Claroty 威胁情报

Claroty xDome 威胁中心精选的威胁情报

随着新设备类型和操作流程的不断引入，能源行业、制造行业、交通运输行业、医疗保健行业等关键基础设施领域的攻击面显著扩大，针对网络化物理系统（Cyber Physical Systems, CPS）的威胁情报变得愈发重要。而且，运营技术(OT)、物联网(IoT)、医疗物联网(IoMT)设备日益互联，它们更容易遭受复杂的网络攻击，这些攻击可能对现实世界造成影响。因此，需要采用实时、主动的方法妥善补救。如今，人们越来越意识到国家层面的网络安全威胁，同时，监管机构对网络安全的要求（例如 NIST 标准、IEC-62443 标准）变得更加严格，再加上一些广为人知的勒索攻击事件，这些因素都突显了网络安全的重要性。

Claroty提供强大的威胁情报功能，旨在保护工业、医疗保健、商业环境免受不断演变的网络威胁。凭借深厚的领域专业知识，Claroty的威胁情报源、分析和检测机制提供专门针对CPS的主动、可操作的见解。

优势

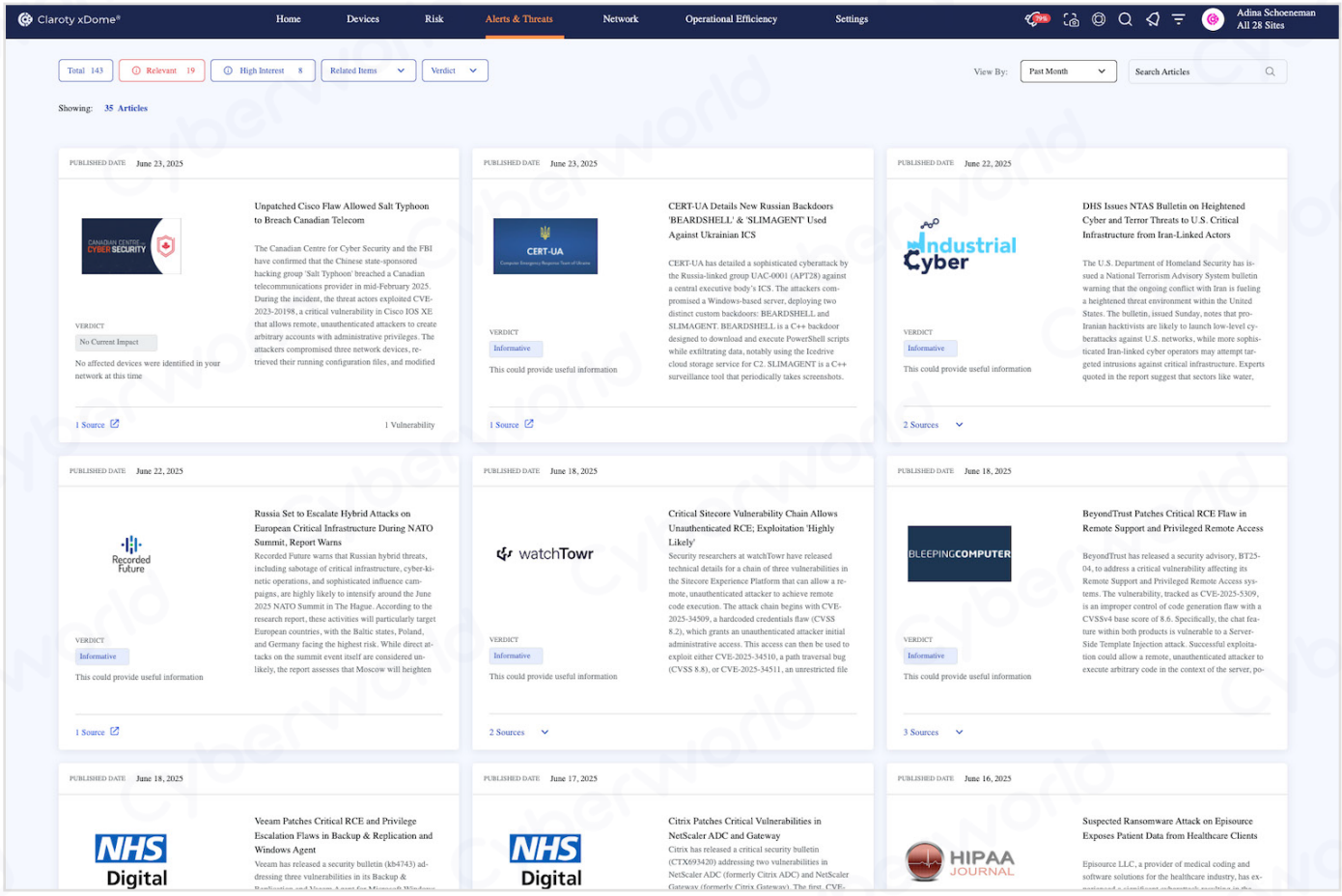
- **消除干扰：**通过实时且相关的威胁情报、关键基础设施的警报通知，主动应对威胁行为者。
- **缩短威胁的潜伏时间：**快速检测和具备上下文的警报，可最大限度地缩短响应时间，精准定位企业面临的直接风险。
- **迅速做出明智决策：**通过关联网络威胁特征、自定义配置的警报、与接收到的威胁情报直接相关的CVE，赋能安全团队。

