CLAROTY

Claroty平台

工业网络安全解决方案

Cyberworld
广州科明大同科技有限公司
中国区总代理
官方网站 www.cyberworld.com.cn
业务电邮 info@cyberworldchina.com
服务专线 400-9988-792

CLAROTY

Claroty 平台

工业网络安全解决方案

Claroty 平台是一项完整的工业网络安全解决方案，包含 Claroty 的持续威胁检测 (Continuous Threat Detection, CTD)、安全远程访问 (Secure Remote Access, SRA) 和 Edge 技术。无论现行的网络安全程序的规模、架构或成熟度如何，该平台都能与任何工业环境无缝对接。高度灵活且快速的部署选项让 Claroty 平台得以揭示和保护网络内部 OT、IoT 和 IIoT 资产，同时通过专有的检测技术自动检测这些资产的威胁的早期指标。为了进一步扩展这些控制措施的价值，Claroty 具备一个巨大的集成生态系统和强效的应用编程接口 (API)，并采用业界唯一的一项解决方案，实现了覆盖整个事件生命周期的集成远程事件管理功能。

Claroty CTD

- 快速发现并管理所有资产，让工业网络全方位可见。
- 实时检测已知威胁和零日威胁，以及行为和操作异常。
- 通过根源分析、风险信息及声誉状况自动拓展警报。
- 将 OT 远程用户活动与异常事件和恶意指标相关联。
- 持续监测完全匹配的漏洞，并提供人工智能驱动的网络分区及分段。
- 可进行内部部署或通过 CTD.Live 部署，CTD.Live 是一项基于“软件即服务”(SaaS)、辅助全企业范围内工业网络安全数据管理的选项。

Claroty SRA

- 获取、控制及简化工业网络远程访问。
- 降低远程用户和第三方用户引发的风险。
- 根据“零信任及最小特权”(Zero Trust & Least Privilege)原则执行 IT 与 OT 最佳安全措施。
- 对所有 OT 远程会话进行全面监控，以监测未经授权的更改、实时故障排除及紧急断开连接。
- 为维护、遵从性和法务目的提供持续审计。
- 提供高度便利、灵活的配置选项、目录服务和防病毒解决方案集成。

Claroty Edge

- 让某一工业环境内部所有 OT、IoT 和 IT 资产即时可视。
- 提高识别和管理风险和漏洞的速度、易用性和有效性。
- 无需硬件、网络变更、配置或任何实体足迹。
- 无论地域分布或架构如何，都适用于任何网络。
- 有助于优化事件响应的相关工作，包括影响评估、范围界定和事件后的取证。
- 擅长为审计合规或并购尽职调查提供即时的详细信息。

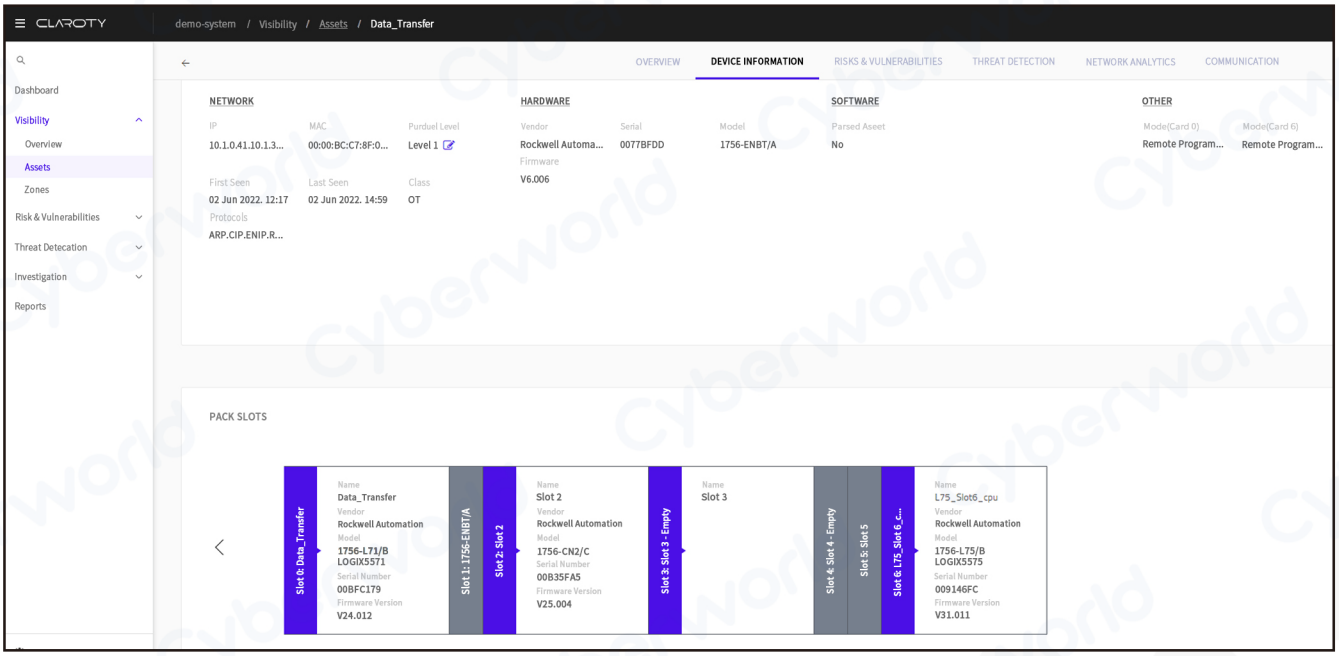
检测 → 调查 → 响应

通过行业最全面的工业网络安全控制和集成的远程事件管理能力，
在最宽泛的攻击面区域内保护您的工业环境。

揭示

有效的工业网络安全始于了解什么需要保护。Claroty 平台支持业内工业环境中最全面的协议列表，包括一系列无与伦比的专有和标准 OT、IoT、IIoT、BMS 和 IT 协议。这种对网络通信的透彻了解带来了不可比拟的资产、网络和进程可见性：

