ivanti neurons

DATASHEET

Ivanti Neurons for App Security Orchestration & Correlation (ASOC)

将基于风险的漏洞管理扩展到应用程序堆栈

使用 Ivanti Neurons for ASOC 将应用程序的漏洞管理发展为基于风险的方法。该 SaaS 产品使您能够快速、明智地决定在哪里进行开发，以提高内部和面向客户的应用程序的安全性。

基于风险的漏洞管理必须包括应用程序

每季度扫描的应用程序数量在 10 年内增加了两倍。扫描频率同期增加了 20 倍。[1] 对于使用传统漏洞管理方法的组织来说，识别应用程序堆栈中构成重大风险的罕见漏洞或弱点毫无疑问是一个缓慢的过程 — 他们被数据淹没了。

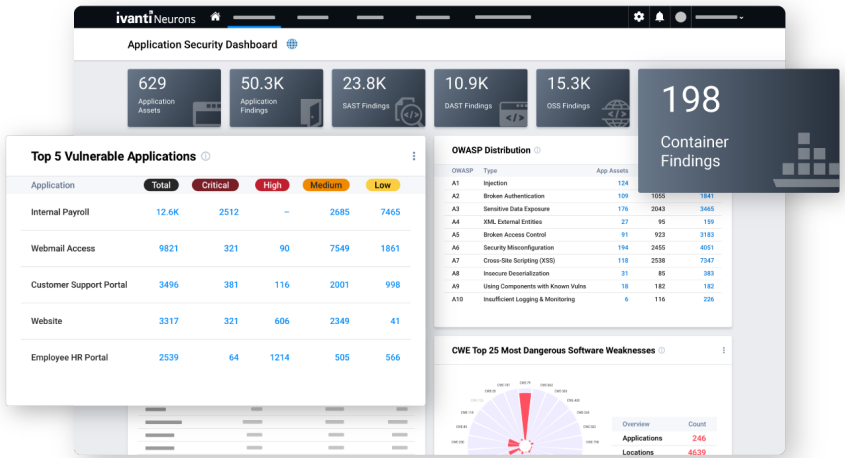
在这些组织开始优先考虑漏洞和弱点进行修复之前，他们必须首先收集一系列不同的数据——SAST、DAST、OSS和容器扫描结果、威胁情报等等——规范这些数据并准备使用。如果手动完成，这些过程需要数周时间才能完成，并且很容易出现人为错误。

优先级排序过程也好不到哪去。考虑勒索软件漏洞。74% 的漏洞在 CVSS v3 下未被评为“严重”，CISA 已知利用漏洞 (KEV) 目录中缺少 156 个漏洞。此外，三款非常流行的扫描仪仍未针对总共 20 个勒索软件漏洞添加插件和检测签名。[2]

最重要的是，相关团队之间缺乏合作被认为是防御网络攻击的最大挑战。[3]漏洞管理利益相关者之间的这种摩擦可能会减慢修复速度，并使组织容易受到攻击。

Ivanti Neurons for ASOC

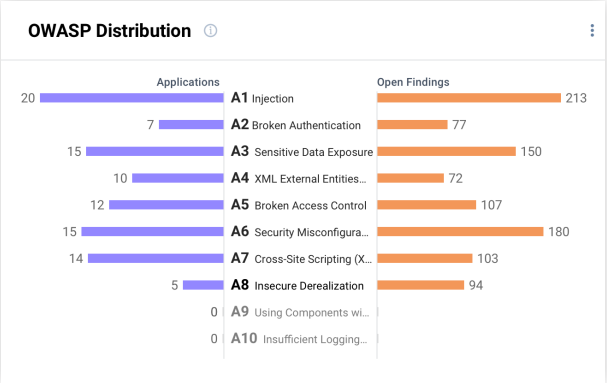
借助 Ivanti Neurons for ASOC 中的功能，对您的应用程序堆栈采用基于风险的方法进行漏洞管理。这些功能打包在一个界面中，因此您可以逐步淘汰过去定义的漏洞管理实践的“转椅”方法。



关键能力

实现应用程序风险暴露的全栈可见性

获得从开发到生产的应用程序风险暴露的全栈可见性。Ivanti Neurons for ASOC 统一了所有应用程序扫描数据（SAST、DAST、OSS 和容器），以定位漏洞和弱点并确定修复的优先级。



Ivanti Neurons for ASOC 与扫描仪无关，允许开发运营人员在开发生命周期的不同部分选择所需的各种扫描工具。该产品将所有应用程序漏洞和扫描结果标准化，然后不断地将它们与野外的活动威胁趋势相关联，使用户能够立即知道哪些结果对其组织来说是最大的风险。用户还可以深入了解这些发现所在的应用程序堆栈中的确切代码位置。

