CLAROTY

案例研究

汽车制造行业

汽车制造商运用 Claroty 发展全方位的营运技术（OT）安全

随着汽车制造商的营运范围扩大，其安全需求的复杂度通常会大幅增加。尽可能洞悉公司营运技术（OT）安全结构的全貌，这家大型汽车制造商最初选择 Claroty 以提供公司全方位 OT 资产的可视性。这项发现带来许多其他好处，最终协助公司提升其整体 OT 环境的可用性、可靠性与安全性。

挑战

和其同产业中的许多其他公司一样，为了主动强化公司 OT 安全，并且能以更有效的方式管理内部风险，该公司寻求一种方式能够检视、监控与管理其为数众多之生产基地的安全，其每座基地内有数百项资产。

1. **复杂多变的攻击面**：汽车制造商通常拥有许多厂房，而这些厂房的分布范围通常很广，每座厂房都有多种连上网路的装置。因此，对于寻找可扩充但一致取得 OT 安全的方法来说，这尤其是项挑战，因为各个使用案例与供应商对 OT 装置的技术需求极不相同。

2. **未经授权的使用者和错误设定：**由于营运复杂度，许多汽车制造商难以有效监控和管理未授权远程登录 OT 环境。此外，许多汽车制造商也难以防范对 OT 资产进行未授权的变更，因而导致错误设定和营运停机。

3. **缺乏生产相关警示：**直到真正开始对生产造成影响之前，OT 安全事件通常都难以侦测，因此会对营运造成连锁效应。此时需要精确与自动化的警示，才能让员工迅速响应并维持工厂运作。

客戶引言

「我们在两大洲有数十座生产基地。这表示我们的整体制造营运中有数以千计的资产，因此您应该不难想像建立一套可靠 OT 网络安全结构所面临的挑战。即便只是想要一窥我们生态系统的全貌，也是一项艰钜的挑战，而且大部分的解决方案甚至连基本的工作都无法顺利完成。在我们评价的所有平台中，只有 Claroty 能够为我们提供所需的整合视图和完整控制，且营运完全没有停机。老实说，甚至没有任何平台可以相提并论。」

解决方案

经过完整的评价流程之后，Claroty 平台获选并部署到汽车制造营运中，遍及两大洲超过 40 座工厂中。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 网络避免潜在的错误设定和未经授权的使用者（包括第三方承包商）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，以及提供跨多座厂房的资产、活动和警示的整合视图。这个平台也可以在适当的场所，透过 IT 安全基础结构的 EMC 进行无缝整合。

CTD 可以立即分析公司网络中的所有资产，并且就每项资产提供深入且大量的详细评价，这点任何其他供应商都无法做到。这项流程可以在无中断营运流程的情况下达成。

SRA 可以强制采用安全稳固、单一存取路径供远端诊断与维护作业使用，借此排除远端使用者和网络资产之间的直接互动。这种排除直接互动的方式，可以大幅提高整个 OT 面的信息安全最佳实务。

为公司提供生态系统中所有装置的整合视图，甚至可以辨识、监控和保护自现代化网络安全为主要设计考察之前便使用至今的传统装置。这种全方位的 OT 可视性和实时威胁侦测，让公司具备可以主动防范更多种威胁的能力。

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。