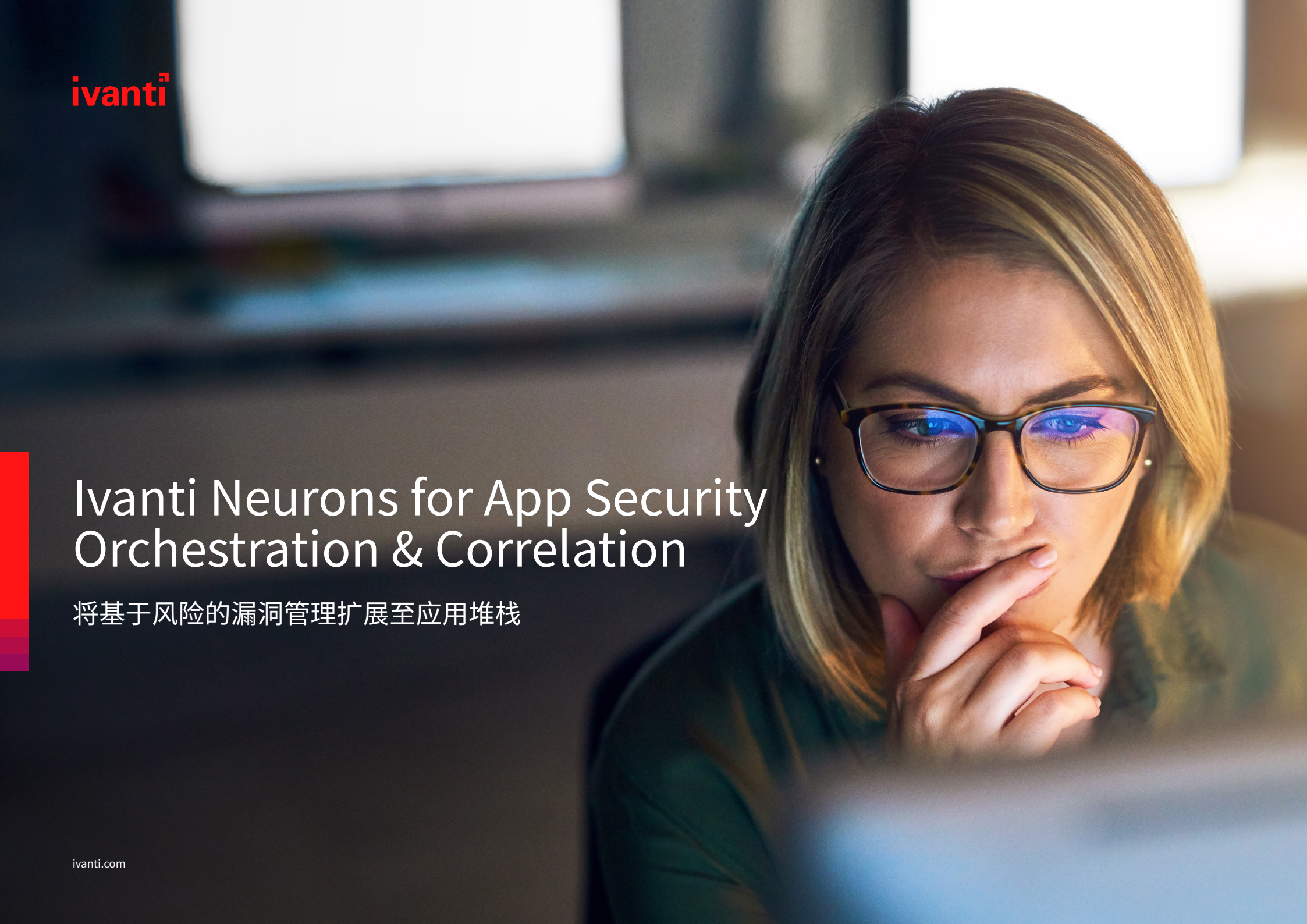


Ivanti Neurons for App Security Orchestration & Correlation

将基于风险的漏洞管理扩展至应用堆栈

Ivanti Neurons for App Security Orchestration & Correlation 统一协调所有应用安全数据（SAST、DAST、OSS、容器），以定位企业应用堆栈中的漏洞和缺陷，并对修复举措加以排序。这个 SaaS 解决方案使企业能够通过快速知情决定，引导开发部门有针对性地修复漏洞和缺陷，从而提高内部和面向客户的应用的安全性。

