ivanti neurons

Ivanti Neurons for App Security Orchestration & Correlation (ASOC)

Ausweitung des risikobasierten Schwachstellenmanagements auf den Anwendungsstack

Entwickeln Sie das Schwachstellenmanagement für Ihre Anwendungen hin zu einem risikobasierten Ansatz mit Ivanti Neurons for ASOC. Dieses SaaS-Angebot ermöglicht es Ihnen, schnelle und fundierte Entscheidungen darüber zu treffen, wohin die Entwicklung gelenkt werden soll, um die Sicherheit interner und kundenorientierter Anwendungen zu verbessern.

Risikobasiertes Schwachstellenmanagement muss Anwendungen einbeziehen

Die Anzahl der pro Quartal gescannten Anwendungen hat sich in 10 Jahren verdreifacht. Die Scan-Kadenz hat sich im gleichen Zeitraum um das 20-fache erhöht.[1] Kein Wunder, dass die Identifizierung der seltenen sehr gefährlichen Schwachstellen oder Schwachstellen im Anwendungsstack für Unternehmen, die herkömmliche Ansätze für das Schwachstellenmanagement verwenden, ein recht langsamer Prozess ist. Sie verlieren den Überblick über das hohe Datenvolumen.

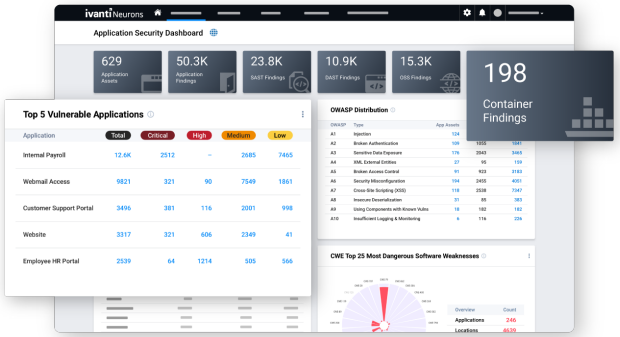
Bevor solche Unternehmen überhaupt damit beginnen können, Abhilfemaßnahmen für Schwachstellen zu priorisieren, müssen sie zunächst eine Reihe unterschiedlicher Daten sammeln – alle Daten über Sicherheitsrisiken, die SAST, DAST, OSS- und Container-Scanner findet, Bedrohungsdaten und mehr –, diese Daten standardisieren und für die Verwendung vorbereiten. Bei manueller Durchführung dauern diese Prozesse Wochen und sind anfällig für menschliche Fehler.

Beim Prozess der Priorisierung sieht es nicht anders aus. Denken Sie an die Schwachstellen von Ransomware. 47 % Prozent sind nach CVSS v3 nicht als kritisch eingestuft und 156 fehlen im KEV-Katalog (Known Exploited Vulnerabilities) der CISA. Außerdem haben drei sehr beliebte Scanner bisher immer noch keine Plugins und Erkennungssignaturen für insgesamt 20 Ransomware-Schwachstellen.[2]

Darüber hinaus wurde die mangelnde Zusammenarbeit zwischen den beteiligten Teams als größte Herausforderung bei der Abwehr von Cyberangriffen genannt.[3] Diese Spannungen zwischen den im Schwachstellenmanagement involvierten Mitarbeitenden können die Abhilfemaßnahmen verzögern und das Unternehmen anfällig für Angriffe machen.

Einführung von Ivanti Neurons for ASOC

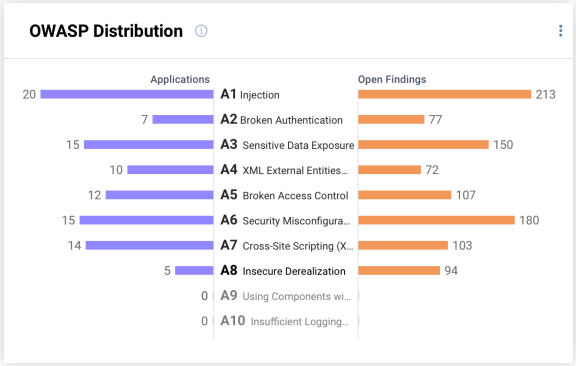
Verwenden Sie einen risikobasierten Ansatz für das Schwachstellenmanagement in Ihrem Anwendungsstack mit den Funktionen von Ivanti Neurons for ASOC. Diese Funktionen sind in einer einzigen Schnittstelle zusammengefasst, so dass Sie auf den „Drehstuhl“-Ansatz, der die Vorgehensweisen im Schwachstellenmanagement in der Vergangenheit bestimmt hat, verzichten können.



