tenable | Datenblatt

Schwachstellen

Die weltweit führende Vulnerability Management-Lösung – mit On-Prem-Verwaltung und erweiterten Priorisierungsfunktionen

Bewerten und beheben Sie Ihre Cyber-Sicherheitslücken

Angesichts sich wandelnder IT-Landschaften und wachsender Cyberbedrohungen bieten periodische Scans und Compliance-Audits keinen wirksamen Schutz vor modernen Cyberangriffen mehr. Um die Sicherheit Ihres Unternehmens zu gewährleisten, ist eine Vulnerability Management-Lösung gefordert, die Ihre Angriffsfläche komplett sichtbar macht, sodass Sie Ihre Cyber Exposure effektiv messen und verwalten können.

Tenable Security Center Plus basiert auf führender Nessus-Technologie und ist eine marktführende Vulnerability Management-Plattform, die ein On-Prem-Schwachstellen-Management der nächsten Generation bietet. Durch erweiterte Analysen sowie anpassbare Dashboards, Berichte und Workflows hilft Ihnen Tenable Security Center Plus dabei, das Schwachstellen-Management in den Griff zu bekommen und das Geschäftsrisiko zu verringern.

Nutzen Sie das Vulnerability Priority Rating (VPR) von Tenable, das Daten und Threat-Intelligence aus mehreren Quellen kombiniert, um die Wahrscheinlichkeit der Ausnutzung einer Schwachstelle vorherzusagen – unter Berücksichtigung der Kritikalität Ihrer dynamischen Assets in einer sich ständig verändernden Umgebung. Das Ergebnis: Sie erhalten Einblick in Schwachstellen sowie in die jeweils betroffenen kritischsten Assets und können diese handlungsrelevanten Erkenntnisse nutzen, um Ihr Unternehmen vor geschäftsschädigenden Sicherheitsverletzungen zu schützen.

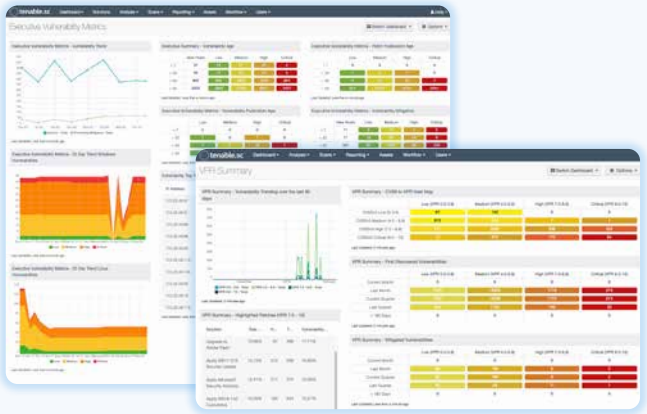

Abbildung 1: Hochgradig anpassbare Dashboards, Berichte, Workflows und Sicherheitsrichtlinien für die spezifischen Anforderungen Ihres Unternehmens

Wichtige Vorteile

- **Kontinuierliche Sichtbarkeit**
  Verfolgen Sie bekannte Assets kontinuierlich und erfassen Sie unbekannte Assets sowie deren Schwachstellen. Identifizieren Sie Bedrohungen und unerwartete Netzwerkveränderungen, bevor sie zu Sicherheitsverletzungen führen.
- **Passive Schwachstellenerkennung**
  Gehen Sie über punktuelle Scans hinaus und beseitigen Sie blinde Flecken durch passive Schwachstellenerkennung für Assets, Protokollerfassung sowie weitere Analysen zur Erkennung von Asset-Änderungen.
- **Priorisieren von Assets und Schwachstellen**
  Die Kombination von Asset- und Schwachstellendaten, Threat-Intelligence und Datenwissenschaft führt zu leicht verständlichen Risikobewertungen. Auf diese Weise lassen sich schnell die Schwachstellen sowie die davon betroffenen kritischsten Assets ermitteln, die das größte Geschäftsrisiko darstellen.
- **Reichweite der Abdeckung**
  Tenable Research arbeitet eng mit der Security-Community zusammen, um neue Schwachstellen aufzudecken und Erkenntnisse bereitzustellen, mit denen Unternehmen ihre Verfahren zur Schwachstellenbewertung optimieren können. Mit mehr als 92.000 Schwachstellen bietet Tenable die branchenweit umfassendste Unterstützung für CVEs und Sicherheitskonfigurationen, damit Sie alle Ihre Risiken nachvollziehen können.
- **Automatisieren von Prozessen**
  Nutzen Sie eine ausführlich dokumentierte API und vorgefertigte Integrationen zum Importieren von Drittanbieterdaten, Automatisieren von Scans sowie zur Weitergabe von Daten an Ihre IT-Systeme.