应用安全性不可忽视

企业的应用属于其最重要的资产。遗憾的是，当涉及到安全问题时，它们往往不如网络那样受到重视。90% 的网络安全负责人会扫描其基础设施是否存在漏洞，但只有 69% 会扫描其应用，64% 会扫描其网站，40% 会扫描其容器库。[1]

对于那些确实优先考虑应用安全的企业来说，情况可能很严峻。过去十年来，每季度扫描的应用数量增加了两倍。同期，扫描频次增加了20倍。[2] 所有这些扫描的结果是海量数据。

与海量扫描数据相伴而来的是同样数量庞大的漏洞和缺陷。美国国家漏洞数据库 (NVD) 目前包含超过 13.4 万个漏洞，而且每天增加 61 个。[3] 好消息是，企业不需要修复每个漏洞和缺陷。事实上，在所有的常见漏洞和风险 (CVE) 中，只有 4% 被公开利用。[4] 坏消息是，那些依赖传统漏洞排序方法的企业，难以识别对他们构成重大风险的特定漏洞和弱点。

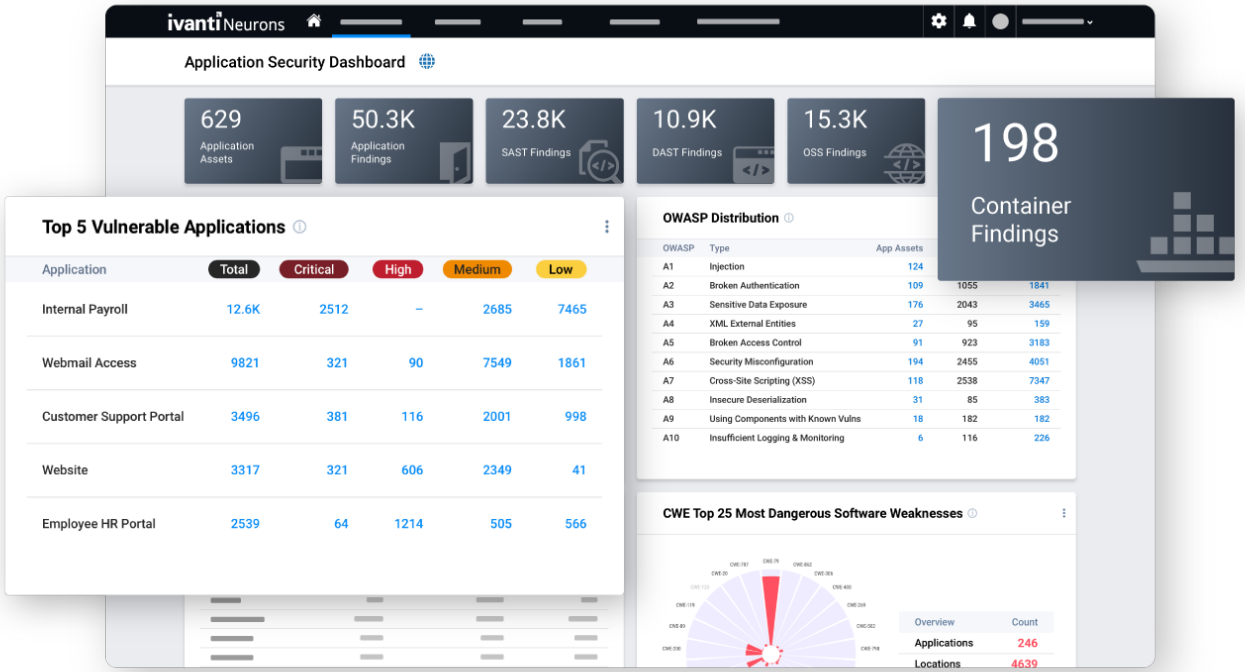
让问题更加复杂的是，企业通常需要先从一系列不同的来源——从内部扫描工具到外部威胁情报来源——收集数据，再对其进行规范化处理和准备，然后才能利用它开始对漏洞和弱点进行排序和修复。这些过程通常是手动进行的，可能需要数周时间才能完成。这可能解释了为什么在第三方库中有超过四分之三的缺陷在三个月后仍未得到修复。[2]

