Claroty 持续威胁检测 (CTD)

工业网络安全挑战与 Claroty CTD

工业安全挑战

数字化转型和远程劳动力的扩张改变了企业的运营模式，曾经孤立的OT与IT环境，现已相互关联。IT与OT网络融合的兴起提供了在工业环境中加强创新和效率的绝佳机会。虽然网络化物理连接存在显著优势，但它会在许多独特和陌生的设备上生成一个扩展的攻击面。传统的IT安全解决方案已不适用于保护专有协议通信。

为了实现运营和网络弹性，Claroty持续威胁检测(CTD)旨在战胜工业环境中网络化物理连接的挑战。CTD具有无与伦比的工业协议库、资产发现方法和专有DPI技术支持，这是在工业环境中实现独一无二可视化的必要条件。

这能够进一步实施涵盖整个网络化物理安全进程的核心网络安全控制，包括：

- 资产发现
- 漏洞和风险管理
- 网络保护
- 威胁检测
- 资产与变更管理
- 远程事件管理

CTD 优势一览

- 通过多种发现方法和部署机制，提供对工业环境的完整可视化。
- 支持完整的网络化物理系统(CPS)的网络安全之旅，从资产发现到网络集成和优化。
- 为所有警报提供情境化根本原因分析和风险评分。
- 与Claroty安全远程访问(SRA)集成，增强远程会话事件响应和调查。
- 与现有IT基础设施（如SIEM、防火墙、SOAR、CMDB工具等）集成，将核心网络安全功能扩展到工业环境中。

资产发现

有效的工业网络安全始于了解需要保护的内容。CTD涵盖了业界最全面的工业协议，采用多种发现方法，确保生成最完整的网络拓扑图。CTD大范围覆盖的发现方法比其他的单一发现方法更容易查出部分网络信息，可以在CPS环境中实现独一无二的可视化。这种发现的深度体现在可视化的三个方面：

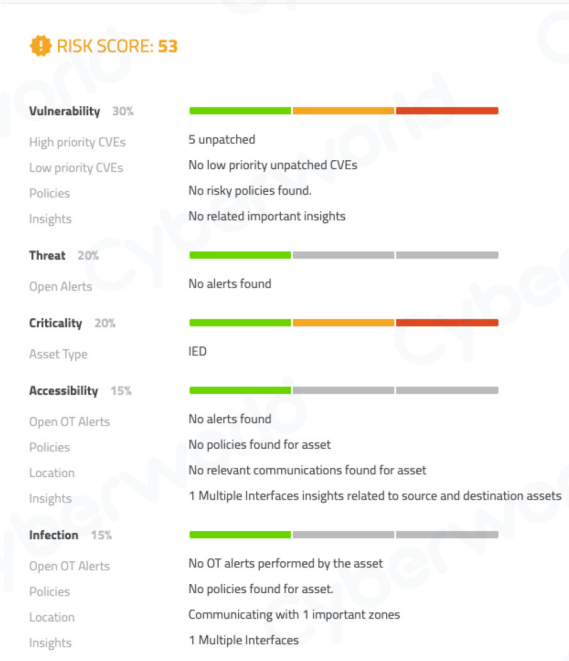
- **资产可视化：**包括工业网络上的所有CPS资产，其中的串行网络，以及每个资产的广泛属性。
- **会话可视化：**包括所有工业网络会话及其带宽、采取的操作、所做的更改、连接路径和其他相关详细信息。
- **过程可视化：**包括跟踪所有工业操作，涉及CPS资产的所有流程代码部分和标签值，以及资产流程值的所有异常变化，这些变化能预示流程完整性是否受到威胁。

使用 Claroty CTD 的资产发现 —— 机架插槽

漏洞和风险管理

Claroty大型数据库包含了屡获殊荣的Team82研究人员跟踪的不安全协议、常见漏洞与披露(CVE)、配置、不合标准的安全实践和其他漏洞，CTD能自动将OT环境中的每项资产与Claroty大型数据库进行对比匹配，用户可以更有效地识别、优先处理和修复工业网络中的漏洞。

