ivanti neurons

Ivanti Neurons for App Security Orchestration & Correlation (ASOC)

Extend risk-based vulnerability management to the application stack

Evolve vulnerability management for your applications to a risk-based approach with Ivanti Neurons for ASOC. This SaaS offering enables you to make fast, informed decisions on where to direct development to improve the security of internal and customer-facing applications.

Risk-based vulnerability management must include apps

The number of applications scanned per quarter has tripled in 10 years. Scan cadence has increased 20x over the same period.[1] No wonder identifying the rare vulnerability or weakness in their application stack that poses significant risk is a slow process for organizations using traditional approaches to vulnerability management — they're drowning in data.

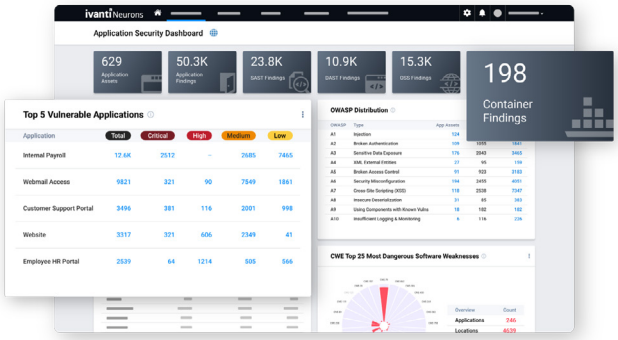
Before such organizations can even begin prioritizing vulnerabilities and weaknesses for remediation, they must first gather a range of disparate data — SAST, DAST, OSS and container scanner findings, threat intelligence and more — normalize that data and prepare it for use. When done manually, these processes take weeks to complete and are prone to human error.

The prioritization process is no better. Consider ransomware vulnerabilities. Seventy-four percent aren't rated Critical under CVSS v3 and 156 are missing from the CISA Known Exploited Vulnerabilities (KEV) catalog. Additionally, three highly popular scanners still haven't added plugins and detection signatures for a combined 20 ransomware vulnerabilities.[2]

On top of all that, a lack of cooperation between involved teams has been cited as the top challenge in defending against cyberattacks.[3] This friction between vulnerability management stakeholders can slow remediation and leave the organization prone to attack.

Introducing Ivanti Neurons for ASOC

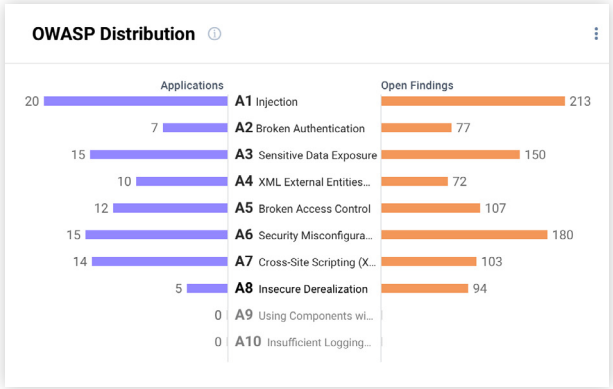
Adopt a risk-based approach to vulnerability management for your application stack with the capabilities found in Ivanti Neurons for ASOC. These capabilities come packaged in a single interface so you can phase out the 'swivel chair' approach that's defined vulnerability management practices of the past.



Key capabilities

Achieve full-stack visibility of application risk exposure

Gain full-stack visibility of application risk exposure from development to production. Ivanti Neurons for ASOC unifies all application scan data — SAST, DAST, OSS and container — to locate vulnerabilities and weaknesses and prioritize remediation.



Ivanti Neurons for ASOC is scanner agnostic, allowing DevOps to select the various scanning tools needed across the different parts of the development lifecycle. The product normalizes all application vulnerability and scan findings and then continuously correlates them to active threats trending in the wild, enabling users to know immediately which findings are the greatest risk to their organization. Users can also drill down to the exact code locations where those findings reside within the application stack.

Further, the product's Application Security Dashboard lets users view the progress of application development in addressing security debt by offering a comprehensive view of the vulnerabilities, CWEs and OWASP findings that expose organizations, along with the balance of new scan findings and the rate in which they are remediated.