如果说这个局面还不够困难，那么安全和 IT 决策者实际上将内部团队之间缺乏协作列为他们在努力防御网络攻击时所面临的最大挑战。[5] 由于缺乏相关且及时的报告，企业各部门的安全利益相关者之间往往不能开展良好的沟通和协作。

引入 Ivanti Neurons for ASOC

Ivanti Neurons for App Security Orchestration & Correlation (ASOC) 让企业能够对其应用堆栈采取基于风险的漏洞管理方法。该平台帮助企业对其真正的网络安全风险加以衡量和控制，以便他们能够更好地防范数据泄露、勒索软件和其他网络威胁。

Ivanti 专有的漏洞风险评级 (VRR) 可以量化恶意风险，因此客户可以采取基于风险的排序行动。一系列自动化功能提高了漏洞管理过程的效率和效能。此外，基于角色的访问控制 (RBAC) 功能，加上通过现成和定制视图所获取的信息，使安全领域利益相关者之间能够更好地沟通和协作。



主要功能

实现应用风险敞口的全栈可见性

实现对应用风险敞口从开发到生产等各个阶段的全栈可见性 Ivanti Neurons for ASOC 将所有的应用扫描数据（SAST、DAST、OSS和容器）汇总起来，以查找漏洞和缺陷，并确定修复措施的先后次序。

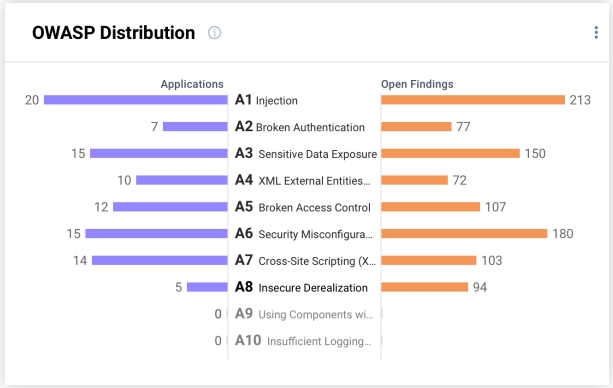
Ivanti Neurons for ASOC 与扫描程序无关，允许 DevOps 在开发生命周期的不同部分选择所需的各种扫描工具。平台将所有应用漏洞和扫描结果规范化，然后持续不断地将它们与现行活跃威胁予以关联，这让用户能够立即知道哪些是对其组织威胁最大的风险，并且有能力深入了解它们在应用堆栈中的确切代码位置。