- **资产可见性**涵盖了工业网络上的全部设备，包括串行网络以及关于每个设备的广泛属性，如型号、防火墙版本和自定义资产属性。
- **网络可见性**涵盖了全部网络会话，包括远程访问以及它们的带宽、采取的行为、作出的变更和其他有关详情。
- **流程可见性**追踪所有的 OT 操作，涉及工业资产全部流程的代码段和标签值。



CTD 资产详情页

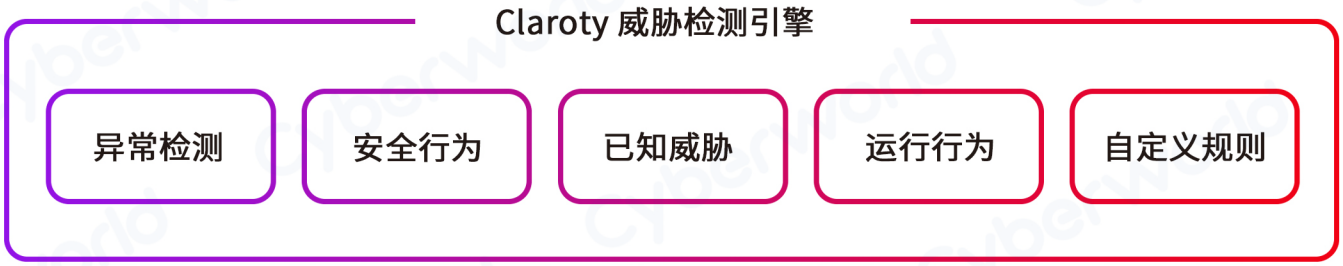
保护

Claroty 平台让人得以了解网络内部存在的内在风险。这些风险包括关键漏洞和错误配置、工作人员和供应商的不良安全举措，以及不可靠、未受监控且效率低下的远程访问机制。这使得用户不但可以识别风险领域和确定其优先级，还可以采取积极主动的控制和缓解措施来管理网络暴露。

- **虚拟区：**在正常情况下，基于网络通信的自动虚拟网络分割，为物理分割创造了一种成本效益高的替代方案，并提供了针对跨区域违规的实时警报机制。
- **攻击媒介映射：**识别并分析工业环境内部的漏洞及风险，以推测攻击者破坏网络最有可能的场景。
- **远程访问控制：**SRA 结合使用了多因素认证、基于使用和群组的分级访问权限和即时调配设置，来严格控制、监测和简化网络远程访问。

检测

Claroty 灵活的威胁检测模型分析了工业网络中的全部资产、通信和进程，以建立精细的行为基线，为我们的五个威胁检测引擎赋能。Claroty 平台让企业具备了在警报出现时快速、有效响应的能力，在分秒必争的紧急情况下提供了节省时间所需的环境及信息。



在最新威胁情报的支持下，Claroty 持续监测已知和未知的威胁，自动排除误报，将相关警报链接至一系列事件中，并为如何在威胁影响运行之前减轻威胁提供明确的指导。

- **上下文警报风险评分：**由独特的算法产生的单一指标，提供触发每个警报的环境的上下文。
- **根源分析：**与同一攻击或事件相关的所有事件都被划归为同一警报，以提供关于事件链的统一视角和根源分析。
- **远程会话监测与审查：**OT 远程会话可实时监测，完整长度的记录可轻易审查。

连接

企业之间的互联互通促使了带有复杂及广泛攻击表面的相互交织的 IT/OT 工业网络的兴起。Claroty 平台消除了长期以来限制工业网络与其他业务安全、有效连接的障碍，通过集成协同效应造就了更具效率的运行以及更低的总拥有成本：

- **集成生态系统：**Claroty 拥有一系列 IT 安全工具，例如安全信息与事件管理(SIEM)、安全编排自动化与响应(SOAR)和配置管理数据库 (CMDB) 解决方案，简化了系统管理并降低工业网络安全的学习难度。
- **API Explorer：**基于 Swagger 框架，API Explorere 让用户得以利用 CTD 提供的大量网络信息，在 Claroty 环境外构建自定义馈送。
- **Claroty Edge & CTD.Live：**Edge 提供的对资产和网络风险的可见性，配合 CTD.Live 基于云端的报告构建功能，有助于将组织的网络安全程序与其治理、企业范围风险与合规程序联系起来。

关于Claroty

Claroty 是一家工业网络安全公司。Claroty 深受全球性大型企业的信赖，可帮助客户揭示、保护和管理其 OT、IoT 和 IIoT 资产。它的综合平台与客户现有的基础设施和计划无缝连接，同时提供全方位的工业网络安全控制，以实现可视化、威胁检测、风险和漏洞管理以及安全远程访问， 所有这些都大大降低了总拥有成本。Claroty 得到了领先的工业自动化供应商的支持和采用，拥有广泛的合作伙伴生态系统和屡获殊荣的研究团队。

了解更多，请访问 www.claroty.com

Cyberworld
广州科明大同科技有限公司
中国区总代理
官方网站 www.cyberworld.com.cn
业务电邮 info@cyberworldchina.com
服务专线 400-9988-792