

New Module (July 12): Vulnerability Assessment and Management

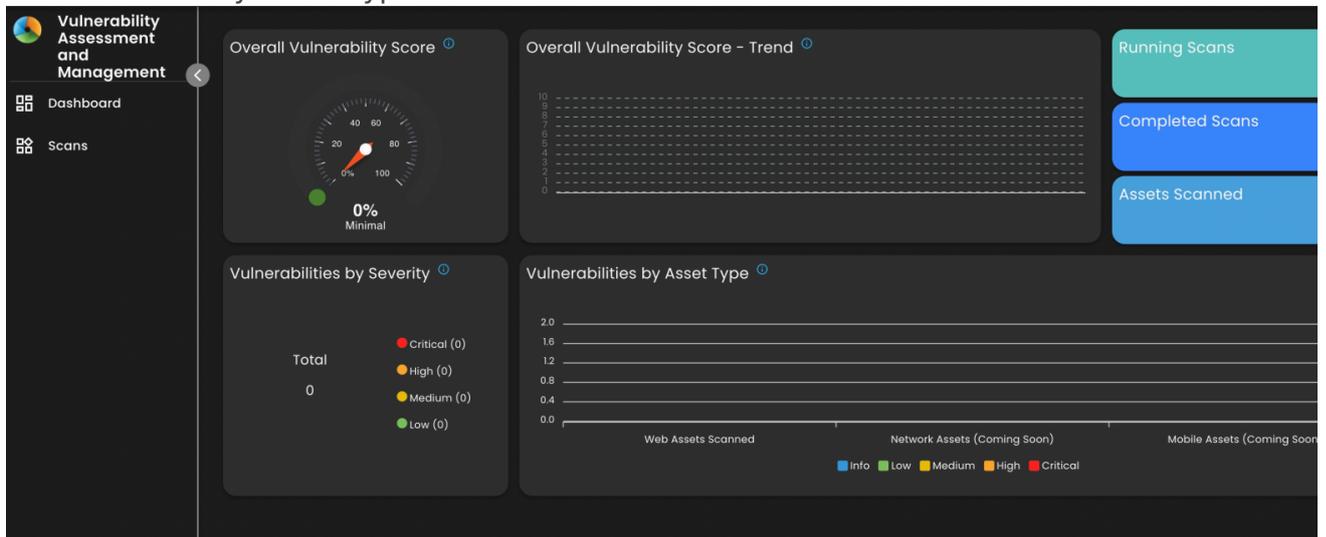
☐ New Module Release

We've just dropped a new module: **Vulnerability Assessment and Vulnerability Management**

☐ New Features:

