



ANTARES
NETLOGIX

VULNERABILITY LIFECYCLE MANAGER: SCHWACHSTELLEN LANGFRISTIG BEHEBEN

DOMINIK HANDL

Unser Antares Red Team Experte im VLM-Interview

Dominik Handl war jahrelang Leiter des Antares Operations Centers und führt jetzt als Chef des Red Teams Sicherheitsüberprüfungen und Penetrationstests durch. Außerdem plant er IT-Sicherheitsarchitekturen und berät und begleitet unsere Kunden mit seiner reichhaltigen Expertise in sicherheitstechnischen Fragen.



WAS IST EIGENTLICH VULNERABILITY MANAGEMENT UND WO LIEGEN DIE „SCHWACHSTELLEN“ DIESER SYSTEME?

Vulnerability Management hat das Ziel, im Rahmen regelmäßiger Schwachstellen-Scans unterschiedlichste **Sicherheitsrisiken** im Unternehmen **aufzudecken**. Dazu gehören beispielsweise fehlende Patches, Schwachstellen aufgrund von Konfigurationsfehlern oder nicht vertrauenswürdige Zertifikate. Ein Vulnerability Scan liefert jedoch eine **oft unüberschaubare Menge an Ergebnissen**.

Die Kategorisierung dieser Findings, ihre Zuweisung zu den jeweiligen System- oder Software-Verantwortlichen, sowie die Nachverfolgung des Bearbeitungsstandes kosten somit regelmäßig sehr viel Zeit. Weil wir von Antares-Netlogix erkannt haben, dass viele unserer Kunden Unterstützung bei der Handhabung dieser Scans benötigen, haben wir dafür eine **spezielle Lösung entwickelt: Unseren Vulnerability Lifecycle Manager (VLM)**.

WAS SAGEN EURE KUNDEN ZUM VLM?

Für unsere Kunden bietet der VLM echte Vorteile: Sie verfügen endlich über eine **zentrale Anlaufstelle** für ihr Schwachstellen-Management. Anhand **aussagekräftiger Reports und grafischer Darstellungen** können sie die Ergebnisse der Vulnerability Scans einfach und schnell nachvollziehen.

Dabei profitieren sie von der Unterstützung unserer Analysten, die mit ihrer Erfahrung die Einstufungen der Sicherheitslücken zuverlässig vornehmen können. So werden endlich auch Security Reports für den CISO automatisiert ermöglicht. Und natürlich stehen wir mit unseren Services auch bei der Behebung der Sicherheitslücken zur Seite.

WELCHE KERNFUNKTION BIETET DER VLM?

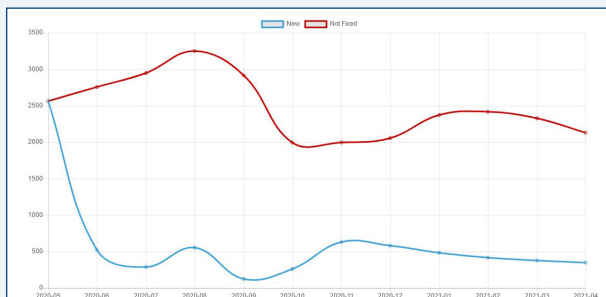
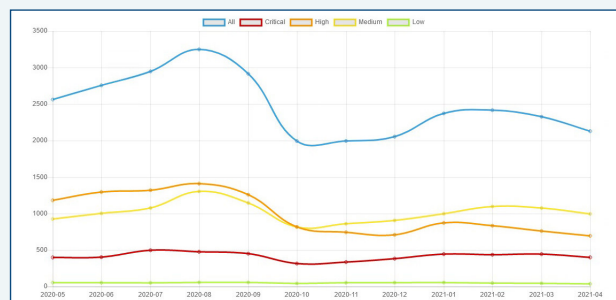
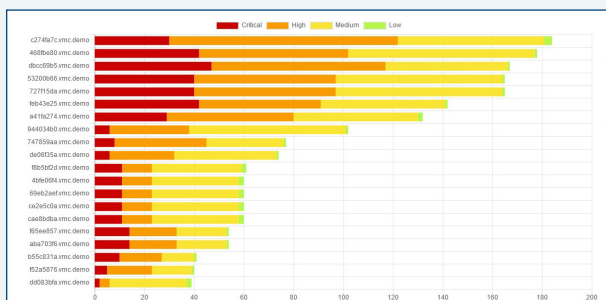
Die Aufgabe des VLM ist es, die genannten **Tasks** weitgehend zu **automatisieren**, damit mehr Zeit auf die eigentliche Behebung der Schwachstellen verwendet werden kann.

