用于 IoT/OT 安全的 Microsoft Defender

Azure IoT 学院专题三: 动手实验一 用于 IoT/OT 安全的 Microsoft Defender

Microsoft Defender for IoT 动手实验

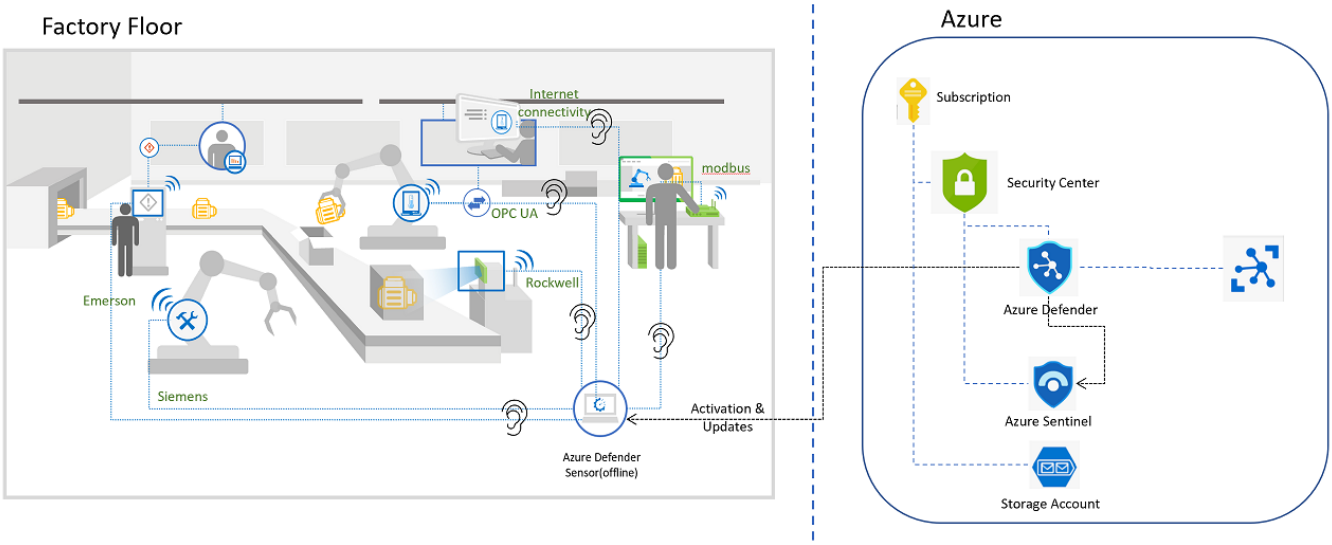
架构图

在本次动手实验中，我们将专注于为 IoT 传感器、在线警报和离线场景设置 Microsoft Defender。

将学习如何配置环境、评估结果以及与 Microsoft Sentinel 等 SIEM 系统集成。

此动手实验室 (HOL) 将专注于保护您的物联网设施。

下面的场景是应用场景之一，还包括石油、天然气、公用事业和能源公司等场景



注意

本文档中的信息，包括 URL 和其他 Internet 网站引用，如有更改，恕不另行通知。除非另有说明，否则此处描述的示例公司、组织、产品、域名、电子邮件地址、徽标、人员、地点和事件均为虚构，与任何真实的公司、组织、产品、域名、电子邮件地址、徽标、人物、地点或事件旨在或应被推断。遵守所有适用的版权法是用户的责任。在不限制版权权利的情况下，不得复制、存储或引入检索系统，或以任何形式或通过任何方式（电子、机械、影印、录音或其他）传输本文档的任何部分，或用于任何目的，未经 Microsoft Corporation 的明确书面许可。

Microsoft 可能拥有涵盖本文档主题的专利、专利申请、商标、版权或其他知识产权。除非 Microsoft 的任何书面许可协议中明确规定，提供本文档并不授予您对这些专利、商标、版权或其他知识产权的任何许可。

提供制造商、产品或 URL 的名称仅供参考，Microsoft 不对这些制造商或产品与任何 Microsoft 技术的使用做出任何明示、暗示或法定的陈述和保证。包含制造商或产品并不意味着 Microsoft 认可该制造商或产品。链接可能会提供给第三方网站。此类站点不受 Microsoft 控制，Microsoft 不对任何链接站点的内容或链接站点中包含的任何链接或此类站点的任何更改或更新负责。 Microsoft 不对从任何链接站点收到的网络广播或任

何其他形式的传输负责。 Microsoft 向您提供这些链接只是为了方便，包含任何链接并不意味着 Microsoft 认可该网站或其中包含的产品。

Microsoft 和 https://www.microsoft.com/en-us/legal/intellectualproperty/Trademarks/Usage/General.aspx 中列出的商标是 Microsoft 集团公司的商标。 所有其他商标均为其各自所有者的财产。

受众:

从事与互联设备、智能场所、未来工厂、工业物联网、能源、石油和天然气相关的项目的团队。

建议参与人群:

- 安全团队
- 运营技术/工程 (ICS) -（人员保护设施，如工厂车间、变电站、石油和天然气设施）。

面向行业: - 能源 - 效用 - 制造业 - 石油和天然气

课程目标:

- 本课程是一天的培训， 与讲师一起动手操作，不需要以前的 Azure 知识。 你会边做边学。 要求具备安全或工业控制系统工程背景的相关人士。

Microsoft Defender for IoT 的关键词

传感器 - Sensor：运行 Microsoft Defender for IoT 的基于网络的物理硬件，内置基于物联网的 Linux 系统

管理设备 - Manager：运行 Microsoft Defender for IoT 的基于网络的物理硬件，内置基于物联网的 Linux 系统。它连接到多个传感器以汇总数据，跨多个系统发出警报，携带 PCAP 配置和新更新。 Central Manager 可用于更新传感器的版本和威胁情报，如果需要，还可以连接到许多 SIEM 系统。

IoT：统称为物联网。现代、新标准的连接设备。

IIoT：工业物联网。

OT：运营技术、旧设备和技术（例如传送带、PLC）。

Brownfield devices：指的是孤立地执行离散功能的遗留设备和遗留软件的类型，通常没有人愿意修改现有的、运行良好的遗留资产。

ICS：工业控制系统

Greenfield devices：新的智能“网络物理系统”，支持新的软件环境，例如开放通信协议和开放标准，例如 MQTT、REST API、AMQP、OPC-UA、MTConnect 和 CodeSys。

SIEM：安全信息和事件管理

Section 52：Microsoft 团队致力于在 IoT 和 OT 世界中发现安全威胁

PCAP 文件：数据包捕获或 PCAP（也称为 libpcap）是一种应用程序编程接口 (API)，可从 OSI 模型第 2-7 层捕获实时网络数据包数据。

零信任原则 - Zero Trust Principles：假设所有访问都是不合规的，明确验证，使用最小权限访问（网络身份）。

XDR：交叉检测和响应

Purdue Model

- 0 级 - 过程：物理机械（执行器、泵、刀具、机械臂等）。
- 1 级 - 基本控制
- 2级 - 监督控制
- 3 级 - 站点操作，Linux 等计算机向操作员提供站点信息
- 4/5 级 - IT 环境