tenable.ep™
exposure platform

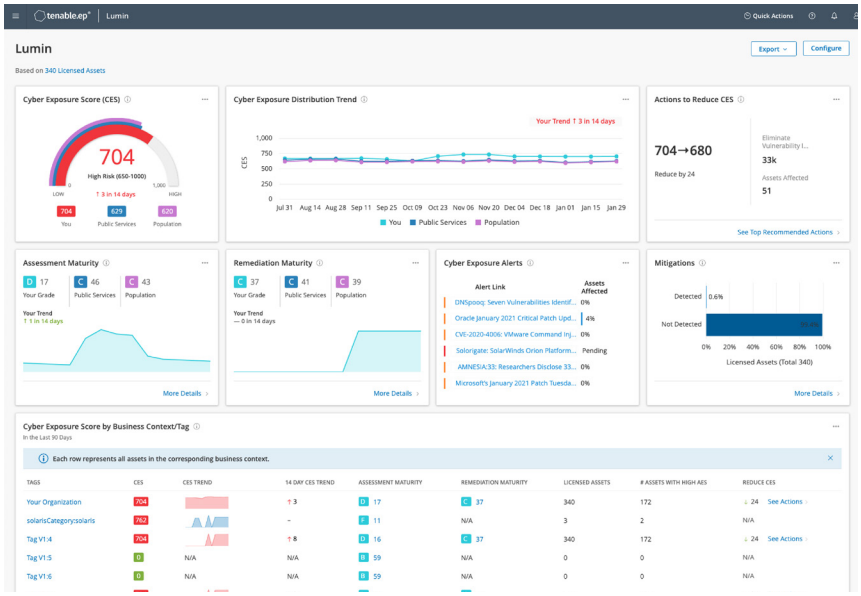
DATENBLATT

TENABLE EXPOSURE PLATFORM

ALLES SEHEN. HANDELN, UM RISIKEN ZU MINDERN. ALLES IN EINEM EINZIGEN PRODUKT.

Tenable.ep bietet vollständigen und kontinuierlichen Einblick in Ihre Cyberrisiken über eine einzige, einheitliche Plattform. Zum ersten Mal können Sie jedes Asset und jede Exposition identifizieren, vorhersagen, bei welchen Schwachstellen die Wahrscheinlichkeit einer Ausnutzung auf Ihren kritischen Assets am höchsten ist, und handeln, um kritische Risiken zu mindern, die Prozessreife zu verbessern und so Ihr Unternehmen abzusichern. Hierzu müssen Sie keine separaten Produkte erwerben und unterschiedliche Lizenzmodelle verwalten.

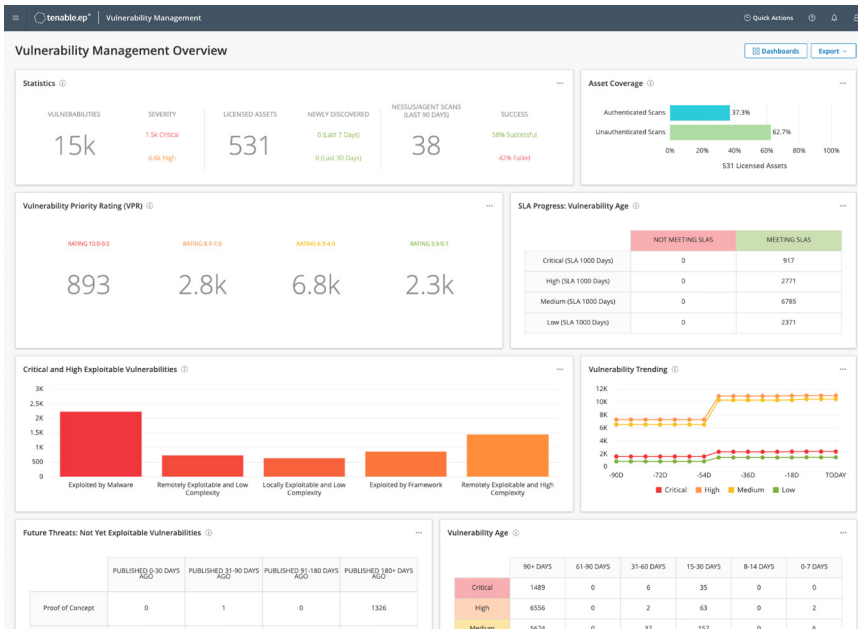
Tenable.ep vereint Tenable.io Vulnerability Management, Tenable.io Web Application Scanning, Tenable.cs, Tenable.ad und Tenable Lumin in einer einzigen Plattform. Nutzen Sie die Vorteile eines einzigen, flexiblen Asset-basierten Lizenzmodells und profitieren Sie einer unkomplizierten Beschaffung und einfachen Bereitstellung. Ein zentrales Dashboard bietet Ihnen einen einheitlichen, risikobasierten Überblick über all Ihre Schwachstellendaten, damit Sie die wichtigsten Schwachstellen und Behebungsmaßnahmen exakt priorisieren können. Sie erhalten Erkenntnisse dazu, wie erfolgreich Sie Ihrer Aufgabe nachkommen, das Cyberrisiko allmählich zu reduzieren. Darüber hinaus können Sie den Reifegrad der Sicherheitsverfahren Ihres Unternehmens messen, um Problembereiche besser zu verstehen und die Effizienz zu verbessern.



