Ivanti Neurons for Risk-Based Vulnerability Management (RBVM)

Entwickeln Sie Ihre Strategie zur Verwaltung von Schwachstellen mit Ivanti Neurons for RBVM zu einem risikobasierten Ansatz weiter. Mit diesem SaaS-Angebot können Sie die Sicherheitslücken und Schwachstellen, die für Sie das größte Risiko darstellen, effizient und effektiv priorisieren und beheben, um sich besser vor Datenmissbrauch, Ransomware und anderen Cyber-Bedrohungen zu schützen.

Zeit für einen neuen Ansatz bei der Verwaltung von Schwachstellen

Es gibt über 270.000 bekannte Schwachstellen[1] Glücklicherweise müssen Unternehmen nicht jede Sicherheitslücke und Schwachstelle beheben, die in ihren IT-Umgebungen auftritt. Leider ist die Identifizierung der seltenen Schwachstellen oder Schwachstellen, die ein erhebliches Risiko darstellen, für Unternehmen, die herkömmliche Ansätze zur Verwaltung von Schwachstellen verwenden, ein zeitaufwändiger und fehleranfälliger Prozess.

Bevor solche Unternehmen überhaupt damit beginnen können, Sicherheitslücken und Schwachstellen für die Behebung zu priorisieren, müssen sie zunächst eine Reihe unterschiedlicher Daten sammeln – von Scannerbefunden bis hin zu Informationen über Bedrohungen (Bedrohungsintelligenz), diese Daten normalisieren und für die Verwendung vorbereiten. Wenn diese Prozesse manuell durchgeführt werden, kann es Tage, Wochen oder Monate dauern, bis sie abgeschlossen sind, und es können sich immer menschliche Fehler einschleichen.

Der Prozess der Priorisierung ist nicht besser. Berücksichtigen Sie Ransomware-Schwachstellen. Vierundsiebzig Prozent sind nach CVSS v3 nicht als kritisch eingestuft und 156 fehlen im KEV-Katalog (Known Exploited Vulnerabilities) der CISA. Darüber hinaus wurden bei drei sehr beliebten Scannern noch immer keine Plugins und Erkennungssignaturen für insgesamt 20 Ransomware-Schwachstellen hinzugefügt.[2]

Und zu allem Überfluss nennen Sicherheits- und IT-Entscheidungsträger die mangelnde Zusammenarbeit zwischen ihren Teams als größte Herausforderung bei der Abwehr von Cyberangriffen.[3] Diese Unstimmigkeiten zwischen den Stakeholdern bei der Verwaltung von Schwachstellen können die Behebung von Problemen verlangsamen und das Unternehmen anfällig für Angriffe machen.

WichtigeFähigkeiten

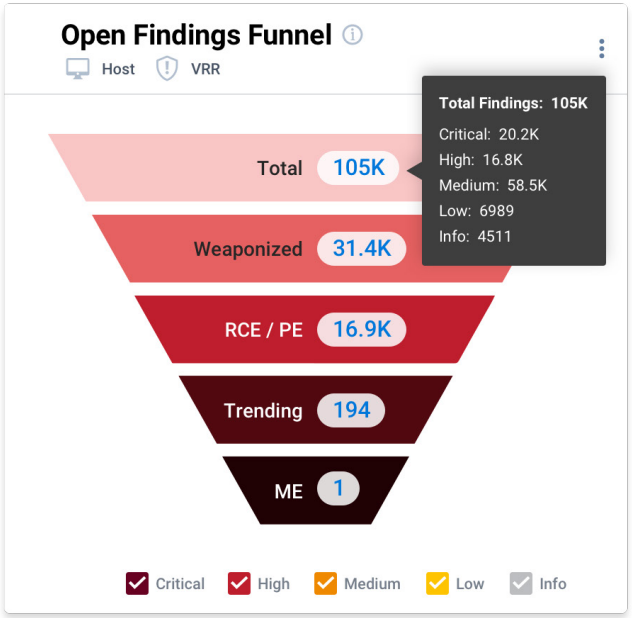
Priorisieren Sie Sofortmaßnahmen auf der Grundlage des Bedrohungsrisikos

Mit einer kontextbezogenen, risikobasierten Ansicht der Cybersicherheitslage Ihres Unternehmens können Sie innerhalb von Minuten – und nicht erst nach Monaten – von der Erkennung von Schwachstellen und Sicherheitslücken zu deren Behebung übergehen. Ivanti Neurons for RBVM misst Risiken und priorisiert Abhilfemaßnahmen durch einen Prozess, der eine kontinuierliche Korrelation der Infrastruktur eines Unternehmens einschließt:

- Interne und externe Schwachstellendaten.
- Bedrohungsintelligenz.
- Manueller Pen-Test und forschungsbasierte Erkenntnisse.
- Kritikalität der geschäftlichen Assets.