- **漏洞库匹配：**根据供应商、型号和固件版本将确切资产与已知CVE准确匹配，高效地确定修复网络漏洞优先级。
- **攻击向量映射：**通过识别和分析已知风险，计算出最有可能被攻击者破坏的网络场景，更好地了解风险状况。
- **风险评分：**基于漏洞带来的网络风险，自动对其进行评估与评分，从而实现更高效的优先级排序与修复。



CTD 的多因素风险评分

网络保护

在Claroty深厚的、专业的领域知识支持下，CTD用其深入的可视化功能，自动对工业网络进行虚拟分段，虚拟区域则是在基线情况下相互通信的逻辑资产组。为了适应您环境中独有的通信路径，CTD可以定制虚拟区域，并提供网络行为可视化拓扑图。作为一种网络分段方法，虚拟区域有助于：

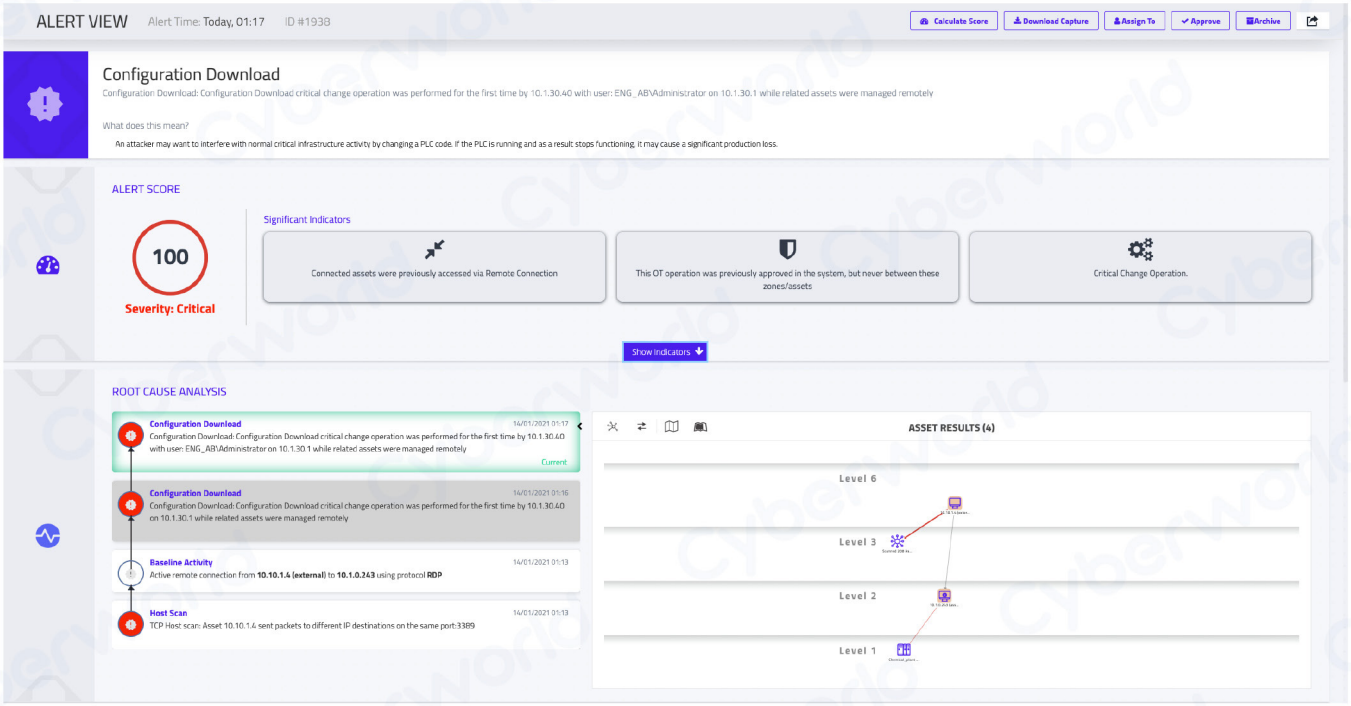
通过异常通信警报 来驱动威胁检测	为高成本的物理分段程序 提供经济高效的替代方案	将现有网络通信基础设施 扩展到工业环境中