为关键环境打造的实时威胁见解

Claroty xDome 威胁中心（Threat Center）提供对 CPS 威胁的实时可视化及可操作的见解，让安全团队更快、更准确地检测威胁、确定优先级并响应事件。

安全团队使用 Claroty xDome 威胁中心，能够将资产概况与当前的威胁事件关联起来。Claroty xDome 威胁中心是直接集成到异常和威胁检测（Anomaly and Threat Detection）模块中，不仅提供当前的事件信息，还提供内容丰富的CPS威胁情报，深入了解威胁是否直接影响其环境，并帮助企业主动识别新兴风险，包括零日漏洞和国家支持的攻击模式，在其影响关键运营之前加以应对。**主要功能包括：**

- **威胁中心文章（Threat Center Articles）：**Claroty 的威胁情报由 Claroty 内部精选的第三方资源以及 Claroty Team82 研究团队提供支持。Claroty xDome 威胁中心的文章可确保企业在其网络化物理环境中始终领先于新兴威胁。
- **威胁判定（Threat Verdict）：**Claroty xDome 威胁中心推送的每篇文章都提供了威胁判定结果，以便安全团队评估该威胁在其设备资产中的相关性及潜在影响。判定结果会识别该威胁是否与您的网络设备相关、是否具有信息价值、是否对设备暂无影响。