此外，该产品的应用程序安全仪表板通过提供暴露组织的漏洞、CWE 和 OWASP 结果的全面视图，以及新扫描结果的和已得到修复的比率，让用户可以查看应用程序开发在解决安全债务方面的进展。

根据威胁风险等级优先考虑并立即采取的行动

通过基于情境的、基于风险的组织网络安全态势视图，从检测漏洞和弱点到在几分钟（而不是几个月）内进行修复。Ivanti Neurons for ASOC 通过一个流程来衡量风险并确定补救活动的优先级，该流程涉及组织的应用程序与以下内容的持续关联：

- 内部和外部漏洞数据。
- 威胁情报。
- 手动笔测试和基于研究的结果。
- 业务资产的重要性。

最重要的是：您几乎不需要甚至不需要任何手动操作即可制定完全知情的攻击计划。

此外，与 CVSS 不同，Ivanti 专有的漏洞风险评级 (VRR) 可让组织准确衡量影响并确定漏洞被利用的可能性。Ivanti Neurons for ASOC 还专门识别远程代码执行、权限升级、勒索软件以及趋势和活动漏洞。此信息可帮助组织关注那些给他们带来最大风险的漏洞。

专注于补救，而不是管理

通过一系列自动化和其他提高效率的功能，无需花费传统上与此相关的所有时间、精力和错误即可改善您的网络安全状况：

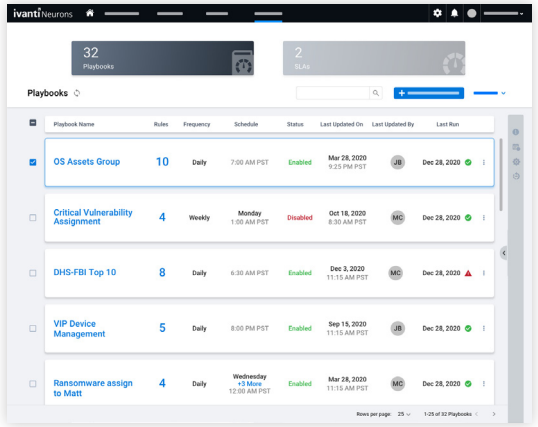
- 创建剧本以自动执行传统上由安全分析师处理的常见或重复性任务。
- 如果需要，可通过服务级别协议自动化自动设置漏洞关闭截止日期。
- 在产品外部接收近乎实时的警报，该警报链接回包含与订阅事件相关的信息的产品页面。
- 使用Ivanti 安全团队推出的系统视图，通过趋势标准轻松过滤应用程序和应用程序发现结果，这些趋势标准揭示了最严重漏洞的暴露情况（例如勒索软件和趋势CVE）。