CTD 虚拟区域的网络拓扑图

威胁检测

工业网络威胁往往是不断变化的。看似简单，其实是利用对工作流程的守规性引入风险。CTD利用多个检测引擎自动分析工业网络中的所有资产、通信和流程，生成行为基线，描述合法流量的特征，消除误报，并实时提醒用户注意异常，以及已知、未知和新出现的威胁。

- **检测已知与未知威胁：**通过描述合法流量的特征来检测异常通信，识别威胁，剔除误报，并实时提醒用户注意已知、未知和新出现的威胁。
- **操作事件警报：**持续监察行业环境中关键变更操作、工作流程完整性和正常运行时间，接收相关配置下载等操作的警报，从而深入了解文件中的确切代码更改。
- **将警报映射到 MITRE ATT&CK 框架：**传入的警报会映射到针对工业控制系统的MITRE ATT&CK框架，能更加了解事件发生的背景，确定需要采取的补救措施。
- **根本原因分析：**把相关的警报和指标关联到同一个事件中，减少网络噪音、误报和整体警报疲劳，并提供警告活动的综合视图。

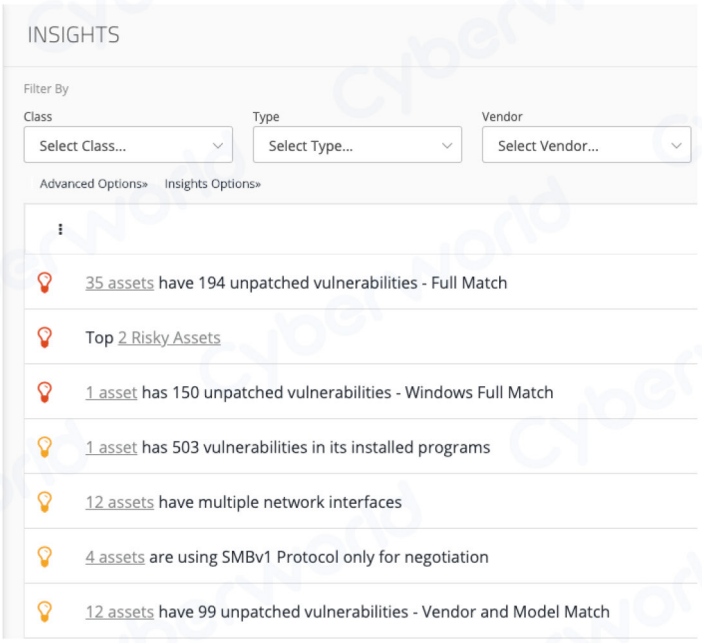


CTD 警报视图，包含关键指标、事件链、根本原因分析

资产与变更管理

在强大且深入的网络可视化支持下，Claroty CTD简化了企业的资产与变更管理。操作员能使用CTD自定义属性，如关注EoL指标、识别运营流程价值以及持续监察新增资产、更新资产或已停用资产等，致使简化资产管理的工作流程，节省时间和减少操作人员的维护窗口。CTD为用户提供的方法如下：

- **监察资产更新：**CTD持续监察漏洞、旧版软件、EoL指标和其他需要更新的变更，保持资产可用性。
- **简化 SLA 合规性：**CTD 的可行性和自定义属性，可以轻松识别、报告特定资产的 SLA 合规状态。
- **识别资产变动：**网络添加、配置更改和异常是 CTD 监察的众多变量中的一部分，支持变更管理程序。

