tenable | Datenblatt

Exposure Management-Plattform Tenable One

Die einzige KI-gestützte Exposure Management-Plattform

Angreifern stets einen Schritt voraus

Bedrohungsakteure halten sich nicht an Silos im Sicherheitsbereich. Sie suchen nach Schwachstellen aller Art, um sie auszunutzen und sich seitwärts durch die Umgebung fortzubewegen. Doch die Tools, auf die wir uns zur Absicherung der Angriffsfläche verlassen, konzentrieren sich nach wie vor auf einzelne Technologien – Cloud, Identität, IT, OT, IoT, Anwendungen – und erzeugen eine enorme Menge unnötiger Daten. Ihnen fehlt die kritische „Angreiferperspektive“: eine bereichsübergreifende Ansicht der Beziehungen zwischen Assets, Identitäten und Risiken,, durch die Angriffe ermöglicht werden, und noch wichtiger – der Auswirkungen auf das Unternehmen, ob bezogen auf Umsatz, Datenhoheit, Compliance oder andere kritische Messgrößen.

Als einzige Plattform für lückenloses Exposure Management vereinheitlicht Tenable One Sichtbarkeit, Erkenntnisse und Maßnahmen auf der gesamten Angriffsfläche radikal. Sie bietet modernen Unternehmen das notwendige Rüstzeug, um vorrangige Cyberrisiken zu isolieren und zu beseitigen – angefangen bei IT-Infrastrukturen über Cloud-Umgebungen bis hin zu kritischen Infrastrukturen und allen dazwischen liegenden Bereichen. Mithilfe von Tenable One können Unternehmen inmitten einer Flut von nebensächlichen Feststellungen erkennen, welche Risikokombinationen tatsächlich eine Gefährdung darstellen. Dies führt zu höherer Produktivität des vorhandenen Personals und gezielteren Investitionen, die dazu beitragen, die Sicherheitslage und Compliance insgesamt zu optimieren.

Gewinnen Sie mit einem einheitlichen Ansatz

Tenable One ist eine einzigartige Plattform, die entwickelt wurde, um die zentrale Herausforderung moderner Sicherheit zu meistern: ein zutiefst uneinheitlicher Ansatz bei der Erkennung und Bekämpfung von Cyberrisiken.

Einheitliche Sichtbarkeit

Führen Sie unternehmensweite Ansichten des Cyberrisikos auf der gesamten Angriffsfläche zusammen und decken Sie die Lücken auf, die Ihr Unternehmen anfällig für Angriffe auf allen Arten von Assets und Übertragungswegen machen.

Einheitliche Erkenntnisse

Analysieren Sie Kontext und Erkenntnisse über Cyberrisiken auf der gesamten Angriffsfläche und stellen Sie Zusammenhänge her, um die wahren Gefährdungen zu erkennen, die den Wert, die Reputation und die Vertrauenswürdigkeit Ihres Unternehmens bedrohen.

Vereinheitlichte Maßnahmen

Vereinen Sie Führungskräfte und Sicherheitsteams im gemeinsamen Kampf gegen Risiken und mobilisieren Sie alle Unternehmensressourcen, um Sicherheitsrisiken mit der höchsten Angriffswahrscheinlichkeit und den größten Auswirkungen auf das Geschäft aufzuspüren und zu beheben.

Wichtige Vorteile

- Informieren Sie den Vorstand, Geschäftsbereiche und Teams ganz einfach über die Risikolage.
- Senken Sie Cyberrisiken in messbarem Umfang und weisen Sie parallel dazu Compliance nach.
- Konsolidieren Sie Tools und priorisieren Sie Investitionen in Bereichen, in denen sie die größte Wirkung entfalten.
- Optimieren Sie Produktivität, reduzieren Sie Personalfluktuation und skalieren Sie begrenzte Ressourcen und Kompetenzen.