Und das Beste daran: Sie erhalten einen fundierten Aktionsplan, der wenig bis gar keinen manuellen Aufwand erfordert.

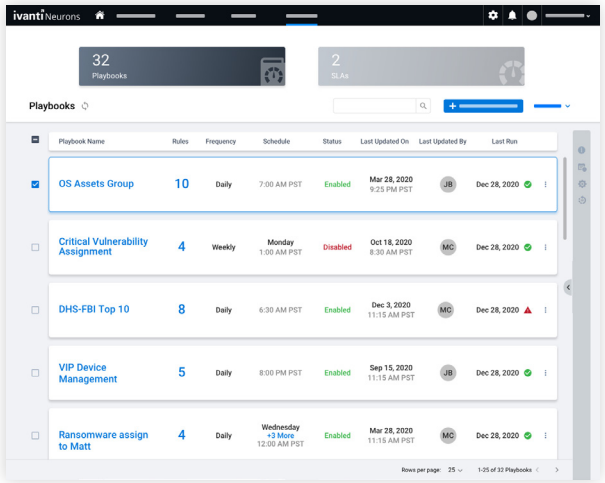
Im Gegensatz zu CVSS können Unternehmen mit dem von Ivanti entwickelten Vulnerability Risk Rating (VRR) die Auswirkungen genau messen und die Wahrscheinlichkeit bestimmen, dass eine Sicherheitslücke ausgenutzt wird. Ivanti Neurons for RBVM identifiziert auch speziell Remote-Code-Ausführung, Privilegienerweiterung, Ransomware sowie aktuelle und aktive Schwachstellen. Diese Informationen helfen Unternehmen, sich auf die Schwachstellen zu konzentrieren, die für sie das größte Risiko darstellen.



Konzentrieren Sie sich auf Abhilfemaßnahmen, nicht auf Verwaltung

Verbessern Sie Ihre Cybersicherheit ohne den damit verbundenen Zeit-, Arbeits- und Fehleraufwand durch eine Reihe von Automatisierungen und anderen effizienzsteigernden Funktionen:

- Erstellen Sie Ablaufpläne, um häufige oder sich wiederholende Aufgaben zu automatisieren, die traditionell von Sicherheitsanalysten durchgeführt werden.
- Legen Sie Fälligkeitstermine für die Schließung von Sicherheitslücken automatisch fest, falls gewünscht mit Service-Level-Automatisierungen.
- Erhalten Sie nahezu in Echtzeit Warnmeldungen außerhalb des Produkts, die auf eine Produktseite mit Informationen zu dem betreffenden Ereignis verweisen.
- Filtern Sie Hosts und Host-Ergebnisse einfach nach Trendkriterien, die ihre Gefährdung durch die wichtigsten kritischen Schwachstellen – wie Ransomware und aktuelle CVEs – aufzeigen, indem Sie Systemansichten verwenden, die vom Ivanti-Sicherheitsteam bereitgestellt werden.
- Priorisierte Schwachstellen werden direkt an Ivanti Neurons for Patch Management zur Behebung weitergeleitet – kein Versenden von CSVs mit CVE-IDs per E-Mail und Chat mehr.