Prioritize immediate actions based on threat risk

Move from detection of vulnerabilities and weaknesses to remediation in minutes — not months — with a contextualized, risk-based view of your organization's cybersecurity posture. Ivanti Neurons for ASOC measures risk and prioritizes remediation activities through a process that involves continuous correlation of an organization's applications with:

- Internal and external vulnerability data.
- Threat intelligence.
- Manual pen test and research-based findings.
- Business asset criticality.

Best of all: you arrive at a fully informed plan of attack with little to no manual effort required.

Further, unlike CVSS, Ivanti's proprietary Vulnerability Risk Rating (VRR) lets organizations accurately measure impact and determine the likelihood a vulnerability will be exploited. Ivanti Neurons for ASOC also specifically identifies remote code execution, privilege escalation, ransomware, and trending and active vulnerabilities. This information helps organizations focus on those vulnerabilities that pose them the most risk.

Focus on remediation, not administration

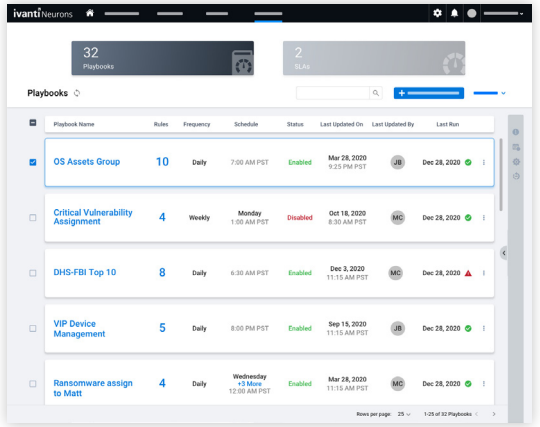
Improve your cybersecurity posture without all the time, effort and errors traditionally associated with doing so through a range of automations and other efficiency-enhancing features:

- Create playbooks to automate common or repetitive tasks traditionally handled by security analysts.
- Set vulnerability closure due dates automatically if desired with service-level agreement automations.
- Receive near-real-time alerts outside the product that link back to a product page containing information related to the subscribed event.
- Easily filter applications and applications findings by trending criteria that reveal their exposure to the top critical vulnerabilities — like ransomware and trending CVEs — using system views pushed by the Ivanti security team.

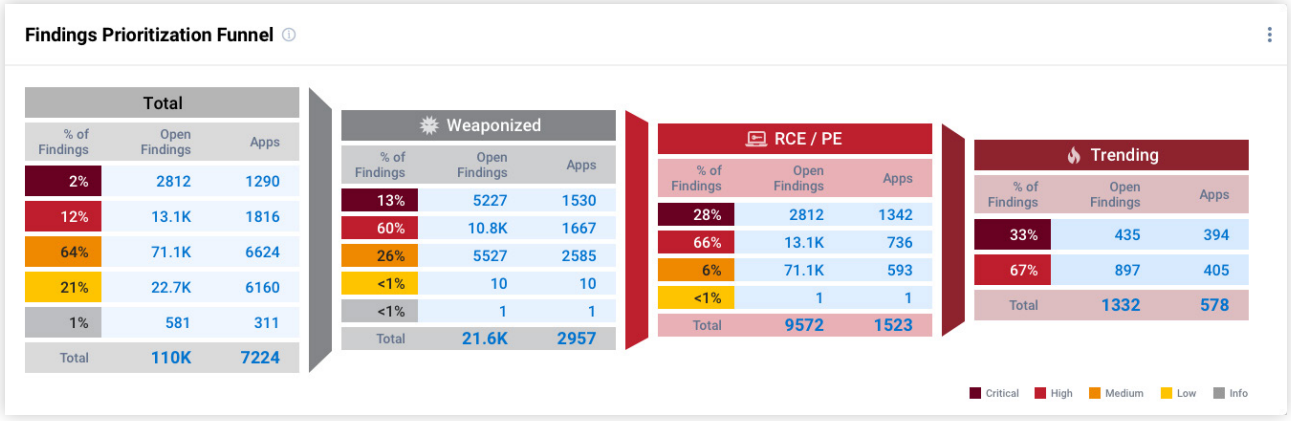
Enable better collaboration amongst security stakeholders

