辉瑞（Pfizer）如何与 Claroty 合作建立并强化工业网络安全体系保障生产连续性与安全性

辉瑞全球自动化工程主管 Jim LaBonty 与 Claroty 全球客户服务高级副总裁 Guilad Regev 进行了交流，分享了辉瑞在工业网络安全方面的经验，包括如何保障正常生产。以下摘录了他们对话中的一些精彩片段。

Q: 为什么辉瑞决定采用以 OT 为核心的解决方案来保护生产基地？

2017 年，辉瑞的竞争对手默沙东（Merck MSD）遭受了 NotPetya 网络攻击，全球生产和供应链受到严重干扰。

辉瑞早在 2015 年左右启动工业网络安全项目，部署了相关技术来保护生产环境。但直到 2017 年底，董事会才强烈要求我们把重点放在保护 OT 环境，即生产车间和工业控制系统。

Q: 辉瑞董事会决定投入更多资源加强 OT 安全后，下一步是什么？

董事会的决定促成了 IT 部与工程部的紧密合作。我们成立了项目管理组（PMO, Project Management Organization），启动了一个项目，明确为实现目标需要采取的措施，确定了合作的技术伙伴和网络安全顾问等。

前期的分析工作是在2018年春季进行的。当时，我们还不清楚哪些 IT 工具适用于 OT 环境，哪些不适用。于是，我们开展了一系列试点测试，尝试各种技术，经过深入研究和分析，最终聚焦于几项关键技术，用于生产车间环境。

Q: 为什么辉瑞选择与 Claroty 合作？

我们无法保护我们不知道它存在的东西。只有识别出来，才能保护它。我们需要一款能全面了解生产环境的工具。Claroty 可梳理 OT 资产、建立资产清单、了解哪些设备在通信。

我们的工业网络安全策略主要参考 NIST 网络安全框架。它非常实用，我们至今仍在使用。而 Claroty 的解决方案可以一一对应 NIST 框架。

我们还参考了 NIST 800.82 指南，很好理解如何保护工业控制系统（ICS）环境。

Q: 自 2017 年以来，您们取得了哪些里程碑？在这个过程中有哪些经验教训？对于刚开始工业网络安全之路的企业，您有什么建议或捷径？

过去几年，我们看到攻击者通过钓鱼邮件成功地将恶意软件传入没有做好网络隔离的 OT 环境。

如果公司的电子邮件系统和生产环境没有隔离，那就很危险。如果您的网络结构是扁平的，一旦遭遇钓鱼攻击，恶意软件就可能在整个网络中蔓延。

在辉瑞，我们认为网络隔离是一种有效的防御机制，它可以保持生产车间与 IT 系统连接，限制通信范围。我们只允许关键业务功能之间的数据流动，其他的都不开放。

早在 2015 年，我们就建立了一个防火墙，用来连接企业 IT 和制造 IT 系统。之后，我们又增加了一层工业级防火墙，把制造 IT 资产与生产车间的 OT 系统隔离开来。

Q: 辉瑞是一家业务遍及全球的大型生物制药公司，地理因素是否会影响网络安全策略？

项目启动之初，我们在项目管理组（PMO）设立了三位项目经理。因为北美、欧洲、亚太、非洲的文化、环境和生产力各不相同，各区域的许多活动大同小异，但执行速度却有所不同。

举例来说，我们在非洲的大多数生产设备是与IT系统隔离的。它们就像一个个与外界物理隔离的自动化孤岛，尤其是在生产车间。这些OT站点缺乏互联互通，自然就不需要像其他地区那样采取额外的安全措施来保护IT与OT之间的连接，因为物理隔离环境本身就具有隔离性。

但即便在非洲的物理隔离环境中，我们也意识到需要一种扫描移动设备的工具，因为我们的IT环境和生产车间之间仍然存在信息传输。没有万全之策。我们尝试过大约 5 种不同的技术，每种技术都为整体安全架构提供了一部分保障。每一种技术都向我们的全球安全运营中心（SOC）提供威胁检测数据。