„Die Komplettlösung von Tenable ist ein echter Volltreffer. Mit ihr kann ich jederzeit Sicherheitsrisiken priorisieren und die Sicherheitslage meines Unternehmens basierend auf den Geschäftszielen bewerten.“

Gesundheitsdienstleister

Wichtige Funktionen

Daten managen, auf Ihre Weise

Tenable Security Center Plus ist die führende On-Prem-Option für Schwachstellen-Management. Verwalten Sie Ihre Daten nach Ihren Vorstellungen mit On-Premises- oder hybriden Bereitstellungsoptionen, die auf Ihre komplexesten Anforderungen abgestimmt sind, und reduzieren Sie gleichzeitig das Risiko für Ihr Unternehmen.

Umfassende Bewertungsoptionen

Tenable Security Center Plus bietet Ihnen eine einheitliche Transparenz über Ihre gesamte Angriffsfläche. Die Lösung setzt Nessus-Sensoren sowie eine Kombination aus aktiven Scannern, Agents, passivem Netzwerk-Monitoring und CMDB-Integrationen ein, um die Scan-Abdeckung in der gesamten Infrastruktur zu maximieren und blinde Flecken bei Schwachstellen zu reduzieren. Dieser Mix aus verschiedenen Datensensoren hilft Ihnen, sowohl bekannte als auch unbekannte Assets sowie deren Schwachstellen zu verfolgen und zu bewerten.

Passive Schwachstellenerkennung

Gehen Sie über punktuelle Scans hinaus und beseitigen Sie blinde Flecken durch passive Schwachstellenerkennung für Assets, Protokollerfassung sowie weitere Analysen zur Erkennung von Asset-Änderungen.

Priorisierung von Schwachstellen anhand des tatsächlichen Risikos

Tenable Security Center Plus kombiniert Schwachstellendaten, Threat-Intelligence und Data Science, um Ihnen einen leicht verständlichen Risiko-Score zu liefern, damit Sie Schwachstellen priorisieren können und wissen, was Sie zuerst beheben müssen. So können Sie Risiken schnell beurteilen und die Schwachstellen mit den größten Auswirkungen auf Ihr Unternehmen identifizieren.

Vereinfachtes Schwachstellen-Management

Durch intuitive Berichte, Dashboard-Visualisierungen und eine benutzerfreundliche Oberfläche werden gängige Aufgaben wie das Konfigurieren von Scans, Durchführen von Bewertungen und Analysieren von Ergebnissen mit Tenable Security Center Plus leichter denn je. Dank vordefinierter Scan-Vorlagen, Konfigurationsprüfungen und Checks für Compliance-Audits, die sich an Best Practices-Frameworks orientieren, benötigen Sie nur noch einen Bruchteil des bisherigen Aufwands, um Ihr Unternehmen zu schützen. Passen Sie Ihre Berichte und Analysen mit vorkonfigurierten, einsatzfertigen Dashboards an oder erstellen Sie mithilfe von Vorlagen eigene Dashboards, die den Anforderungen des Unternehmens gerecht werden.

Proaktive Kontextualisierung von Bedrohungen

Mit Vulnerability Intelligence können Sie Schwachstellen suchen, kontextualisieren und beheben – auf Grundlage der branchenweit umfangreichsten Daten- und Informationsquellen, die von Tenable Research bereitgestellt werden. Durch Normalisierung von 50 Billionen Datenpunkten bietet Vulnerability Intelligence umfassende Deep Dives zu jeder Schwachstelle. Identifizieren Sie wichtige Schwachstellen, die bereits aktiv ausgenutzt werden, oder suchen Sie in natürlicher Sprache oder mithilfe der erweiterten Suche nach bestimmten Schwachstellen.

