CLAROTY

案例研究

优化事件管理

使用 Claroty 平台

Claroty 平台是一个完整的运营技术 (OT) 安全解决方案，包括 Claroty 的持续威胁检测 (CTD) 和安全远程访问 (SRA) 产品，以及它们提供的无数基本安全控制功能。这些控制功能显示了 OT 和 IT 员工的需求和优先事项，该平台能够让这两种类型的员工通过最少的培训和无停机时间来管理工业环境中的风险。因此，该平台支持许多用例，这些用例同时涉及 OT 和 IT 员工，并促进他们之间的工作协调。事件管理就是这样一个用例。

以下案例研究，展示了 IT 安全运营中心 (SOC) 人员和 OT 人员如何利用 Claroty 平台优化 OT 远程访问会话期间触发的警报管理。

事件响应

本案例中 IT SOC 人员和 OT 人员各自的角色和职责包括：

IT SOC 人员	OT 人员
• OT 网络安全风险管理	• OT 可用性、可靠性和安全性
• 监控和响应 OT 远程访问事件	• 使用 SRA 远程访问和维护 OT 资产
• 使用 CTD 检测 OT 网络上的异常活动	• 依靠 IT SOC 检测 OT 网络异常

第一部分

OT 工程师提交变更管理 (MoC) 证明，请求授权，希望通过 SRA 链接到工程工作站以对可编程逻辑控制器 (PLC) 进行维护。OT 经理收到工程师的 MoC 证明后，直接在 SRA 内授权请求。

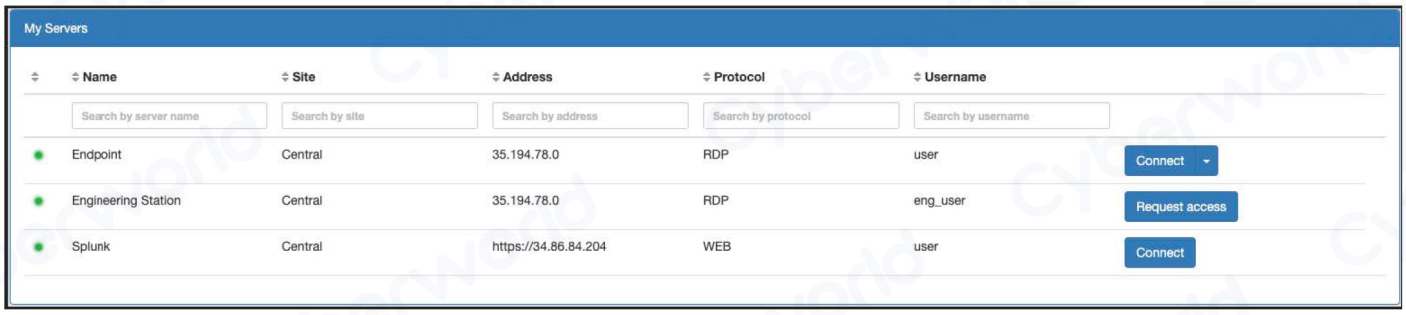

图 1：该图从 OT 工程师的视角显示了 SRA，该工程师请求访问工程工作站对 PLC 进行维护。SRA 支持基于最小权限原则为所有用户实现细粒度身份验证和访问控制。。

第二部分

OT 工程师在使用 SRA 访问工程工作站对 PLC 进行维护时，错误地将新配置下载到 PLC 中。此操作未包含在 MoC 证明中，且未经授权，因此立即在 CTD 中触发配置下载警报。

与 Claroty 所有警报一样，此警报有上下文信息，包括根本原因分析、相关指标、资产和 SRA 会话。它还包括一个警报分数，该分数反映了触发警报的 OT 环境所面临的特定风险级别，此信息有助于减少误报并加快警报分类和调查过程。

