



## neo42 Tenable Connector

Mit dem neo42 TenableConnector können Sie die Abarbeitung von Alarmmeldungen aus Tenable heraus automatisieren und in entsprechende Matrix42 Service Desk Tickets überführen

### Unternehmerische Herausforderung

Unternehmen stellen sich immer öfter der Herausforderung Prozesse zu digitalisieren, um Zeit für die wichtigen Dinge zu bekommen. So ist es auch im Bereich der IT-Sicherheit extrem wichtig, Sicherheitslücken schnell zu schließen. Häufig entstehen hier hohe Aufwände bei der Koordination, Eskalation und Benachrichtigung der Systemverantwortlichen.

### Wichtigste Vorteile

Folgende Vorteile bietet die Integration:

- Optimale Transparenz der Schwachstelleninformationen in Matrix42
- Keine weitere Oberfläche für Asset-Verantwortliche
- Automatisierung des Schwachstellen- sowie Eskalationsmanagements

### Lösung

Der neo42 TenableConnector wurde entwickelt, um genau das Problem anzugehen. Er überwacht anhand von Schwellwerten den Lebenszyklus bestehender Schwachstellen und benachrichtigt die Verantwortlichen im Falle eines Verstoßes.

### Technische Komponenten

Zur Nutzung des neo42 TenableConnector für die Enterprise Service Management Lösung der Firma Matrix42 werden die Module Asset Management und Service Desk benötigt, um mit der Tenable Security Center zu interagieren.

### Nutzen

Die Integration von Tenable in die Matrix42-Umgebung bietet eine große Zeitersparnis durch die Automatisierung komplexer Prozesse im Schwachstellenmanagement.



# neo42 Tenable Connector

## Eigenschaften

### Hauptmerkmale:

- Darstellung der Schwachstellen für Asset-Verantwortliche
- Automatisierte Problem- und Aufgabenerzeugung im Eskalationsfall
- Komfortable Bedienung zum Starten von Remediation-Scans über die Matrix42 Oberfläche
- Abgleich der durch Tenable gefunden Netzwerkgeräte mit den Daten des Asset Management der Matrix42-Lösung

## Funktionsweise

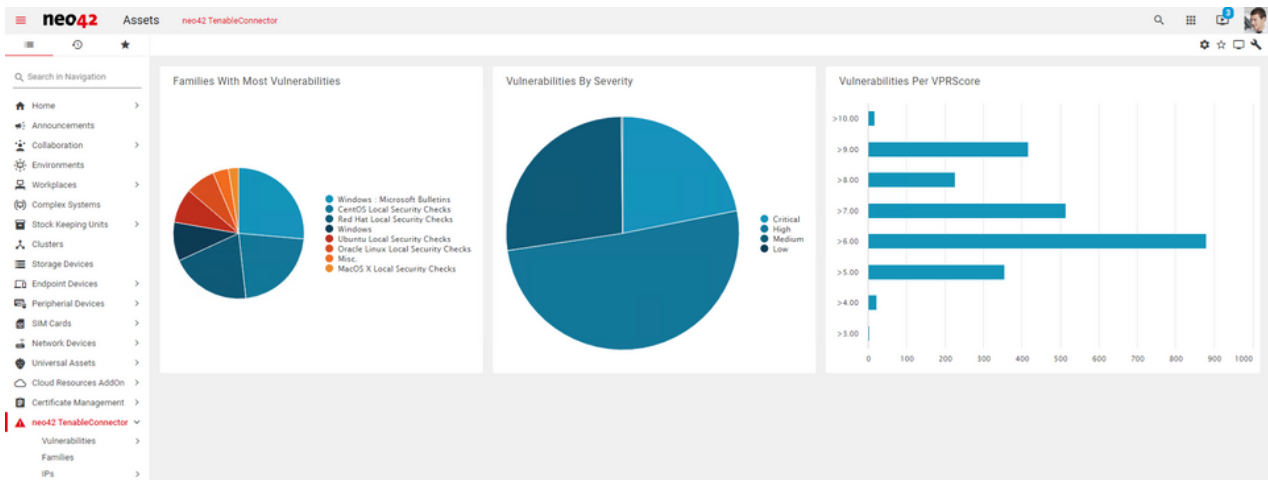
- Automatische Generierung von Problemen im Matrix42 für Findings, welche gegen konfigurierte Schwellwerte verstoßen
- Dynamische Verteilung von Aufgaben an Asset-Verantwortliche über das Problem-Objekt im Matrix42
- Abarbeitung der Aufgaben durch Asset-Verantwortliche, indem diese Patches installieren
- Start eines Remediation-Scans am Asset durch den Bearbeiter
- Regelmäßiger Abgleich der Findings
- Automatische Schließung der Aufgaben & Probleme

