For the SKYWATCH WEB the refresh rate is once every day. The information represents data from the last 30 days. This information can be used to monitor the amount of vulnerabilities on your network and if they are increasing or decreasing.
Most Vulnerable Host	Displays the top 10 most vulnerable hosts on your network. For the SKYWATCH WEB the refresh rate is once every day. The information represents data from the last 30 days. This information can be used to see which hosts are the weakest and should be addressed first.
Vulnerability Distribution	Displays how many vulnerabilities and in what risk category they belong to on a pie chart. For the SKYWATCH WEB the refresh rate is once every day. The information represents data from the last 30 days. This information can be used to see how many high level vulnerabilities are present on a pie chart.
Top 10 Most Common Vulnerabilities	Displays the top 10 vulnerabilities on your network. For the SKYWATCH WEB the refresh rate is once every day. The information represents data from the last 30 days. This information can be used to see which vulnerabilities are most common and should be addressed first.
Vulnerable Host History	Displays how many vulnerable hosts a network has on a graph over the span of 6 months. For the SKYWATCH WEB the refresh rate is once every day. The information represents data from the last 6 months. This information can be used to see what your network history is with your vulnerable devices.
Vulnerability Severity History	Displays the history of the different levels of the vulnerabilities over the span of 6 months. For the SKYWATCH WEB the refresh rate is once every day. The information represents data from the last 6 months. This information can be used to see what your network history is with your vulnerable devices and their levels of vulnerabilities.

Discovered Host History	Displays the history of the discovered hosts in the network over the span of 6 months. For the SKYWATCH WEB the refresh rate is once every day. The information represents data from the last 6 months. This information can be used to see what your network history is with your discovered devices.
Vulnerabilities Compared To Previous Month	Displays the amount of vulnerabilities on a device currently to how many it had in the previous month. For the SKYWATCH WEB the refresh rate is once every day. The information represents data from the last 60 days. This information can be used to see if your device's vulnerability count is improving.
Open Ports	Displays all of the open ports on each machine in the network. For the SKYWATCH WEB the refresh rate is once every day. The information represents data from the last 7 days. This information can be used to see what ports you have open on your devices and monitor those ports.
Recent Scans	Displays the recent scans on websites, how long they took and how many pages were scanned. For the SKYWATCH WEB the refresh rate is once every day. The information represents data from the last 30 days. This information can be used to monitor your recent website scans.
Vulnerability Counts	Displays the total amount of vulnerabilities broken up into different levels of risk from the recent scans. For the SKYWATCH WEB the refresh rate is once every day. The information represents data from the last 7 days. This information can be used to monitor how many vulnerabilities are on the website scanned and how severe they are.
Vulnerable Pages	Displays the total amount of pages scanned that have vulnerabilities. For the SKYWATCH WEB the refresh rate is once every day. The information represents data from the last 7 days. This information can be used to monitor how many pages from the recent scans are vulnerable.
Risk Distribution	Displays a pie chart of the risk distribution for the vulnerabilities from the scans. For the SKYWATCH WEB the refresh rate is once every day. The information represents data from the last 7 days. This information can be used to monitor what types of vulnerabilities are currently found in the scan.
Vulnerabilities	Displays a table that shows all of the vulnerabilities found in the website scans. For the SKYWATCH WEB the refresh rate is once every day. The information represents data from the last 7 days. This information can be used to monitor which vulnerabilities are more critical then others and should be fixed first.

REPORT	This action button will generate a MSS-VME REPORT based on the data of the dashboard with the corresponding TLP AMBER designation.