Wichtige Fähigkeiten

Umfassende Transparenz der Anwendungsrisiken

Verschaffen Sie sich einen umfassenden Überblick über das Anwendungsrisiko von der Entwicklung bis zur Produktion. Ivanti Neurons for ASOC vereint alle Anwendungs-Scandaten – SAST, DAST, OSS und Container –, um Schwachstellen und Sicherheitslücken zu lokalisieren und entsprechende Abhilfemaßnahmen zu priorisieren.



Ivanti Neurons for ASOC ist scannerunabhängig und ermöglicht DevOps, die verschiedenen Scan-Tools auszuwählen, die für die verschiedenen Teile des Entwicklungszyklus benötigt werden. Das Produkt trägt alle Schwachstellen- und Scan-Ergebnisse der Daten über Sicherheitsrisiken von Anwendungen zusammen und korreliert sie dann kontinuierlich mit aktiven Bedrohungen, die in der Praxis auftreten. Dadurch wissen die User sofort, wo das größte Risiko für ihr Unternehmen liegt. Die User können auch die genauen Codestellen aufschlüsseln, wo sich die Daten über Sicherheitsrisiken innerhalb des Anwendungsstacks befinden.

Darüber hinaus ermöglicht das Application Security Dashboard den Usern, den Fortschritt der Anwendungsentwicklung beim Schließen von Sicherheitslücken zu verfolgen. Denn es bietet einen umfassenden Überblick über die Schwachstellen, CWEs und OWASP-Daten über Sicherheitsrisiken, denen Unternehmen ausgesetzt sind, sowie über die Bilanz neuer Scan-Erkentnisse und die Geschwindigkeit, mit der sie behoben werden.

Priorisierung von 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 entsprechenden Abhilfemaßnahmen übergehen. Ivanti Neurons for ASOC misst Risiken und priorisiert Abhilfemaßnahmen durch einen Prozess, der eine kontinuierliche Korrelation der Anwendungen eines Unternehmens einschließt:

- Interne und externe Schwachstellendaten.
- Bedrohungsdaten.
- Manueller Pen-Test und forschungsbasierte Ergebnisse.
- Kritikalität der Unternehmensdaten.

Das Beste daran ist, dass Sie mit wenig oder gar keinem manuellen Aufwand einen vollständig fundierten Angriffsplan erhalten.

Im Gegensatz zu CVSS können Unternehmen mit dem von Ivanti entwickelten Vulnerability Risk Rating (VRR) die Auswirkungen genau messen und die Wahrscheinlichkeit ermitteln, mit der eine Schwachstelle ausgenutzt wird. Ivanti Neurons for ASOC identifiziert auch insbesondere 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.

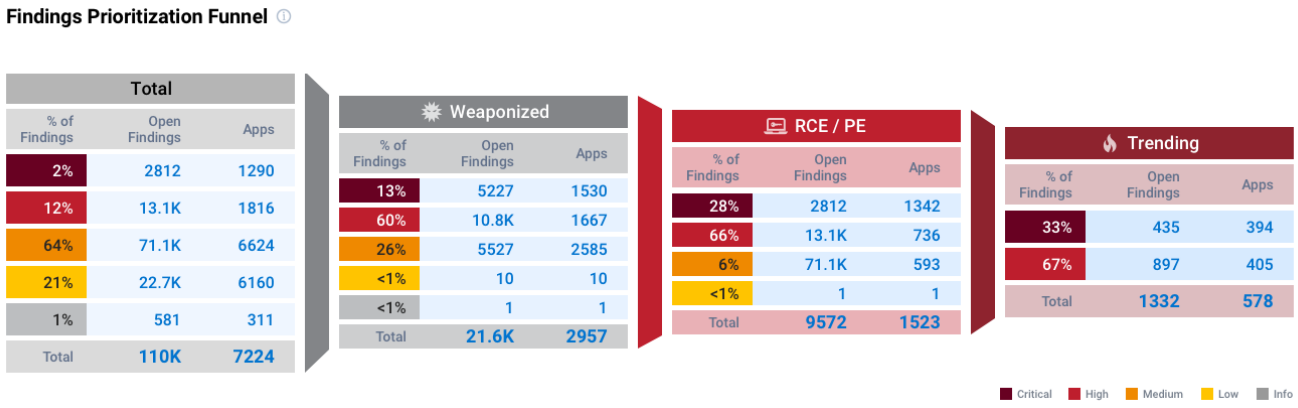
Fokus auf Abhilfemaßnahmen, nicht auf Verwaltung