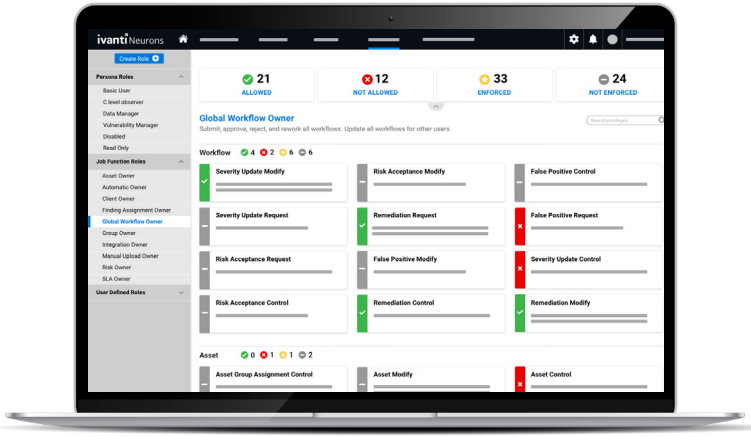
Cultivate communication and cooperation among security stakeholders from across the organization by providing them with timely information relevant to their roles. Ivanti Neurons for ASOC employs role-based access control (RBAC) so product access can be safely provided to all applicable personnel.

Once inside the product, users have access to dashboards designed for personnel from the SOC to the C-suite. They can modify these dashboards to fit more specific use cases, or even leverage user widgets to create custom dashboards that meet the exact needs of different roles and teams.



Additionally, the product quantifies an organization's risk profile in the form of an Ivanti RS^3 score. This score ensures all security stakeholders are in alignment on the organization's overall security level. Bidirectional integrations with ticketing systems like Ivanti Neurons for ITSM improve coordination between those working to improve that security level.





Features & functions

Feature	Function
Diverse data sources	Achieve a wide view of cyber risk with a product that ingests data from application scanners (SAST, DAST, OSS, container), vulnerability findings from 100+ sources, manual findings from research and pen testing teams, and custom data sources.
Threat engine	Gain unparalleled insights on vulnerabilities — like which are tied to ransomware — via human-generated and AI-driven threat intelligence sourced from Ivanti Neurons for Vulnerability Knowledge Base.
Vulnerability Risk Rating (VRR)	Quickly determine the risk posed by a vulnerability with numerical risk scores that consider its intrinsic attributes and real-world threat context.
Ivanti RS^3	Attain a quantified view of your organization's risk profile via a proprietary scoring methodology that considers VRR, asset business criticality, threat intelligence and external accessibility.
Automation	Replace a range of manual tasks with automation so employees can focus on remediation actions and strategic initiatives rather than administration.
Alerts and notifications	Gain instant awareness of pertinent events via near-real-time alerts sent from a notification engine. Similarly, direct other users to important information within the product using deep links.
Customizable data organization	Uncover actionable insights with user widgets that allow for the creation of custom dashboards, plus the ability to pivot data in list views.
Dashboards	Realize superior visual query and risk discovery capabilities across assets and infrastructure via readymade and customizable dashboards equipped with drill-down capabilities.
Threat-based views	Quickly discover how top critical vulnerabilities — like Log4j and those associated with Patch Tuesday releases — manifest themselves in your environment by utilizing threat-based views. Also create and share your own custom views.
Neurons integrations	Pair Ivanti Neurons for ASOC with Ivanti Neurons for RBVM to extend risk-based vulnerability management across a greater area of your attack surface. Leverage an out-of-the-box integration with Ivanti Neurons for ITSM to empower vulnerability management practitioners throughout the organization to perform their tasks more efficiently and effectively.

About Ivanti

Ivanti elevates and secures Everywhere Work so that people and organizations can thrive. We make technology work for people, not the other way around. Today's employees use a wide range of corporate and personal devices to access IT applications and data over multiple networks to stay productive wherever and however they work. Ivanti is one of the only technology companies that finds, manages, and protects each IT asset and endpoint in an organization. Over 40,000 customers, including 88 of the Fortune 100, have chosen Ivanti to help them deliver an excellent digital employee experience and improve IT and security team productivity and efficiency. At Ivanti, we strive to create an environment where all perspectives are heard, respected, and valued, and we are committed to a more sustainable future for our customers, partners, employees, and the planet.

For more information, visit ivanti.com and follow @GoIvanti.

ivanti

For more information, or to contact Ivanti, please visit 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/