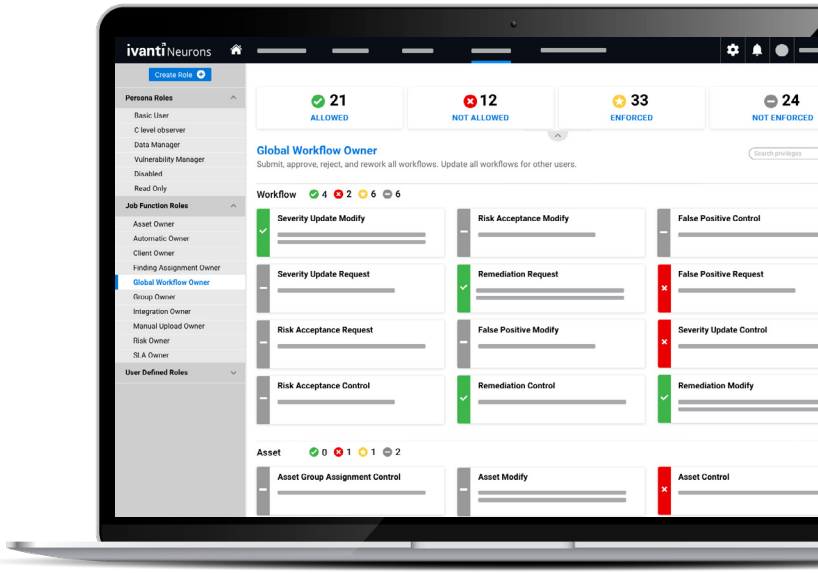


Fördern Sie eine bessere Zusammenarbeit zwischen den Sicherheitsverantwortlichen

Fördern Sie die Kommunikation und Zusammenarbeit zwischen den Stakeholdern aus dem gesamten Unternehmen, indem Sie sie rechtzeitig mit Informationen versorgen, die für ihre Aufgaben relevant sind. Ivanti Neurons for RBVM verwendet eine rollenbasierte Zugriffskontrolle (RBAC), so dass der Produktzugriff sicher für alle zuständigen Mitarbeiter erfolgen kann.

Sobald die Benutzer das Produkt nutzen, haben sie Zugriff auf Dashboards, die für Mitarbeiter vom SOC bis zum Vorstand konzipiert sind. Sie können diese Dashboards an spezifische Anwendungsfälle anpassen oder sogar Benutzer-Widgets verwenden, um benutzerdefinierte Dashboards zu erstellen, die genau den Anforderungen verschiedener Rollen und Teams entsprechen.

Zusätzlich quantifiziert das Produkt das Risikoprofil eines Unternehmens in Form eines Ivanti RS3-Scores. Dieser Wert stellt sicher, dass alle an der Sicherheit Beteiligten sich über das gesamte Sicherheitsniveau des Unternehmens einig sind. Die zweiseitige Integration mit Ticketing-Systemen wie Ivanti Neurons for ITSM verbessert die Koordination zwischen denjenigen, die an der Verbesserung des Sicherheitsniveaus arbeiten.



Merkmale und Funktionen

Merkmal	Funktion
Vielfältige Datenquellen	Verschaffen Sie sich einen umfassenden Überblick über Cyberrisiken mit einem Produkt, das Daten von Netzwerkscannern, Endpunkten, Datenbanken und IoT-Geräten, Schwachstellen aus über 100 Quellen, manuelle Ergebnisse von Forschungs- und Pen-Testing-Teams sowie benutzerdefinierte Datenquellen aufnimmt.
Bedrohungs-Engine	Gewinnen Sie beispiellose Einblicke in Schwachstellen – z.B. in Verbindung mit Ransomware – durch von Menschen erzeugte und KI-gesteuerte Informationen über Bedrohungen, die aus der Ivanti Neurons for Vulnerability Knowledge Base stammen.
Vulnerability Risk Rating (VRR)	Ermitteln Sie schnell das Risiko, das von einer Schwachstelle ausgeht, mit numerischen Risikobewertungen, die die intrinsischen Attribute der Schwachstelle und ihren realen Bedrohungskontext berücksichtigen.
Ivanti RS³	Verschaffen Sie sich einen quantifizierten Überblick über das Risikoprofil Ihres Unternehmens mithilfe einer proprietären Bewertungsmethode, die VRR, die Geschäftskritikalität der Assets, Informationen über Bedrohungenund externe Zugänglichkeit berücksichtigt.
Automatisierung	Ersetzen Sie eine Reihe von manuellen Aufgaben durch Automatisierung, damit sich die Mitarbeitenden auf Abhilfemaßnahmen und strategische Initiativen konzentrieren können, statt auf die Verwaltung.
Warnungen und Benachrichtigungen	Erhalten Sie sofortige Kenntnis von relevanten Ereignissen durch Benachrichtigungen, die nahezu in Echtzeit von einer Notification Engine gesendet werden. Leiten Sie andere Benutzer über Deep Links zu wichtigen Informationen innerhalb des Produkts.
Anpassbare Datenorganisation	Mit Benutzer-Widgets, die die Erstellung benutzerdefinierter Dashboards ermöglichen, und der Möglichkeit, Daten in Listenansichten zu drehen, erhalten Sie verwertbare Erkenntnisse.
Dashboards	Finden Sie schnell heraus, wie sich die wichtigsten Schwachstellen – wie Log4j und die mit den Patch Tuesday - Versionen zusammenhängenden – in Ihrer Umgebung manifestieren, indem Sie bedrohungsbasierte Ansichten verwenden. Erstellen und teilen Sie auch Ihre eigenen benutzerdefinierten Ansichten
Bedrohungsbasierte Ansichten	Finden Sie schnell heraus, wie sich spezifische Bedrohungen wie BlueKeep, WannaCry oder die Top 10 der vom FBI/DHS/CISA ausgenutzten Schwachstellen in der Umgebung Ihres Unternehmens manifestieren, indem Sie bedrohungsbasierte Filter verwenden. Sie können auch Ihre eigenen benutzerdefinierten Filter erstellen und weitergeben.
Neurons-Integrationen	Kombinieren Sie Ivanti Neurons for RBVM mit Ivanti Neurons for ASPM, um das risikobasierte Schwachstellenmanagement auf einen größeren Bereich Ihrer Angriffsfläche auszuweiten. Nutzen Sie die sofort einsatzbereiten Integrationen mit Ivanti Neurons for ITSM und Ivanti Neurons for Patch Management, um die Verwaltung von Schwachstellen im gesamten Unternehmen effizienter und effektiver zu gestalten.

