CLAROTY

案例研究

食品和饮料

携手 Claroty 公司，国际食品和饮料公司的数字化转型得到安全保障

一家国际食品和饮料公司的数字化转型战略提高了其生产力和效率，该公司对此感到十分自豪。这家公司将数字化创新和连接扩展至全球的工厂和装瓶商合作伙伴，可随时随地查看生产情况，让效益倍增。同时该公司认识到进行数字化转型一定要确保安全，这就意味着要获取运营技术(OT)网络的可视性，以便其安全团队能随时随查看威胁以及技术(IT)和运营技术(OT)环境。

挑战

该公司对其用例进行优先排序，以解决威胁其生产环境持续运营可用性、安全性、可靠性的三大风险领域。

1. **恶意软件感染：**虽然 IT 和 OT 网络融合解锁了商业价值，但同时也可能带来全新安全风险。如果没有恰当的控制措施，目标威胁和非目标威胁都可从 IT 环境转移到 OT 环境。对 OT 网络的恶意攻击所产生的潜在溢出效应可能会导致巨大的损失—产出中断或停止，同时造成安全和合规问题。
2. **第三方远程访问威胁：**外部供应商通过远程访问工厂的 OT 网络来维修服机器。如果授权方的系统感染了恶意软件或其访问凭证被盗、安全卫生不达标，车间系统和控制器就会遭受潜在损害。公司需重点关注未授权访问和不正当访问。
3. **远程设备的控制器操作发生改变：**公司水处理设备与工厂采用物理隔离。运行设备的系统每天以同样方式运行。任何变化都可能表明水质受到污染，但由于公司对系统缺乏详细了解，因此无法理解和解释这些变化。

解决方案

Claroty 平台部署在现有的海上 OT 网络基础结构之上，然后透过现有的卫星通讯网路连线至公司的陆上安全营运中心（SOC）。这个平台利用的元件包括：

- **持续威胁侦测（CTD）**，可以实现全方位的 OT 资产可视性、持续安全监控和即时风险分析，而不会对营运流程和基本装置造成任何影响。
- **安全远程访问（SRA）**，可以防范 OT 网络避免远端使用者（员工和第三方供应商）未受管理且未监控存取之下所引发的威胁。
- **企业管理主控台（EMC）**，可以简化整体管理，整并来自跨 Claroty 平台的数据，以及提供跨多座基地的资产、活动和警示的整合视图。这个平台也整合。

结果

利用 Claroty 平台，这家公司能够：

在部署的两个星期内发现和分析全球多个 MODU 的所有 OT 资产、通信和处理程序。

将平台与其现有 IT 安全基础结构整合，建立一种非常有效与整合的 IT/OT SOC，因此可以大幅提高 IT 与 OT 安全以及与 E&P 承包商之间的一致性与合作。

利用 SRA 的可自定义使用者访问控制、最小特权政策与稽核功能来监控和尽可能降低由远程登录所引发的风险。

提供其 E&P 承包商容易使用的专用 OT 界面，让他们能够从远端以轻松且安全的联机，来维修 OT 资产。

主动防止安全事件，因此可以减少其海上钻井作业所面临的可用性、可靠性与安全性风险。

关于 Claroty

Claroty 可以缩短信息技术（IT）和营运技术（OT）环境之间的工业网络安全差距。面临重大的信息安全与财务风险时，拥有高度自动化生产基地与工厂的企业组织特别需要缩短这个差距。有了 Claroty 的整合 IT/OT 解决方案，这些企业和关键基础结构营运商即可利用其现有的 IT 安全流程与技术无缝提升其 OT 资产与网络的可用性、安全性与可靠性，而不需要停机或专属团队。如此可以延长运作时间并提升企业和生产营运整体效率。