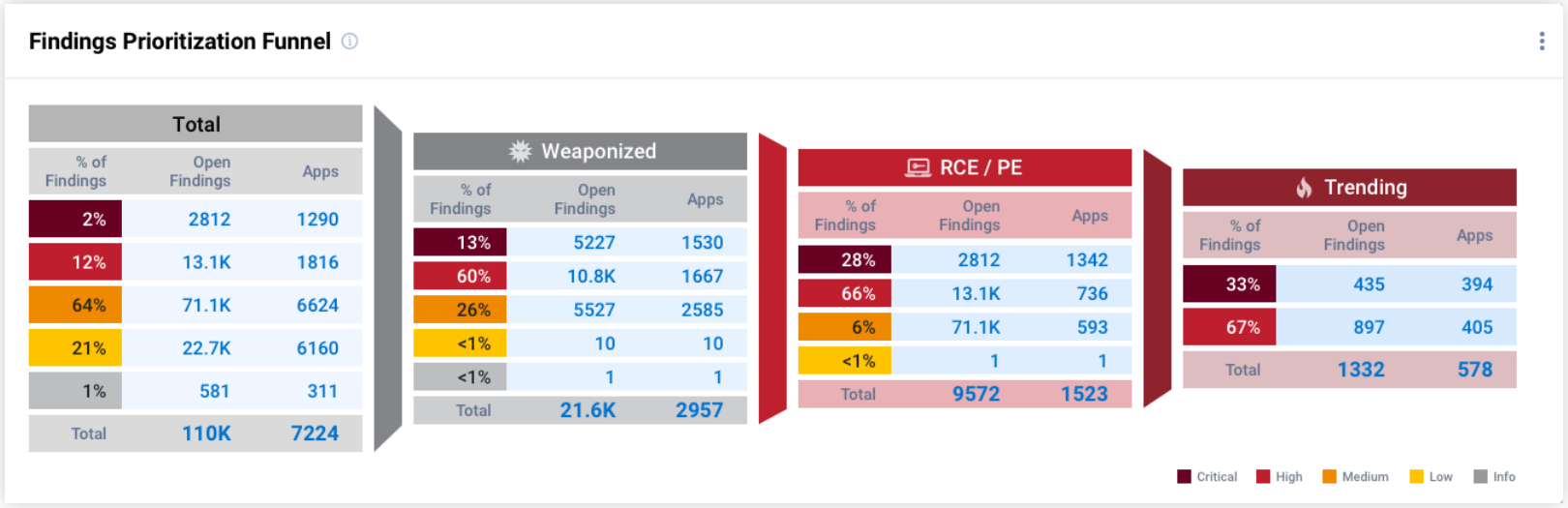
此外，平台的应用安全仪表板让用户能够全面掌握会给企业带来风险的漏洞、CWE 和 OWASP 发现结果，以及新的扫描发现结果数量及其修复速度，从而让用户能够洞察应用开发部门在解决积压安全任务方面的进度。

根据威胁风险对立即行动加以排序

从风险角度全面审视企业的网络安全态势，从检测发现漏洞和缺陷到修复只需几分钟——而不是几个月。Ivanti Neurons for ASOC 将组织基础设施与全面的内部和外部漏洞数据、威胁情报、人工渗透测试结果和业务资产关键性等因素持续挂钩，以衡量风险、提供漏洞武器化的早期预警、预测攻击并对修复活动加以排序。

与 CVSS 不同，该平台专有的 VRR 评分使企业能够准确地衡量影响，并确定漏洞被利用的可能性大小。Ivanti Neurons for ASOC 还专门识别远程代码执行 (RCE) 和特权升级 (PE) 漏洞、与勒索软件有关的漏洞，以及正在流行和活跃的漏洞。这些信息帮助企业专注于那些给他们带来最大风险的漏洞。