Über Ivanti

Ivanti ist ein globaler Anbieter für IT- und Sicherheitssoftware, der Unternehmen dabei unterstützt, ihr volles Potenzial zu entfalten und kontinuierliche Innovation zu fördern – durch effizientes Management, Automatisierung und den Schutz von Daten und Systemen. Mit anpassungsfähigen Softwarelösungen, die auf die individuellen Anforderungen der Kunden zugeschnitten sind, unterstützt Ivanti IT- und Sicherheitsteams dabei, die betriebliche Effizienz zu steigern, Kosten zu senken und Sicherheitsrisiken proaktiv zu minimieren. Im Zentrum des Angebots steht die KI-gestützte Plattform Ivanti Neurons, die die Arbeitsweise von IT- und Sicherheitsteams grundlegend verändert. Durch die Bereitstellung einheitlicher, wiederverwendbarer Services und Tools sorgt die Plattform für konsistente Transparenz, Skalierbarkeit und eine sichere Umsetzung von Lösungen – damit Teams intelligenter und effizienter arbeiten können. Mehr als 34.000 Kunden, darunter 85 der Fortune-100-Unternehmen, haben sich für Ivanti entschieden, um die Herausforderungen zu meistern. Basierend auf den „Secure by Design"-Prinzipien entwickelt Ivanti skalierbare Softwarelösungen, die mit den Anforderungen seiner Kunden wachsen – mit dem Ziel, die betriebliche Effizienz zu steigern, Kosten zu senken und Risiken in IT und Sicherheit proaktiv zu minimieren. Ivanti fördert ein inklusives Umfeld, in dem verschiedene Meinungen gehört, respektiert und geschätzt werden. Und wir setzen uns für eine nachhaltigere Zukunft für unsere Kunden, Partner, Mitarbeitenden und unseren Planeten ein.

Erfahren Sie mehr unter ivanti.de und folgen Sie uns auf den sozialen Medien @GoIvanti.

ivanti neurons

ivanti.de/neurons
+49 (0)69 66 77 80 134
contact@ivanti.de

1. Daten aus der Ivanti Neurons for Vulnerability Knowledge Base vom 29. Juni 2023
2. Cyber Security Works, Cyware, Ivanti, Securin: „2023 Spotlight Report: Ransomware Through the Lens of Threat and Vulnerability Management", 16. Februar 2023. https://www.securin.io/ransomware/
3. ExtraHop: „Cyber Confidence Index 2022", 1. März 2022. https://www.extrahop.com/resources/papers/cyber-confidence-index-2022/