TENABLE.OT 主动查询技术

业务挑战

当今融合的 IT/OT 环境具有庞大的攻击面及众多攻击载体，这些都可作为利用 IT、IoT 和 OT 资产的媒介。要想降低工业或重要基础设施环境中的风险等级和 Cyber Exposure，单靠网络监控还不够。事实上，单纯利用网络检测可能会错过多达 50% 的信息和洞察，而这些往往是确保企业安全的必要条件。

企业需要能够得到详细信息，其中可以从网络和设备级别提供深入的分析和洞察。如果做不到这一点，那就只能祈祷工业基础设施不会遭到未经授权的活动或外部威胁的破坏。

解决方案

Tenable.ot™ 拥有获专利的主动查询技术（美国专利号 10261489），能够在本机设备通信协议中使用只读查询。该技术以安全方式针对每项工业资产的状态生成详细信息，而不会对被查询设备产生任何影响。

主动查询是经过与控制器供应商密切合作，并对 OT 设备进行了大量实验室测试后的成果。这么做可以确保查询不会对控制器产生任何影响，也不太可能造成任何中断。

主动查询能够产生更全面的信息集合，有助于：

- **发现**网络上的所有资产，包括可编程逻辑控制器 (PLC)、远程终端单元 (RTU) 等设备。
- **揭示**所有不在网络上通信的"休眠"资产。
- **分类**每项资产，以设备类型为依据。
- **收集**所有相关配置和元数据，包括修补程序级别、固件版本、用户和底板信息。如果出现漏洞或安全事件，则会优先处理警报事宜，并将详细信息发送给相关人员。
- **追踪**任何资产上的所有配置更改，以及提供完整快照，由此突出显示"前后"变化的丰富信息。

工业网络安全专业人员之所需

- 一套全面的解决方案，能够在融合 IT/OT 环境中灵活扩展
- 所有资产及其所在网络的最新关键数据和态势感知
- 上下文和有意义的警示，能够进行深入分析从而实现根本原因分析
- 对控制设备所做的任何更改发出警报
- 能够根据需求的变化灵活地应对当今 OT 安全挑战

价值

Tenable.ot 可确保工业网络的完整性。该平台在提供深入态势感知的同时，还能够追踪网络中每个设备所做的每一个更改。其中包括从操作系统和软件到固件和配置，最终到梯形逻辑的所有信息。

其优势包括：

- 及时的 OT 网络洞见，包括最详细的信息，如操作系统、固件、配置、梯形逻辑等
- 所有资产、漏洞和安全风险的最新关键数据
- 对控制设备所做的任何更改发出警报
- 更多上下文参考和有意义的警报；减少误报

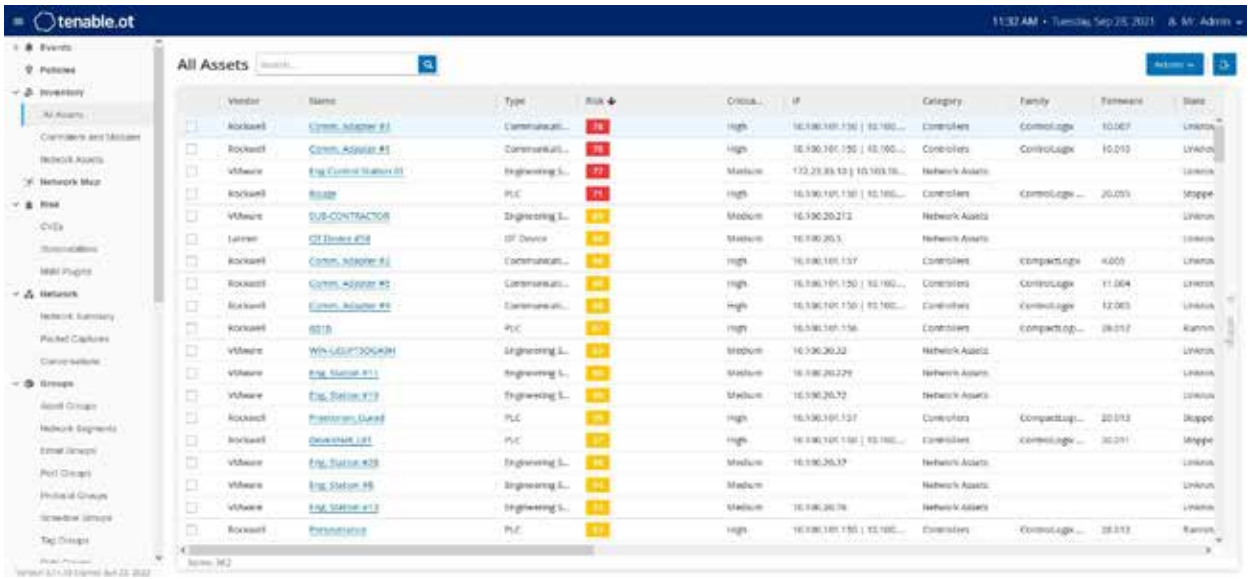

图 1. 带有 OT 所有资产深度详情的企业级态势

为何需要主动查询

- 仅仅依靠网络嗅探无法收集到全面确保 OT 可见性或安全所需的一切相关信息
- 全面且详细的警报能够从网络和设备层面提供完整的上下文，实现更加高效、即时的事件响应
- 搜寻不会通过网络通信的休眠设备
- 任何更改都必须可见，即使直接在设备上完成的更改
- 检测并追踪直接或通过网络对 OT 设备进行的所有更改
- 以 PLC 和 DCS 的本机语言与之进行稳定高效的通信

关于 TENABLE

Tenable®, Inc. 是一家 Cyber Exposure 公司。Tenable 帮助全球 30000 多家企业了解和减少网络风险。Tenable 是 Nessus® 产品发明者，凭借在漏洞方面的专业技术，推出了全球首个检查和保护各种计算平台上数字资产风险的平台。Tenable 的客户包括 50% 以上的《财富》500 强企业、30% 以上的全球 2000 强企业和大型政府机构。

详情请访问 zh-cn.tenable.com。

工作原理

- 主动发现设备时，以本机语言查询设备。
- 主动查询不会使用设备不支持或非本机的命令。
- 主动查询属于只读的带外查询。因此从设计上就没有能力更改任何设备的配置和设置。

立即开始使用 TENABLE.OT

单纯的被动网络监控会遗漏保护 OT 环境所必需的关键设备数据和深度态势感知。Tenable.ot 利用被动检测和获专利的主动查询技术，可减少 Cyber Exposure 和 OT 威胁。

访问 Tenable 解决方案网页，立即了解我们如何帮助度量现有的 OT 安全能力、评估计划中的不足并制定全套计划，以便开启 IT 和 OT 基于风险的统一安全平台之旅。