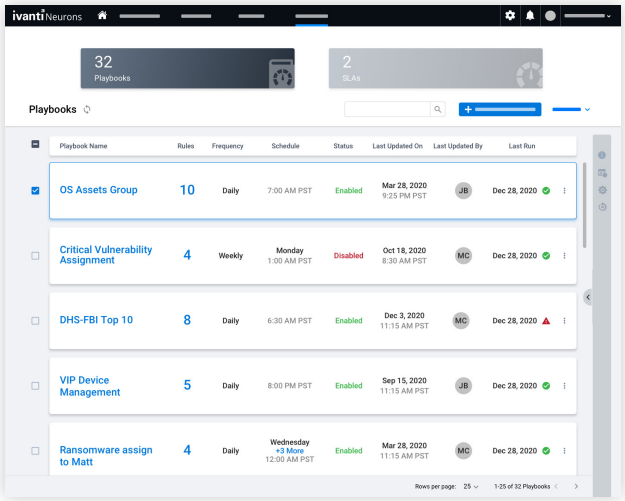




提高漏洞管理流程的效率

Ivanti Neurons for ASOC 可以帮助您改善网络安全态势，同时减少所需的时间和精力：

- 该平台持续不断地关联并分析全面的内部和外部漏洞数据、威胁情报、人工渗漏测试结果和企业资产关键性，以帮助用户充分了解相关攻击计划——如果人工执行，那么这一过程通常需要数周时间。
- 指导手册让那些常见或重复性任务得以自动化，因此用户可以将时间和精力集中在修补操作而不是管理上。
- 服务级协议自动化 (SLA) 允许自动设置漏洞关闭的到期日期。
- 可定制的自动化通知提供平台外的近实时警报，将用户直接链接到包含订阅事件相关信息的平台页面。
- 由 Ivanti 安全团队推送的系统筛选器可以依据漏洞流行标准（例如勒索软件、流行的 CVE、FBI/DHS/CISA 十大最常被利用的漏洞或跨站脚本），轻松筛选应用和应用发现结果，定期揭示那些最紧要的漏洞。



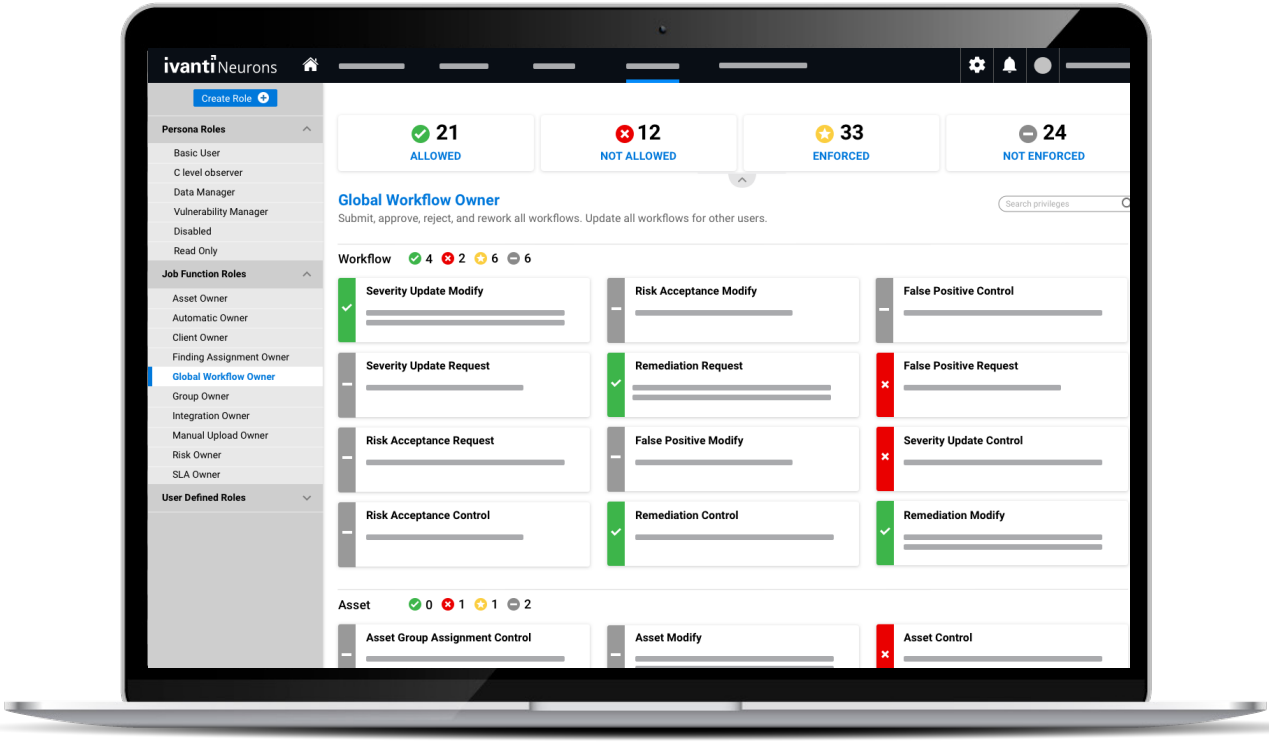
使安全利益相关者彼此之间能够更好地协作

及时向整个组织范围内的安全利益相关者提供与其角色相关的信息，促进技术部门好和业务部门安全利益相关者之间更好地开展沟通和协作。Ivanti Neurons for ASOC 使企业能够安全地对所有适用人员提供平台访问权限。