Asset-Kritikalität nachvollziehen

Nutzen Sie das in Tenable Security Center Plus zur Verfügung stehende Asset Criticality Rating (ACR) von Tenable, um die Priorität von Assets vorherzusagen – basierend auf Indikatoren für geschäftlichen Wert und Kritikalität. Die Kombination von Asset-Kritikalität und Predictive Prioritization bietet einen maßgeschneiderten Ansatz für das Schwachstellen-Management, der aufzeigt, welche Schwachstellen und damit verbundenen Assets priorisiert werden sollten.

Tenable One-Integration

Binden Sie Daten aus Tenable Security Center mühelos in Tenable One ein und gehen Sie von Schwachstellen-Management zu Exposure Management über. Nutzen Sie innovative Funktionen wie Lumin Exposure View, Attack Path Analysis und Asset Inventory, um einen einheitlichen Überblick über Ihre gesamte moderne Angriffsfläche zu erhalten und Ihre Cyber Exposure proaktiv zu managen.

Optimierte Compliance

Mithilfe von vordefinierten Checks, Metriken und proaktiven Warnmeldungen bei Verstößen gegen Branchenstandards und gesetzliche Auflagen können Sie sich ein Bild der Compliance machen und entsprechende Berichte erstellen. Zu den Branchenstandards gehören CERT, NIST, DISA STIG, DHS CDM, FISMA, PCI DSS, HIPAA/HITECH und viele weitere mehr.

Tenable Research

Tenable Security Center Plus wird von Tenable Research unterstützt. Unser Forschungsbereich liefert erstklassige Cyber Exposure-Informationen, datenwissenschaftliche Erkenntnisse, Warnmeldungen und Sicherheitsempfehlungen. Dank häufiger Updates von Tenable Research sind die neuesten Schwachstellen-Checks, Zero-Day-Forschungsergebnisse und Konfigurations-Benchmarks zum Schutz Ihres Unternehmens unmittelbar verfügbar.

Integration mit Tenable Patch Management

Optimieren Sie die Schwachstellenbehebung mit Tenable Patch Management, das branchenführende Priorisierung mit autonomem Patching kombiniert. Gewinnen Sie detaillierte Kontrolle über Bereitstellungen, Tests und Genehmigungen und beheben Sie Schwachstellen parallel dazu auf effiziente Weise und in beliebigem Umfang.

Vorgefertigte Integrationen sowie eine dokumentierte API und ein integriertes SDK

Tenable Security Center Plus verfügt über sofort einsetzbare Integrationen für Credentialed Scanning, SIEM, SOAR, Ticketing- und Patching-Systeme sowie weitere ergänzende Lösungen, sodass Sie Ihren Schwachstellen-Management-Prozess ganz einfach optimieren können. Dank einer vollständig dokumentierten API können Sie zudem ganz einfach eigene Integrationen erstellen. Diese Tools verursachen keine zusätzlichen Kosten, maximieren jedoch den Nutzwert Ihrer spezifischen Anwendungsfälle im Bereich Schwachstellen-Management.

Über Tenable

Tenable®, das Unternehmen für Exposure Management, identifiziert und schließt Sicherheitslücken, die den Wert, die Reputation und die Vertrauenswürdigkeit von Unternehmen gefährden. Die KI-gestützte Exposure Management-Plattform von Tenable bietet umfassende Sichtbarkeit und handlungsrelevante Erkenntnisse entlang der gesamten Angriffsfläche und ermöglicht es Unternehmen, sich vor Cyberangriffen zu schützen – von IT-Infrastrukturen über Cloud-Umgebungen bis hin zu kritischen Infrastrukturen und allen dazwischenliegenden Bereichen. Rund 44.000 Kunden weltweit verlassen sich auf Tenable, wenn es darum geht, Sicherheits- und Geschäftsrisiken zu minimieren. Weitere Informationen finden Sie auf de.tenable.com.

Kontakt

Bitte senden Sie eine E-Mail an sales-de@tenable.com oder besuchen Sie de.tenable.com/contact.

111924