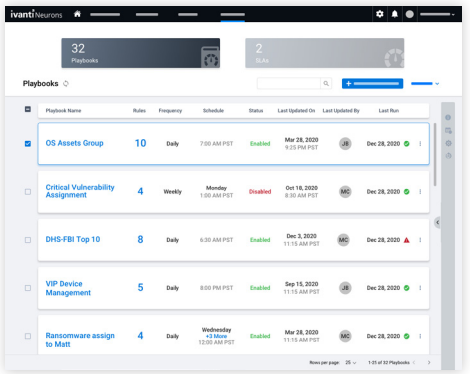
Verbessern Sie Ihre Cybersicherheit ohne den damit verbundenen Zeit-, Arbeits- und Fehleraufwand – durch eine Reihe von Automatisierungen und anderen effizienzsteigernden Funktionen:

- Erstellen Sie Playbooks, um häufige oder sich wiederholende Aufgaben zu automatisieren, die üblicherweise von Sicherheitsanalysten durchgeführt werden.
- Legen Sie die Fälligkeitstermine für die Schließung von Schwachstellen automatisch fest, falls dies im Rahmen von Service-Level-Automatisierungen gewünscht wird.
- Erhalten Sie nahezu in Echtzeit Warnmeldungen außerhalb der Benutzeroberfläche, die auf eine Produktseite mit Informationen zu dem abonnierten Ereignis verweisen.
- Filtern Sie ganz einfach Anwendungen und Anwendungsergebnisse nach Trendkriterien, die ihre Gefährdung durch die kritischsten Schwachstellen – wie Ransomware und aktuelle CVEs – anzeigen. Dies erfolgt mittels Systemansichten, die vom Ivanti-Sicherheitsteam bereitgestellt werden.

Bessere Zusammenarbeit zwischen den Sicherheitsverantwortlichen

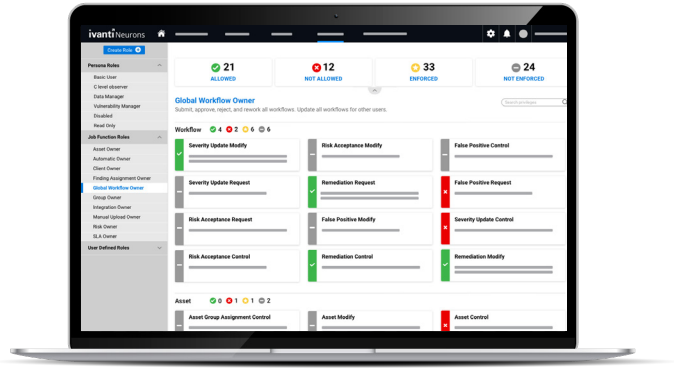
Fördern Sie die Kommunikation und Zusammenarbeit zwischen den Sicherheitsverantwortlichen im gesamten Unternehmen durch die rechtzeitige Bereitstellung von Informationen, die für ihre Aufgaben relevant sind. Ivanti Neurons for ASOC verwendet eine rollenbasierte Zugriffskontrolle (RBAC), sodass der Produktzugriff für alle zuständigen Mitarbeitenden scher erfolgen kann.





Sobald die User in das Produkt eingearbeitet sind, können sie auf Dashboards zugreifen, die für Mitarbeitende vom SOC (Security Operations Center) bis zur Vorstandsebene konzipiert sind. Sie können diese Dashboards an spezifische Anwendungsfälle anpassen oder sogar User-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 Score stellt sicher, dass alle in die Sicherheit involvierten Mitarbeitenden sich über das Gesamtsicherheitsniveau des Unternehmens einig sind. Bidirektionale Integrationen mit Ticketing-Systemen wie Ivanti Neurons for ITSM verbessern die Koordination zwischen denjenigen, die an der Verbesserung dieses Sicherheitsniveaus arbeiten.