Deshalb besteht eine der Kernfunktionalitäten des VLMs in der Möglichkeit, **Verantwortliche für Systeme und Applikationen zu definieren**, denen identifizierte Schwachstellen automatisch zugewiesen werden können.

WOHER KOMMEN DIE DATEN, DIE DER VLM NUTZT?

Die Daten liefern bewährte **Schwachstellen-Scanner** wie Tenable Nessus oder Microsoft Defender Vulnerability Management, die bei vielen unserer Kunden bereits im Einsatz sind. Durch unsere langjährige Erfahrung bringen wir hier detaillierte Produktkenntnisse mit und können auch bei der Implementierung unterstützen.

EINBLICKE IN UNSER VLM



Name	Severity	Host	IP-Address	Alias	Port	New	Site	Date
Unsupported Windows OS (remote)	Critical	13aaace vnc demo	192.168.1.1		445	0	0	2021-08-13 04:10:36
MS000000: Windows Security Update (March 2021)	Critical	3aef1c73 vnc demo	192.168.1.1		445	0	0	2021-05-13 04:15:00
Microsoft Windows 7 / Server 2008 R2 Unsupported Version D.	Critical	131aaace vnc demo	192.168.1.1		445	0	0	2021-05-13 04:14:42
MS000000: Windows Security Update (March 2021)	Critical	69e02baef vnc demo	192.168.1.1		445	0	0	2021-05-13 04:14:42
Unsupported Windows OS (remote)	Critical	7277155a vnc demo	192.168.1.1		445	0	0	2021-01-09 14:42:16
KB4471201: Windows 10 Version 1807 and Windows Server 2.	Critical	8c220a4 vnc demo	192.168.1.1		445	0	0	2020-06-12 10:30:26
Microsoft PowerPoint Viewer Unsupported Version Detection	Critical	43aaf783 vnc demo	192.168.1.1		445	0	0	2020-04-08 19:24:17
Windows Service Pack Out-of-Date	Critical	28a1556d vnc demo	192.168.1.1		445	0	0	2020-05-08 19:11:16
MS16-120: Security Update for Microsoft Graphics Componen.	Critical	f71be4de vnc demo	192.168.1.1		445	0	0	2020-05-08 19:11:28
MS000000: Windows Security Update (March 2021)	Critical	38a2b07d vnc demo	192.168.1.1		445	0	0	2021-04-10 04:16:17
Unsupported Windows OS (remote)	Critical	7a60c03 vnc demo	192.168.1.1		445	0	0	2021-04-10 04:17:22
Adobe Flash Player Unsupported Version Detection	Critical	1425864 vnc demo	192.168.1.1		445	0	0	2021-04-10 04:20:19
Google Chrome - 89.0.4389.114 Multiple Vulnerabilities	Critical	8440340 vnc demo	192.168.1.1		445	0	0	2021-04-10 04:21:25
KB458786: Windows 10 Version 1903 and Windows 10 Vers.	Critical	9d00755a vnc demo	192.168.1.1		445	0	0	2021-04-10 04:20:53
Microsoft Access Unsupported Version Detection	Critical	6d00755a vnc demo	192.168.1.1		445	0	0	2021-04-10 04:20:53
Microsoft Office 365 Unsupported Channel Version Detection	Critical	6d00755a vnc demo	192.168.1.1		445	0	0	2021-04-10 04:20:53

DIE BESTEN FEATURES

Zentrale Verwaltung von Vulnerability-Scannergebnissen für eine beliebige Anzahl von Scannern und automatische Übernahme der Scannergebnisse.

Grafische Aufbereitung von Statistiken (Dashboard), z.B. neue, geschlossene und nicht geschlossene Schwachstellen, PDF-Report / Management-Summary, Delta-Reports im zeitlichen Verlauf.

Zuweisung von Verantwortlichen für Schwachstellenbehebung (Vulnerability Ticketing), Self-Service-Portal für den Kunden, Zwei-Faktor-Anmeldung für die User.