案例研究

制药业

跨国制药公司采用 Claroty 以保护其 OT 环境

这家拥有大量知识产权(IP)的全球制药公司意识到保护其生产运营的重要性。由于各个制造厂的运营都依赖于与运营技术(OT)网络连接的关键性程序和机器，该公司意识到要确保其安全生产，必须保证 OT 环境的安全。在评估了多家供应商后，公司选择了 Claroty，因为 Claroty 平台有着无可比拟的 OT 可视性和全面的 OT 安全控制。

挑战

正如处在这个高度管制行业的其他公司一样，这家公司在解决其 OT 安全问题时面临着一系列复杂的挑战。

1. **由于收购导致的安全隐患：**收购在制药业中非常常见，这家公司之前收购了几家公司，因此它不仅沿用了之前公司的一系列安全措施，而且还沿用了它们用来服务和维修不同 OT 资产的不同供应商的补丁。
2. **勒索软件风险：**由于规模、经营范围和概况，这家公司在内的主要制药公司往往成为勒索软件攻击的目标。这些攻击通常通过 VPN 连接侵入，然后从 IT 网络扩散到 OT 网络，从而会导致严重的停机和运营中断。
3. **缺乏 OT 异常检测能力：**尽管该公司的 IT 安全团队拥有有限的 OT 专业知识，但仍被指派去处理其 OT 安全问题。由于该公司所有制造厂的 OT 网络没有安装异常检测系统，其团队尝试应用公司 IT 网络所用的同样系统。然而其团队很快意识到这些系统与 OT 环境不兼容。因此团队无法识别公司 OT 网络内的潜在恶意活动，更不用说评估或缓解了。

客户评价

> *“我们与罗克韦尔、西门子和施耐德电气都有着合作关系，这三家公司非常支持我们采用 Claroty 来应对 OT 安全挑战。他们的支持是我们做出决定的重要因素。事实上 Claroty 为我们提供了有史以来最好的资产库存视图。他们的平台确实超出了我们的预期。如果我们扪心自问：哪家公司会长久不衰，哪家公司对我们来说是非常重要的合作伙伴？我们的唯一答案是 Claroty。”*

解决方案

在短暂的测试期间，Claroty 平台远超预期。因此这家公司的每个生产基地都部署了 Claroty 平台。采用的平台组件包括：

- **持续威胁检测(CTD)**，可提供全面的 OT 资产可见性、持续安全监控和实时风险洞察，并且不会对操作程序和底层设备造成影响。
- **安全远程访问(SRA)**，可保护 OT 网络免受远程用户(包括雇员和第三方供应商)在未受管理和监控的情况下进行访问时所带来的威胁。
- **企业管理控制台(EMC)**，可全面优化管理系统，集合来自 Claroty 全平台的数据，提供多个站点的资产、活动和示警信息的一体化可视性图表。该平台还可通过 EMC 实现 IT 安全基础设施的无缝整合。

效果

采用 Claroty 平台，该公司能：

实现 OT 完全可视性：持续威胁检测(CTD)可快速发现并分析全部的 OT 资产，且提供前所未有的细节。例如，在一个测试点，该公司发现了 65 个资产，但 Claroty 发现了 95 个。

OT 安全远程访问连接：安全远程访问(SRA)可为工厂员工和第三方供应商提供一个用户友好界面，通过该界面远程安全、轻松地访问和维修 OT 资产。除了其他的绝佳措施，该界面还可执行特权访问控制和主动监测，从而将远程用户导致的风险降到最低。

充分运用 IT 安全工具加强 OT 安全：Claroty 平台与 IT 安全基础设施完全无缝整合。将平台与 SIEM 解决方案相整合，让公司的 IT 安全团队能利用现有的熟悉工具来实现整个 OT 环境的全面安全。

关于 Claroty

Claroty 弥补了信息技术(IT)和操作技术(OT)环境之间的工业网络安全差距。拥有高度自动化生产基地的组织和面临着巨大安全和财务风险的工厂，尤其需要填补这种差距。采用 Claroty 的 IT 和 OT 融合解决方案，在无需停机和专门团队的情况下，这些企业和关键基础设施运营商可利用现有的 IT 安全程序和技术，无缝地提高 OT 资产和网络的可用性、安全性及可靠性。因此业务和生产运营整体上有了更多的正常运行时间和更高的效率。

由于全球领先的工业自动化供应商对 Claroty 的支持和采用，让 Claroty 在全球七大洲均有部署。Claroty 公司总部位于纽约，自 2015 年由著名的 Team8 团队推出以来，已获得 1 亿美元的资金。

CLAROTY

联系我们
contact@claroty.com