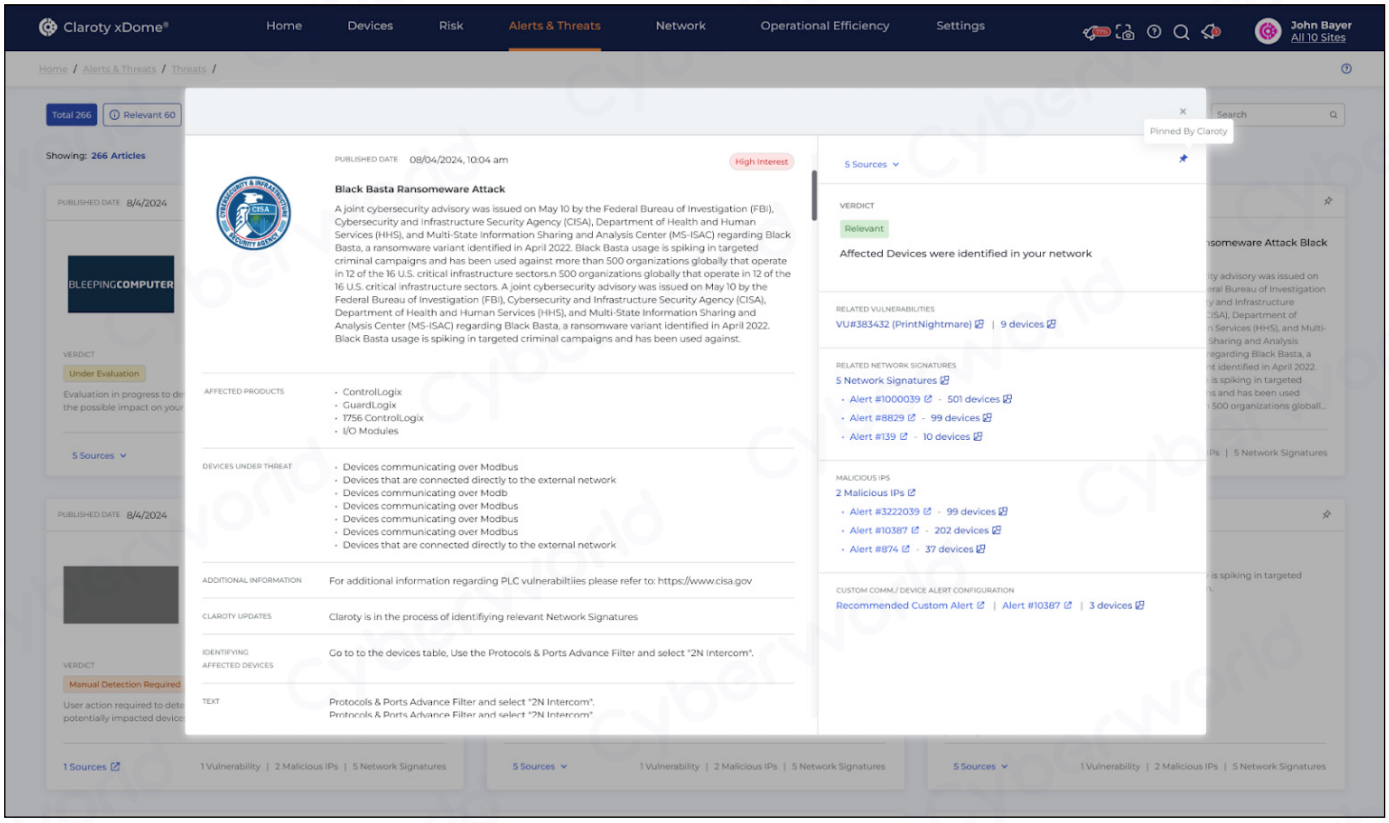
Claroty xDome 威胁中心的威胁判定

VERDICT

具有信息价值 (Informative)	评估中 (Under Evaluation)	需要手动检测 (Manual Detection Required)	相关 (Relevant)	无关 (Irrelevant)	暂无影响 (No Current Impact)
提供有价值的见解，但对用户网络没有直接影响	正在分析其对网络的潜在影响	网络中可能存在受影响的设备，需人工输入确认	该文章与用户网络中的设备直接相关	对网络无直接影响，也不存在相关项（Related Items）	虽然存在相关项（Related Items），但目前与该文章无直接关系

- **相关项（Related Items）**的见解与 Claroty xDome 威胁中心的文章相关，例如受影响设备的品牌、型号、制造商、相关漏洞、恶意网络签名、IP地址、与文章直接相关的警报。这些洞察全面展现了威胁对您环境的潜在影响。

通过将威胁情报与资产环境、风险态势相结合，Claroty xDome可帮助减少警报疲劳、加快调查速度，并在 CPS 网络中推动更明智、更符合业务目标的决策。



为每一层防御构建的实用威胁情报

为您的安全运营中心(SOC)提供实时、相关的情报，包括战略见解(strategic insights)、战术指标(tactical indicators)、操作情况(operational context)，实现更快地检测、更智能地响应、更有效地降低风险。在对抗不断演变的威胁的斗争中，掌握最新动态就意味着保持安全。使用 Claroty xDome 威胁中心，您可以在每日推送的文章中了解最新动态。

Claroty 的威胁情报产品不仅仅是一个信息源，而是一个集成的、持续更新的知识库，专为满足 CPS 安全需求而设计。通过弥补传统 IT 威胁情报与 CPS 实际情况之间的差距，Claroty 帮助企业更快、更准确地检测、理解和应对网络威胁。

关于 Claroty

Claroty 凭借以工业为主的平台重新定义了网络化物理系统 (Cyber Physical Systems, CPS) 防护。Claroty 平台旨在保护关键任务型基础设施，提供市场上最深入的资产可视化、最广泛的 CPS 安全解决方案，涵盖了风险管理、网络保护、安全访问、威胁检测，可以在云端使用Claroty xDome，也可以在本地部署Claroty CTD。Claroty 平台以屡获殊荣的 Team82 研究团队、庞大的技术集成联盟为后盾，帮助企业有效降低 CPS 风险，提供最快的价值实现时间 (TTV) 和更低的总拥有成本 (TCO) 。在全球范围内，已有数百家企业在数千个站点部署了Claroty。