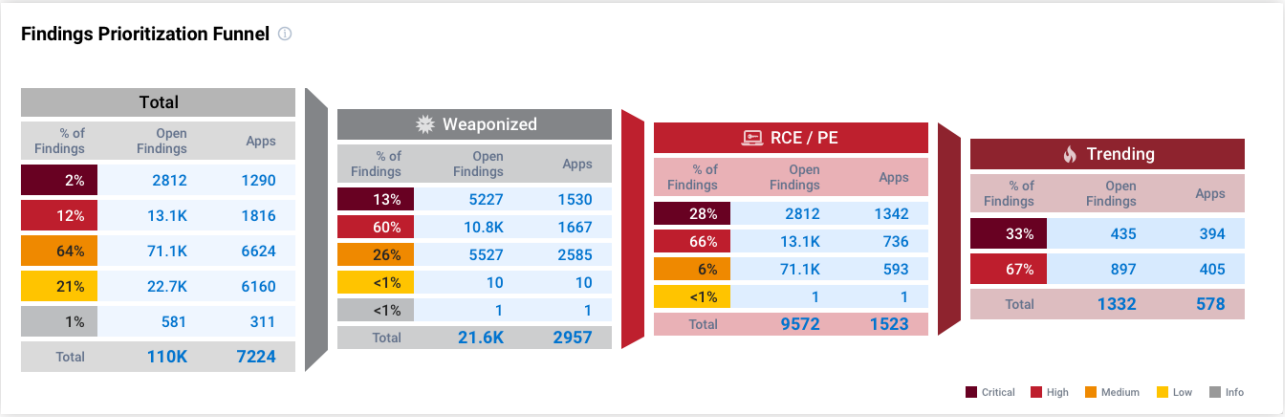
促进安全利益相关者之间更好的协作

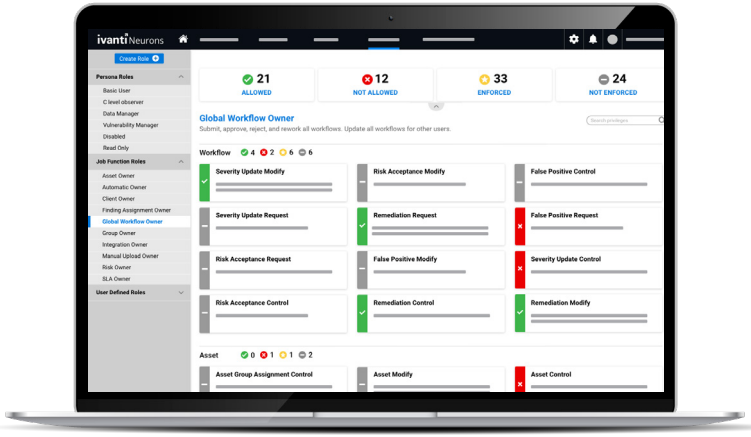
通过向整个组织的安全利益相关者提供与其角色相关的及时信息，促进他们之间的沟通与合作。Ivanti Neurons for ASOC 采用基于角色的访问控制 (RBAC)，因此可以安全地向所有相关人员提供产品访问权限。

使用产品后，用户就可以访问为从 SOC 到管理层的人员设计的仪表板。他们可以修改这些仪表板以适应更具体的场景，甚至利用用户小部件来创建自定义仪表板，以满足不同角色和团队的确切需求。

此外，该产品还以 Ivanti RS3 评分的形式量化组织的风险状况。该分数可确保所有安全利益相关者在组织的整体安全级别上保持一致。与 Ivanti Neurons for ITSM 等票务系统的双向集成可改善致力于提高安全级别的人员之间的协调。







特点与功能

特点	功能
多样化的数据源	使用从应用程序扫描仪（SAST、DAST、OSS、容器）获取数据、来自 100 多个来源的漏洞发现结果、研究和笔测试团队的手动发现结果以及自定义数据源的产品，获得对网络风险的广泛了解。
威胁引擎	通过源自 Ivanti Neurons 漏洞知识库的人工生成和 AI 驱动的威胁情报，获得对漏洞（例如与勒索软件相关的漏洞）无与伦比的洞察。
漏洞风险评级 (VRR)	通过考虑漏洞内在属性和现实威胁背景的数字风险评分，快速确定漏洞带来的风险。
Ivanti RS^3	通过考虑 VRR、资产业务关键性、威胁情报和外部可访问性的专有评分方法，获得组织风险状况的量化视图。
自动化	用自动化取代一系列手动任务，以便员工可以专注于补救措施和战略计划，而不是管理。
警报和通知	通过通知引擎发送的近乎实时的警报，即时了解相关事件。同样，使用深层链接将其他用户引导至产品内的重要信息。
定制数据组织	使用用户小部件发现可操作的见解，这些小部件允许创建自定义仪表板，并且能够在列表视图中透视数据。
仪表板	通过配备向下钻取功能的现成且可定制的仪表板，实现跨资产和基础设施的卓越可视化查询和风险发现功能。
基于威胁的观点	通过利用基于威胁的视图，快速发现最重要的漏洞（例如 Log4j 以及与星期二补丁发布相关的漏洞）如何在您的环境中显现出来。还可以创建并共享您自己的自定义视图。
Neurons 整合	将适用于 ASOC 的 Ivanti Neurons 与适用于 RBVM 的 Ivanti Neurons 配对，可将基于风险的漏洞管理扩展到更大的攻击面区域。利用与 Ivanti Neurons for ITSM 的开箱即用集成，使整个组织的漏洞管理从业者能够更高效地执行任务。

关于Ivanti

Ivanti 提升并保护无处不在的工作，以便人员和组织能够蓬勃发展。我们让技术为人们服务，而不是相反。当今的员工使用各种公司和个人设备通过多个网络访问 IT 应用程序和数据，以便随时随地保持高效工作。Ivanti 是唯一能够发现、管理和保护组织中每个 IT 资产和端点的技术公司之一。超过 40,000 家客户（包括财富 100 强中的 88 家客户）选择 Ivanti 来帮助他们提供卓越的数字化员工体验，并提高 IT 和安全团队的生产力和效率。在 Ivanti，我们努力创造一个让所有观点都能被倾听、尊重和重视的环境，并致力于为我们的客户、合作伙伴、员工和地球创造一个更加可持续的未来。

ivanti

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

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/