



Ivanti Neurons for App Security Orchestration & Correlation

Extend risk-based vulnerability management to the application stack

Ivanti Neurons for App Security Orchestration & Correlation unifies all application security data (SAST, DAST, OSS, container) to locate vulnerabilities and weaknesses in an organization's application stack and prioritize remediation. This SaaS solution enables organizations to make fast, informed decisions on where to direct development to fix those vulnerabilities and weaknesses and improve the security of their internal and customer-facing applications.

Application security cannot be overlooked

An organization's applications are some of its most important assets. Unfortunately, they often take a backseat to the network when it comes to security. While 90% of cybersecurity leaders scan their infrastructure for vulnerabilities, only 69% scan their applications, 64% their websites and 40% their container repositories.¹

For the organizations that do place a priority on application security, the situation can be overwhelming. The number of applications scanned per quarter has tripled over the past decade. Scan cadence has increased 20x over the same period.² The result of all these scans is a tremendous amount of data.

Coupled with this tremendous amount of scan data is an equally overwhelming number of vulnerabilities and weaknesses. The National Vulnerability Database (NVD) currently contains over 134,000 vulnerabilities, and 61 more are added every day.³ The good news is that organizations do not need to remediate every vulnerability and weakness. In fact, only 4% of all Common Vulnerabilities and Exposures (CVEs) have been publicly exploited.⁴ The bad news is that identifying the select vulnerabilities and weaknesses that pose them significant risk is difficult for organizations relying on traditional approaches to vulnerability prioritization.

Further complicating matters is the fact that organizations usually cannot begin prioritizing vulnerabilities and weaknesses for remediation until after data has been gathered from a range of disparate sources – from internal scanners to external threat intelligence sources – normalized and prepared for use. These processes are often conducted manually and can take weeks to complete – which may explain why over three-quarters of flaws in third-party libraries remain unfixed after three months.²

As if the situation were not already difficult enough, security and IT decision makers actually cite the lack of cooperation between internal teams as the top challenge they face as they attempt to defend against cyberattacks.⁵ Communication and collaboration between security stakeholders across all parts of the organization often suffers due to a lack of relevant and timely reporting.

Introducing Ivanti Neurons for ASOC

Ivanti Neurons for App Security Orchestration & Correlation (ASOC) enables organizations to take a risk-based approach to vulnerability management for their application stack. The platform helps organizations measure and control their true cybersecurity risk so they can better protect against data breaches, ransomware and other cyber threats.

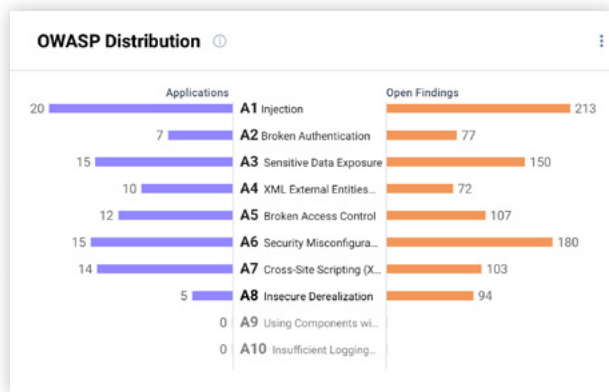


Ivanti's proprietary Vulnerability Risk Rating (VRR) quantifies adversarial risk so customers can take risk-based prioritized action. A range of automations increase the efficiency and effectiveness of vulnerability management processes. Additionally, role-based access control (RBAC) plus information available in both ready-made and customizable views enable better communication and collaboration among security stakeholders.

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 platform 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 ones are the greatest risk to their organization and providing them the ability to drill down to the exact code locations where they reside within the application stack.

