Microsoft Defender for IoT/OT Security

Hands-on lab workshop, Microsoft Defender for IoT/OT Security.

January 2022.

Audience:

Teams working in projects related to Connected Devices, Smart Places, Factory of the Future, Industrial IoT, Energy, Oil and Gas.

Ideal attendee will be:

- Security Teams
- Operational Technology/Engineering(ICS) - (Personnel securing facilities such as factory floors, substations, oil and gas facilities).

Industries:

- Energy
- Utility
- Manufacturing
- Oil & Gas

What to expect:

- Session: This session is 100% Hands-on, no previous knowledge in Azure is required. You will learn by doing. It is important you are a person with Security experience or that you have an Industrial Control System Engineering background, working in facilities. You will work with us all day. Please block any distractions during this day. Explanations will happening while we are building the solution.

  This session will not be recorded

Dates:

- Americas: Oct/21/2021 (Time: 9am to 5pm EST Time)
- EMEA: Feb/01/2022 (Time: 9am to 5pm CET Time)

This workshop is **by invitation only**. Azure Passes will be provided as part of the training to make sure all the attendees can complete the labs without issues.

> NOTE: It is possible to run the workshop on your own if you already have an existing Azure subscription. In this case you will be charged for running some of the services used in this HOL.

Contact Info:

For any questions please send an email to: iotacademy@microsoft.com

This workshop is delivered by SMEs in IoT and Cybersecurity at Microsoft.

Microsoft Defender for IoT Vocabulary

Sensor: Linux machine, physical hardware running Microsoft Defender for IoT connected to the network.

Manager: Linux machine, physical hardware running Microsoft Defender for IoT connected to the network. It connects to multiple sensors to summarize data, alerts across multiples systems, carries the PCAP Configuration and new updates. Central Manager can be used to update the sensor's version and threat intelligence, can also connect to many SIEM systems if needed.

IoT: Internet of Things. Modern, new standard connected devices.

IIoT: Industrial IoT.

OT: Operational Technology, old equipment and technology (e.g, conveyer belts, PLCs).

Brownfield devices: Type of legacy equipment and legacy software that performs discrete function in isolation, usually nobody is willing to modify existing, well-functioning legacy assets.

ICS: Industrial Control systems

Greenfield devices: New and smart "cyber-physical systems", supporting new software landscapes such as open communication protocols and open standards such as MQTT, REST APIs, AMQP, OPC-UA, MTConnect and CodeSys.

SIEM: Security Information and Event Management

Section 52: Microsoft Team dedicated to search for threats in the IoT and OT World.

PCAP file: Packet Capture or PCAP (also known as libpcap) is an application programming interface (API) that captures live network packet data from OSI model Layers 2-7.

Zero Trust Principles: Assume breach, verify explicitly, use least privilege access (identity at network).

XDR: Cross detection and response

Purdue Model

- Level 0 - Process: Physical Machinery (actuators, pumps, cutters, mechanical arms, etc).
- Level 1 - Basic Control
- Level 2 - Supervisory Control
- Level 3 - Site operations, computers such as linux providing site information to operators
- Level 4/5 - IT Environments