Einheitliche Sichtbarkeit

Erfassung der gesamten Angriffsfläche

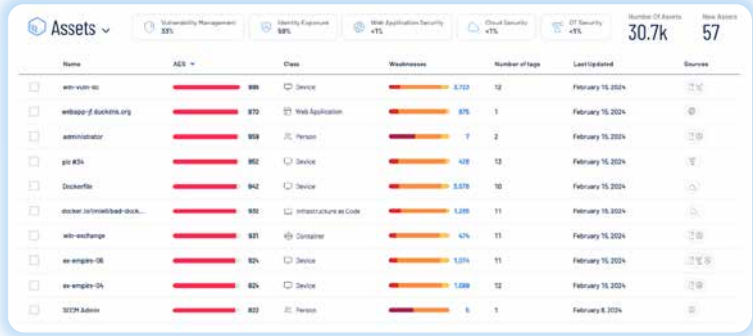
Eliminieren Sie blinde Flecken durch eine umfassende Erfassung Ihrer Angriffsfläche, einschließlich extern und intern zugänglicher Assets: Cloud, IT, OT, IoT, Container, Kubernetes, Anwendungen und verborgene Assets sowie Personen- und Maschinenidentitäten.

Identifizierung von Asset- und identitätsbezogenen Risiken

Bewerten Sie Assets und Identitäten und gewinnen Sie einen umfassenden Überblick über die drei Arten von Risiken, die sämtliche Angriffe möglich machen: Schwachstellen, Fehlkonfigurationen und übermäßige Berechtigungen – On-Premises wie auch in all Ihren Clouds.

Vereinheitlichung Ihres Asset-Bestands

Die Assets und Identitäten auf Ihrer gesamten Angriffsfläche sind in einer zentralen Ansicht zusammen mit fundierten Asset-Informationen sichtbar, darunter Details zur Asset-Konfiguration, Schwächen, Tagging, Asset Criticality Rating (ACR), allgemeiner Asset Exposure Score (AES), zugehörige Angriffspfade und vieles mehr.



„Unsere Sicherheitsgefährdungen in einer gemeinsamen Ansicht überblicken zu können, ist sehr wichtig. Tenable One hilft uns, kostspielige Einzellösungen zu konsolidieren und über eine zentrale, einheitliche Ansicht einen besseren umfassenden Einblick in unsere gesamte Angriffsfläche zu gewinnen.

Die Reporting-Funktion in Tenable One ist zudem eine Triebfeder für den geschäftlichen Bereich. Ob zur Kommunikation der Cybersecurity-Lage an den Vorstand oder zur Erstellung eines detaillierten Maßnahmenplans für das Team – auf Knopfdruck können wir ganz einfach Berichte vorlegen, die für jedes Zielpublikum geeignet sind.“

Stellvertretender CISO,
Fortune 500-Unternehmen

Einheitliche Erkenntnisse

Bereichsübergreifende Normalisierung von Risikobewertungen

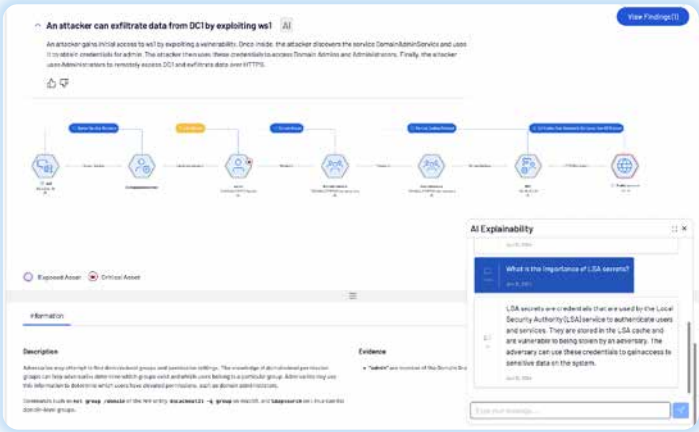
Nutzen Sie einen konsistenten Ansatz zur Messung von Risiken – über Risiko-Arten und Asset-Klassen hinweg. Das Vulnerability Priority Rating (VPR) bewertet statische und dynamische Variablen in der sich verändernden Bedrohungslandschaft, wie etwa die Verfügbarkeit von Exploit-Code und die Nutzungshäufigkeit durch Angreifer, um Risiko-Scores ständig anzupassen. Das VPR wird mit dem ACR kombiniert, um den allgemeinen AES für jedes Asset zu berechnen. Dadurch können Teams schnell bewerten, welche Assets das größte Risiko für das Unternehmen darstellen – für eine priorisierte Behebung.