Tenable.ep liefert eine objektive Messung des Cyberrisikos in Ihrem gesamten Unternehmen und ermöglicht Benchmark-Vergleiche des Risikos mit ähnlichen Unternehmen der Branche.

WICHTIGE VORTEILE

- **Einheitliche Sichtbarkeit erzielen**
  Beseitigen Sie blinde Flecken, damit Sie Ihre gesamte Angriffsoberfläche im Blick haben – darunter IT-Assets, Cloud-Services, Active Directory-Domänen, OT-Geräte, moderne Web-Apps und Container.
- **Cyberrisiko verstehen**
  Sie erhalten eine objektive Messung des Cyberrisikos im gesamten Unternehmen, sodass Sie fundiertere Entscheidungen treffen können.
- **Effektivität verbessern**
  Identifizieren Sie Bereiche für Prozessverbesserungen, indem Sie Ihre Metriken des Cyberrisiko- und Schwachstellen-Management-Reifegrads mit anderen Unternehmen der Branche vergleichen.
- **Sicherheitsprobleme priorisieren**
  Reduzieren Sie die Anzahl der Schwachstellen, die umgehend Aufmerksamkeit erfordern, mithilfe von Predictive Prioritization um bis zu 97 %.
- **Flexible Lizenzierung**
  Teilen Sie Produktlizenzen gemäß den spezifischen Anforderungen Ihrer Angriffsoberfläche zu und ändern Sie diese Zuteilung nach Bedarf.



Mit Tenable.ep sind Sie in der Lage, sämtliche Assets und Schwachstellen auf Ihrer gesamten Angriffsoberfläche – einschließlich IT, Cloud, Container und Web-Apps – in einer einzigen, einheitlichen Ansicht zu überblicken und zu bewerten.

WICHTIGE FUNKTIONEN

Flexible Asset-basierte Lizenzierung

Tenable.ep wird mit einer einzigen Lizenz betrieben, bei der die Definition des Begriffs „Asset" vereinfacht wurde, um Betriebsabläufe zu optimieren. Ob Webapplikation, Cloud-Instanz, Container-Image, Active Directory-Benutzer oder physischer Server: Bei der Zählung von Assets wird dank des einzigartigen Lizenzmodells von Tenable.ep kein Unterschied gemacht. Das Modell ist überaus flexibel und versetzt Sie in die Lage, Lizenzen Ihren spezifischen Anforderungen gemäß zuzuweisen und diese Zuweisung zu modifizieren, wenn sich Ihre Angriffsoberfläche weiterentwickelt.

Umfassende Bewertungsoptionen

Tenable.ep baut auf Nessus-Technologie auf und setzt aktive Scanner, Web-App-Scanner, Agents, passives Netzwerk-Monitoring und Cloud-Konnektoren ein, um dazu beizutragen, die Scan-Abdeckung in Ihrer 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, einschließlich schwer zu scannender Assets, wie etwa Laptops, und sensible Systeme wie industrielle Steuerungssysteme.

Sichere Cloud-Infrastruktur

Ermöglicht die kontinuierliche Erfassung und Bewertung von Cloud-Ressourcen, ohne dass Sie Agents installieren, einen Scan konfigurieren oder Zugangsdaten verwalten müssen. Erkennen Sie Sicherheitsprobleme schnell, wenn neue Schwachstellen aufgedeckt werden und wenn sich Ihre Cloud-Umgebung durch das Hoch- und Herunterfahren von Instanzen verändert. Prüfen und dokumentieren Sie die Einhaltung von Branchenstandards und bewährten Best Practices wie CIS, PCI und DSGVO. Nutzen Sie über 1.800 Richtlinien aus 20 verschiedenen Standards für eine umfassende Prüfung. Zudem besteht die Möglichkeit, benutzerdefinierte Richtlinien auf Basis Ihrer individuellen Anforderungen zu erstellen.