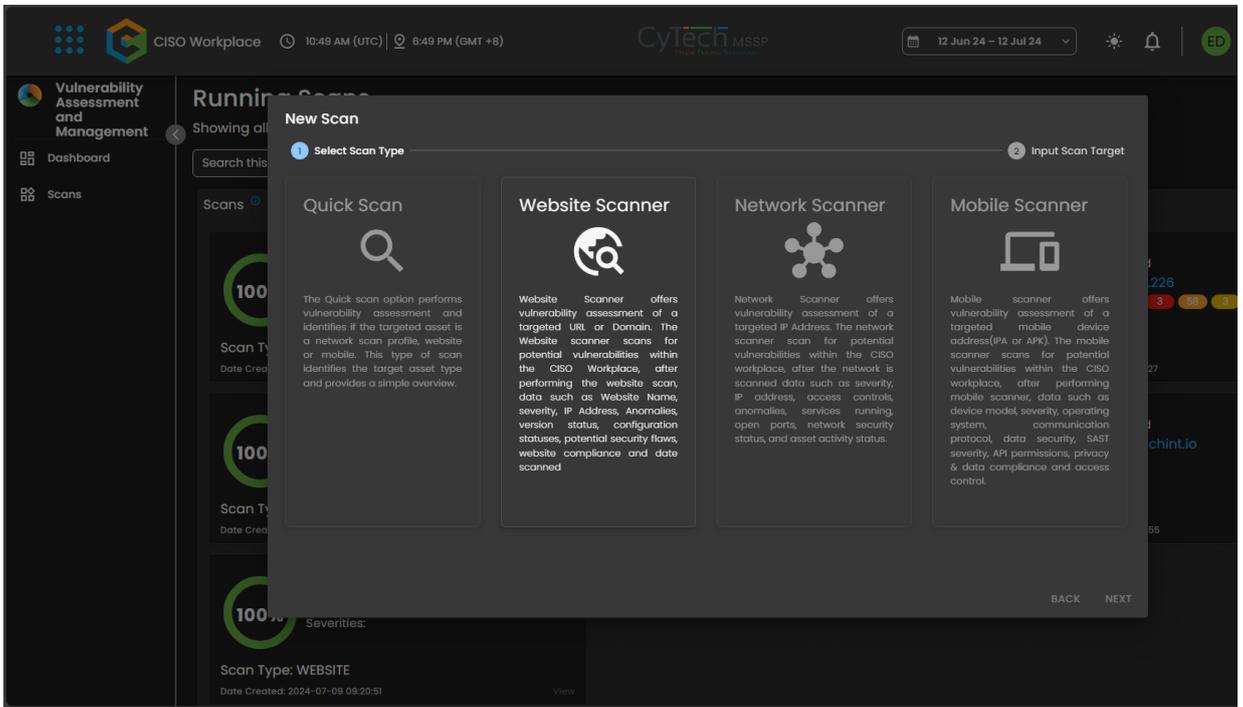
- **Dashboard components:**

- Overall Vulnerability Score
- Overall Vulnerability Score - Trend
- Vulnerabilities by Severity
- Vulnerabilities by Asset Type

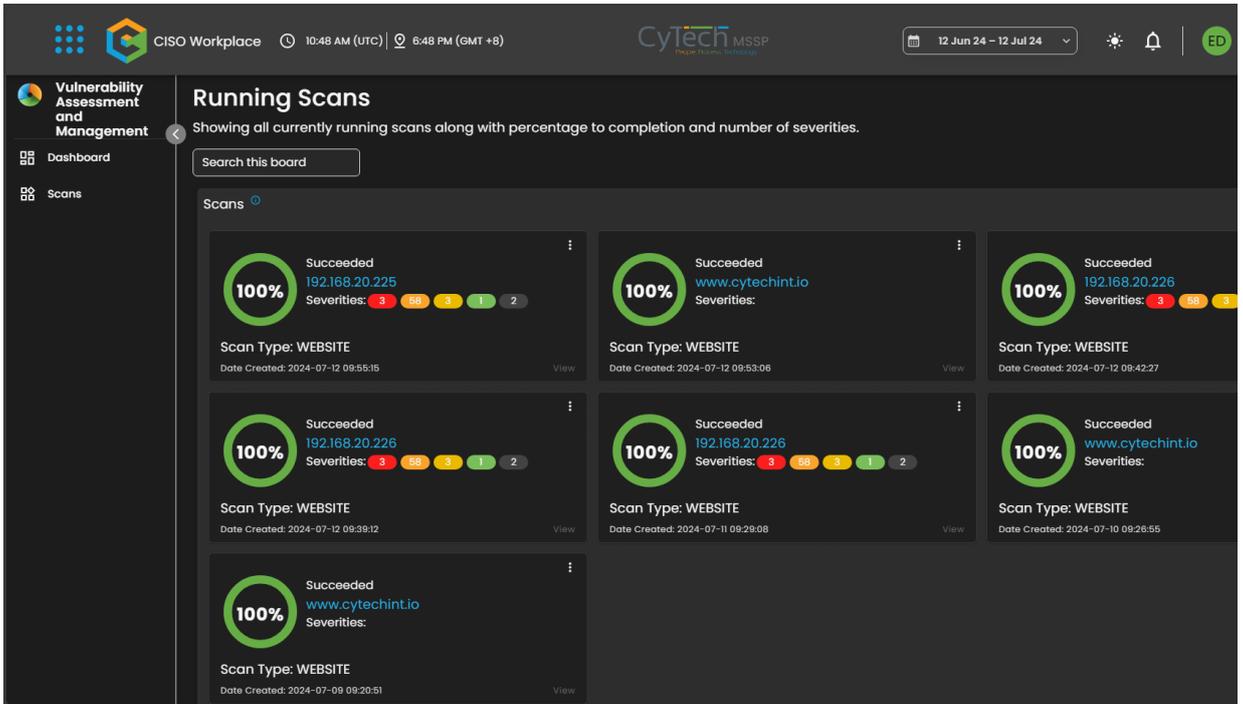


- **Scans Page:** After starting a scan, needs page refresh to see the running scan.

