解决方案说明

SOC 洞察

应用 AI 驱动的分析方法，将大量的事件、网络、生态系统和 DNS 情报数据转化为切实可行的洞察，从而提高 SecOps 效率

SECOPS 效率的障碍

与当今企业或政府组织的其他职能部门一样，现代 SOC 难以利用现有资源做更多工作。根据 SANS 2023 SOC 调查[1]，在妨碍充分利用 SOC 功能的十大 SOC 障碍中，80% 属于以下三个方面：

- 了解和处理警报
- 工具之间的集成或自动化有限
- 利用现有人员和技能执行关键任务

但真正最悲惨的统计数据可能是，十多年来，所有这些障碍一直在挑战 SOC。从简单地根据恶意软件排名和其他基本过滤器自动确定事件优先级开始逐步改进，仍然无法跟上可能需要 SOC 分析师关注的警报和其他事件的增长。所以，情况只会变得更糟。

人工智能驱动的 SOC 洞察

现代持续性威胁依赖灵活的攻击者基础设施和动态 C2 系统来托管和部署单次攻击中涉及的众多渗透测试、漏洞利用、加密和其他工具。这使得他们极度依赖 DNS，并突出了防御者可以用于检测和破坏这些威胁的关键弱点。

无论协议、平台、操作系统、应用甚至位置如何，DNS 都能看到合法活动和恶意活动。凭借这种独特的可见性，美国国家安全局 (NSA) 网络安全局局长主持的一项试点计划显示，确保 DNS 安全可将恶意软件攻击减少 92%[2]！

事实与数据

- 60% 的 SOC 分析师表示，他们的**工作量在不断增加**，65% 的分析师 **可能会**在明年更换工作[4]。
- 55% 的受访者表示，**每周甚至每天**都会经常错过关键警报[5]。
- 64% 的分析师表示，**手动工作占用了他们一半以上的时间**[6]。
- 配置错误是**造成错误相关漏洞的三大因素之一**[3]。
- 妨碍充分利用 SOC 的十大**障碍中有 8 个**涉及警报、工具集成和技能短缺[1]。
- 77% 的首席执行官 (CEO) 对**关键技能的可用性感到担忧**[7]。
- **92% 的恶意软件和 C2 活动可以**通过正确的 DNS 情报和可见性在 DNS 层得到控制[2]。

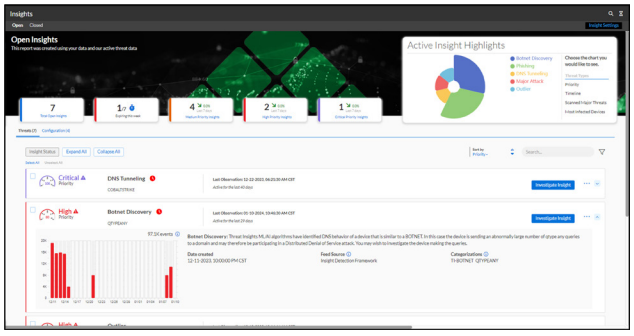

图 1: 借助 SOC *Insights* 摘要页面，分析师仅需点击一次，即可访问最重要的内容。

SOC Insights 与 Infoblox 的 DNS 检测和响应 (DNSDR) 解决方案 BloxOne Threat Defense 配合使用，提供 AI 驱动的独特分析，以检测其他工具忽略的未知威胁活动，提高 SOC 效率，并改善当前安全投资的整体投资回报率。

利用一系列洞察解决多个问题

事件或泄露发生后的调查往往会发现，由于配置错误、安全工具集成难题或简单的警报过载，恶意活动的早期迹象被忽略了。SOC Insights 将 AI 驱动的分析技术应用于大量数据中，帮助应对这些风险。

安全洞察

SOC Insights 的安全插件可用于 BloxOne Threat Defense “Business Cloud” 或 “Advanced”，它使用 AI 将大量事件、网络、生态系统和 DNS 可见性和情报提炼为一组可管理、切实可行的安全洞察。

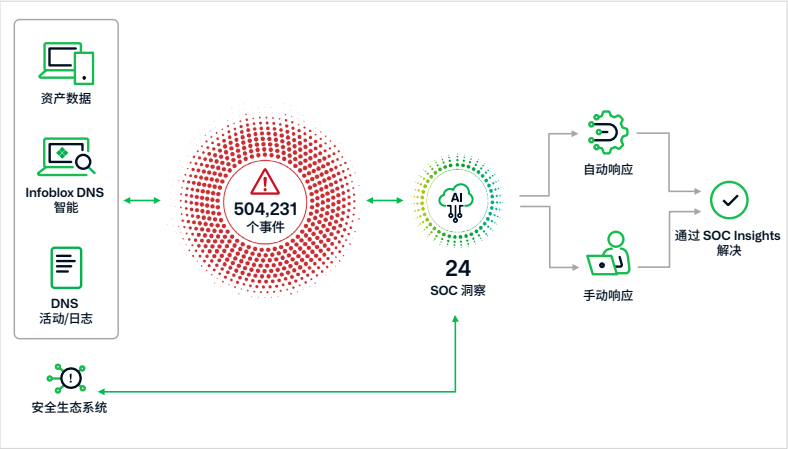

图 2：让 SOC *Insights* 消除警报过载，将堆积如山的事件提炼成一组更易于管理且有意义、切实可行的洞察。

- 零日 DNS™
- 持续性威胁
- 主动威胁传播
- 重大攻击
- 僵尸网络发现
- 异常通信
- 网络钓鱼
- 恶意软件
- 开放式 DNS 解析器
- DNS 隧道
- 数据丢失活动
- 定向攻击
- DNS 错误过多
- Lookalike 域监控