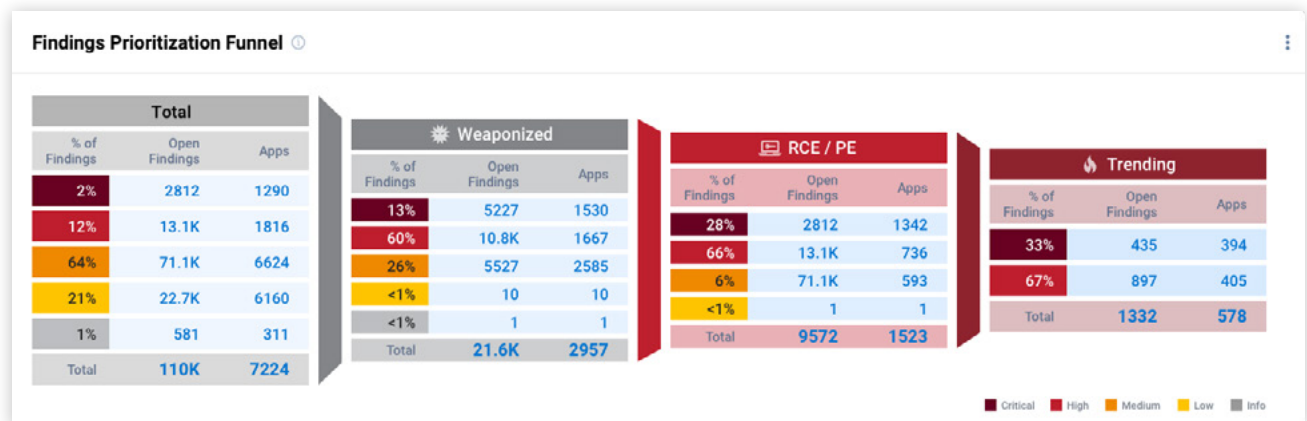


In addition, the platform's Application Security Dashboard provides users the ability to view the progress of application development in addressing security debt by offering a comprehensive view of the vulnerabilities, CWEs and OWASP findings that expose organizations, along with the balance of new scan 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 continuously correlates an organization's applications with comprehensive internal and external vulnerability data, threat intelligence, human pen test findings and business asset criticality to measure risk, provide early warning of weaponization, predict attacks and prioritize remediation activities.

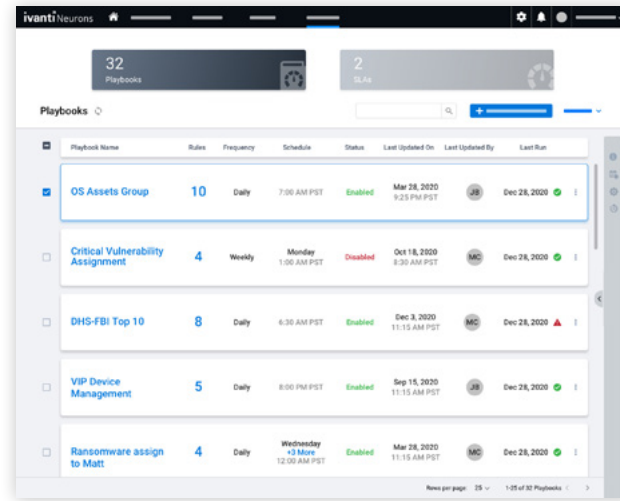
Unlike CVSS, the platform's proprietary VRR scoring enables organizations to accurately measure impact and determine the likelihood that a vulnerability will be exploited. Ivanti Neurons for ASOC also specifically identifies remote code execution (RCE) and privilege escalation (PE) vulnerabilities, vulnerabilities with ties to ransomware, and vulnerabilities that are trending and active. This information helps organizations focus on those vulnerabilities that pose them the most risk.



Improve the efficiency of vulnerability management processes

Ivanti Neurons for ASOC helps you increase your cybersecurity posture while decreasing the time and effort required to do so:

- The platform continuously correlates and analyzes comprehensive internal and external vulnerability data, threat intelligence, human pen test findings and business asset criticality to help users arrive at a fully informed plan of attack – a process that typically takes weeks to conduct manually.
- Playbooks enable the automation of common or repetitive tasks so users can focus time and effort on remediation actions rather than administration.
- Service-level agreement (SLA) automations allow for vulnerability closure due dates to be set automatically.
- Automated, customizable notifications provide near real-time alerts outside the platform that link users directly to a platform page containing information related to the subscribed event.
- System filters pushed by the Ivanti security team allow for easy filtering of applications and application findings by trending criteria that reveal their exposure to the top critical vulnerabilities on a regular basis (e.g., ransomware, trending CVEs, FBI/DHS/CISA top 10 exploited vulnerabilities or cross-site scripting).



Playbook Name	Rules	Frequency	Schedule	Status	Last Updated On	Last Updated By	Last Run
OS Assets Group	10	Daily	7:00 AM PST	Enabled	Mar 28, 2020 9:23 PM PST	JB	Dec 28, 2020
Critical Vulnerability Assignment	4	Weekly	Monday 1:00 AM PST	Disabled	Oct 18, 2020 8:30 AM PST	MC	Dec 28, 2020
DHS-FBI Top 10	8	Daily	6:30 AM PST	Enabled	Dec 3, 2020 11:15 AM PST	MC	Dec 28, 2020
VIP Device Management	5	Daily	8:00 PM PST	Enabled	Sep 15, 2020 11:15 AM PST	JB	Dec 28, 2020
Ransomware assign to Matt	4	Daily	Wednesday 12:00 AM PST	Enabled	Mar 28, 2020 11:15 AM PST	MC	Dec 28, 2020