Infrastructure as Code absichern

Überprüfen Sie IaC-Vorlagen (Infrastructure as Code) – einschließlich Terraform, AWS CloudFormation, Azure Resource Manager und Kubernetes – auf Richtlinienverstöße. Integrieren Sie Cloud-Infrastruktursicherheit in die DevOps-Pipeline, um zu verhindern, dass Sicherheitsprobleme in Produktionsumgebungen gelangen. Beheben Sie IaC-Fehlkonfigurationen im Handumdrehen direkt in Entwicklungstools, um Richtlinien während der Build-Time- und Runtime-Phasen durchzusetzen. Ermitteln Sie Unstimmigkeiten zwischen IaC und der laufenden Cloud-Umgebung, um einen Drift der Cloud-Sicherheitslage zu verhindern.

Automatisiertes Scannen von Webapplikationen

Angesichts des Mangels an Experten für Anwendungssicherheit sind Lösungen gefordert, die Automatisierungsmöglichkeiten bieten, sodass unterbesetzte Sicherheitsteams entlastet werden können. Mit Tenable.ep bewerten Sie Ihre gesamten Webapplikationen schnell und mühelos – dank einer hochgradig automatisierten Lösung, die den manuellen Arbeitsaufwand verringert. Gewinnen Sie Einblick in OWASP Top-10-Schwachstellen sowie Schwachstellen von Web-App-Komponenten und stellen Sie Entwicklern ausführliche Behebungsanweisungen zur Verfügung.

Kubernetes- und Container-Sicherheit

Verschaffen Sie sich Einblick in den Sicherheitsstatus Ihrer Container-Images und -Infrastruktur. Integrieren Sie Sicherheitstests für neue Container-Images und Kubernetes-Konfigurationen in DevOps-Pipelines, um zu gewährleisten, dass neue Builds und IaC den Unternehmensrichtlinien entsprechen. Zeigen Sie Schwachstellendaten, Paketverzeichnisse und Fehlkonfigurationen all Ihrer Container-Images und Kubernetes-Infrastruktur an. Synchronisieren Sie Container-Images aus Drittanbieter-Registrys, um diese kontinuierlich auf neu aufgedeckte Schwachstellen zu prüfen. Sorgen Sie für die Sicherheit von Kubernetes-Bereitstellungen und verhindern Sie Konfigurationsdrift.

Vereinfachtes risikobasiertes Schwachstellen-Management

Durch eine moderne Benutzeroberfläche mit intuitiven Dashboard-Visualisierungen werden gängige Aufgaben wie das Konfigurieren von Scans, Durchführen von Bewertungen und Analysieren von Ergebnissen mit Tenable.ep leichter denn je. Dank vordefinierter Scan-Vorlagen und Konfigurationsprüfungen, die sich an Best-Practices-Frameworks wie CIS und DISA STIG 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.

Priorisierung von Schwachstellen anhand des tatsächlichen Risikos

Tenable.ep priorisiert Schwachstellen auf Grundlage der Wahrscheinlichkeit ihrer Ausnutzung bei einem Angriff. Dazu werden über 150 Datenquellen kombiniert, darunter Schwachstellen- und Bedrohungsdaten von Tenable und Dritten. Mithilfe eines proprietären maschinellen Lernalgorithmus werden jene Schwachstellen identifiziert, bei denen die Wahrscheinlichkeit einer Ausnutzung am größten ist. So können Sie sich zuerst auf die Sicherheitsprobleme konzentrieren, die für Ihr Unternehmen am wichtigsten sind.

Absicherung von Active Directory zur Versperrung von Angriffspfaden

Entdecken und priorisieren Sie Schwachstellen in Ihren bestehenden Active Directory-Domänen proaktiv und reduzieren Sie Ihre Gefährdung durch schrittweise Anleitungen zur Behebung. Profitieren Sie von einer lückenlosen Überwachung und erkennen Sie gegen Active Directory gerichtete Angriffe wie Golden Ticket, DCShadow, Brute Force, Password Spraying, DCSync usw. Die Absicherung von Active Directory kann dazu beitragen, Angreifer aufzuhalten, ihre potenziellen Aktivitäten zu unterbinden und sicherzustellen, dass weniger Sicherheitsverletzungen zu einer Ausweitung von Rechten, Lateral Movement oder der Ausführung von Malware führen.