Q: 是先进行 IT 与 OT 的网络隔离，还是先部署 Claroty ？

在 2017 年，我们认为非常有必要把 IT 和 OT 的通信连接隔离开来。

之前，我们在工业控制系统（ICS）和分布式控制系统（DCS）中做了一些隔离。但我们发现，那些已经有明确隔离层的站点能更快地部署防火墙。

我们也从2014年在其他三四个生产站点部署防火墙的经验中吸取了教训。这些生产站点的防火墙问题极少甚至为零，工业级防火墙非常实用。

我们首先部署了工业级防火墙，等防火墙到位后，才开始部署Claroty。同时，我们还部署了一套用于南北向流量（North-South traffic）的聚合防火墙、一套核心交换机。

我们希望所采用的解决方案能够监控网络和生产环境中的流量，但绝不能以任何形式影响生产运作。Claroty的被动监控（Passive Monitoring）功能非常适合我们的需求，之后开始使用其主动查询（Active Query）功能，以获取更丰富的数据。

Q: 在团队架构方面，IT 和 OT 部门是否各自拥有独立的安全运营中心 (SOC)，还是合并为一个 SOC？您们是否使用托管安全服务提供商 (MSSP)？

我们的 SOC 部署在公司内部，完全整合在公司体系中。我们的 SOC 负责监控业务职能和生产制造。来自四到五种不同技术的数据源会先导入我们使用的SIEM（安全信息与事件管理系统），再由SIEM将数据传送到我们的 SOC 。

我们的SOC会监控所有威胁，包括来自生产环节以及全球所有业务职能部门的威胁。这是一个完全集成的SOC，涵盖了 IT 和 OT。我们曾考虑为 OT 部设立一个独立的 SOC，但从多个角度来看，这并不太合理。

在OT方面，每个制造工厂都是一个独立的实体，需要能够识别并应对该地点特有的威胁，才能有效防御。

Q: 您们与 Claroty 合作，帮助加强了 SOC 筛除误报的能力。能否介绍一下这方面的工作内容？

我非常支持减少误报，不断向 Claroty 提出新想法和创新建议，帮助 SOC 人员专注于最重要的警报。

我推动的一点是，在了解生产环境中正在运行的内容时，要加入上下文信息，更具体地说，要了解环境中哪些资产和流程不应该发生任何变更。

在生产环境中，任何流向这些特定区域的新流量或数据流都应该被列为高优先级。

另一方面，在停机维护期间，这些资产正在进行更新，此时我们不希望 SOC 被大量误报淹没，尤其是在变更还在进行中的时候。在完成更新并恢复生产之前，还有一个最终验证阶段，因此 SOC 需要了解这些变更是有意为之。IT 部门与生产部门之间的沟通对于成功筛除误报至关重要。

Q: 您们在部署 Claroty 的过程中体验如何?

我对 Claroty 的部署速度和简便程度感到非常惊喜。整个过程非常直接明了，我们在一周内就完成了部署。所需的管理工作量非常低，它还能及时向需要的人提供丰富的数据。Claroty 极大简化了对生产环境中资产的了解过程，这一点尤其重要，特别是在您无法雇佣一大批人手的情况下。

“我们需要一个 OT 工具来补充 Claroty CTD 的实时监控，以揭示辉瑞主要制造环境中无法触及的盲点。后来使用 Claroty Edge，快速实现了这一目标。”

—— Jim LaBonty 辉瑞全球自动化工程主管

Claroty CTD 与 Claroty Edge 的演示及介绍文档

Claroty CTD 演示视频

Claroty CTD 介绍文档

Claroty Edge 演示视频

Claroty Edge 介绍文档

文字与图片参考来源：claroty.com、博客文章《Securing Pfizer: An Industrial Cybersecurity Journey》