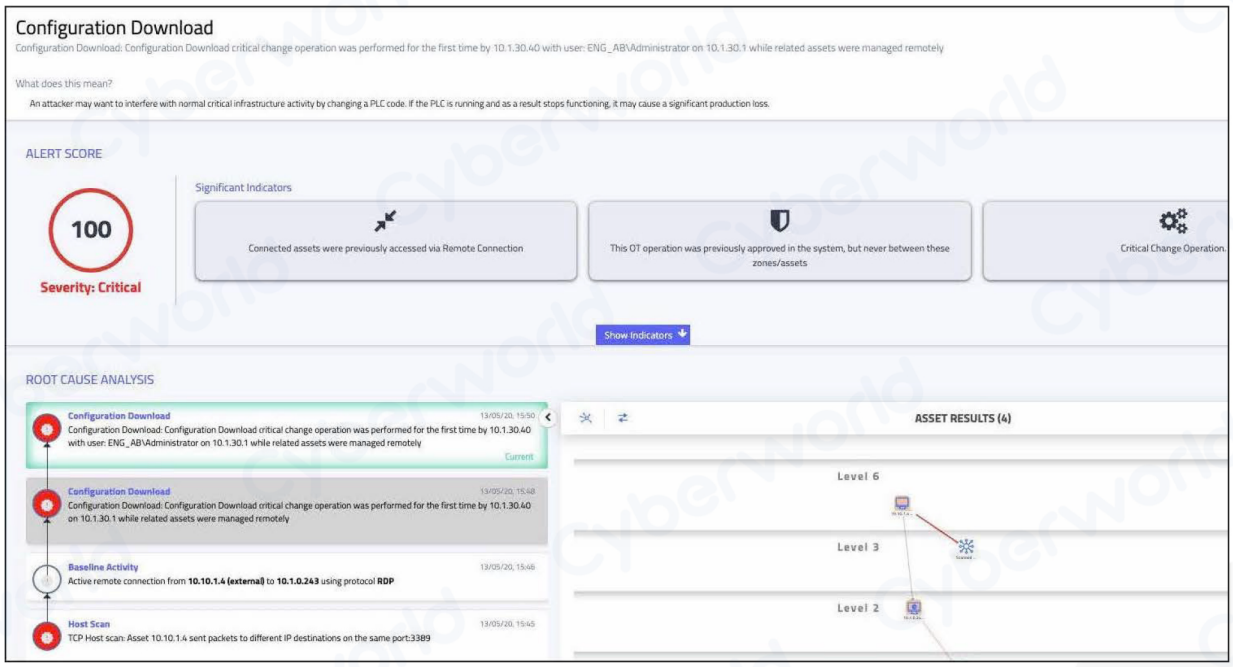

图 2：该图描述了由 OT 工程师操作错误引发警报的根本原因分析、指标、关联资产和风险评分。此警报在 CTD 中可见，IT SOC 分析师能快速查看。

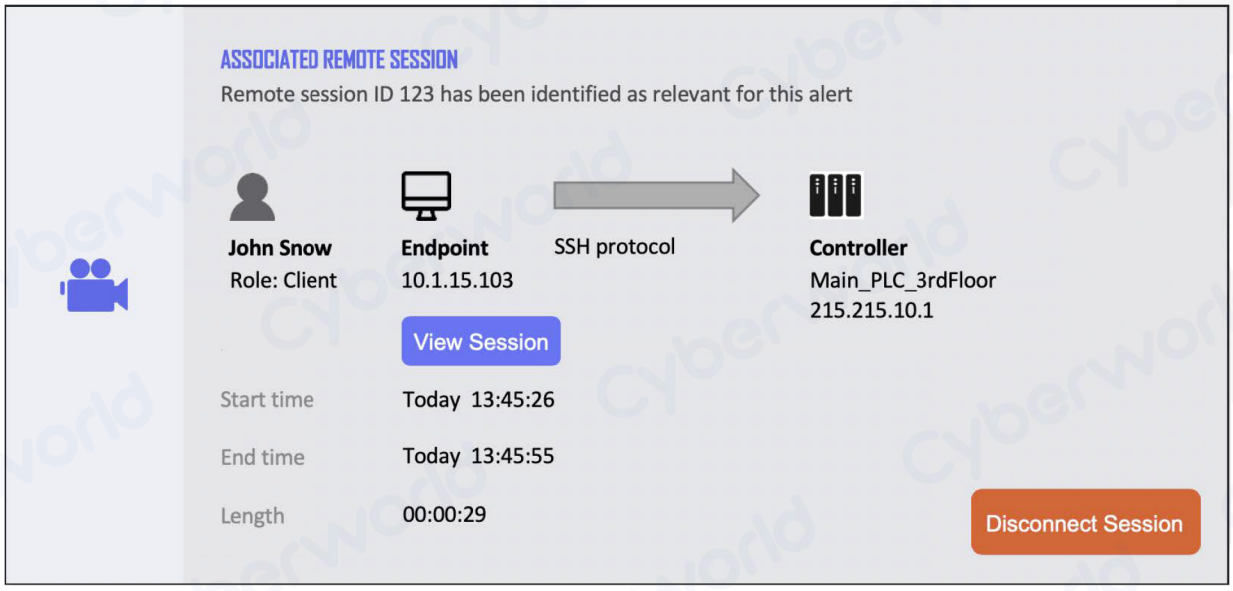

图 3：所有与 SRA 会话相关的警报都链接到该会话。所有 SRA 会话都可以被实时监控，并被完整记录，以供将来的审计和调查之用。SRA 管理员还可以在必要时立即断开正在进行的 SRA 会话。

第三部分

IT SOC 分析师可以快速看到 CTD 中的警报。警报包括原始 MoC 证明、特定 SRA 会话和用户，以及触发它的未授权操作。在查看此信息后，IT SOC 分析师选择将警报升级给 IT SOC 经理。

然后，经理选择直接从 CTD 监控 OT 工程师的实时 SRA 会话，立即决定断开会话，并查看记录以调查触发警报的事件。

OT 工程师识别到他们的 SRA 会话突然终止，试图重新链接到工程工作站，但没有成功。为其会话授予的初始授权不再有效。为了重新链接到工作站，OT 工程师必须请求新会话的授权。

图 4：该图从 OT 工程师的视角描述了 SRA。由于他们之前的 SRA 会话已被 IT SOC 经理断开，工程师无法在没有再次请求和获得批准的情况下启动新会话。此功能有助于减少恶意行为和人为错误。

第四部分

在确定 OT 工程师在 SRA 会话期间将新配置下载到 PLC 是一个无意错误后。IT SOC 经理通知 OT 经理，然后 OT 经理选择授权 OT 工程师重新启动其原始会话的请求。

OT 经理依然选择实时监控此会话，确保它一直无错误和无风险。

CLAROTY

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链接，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。

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