一旦进入该平台，用户可以访问为从安全人员到高管等不同角色设计的一系列现成仪表板。这些标准仪表板也可以进行修改，以适应更具体的用例。此外，用户小部件让用户能够创建完全定制的仪表板，以满足不同角色和团队的具体需求。

为了进一步促进合作，Ivanti Neurons for ASOC 允许用户创建深度链接，与其他用户分享他们当前所看到的平台页面。这有助于消除各孤立团队之间的沟通隔阂，让所有团队都能真正看到同一页面，形成共识。用户还能够分享仪表板、导出模板和筛选器。

最后同样重要的是，该平台以 Ivanti RS³ 评分的形式对组织的风险状况进行量化，确保所有安全利益相关者对企业整体安全水平保持一致认识。与工单系统的双向集成改善了利益相关者在努力提升企业安全水平时彼此之间的协调性，使他们能够在整个修复过程中保持可见性，同时不必麻烦他们带来离开其首选系统。



特性与功能

特性	功能
多样化数据源	借助一个平台从应用扫描程序（SAST、DAST、OSS、容器）抓取数据、从 100 多个数据源抓取漏洞信息，从研究和渗透测试团队抓取手动调查发现，以及从自定义数据源抓取数据，实现对网络风险的广泛了解。
威胁引擎	通过来自 Ivanti Neurons for Vulnerability Knowledge Base 的人工生成及 AI 驱动的威胁情报，获得对漏洞前所未有的清楚认识，比如哪些漏洞与勒索软件有关。
漏洞风险评级 (VRR)	风险评分综合考虑漏洞的内在属性及其现实威胁背景，有助于快速确定漏洞所带来的风险，
Ivanti RS[3]	通过一套专有评分方法综合考虑 VRR、资产的业务关键性、众多威胁情报来源和外部可访问性，实现对企业风险状况的量化认识。
自动化	利用该平台许多自动化功能，免除一系列的手动任务，使员工能够专注于修复行动和战略举措而不是行政管理工作。
警报和通知	平台通知引擎能够发出近实时警报，帮助你立即察觉相关事件。同样，通过利用深度链接，引导其他用户查看平台内的重要信息。
可定制的数据组织结构	通过用户小部件创建自定义仪表板，利用分组功能对数据进行列表透视处理，从中发现可付诸行动的洞见。
仪表板	利用现成可用和可定制的仪表板（并且其中每个视图还能向下深度钻取），实现跨应用的卓越可视化查询和风险发现能力。
筛选器	通过利用基于威胁的筛选器，快速了解 BlueKeep、WannaCry 或 FBI/DHS/CISA 十大最常被利用的漏洞等特定威胁在您的企业环境中的表现。还可以创建并分享您的自定义筛选器。

关于 Ivantii

Ivanti 让无处不在的工作空间成为可能。在无处不在的工作空间，员工使用各种各样的设备访问 IT 网络、应用和数据，以便能够在任何地方保持工作效率。Ivanti 自动化平台连接业界领先的统一端点管理、零信任安全和企业服务管理解决方案，通过单一操作窗口让企业能够为设备提供自我修复和自我保护服务，并为最终用户提供自助服务。已有超过 40,000 家客户，包括 96 家财富百强企业，选择了 Ivanti 来为他们发现、管理、保护和服务从云端到边缘的 IT 资产，并为员工提供卓越的终端用户体验，无论他们在哪里、用什么方式工作。更多信息请访问 ivanti.com.cn。

ivanti

ivanti.com.cn
8610 8541 2999
ContactChina@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/