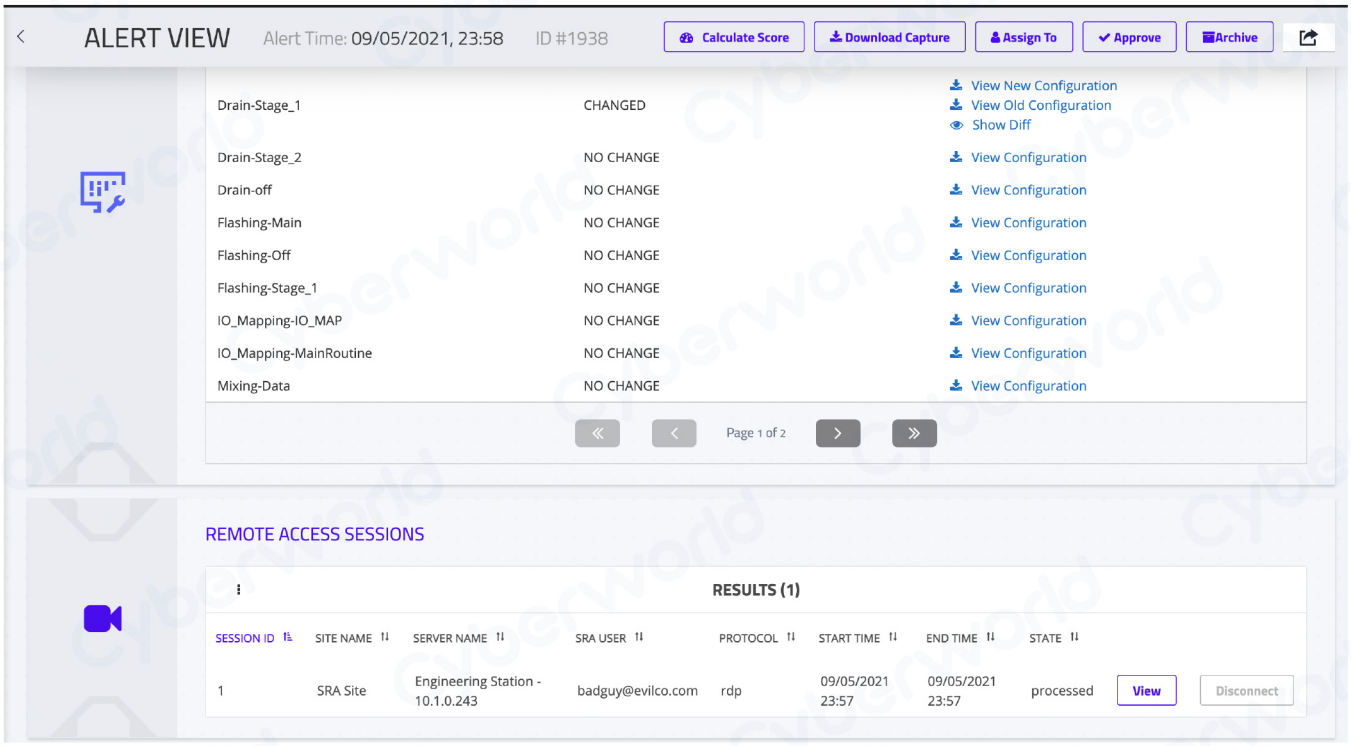


CTD 网络风险排序

远程事件管理

作为CPS网络安全解决方案的一部分，CTD和Claroty安全远程访问(SRA)联合推动增强两种解决方案的警报响应能力。用户能使用这些解决方案从任何位置检测、调查和响应事件。因此，企业可以通过以下方法，为远程、分布式或混合工作环境调整其整体安全态势和工作流程：

直接在 CTD 的远程会话期间 接收事件警报和相关指标	通过访问远程日志、实时监察 和记录的会话来调查远程用户活动	响应远程事件警报 能够立即断开远程会话



CTD 警报视图，包含配置更改详细信息和关联远程会话记录的链接

关于 Claroty

Claroty 使工业、医疗保健和商业机构能够保护其环境中的所有网络化物理系统——扩展物联网 (XIoT)。Claroty平台可以与客户现有的基础设施集成，提供可视化、漏洞和风险管理、威胁检测、安全远程访问的全方位控制。Claroty 得到了全球领先的工业自动化供应商的支持和采用，拥有广泛的合作生态系统以及屡获殊荣的 Team82 研究团队。

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