PluginID	Name	Severity	Family	VPR Score	CVSS v3 Base	CVSS v3 Temp.	Findings	First Import
20007	20007 (443/6) SSL Version 2 and 3 Protocol Detection	Critical	Service detection	9.8			20	06/14/2022
70210	70210 (21/6) Alcatel OmniSwitch Default Credentials (ftp)	Medium	FTP	9.1	9.1		1	06/14/2022
141369	141369 (161/6) Cisco AireOS Software for Cisco Wireless LAN Controllers (WLC) DoS (cisco-sa-losx-...)	High	CISCO	4.4	8.6	7.5	1	06/14/2022
93113	93113 (0/6) Cisco ASA SNMP Packet Handling RCE (CSCva92151) (EXTRABACON)	High	CISCO	7.4	8.8	8.2	1	06/14/2022
136768	136768 (0/6) Cisco Adaptive Security Appliance Software CSRF (cisco-sa-20190501-asa-csrf)	High	CISCO	5.9	8.8	7.7	1	06/14/2022
136916	136916 (0/6) Cisco Adaptive Security Appliance Software SSL/TLS DoS (cisco-sa-ssl-vpn-dos-qy-...)	Medium	CISCO	4.4	8.6	7.5	1	06/14/2022
141831	141831 (0/6) Cisco Adaptive Security Appliance Software Web Services DoS (cisco-sa-asaftd-webo-...)	High	CISCO	4.4	8.6	7.5	1	06/14/2022
149314	149314 (0/6) Cisco Adaptive Security Appliance Software SSL/TLS Session DoS (cisco-sa-asa-ftd-tc-...)	Medium	CISCO	4.4	8.6	7.5	1	06/14/2022
136890	136890 (23/6) Teleafd - Remote Code Execution (CVE-2020-10188)	Critical	Misc.	7.4	9.8	8.5	1	06/14/2022
23938	23938 (22/6) Cisco Device Default Password	Critical	CISCO	9.7	9.8		2	06/14/2022
108720	108720 (0/6) Cisco IOS Software Quality of Service Remote Code Execution Vulnerability	Critical	CISCO	7.4	9.8	9.1	2	06/14/2022
117949	117949 (0/6) Cisco IOS Software IPv6 Hop-by-Hop DoS Vulnerability (cisco-sa-20180926-ipv6hbh)	High	CISCO	4.4	8.6	7.5	2	06/14/2022
130092	130092 (0/6) Cisco IOS Software IP Service Level Agreement Denial of Service Vulnerability	High	CISCO	4.4	8.6	7.5	2	06/14/2022
131325	131325 (0/6) Cisco IOS Software Internet Key Exchange Memory Leak (cisco-sa-20180328-ike)	High	CISCO	6.0	8.6	8.0	2	06/14/2022
132048	132048 (0/6) Cisco IOS Software Software Plug and Play Agent Memory Leak(cisco-sa-20180926-pn-...)	High	CISCO	4.4	8.6	7.5	2	06/14/2022
133000	133000 (0/6) Cisco IOS Web UI Cross-Site Request Forgery (cisco-sa-20200108-ios-csrf)	High	CISCO	5.9	8.8	7.7	2	06/14/2022
33850	33850 (0/6) Unix Operating System Unsupported Version Detection	Critical	General		10.0		22	06/14/2022
55933	55933 (0/6) Juniper Junos Unsupported Version Detection	Critical	Junos Local Security Checks		10.0		2	06/14/2022
130519	130519 (0/6) Junos OS: J-Web Session Fixation Vulnerability (JSA10961)	Medium	Junos Local Security Checks	5.9	8.8	7.7	2	06/14/2022
133303	133303 (0/6) Juniper_JSA10970	High	Junos Local Security Checks	5.9	8.8	7.7	2	06/14/2022
133860	133860 (0/6) Junos OS: Improper handling of specific IPv6 packets (JSA10982)	High	Junos Local Security Checks	4.4	8.6	7.5	1	06/14/2022
133965	133965 (0/6) Juniper_JSA10979	High	Junos Local Security Checks	5.9	8.8	7.7	2	06/14/2022

Ein Blick auf die Darstellung der Schwachstellen vom neo42 TenableConnector



## neo42 Tenable Connector



Ein Blick auf das Dashboard vom neo42 TenableConnector

### Über neo42

neo42 GmbH ist langjähriger Partner von Matrix42 im deutschsprachigen Raum. neo42 ist spezialisiert auf Matrix42 Lösungen im Bereich Enterprise Service Management, Unified Endpoint Management und Software Asset Management, von der Beratung bis zur Implementierung und anschließendem Support. Außerdem entwickelt neo42 eigene Software Lösungen, wie den Tenable Connector, die das Portfolio optimal ergänzen.

### Über Matrix42

Matrix42 unterstützt Organisationen dabei, die Arbeitsumgebung ihrer Mitarbeiter zu digitalisieren und sicherer zu machen. Die Software für Digital Workspace Experience verwaltet Geräte, Anwendungen, Prozesse und Services einfach, sicher und konform. Die innovative Software integriert physische, virtuelle, mobile und cloudbasierte Arbeitsumgebungen nahtlos in vorhandene Infrastrukturen.

### Über Tenable

Tenable® ist das Unternehmen für Exposure Management. Rund 40.000 Unternehmen aus aller Welt verlassen sich auf Tenable, wenn es um die Erkennung und Minimierung von Cyberrisiken geht. Als Erfinder von Nessus® hat Tenable sein Know-how im Bereich des Schwachstellen-Managements erweitert, um die weltweit erste Plattform bereitzustellen, mit der jedes digitale Asset auf jeder beliebigen Computing-Plattform erkannt und abgesichert werden kann. Zu den Kunden von Tenable zählen ca. 60 Prozent der Fortune 500-Unternehmen, ca. 40 Prozent der Global 2000 sowie große Regierungsbehörden. Weitere Informationen finden Sie auf [de.tenable.com](http://de.tenable.com).