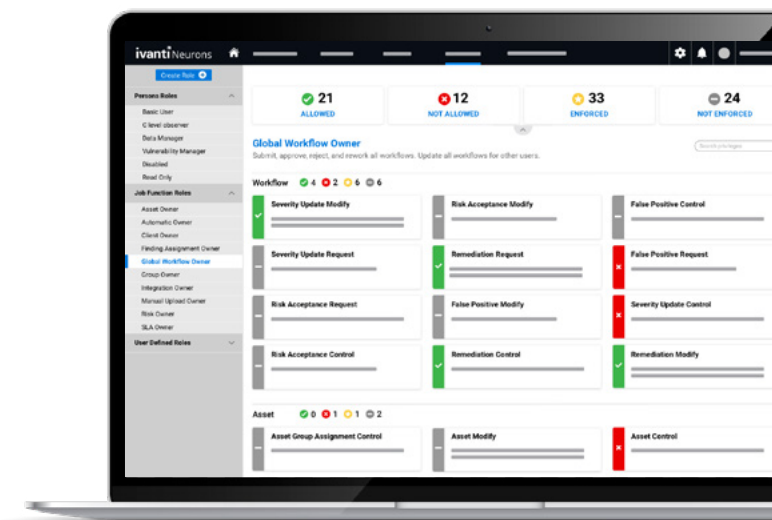
Enable better collaboration amongst security stakeholders

Facilitate improved communication and cooperation among security stakeholders from across the organization – both those on the technical side and the business side – by providing them each with timely information relevant to their roles. Ivanti Neurons for ASOC employs RBAC to enable organizations to safely provide platform access to all applicable personnel.

Once inside the platform, users have access to a range of ready-made dashboards designed for different personas, from security practitioners to executives. These standard dashboards can also be modified to fit more specific use cases. Further, user widgets enable users to create fully customized dashboards that meet the exact needs of different roles and teams.

To further foster collaboration, Ivanti Neurons for ASOC allows users to create deep links to share their exact current view of a platform page with other users. This helps bridge communication gaps between siloed teams by enabling all teams to literally get on the same page. Users also possess the ability to share dashboards, export templates and filters.

Last but not least, the platform quantifies an organization's risk profile in the form of an Ivanti RS³ score that ensures all security stakeholders are in alignment on the organization's overall security level. Bidirectional integrations with ticketing systems – including [Ivanti Neurons for ITSM](#) – improve coordination between stakeholders working to improve that security level by enabling them to maintain visibility throughout the remediation process without the additional burden of leaving their preferred system.



Features & functions

Feature	Function
Diverse data sources	Achieve a wide view of cyber risk with a platform that ingests data from application scanners (SAST, DAST, OSS, container), vulnerability findings from over 100 independent 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 the intrinsic attributes of the vulnerability plus its real-world threat context.
Ivanti RS³	Attain a quantified view of your organization's risk profile via a proprietary scoring methodology that considers VRR, the business criticality of assets, numerous threat intelligence sources and external accessibility.
Automation	Eliminate a range of manual tasks with the platform's many automation capabilities 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 the platform's notification engine. Similarly, direct other users to important information within the platform using deep links.
Customizable data organization	Uncover actionable insights with user widgets that allow for the creation of highly customized dashboards and a group-by capability that permits the pivoting of data in list views.
Dashboards	Realize superior visual query and risk discovery capabilities across applications via ready-made and customizable dashboards with drill-down capabilities in every view.
Filters	Quickly discover how specific threats like BlueKeep, WannaCry or the FBI/DHS/CISA top 10 exploited vulnerabilities manifest themselves in your organization's environment by utilizing threat-based filters. Also create and share your own custom filters.

About Ivanti

Ivanti makes the Everywhere Workplace possible. In the Everywhere Workplace, employees use myriad devices to access IT networks, applications and data to stay productive as they work from anywhere. The Ivanti automation platform connects the company's industry-leading unified endpoint management, zero trust security and enterprise service management solutions, providing a single pane of glass for enterprises to self-heal and self-secure devices, and self-service end users. More than 40,000 customers, including 96 of the Fortune 100, have chosen Ivanti to discover, manage, secure and service their IT assets from cloud to edge, and deliver excellent end user experiences for employees, wherever and however they work. For more information, visit [ivanti.com](https://www.ivanti.com).

The Ivanti logo consists of the word "ivanti" in a bold, lowercase, sans-serif font. The letter "i" is red, while the remaining letters "vanti" are black.A vertical red bar is located to the left of the contact information.

[ivanti.com](https://www.ivanti.com)

1 800 982 2130

sales@ivanti.com

1. Vulcan Cyber, Pulse, "How Are Businesses Mitigating Cyber Risk?", 2021. https://l.vulcancyber.com/hubfs/Infographics/Pulse_research_project_-_2021-07-23_-_How_are_Businesses_Mitigating_Cyber_Risk.pdf
2. Veracode, "State of Software Security v12", 2021. <https://info.veracode.com/report-state-of-software-security-volume-12.html>
3. Cyber Security Works, Cyware, Ivanti, "2022 Ransomware Spotlight Report", 26 January 2022. <https://www.ivanti.com/lp/security/reports/ransomware-spotlight-year-end-2021-report>
4. Cybersecurity and Infrastructure Security Agency (CISA), "Binding Operational Directive 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities", 3 November 2021. <https://cyber.dhs.gov/bod/22-01/>
5. ExtraHop, "Cyber Confidence Index 2022", 1 March 2022. <https://www.extrahop.com/resources/papers/cyber-confidence-index-2022/>