- Scanning Capabilities:
 - Website Scanner only, using NMAP. Network Scanner, Mobile Scanner, and Quick Scan are not yet supported.
 - Able to show CVEs of a website/website port.



○



Asset Details

Asset Name: Nikki Test
 URL: 192.168.20.225
 Hosting Provider: N/A
 Owner: edvirj@cytechint.com
 Asset Type: WEBSITE

Vulnerability Scan Details

Scan Date: July 12th 2024, 9:55:15 am
 Scan Duration: 1 minute(s)
 Total Vulnerabilities Detected: 67

Common Vulnerabilities & Exposures from Target Asset

CVE	Severity Score	Severity	URL
CVE-2023-38408	9.8	High	https://vulners.com/cve/CVE-2023-38408
B8190CDB-3E89-5631-9E28-8064A1575B23	9.8	High	https://vulners.com/github/exploit/B8190CDB-3E89-5631-9E28-8064A1575B23
8FC9C5A8-3968-5F3C-625E-E8D65379A623	9.8	High	https://vulners.com/github/exploit/8FC9C5A8-3968-5F3C-625E-E8D65379A623
PACKETSTORM179290	8.1	High	https://vulners.com/pocketstorm/PACKETSTORM179290
F829ED1-43D7-585C-A197-0D6628820134	8.1	High	https://vulners.com/github/exploit/F829ED1-43D7-585C-A197-0D6628820134
FA3992CE-9C4C-5350-8134-177126E08D3F	8.1	High	https://vulners.com/github/exploit/FA3992CE-9C4C-5350-8134-177126E08D3F
F8981437-1287-5869-93F1-657DFBDC59	8.1	High	https://vulners.com/github/exploit/F8981437-1287-5869-93F1-657DFBDC59
F58A5CB2-2174-586F-9CA9-4C47F8F3885E	8.1	High	https://vulners.com/github/exploit/F58A5CB2-2174-586F-9CA9-4C47F8F3885E
E543E274-C20A-582A-8F8E-F8E3F81C345	8.1	High	https://vulners.com/github/exploit/E543E274-C20A-582A-8F8E-F8E3F81C345
E34FCCCE-228E-5A48-9B1C-BCD6EF7D3257	8.1	High	https://vulners.com/github/exploit/E34FCCCE-228E-5A48-9B1C-BCD6EF7D3257
E24ECC0A-40F7-588C-9E4D-7813522FF915	8.1	High	https://vulners.com/github/exploit/E24ECC0A-40F7-588C-9E4D-7813522FF915
DC798E99-BA77-5F88-9C16-0CF8CDE40E8B	8.1	High	https://vulners.com/github/exploit/DC798E99-BA77-5F88-9C16-0CF8CDE40E8B
DC473885-F54C-5F76-BAFD-D175E4A90CID	8.1	High	https://vulners.com/github/exploit/DC473885-F54C-5F76-BAFD-D175E4A90CID
D85F08E9-D890-55E9-8DD2-22F0198DF360	8.1	High	https://vulners.com/github/exploit/D85F08E9-D890-55E9-8DD2-22F0198DF360
D572250A-BE94-501D-90C4-1A46C9C0AC47	8.1	High	https://vulners.com/github/exploit/D572250A-BE94-501D-90C4-1A46C9C0AC47
CVE-2024-6387	8.1	High	https://vulners.com/cve/CVE-2024-6387
C6FB8D50-F71D-5870-B671-D6A09A95627F	8.1	High	https://vulners.com/github/exploit/C6FB8D50-F71D-5870-B671-D6A09A95627F
C58204A1-8C38-5FF7-5820-ED2078027A0	8.1	High	https://vulners.com/github/exploit/C58204A1-8C38-5FF7-5820-ED2078027A0

Known Issues:

- When there is a running scan, there is no data in the Dashboard. When all scans are finished, there is data present.
- No descriptions for CVEs yet

Stay tuned for more exciting updates!

Revision #3

Created 12 July 2024 15:03:22 by Aldion Pueblos

Updated 16 July 2024 11:59:39 by Aldion Pueblos