配置洞察

SOC Insights 的配置功能包含在 BloxOne Threat Defense “Business Cloud” 和 “Advanced” 中，有助于用户确保他们充分利用当前的最佳实践并避免常见错误。按照视频和其他指南帮助处理错误和漏洞，或针对允许的例外情况停用不必要警告。

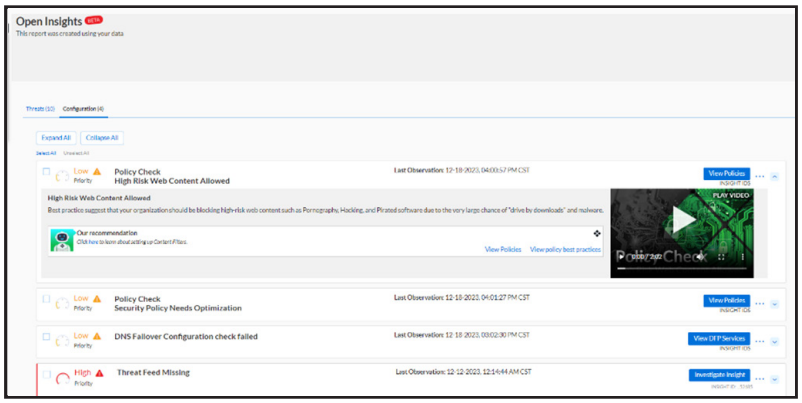

图 3：主动识别薄弱或危险的配置错误，以确保最佳的防御、调查和响应能力。

- DNS 威胁信息缺失
- VirusTotal 免费密钥丢失
- 安全策略需要优化
- DNS 故障转移检查失败
- Feed 操作不匹配
- DFP 隐藏资产详情
- 日志模式下的安全策略
- 网络内容过滤器关闭
- 允许高风险网络内容

对财务、运营和业务产生积极影响

虽然大多数安全工具只能承诺“易于使用”和“减少泄露”，但 SOC Insights 可以做更多事情，包括减少分析师的压力和人员流动率，以及减少扩张、并购和其他业务计划带来的许多安全问题。例如：

- DNS 的特性使其能够在几分钟内（而不是几个月）轻松将新位置或业务合作伙伴统一到通用 DNS 基础设施上。
- 配置洞察具有高度主动性，可以帮助缓解由于“配置错误”而导致的泄露或数据丢失，而“配置错误”是错误相关泄露中报告的三大因素之一[3]。
- “恶意软件”、“网络钓鱼”、“僵尸网络”和其他“重大”或“传播”活动的自相关性使响应者能够同时应对许多威胁，从而提高他们的效率。
- 通过监控“异常值”、“DNS 隧道”和“开放式解析器”等洞察类别，以及 BloxOne Threat Defenses 独有的 Lookalike 和应用可见性功能，转而采取更加积极主动的安全态势。
- 通过提供切实可行的“洞察”，而不仅仅是提供原始日志和事件，安全生态系统的智能集成可以提高整个安全堆栈的投资回报率 (ROI)。
- SOC Insights 自动收集相关数据，并使分析师能够查看和分析这些数据，从而更快、更有把握地得出结论。这有助于减轻压力并提高技能娴熟且经验丰富的安全专业人员的保留率。

令人惊叹的成果

客户报告称，通过配合使用 SOC Insights 和 BloxOne Threat Defense，他们获得了显著效益，包括：

- 将 EDR 和 FW 警报减少了 50%
- 平均每月节省 500 个 SOC 分析师工时
- 每年节省 40 万美元的生产成本

通过洞察提升 SIEM、SOAR 和生态系统的其他部分

SecOps 深知在安全生态系统中共享原始数据的价值和局限性。这使得 SIEM 和 SOAR 专业技能成为大多数组织最具挑战性的技能之一。SOC Insights 可以减轻这些其他工具的负担，并能在整个安全堆栈中共享由此产生的洞察，使其他工具更加有效，从而进一步提高 SecOps 整体效率。

1 “SANS 2023 SOC Survey”，2023 年 6 月，作者：Chris Crowley、Barbara Filkins、John Pescatore

2 “NSA launches pilot program to secure defense contractors”，2020 年 6 月 18 日，作者：Lauren C. Williams，NEXTGOV/FCW

3 “Verizon 2023 DBIR Report”

4 “Voice of the SOC Analyst”

5 “The Orca Security 2022 Cloud Security Alert Fatigue Report”

6 “Voice of the SOC Analyst”

7 https://www.pwc.com/m1/en/publications/five-challenges-cloud-adoption-how-overcome-them.html

Infoblox 将网络和安全融为一体，提供无与伦比的性能和保护。我们深受《财富》100 强公司和新兴创新者的信赖，提供对连接到您网络的人员和内容的实时可见性和控制，因此您的组织可以更快地运行并更早地阻止威胁。

公司总部
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

版本：20240411v2