Behebungsempfehlungen auf Basis des tatsächlichen Risikos

Tenable.ep stellt Sicherheitsteams eine Liste mit Empfehlungen der wichtigsten Maßnahmen zur Verfügung, mit denen sich Cyber Exposure möglichst umfassend reduzieren lässt, damit aus Geschäftsentscheidungen zur Risikobereitschaft technische Maßnahmen für Teams abgeleitet werden können. Teams können detaillierte Daten zu konkreten Schwachstellen und Assets anzeigen, um zusätzliche Informationen zum geschäftlichen und Risikokontext zu erhalten und so effektivere Behebungsmaßnahmen zu ermöglichen.

Cyber Exposure berechnen und kommunizieren

Tenable.ep ermöglicht eine objektive Messung des Cyberrisikos mithilfe des Cyber Exposure Score (CES). Dabei werden Schwachstellendaten mit anderen Risikoindikatoren wie Threat-Intelligence und Asset-Kritikalität kombiniert. Der Wert wird automatisch mithilfe von maschinellen Lernalgorithmen berechnet, wobei die Wahrscheinlichkeit der Ausnutzung einer Schwachstelle und die geschäftliche Kritikalität des betroffenen Assets berücksichtigt werden. Der CES-Wert kann für eine beliebige Gruppe von Assets ermittelt werden, von einem einzelnen Asset bis hin zu allen Assets im gesamten Unternehmen, um detaillierte Analysen und eine fundierte Entscheidungsfindung zu ermöglichen.

Prozessreife-Metriken

Tenable.ep liefert wichtige Kennzahlen für Bewertung und Behebung, die Ihnen helfen, die Effektivität von Programmen und die Cyberhygiene zu verbessern. Das Produkt stellt detaillierte Analysen der Bewertungshäufigkeit, Bewertungstiefe sowie der Reaktionsfähigkeit und Abdeckung von Behebungsmaßnahmen in Ihrem Unternehmen bereit, um Defizite aufzuzeigen, Vergleiche mit ähnlichen Unternehmen anzustellen und umsetzbare Empfehlungen zu ermitteln, mit denen Sie Ihre Werte verbessern können.

Externes und internes Benchmarking

Tenable.ep ermöglicht es Sicherheitsteams, sich mit anderen Unternehmen der Branche und internen Betriebsgruppen zu vergleichen, um Defizite und Stärken schnell zu erkennen. Das Produkt erstellt Benchmarks für eine Reihe von Schlüsselkennzahlen wie Cyber Exposure Score, Assessment Maturity und Remediation Maturity auf der Grundlage von Branchen- und Gesamtdurchschnittswerten, um zu analysieren, wie Unternehmen im Vergleich abschneiden. Das Benchmarking von Tenable.ep beruht auf der umfangreichsten Vulnerability Intelligence der Branche. Dabei werden über 20 Billionen Aspekte von Bedrohungs-, Schwachstellen- und Asset-Daten verarbeitet, um in Kombination mit datenwissenschaftlichen Analysen umfassende und präzise Informationen zu liefern.

Vorgefertigte Integrationen sowie eine dokumentierte API und ein integriertes SDK

Tenable.ep verfügt über vorgefertigte Integrationen für gängige Credential Management-Lösungen, SIEM, Ticketing-Systeme und weitere ergänzende Lösungen, sodass Sie problemlos einen effizienten Prozess für das Schwachstellen-Management einrichten können. Eine vollständige Liste finden Sie hier: https://de.tenable.com/partners/technology. Dank einem vollständig dokumentierten API-Set und SDK können Sie mit Tenable.ep zudem ganz einfach eigene Integrationen erstellen. Für diese Tools, die den Nutzen Ihrer Schwachstellendaten maximieren, fallen keine Zusatzkosten an.

SLA mit Verfügbarkeitsgarantie

Mit einer robusten Service-Level-Vereinbarung (SLA) für Tenable.ep bietet Tenable die erste und einzige Verfügbarkeitsgarantie der Branche für Schwachstellen-Management. Sollte die SLA nicht eingehalten werden, erhält der Kunde eine entsprechende Servicegutschrift, genau wie bei führenden Cloud-Anbietern wie Amazon Web Services.

Unterstützt von Tenable Research

Tenable.ep 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.

Weitere Informationen: Besuchen Sie de.tenable.com
Kontakt: Bitte senden Sie eine E-Mail an sales-de@tenable.com oder besuchen Sie de.tenable.com/contact