Priorisierung von Angriffspfaden, die zu den „Kronjuwelen“ führen

Attack Path Analysis vermittelt ein detailliertes Verständnis der Asset-, Identitäts- und Risikobeziehungen, die von Angreifern zur Kompromittierung der sinnbildlichen Kronjuwelen ausgenutzt werden können – Assets, die mit einem hohen Potenzial für gravierende Schäden im Unternehmen einhergehen. Suchen Sie in einer nach Prioritäten geordneten Liste der Angriffspfade ganz einfach nach gängigen Angriffspfad-Signaturen, die in aufsehenerregenden Angriffen (z. B. SolarWinds) zum Einsatz kamen, und gewinnen Sie Einblick in spezifische MITRE-Techniken. Darüber hinaus erhalten Sie eindeutige Erklärungen zu jedem einzelnen Schritt – dank generativer KI und Abfragen in natürlicher Sprache.

Skalierung von Behebungsmaßnahmen mithilfe von Choke Points

Greifen Sie schnell auf Detailinformationen zu Choke Points mitsamt entsprechenden Behebungsempfehlungen zu, anstatt jede Feststellung bzw. jeden Einzelschritt innerhalb eines Angriffspfads zu untersuchen und zu beseitigen. Durch Einblick in Angriffspfade und Choke Points ist für das Sicherheitspersonal erkennbar, welche Behebungsmaßnahme die potenziell gefährlichsten Angriffspfade zu den Kronjuwelen beseitigt. Unnötige Nebensächlichkeiten, die Personalfluktuation und reduzierte Produktivität zur Folge haben, werden dadurch reduziert.



Vereinheitlichte Maßnahmen

Geschäftsorientierte Ansichten der Exposure

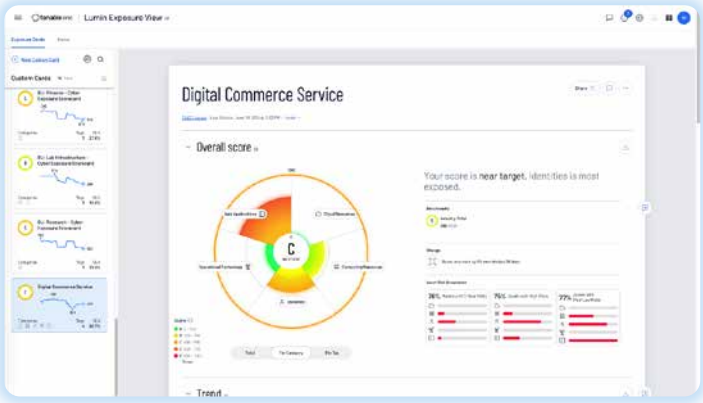
Globale und benutzerdefinierte Exposure-Karten in Lumin Exposure View ermöglichen gezielte Sicherheitsmaßnahmen. Hierzu liefern sie eine klare, geschäftsorientierte Ansicht der Sicherheitslage im gesamten Unternehmen, geordnet nach dem jeweiligen Bereich oder einer beliebigen logischen Asset-Gruppierung.Unternehmen können beispielsweise benutzerdefinierte Exposure-Karten für einen kritischen Business-Service oder Prozess erstellen – oder geordnet nach Anbieter, wie beispielsweise dem jeweiligen Gerätehersteller. Der Cyber Exposure Score (CES) aggregiert die einzelnen AES-Bewertungen für sämtliche Assets in einer Exposure-Karte, wodurch eine individuell zugeschnittene Quantifizierung der Sicherheitslage zur Verfügung steht.

Nachverfolgung von Trends und Optimierung von Investitionen

Trend-Ansichten, SLA-Tracking und Tag-Performance helfen bei der Beantwortung entscheidender Fragen, wie z. B.:

- Wie hat sich unsere Sicherheitslage im Laufe der Zeit verändert?
- Welche Bereiche bzw. Funktionsbereiche erfordern zusätzliche Investitionen?
- Erfüllen wir unsere Remediation-Vorgaben?

Dies führt zu einer besseren Kommunikation und strategischen Abstimmung der Ziele und Budgetausgaben zwischen Stakeholdern und Teams.



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 dazwischen liegenden Bereichen. Mehr als 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.

082024