Leistungsmerkmale und Funktionen

Leistungsmerkmale	Funktion
Vielfältige Datenquellen	Verschaffen Sie sich einen umfassenden Überblick über Cyberrisiken mit einem Produkt, das Daten von Anwendungsscannern (SAST, DAST, OSS, Container), Ermittlung von Schwachstellen aus über 100 Quellen, manuelle Feststellungen von Forschungs- und Pen-Testing-Teams sowie benutzerdefinierte Datenquellen erfasst.
Bedrohungsengine	Gewinnen Sie charakteristische Einblicke in Schwachstellen – z. B. solche, die mit Ransomware in Verbindung stehen – durch von Menschen erstellte und KI-gesteuerte Bedrohungsdaten, die aus der Ivanti Neurons for Vulnerability Knowledge Base stammen.
Vulnerability Risk Rating (VRR)	Bestimmen Sie schnell das Risiko, das von einer Schwachstelle ausgeht – mit numerischen Risikobewertungen, die seine intrinsischen Merkmale und den realen Bedrohungskontext berücksichtigen.
Ivanti RS^3	Verschaffen Sie sich einen quantitativen Überblick über das Risikoprofil Ihres Unternehmens mithilfe einer proprietären Bewertungsmethode, die VRR, Kritikalität der Unternehmensdaten, Bedrohungsdaten und externe Zugänglichkeit berücksichtigt.
Automatisierung	Ersetzen Sie eine Reihe von manuellen Aufgaben mittels Automatisierung, damit sich die Mitarbeitenden auf Abhilfemaßnahmen und strategische Initiativen konzentrieren können, statt auf die Verwaltung.

Leistungsmerkmale und Funktionen

Warnungen und Benachrichtigungen	Sie erhalten sofortige Informationen über relevante Ereignisse durch Warnmeldungen, die nahezu in Echtzeit von einem Benachrichtigungssystem gesendet werden. Leiten Sie andere User über Deeplinks zu wichtigen Informationen innerhalb des Produkts.
Anpassbare Datenorganisation	Mit User-Widgets, die die Erstellung von benutzerdefinierten Dashboards ermöglichen, und der Möglichkeit, Daten in Listenansichten anzuzeigen, können Sie praktisch umsetzbare Erkenntnisse gewinnen.
Dashboards	Realisieren Sie hochwertige visuelle Abfrage- und Risikoerkennungsfunktionen für Assets und Infrastrukturen über vorgefertigte und anpassbare Dashboards mit Drilldown-Funktionen.
Bedrohungsbasierte Ansichten	Finden Sie schnell heraus, wie sich die wichtigsten kritischen Schwachstellen – wie Log4j und die mit den Patch-Tuesday-Releases verbundenen – in Ihrer Umgebung manifestieren, indem Sie bedrohungsbasierte Ansichten verwenden. Sie können auch Ihre eigenen benutzerdefinierten Ansichten erstellen und freigeben.
Neurons-Integrationen	Kombinieren Sie Ivanti Neurons for ASOC mit Ivanti Neurons for RBVM, um das risikobasierte Schwachstellenmanagement auf einen größeren Bereich Ihrer Angriffsfläche auszuweiten. Nutzen Sie die Out-of-the-Box-Integration mit Ivanti Neurons for ITSM, damit die für das Schwachstellenmanagement zuständigen Mitarbeitenden im gesamten Unternehmen ihre Aufgaben effizienter und effektiver erledigen können.

Über Ivanti

Ivanti steigert und sichert Everywhere Work, damit Menschen und Unternehmen erfolgreich sein können. Wir sorgen dafür, dass die Technologie für die Menschen arbeitet, nicht umgekehrt. Die Mitarbeitenden von heute nutzen eine breite Palette von Firmen- und Privatgeräten, um über mehrere Netzwerke auf IT-Anwendungen und Daten zuzugreifen und so produktiv zu bleiben, egal wo und wie sie arbeiten. Ivanti gehört zu den wenigen Technologieunternehmen, die alle IT-Assets und -Endpunkte in einem Unternehmen finden, verwalten und schützen. Mehr als 40.000 Kunden, darunter 88 der Fortune 100, haben sich für Ivanti entschieden, um ihren Mitarbeitenden eine hervorragende digitale Erfahrung zu bieten sowie die Produktivität und Effizienz ihrer IT- und Sicherheitsteams zu verbessern. Unser Ziel bei Ivanti ist, ein Umfeld zu schaffen, in dem alle Meinungen gehört, respektiert und geschätzt werden. Und wir setzen uns für eine nachhaltigere Zukunft für unsere Kunden, Partner, Mitarbeitenden und unseren Planeten ein.

Weitere Informationen finden Sie unter www.ivanti.com und folgen Sie @GoIvanti.

ivanti

Um mehr zu erfahren oder mit Ivanti in Kontakt zu treten, besuchen Sie uns auf ivanti.com

1. Veracode, "State of Software Security v12", 2021. https://info.veracode.com/report-state-of-software-security-volume-12.html
2. Cyber Security Works, Cyware, Ivanti, Securin, "2023 Spotlight Report: Ransomware Through the Lens of Threat and Vulnerability Management", 16 February 2023. https://www.securin.io/ransomware/
3. ExtraHop, "Cyber Confidence Index 2022", 1 March 2022. https://www.extrahop.com/resources/papers/cyber-confidence-index-2022/