TOREON

TOREON

Defender for OT assessment

◆ CREATING TRUST FOR A SAFER DIGITAL SOCIETY ◆

Defender for OT Assessment Objectives

OT Security testing is a process of testing OT devices to find security vulnerabilities that hackers could exploit to access an organizations network, modify their data, shutdown the production environment or steal their information. This can lead to significant financial losses, identity theft, production loss and damage to the reputation of both the business and the manufacturer of the vulnerable device.

With the IoT Security Assessment, organizations can validate virtually any connected device against a broad range of known and unknown attacks to ensure cybersecurity compliance before leaving the development or test lab.

The security assessment will form the basis of a new/improved OT architecture for organizations. In addition, a custom-made roadmap for each customer, mapped against business requirements and risks, will be provided to give guidance for these organizations.

The report will overview network security risks (i.e. Illegal traffic, access points, malware, internet connections, + more), network operations, and provide attack vectors based on data gathered from the customer.

Identification

1. Stakeholders & Business requirements
2. Review network architecture
3. Review current asset list

Preparation

4. Define implementation for Defender for IOT Nodes

Rollout & adoption

5. Implement defender for IOT (and execute assessment)
6. Evaluate results Defender for IOT
7. Roadmap new OT architecture

The next steps

8. Integration SOC (Playbooks, BCP, DRP)
9. Threat Model for OT
10. Define new OT architecture
11. Implement new OT architecture

Identification Phase

Before starting the assessment Toreon recognizes the value of buy-in from the business. Security should be leveraged on all levels.

Hence the following information is retrieved from the organization:

- **Stakeholder and business requirements** – Gather the main stakeholder and business requirements, as well as problem statements, business challenges and questions.
- **Review network architecture** - Review current OT network against IEC62443.
- **Review current asset list** – Some organizations already have an asset list available or architecture in place for OT devices. An asset list, when available, is also checked and validated against later findings in the assessment.

Preparation Phase

In the preparation phase the technical and functional requirements are designed for the assessment:

- **Architecture** – Where to place the sensors (define OT segment), how to integrate with Defender for OT and Scope definition.
- **Licenses** – If the organization does not have the appropriate licenses, these need to be procured or in some cases trial licenses can be used.
- **Permissions** – Some actions might require administrative access to configure.
- **Customer Buy-in** – The organization needs to know what the exact scope and impact is on the organization. Hence in the preparation phase these are also discussed.

Rollout and adoption Phase

During the rollout and adoption phase, the Defender for OT solution is put in place and the assessment is executed. The following steps are included within the assessment:

- **Implement defender for OT (and execute assessment)** – This phase is about actually installing the defender for OT in the customer environment and executing the assessment.
- **Evaluate results defender for OT** – Results are exported and evaluated. Several frameworks and best practices can be applied, according to business requirements and needs. In addition, a risk-based approach can be applied as well. Once evaluated a report will be generated for the organization detailing the findings of the assessment.
- **Roadmap new OT architecture** – A roadmap is created, including the following topics:
    - Business critical assets
    - Key improvements
    - Segregation/segmentation
    - 3rd party access

Next Steps

After the initial assessment took place, the roadmap with next steps was created. In these next steps the following topics are included. Not only will they bring more visibility of OT within the customer environment, but also increase the overall security posture as well.

- **Integration SOC** (Playbooks, BCP, DRP) – Assets are monitored for non-compliance and security breaches. These can then be integrated in the organizations own SOC solution (example Azure Sentinel).
- **Threat model for OT** - Threat modeling works to identify, communicate, and understand threats and mitigations within the context of protecting something of value. It is a structured representation of all the information that affects the security of an asset. It enables informed decision-making about specific asset security risks.
- **Define new OT architecture** – Findings of the assessment will, without doubt, lead to new insights. These new insights can then be used to finetune or setup new OT Architecture for the organization.
- **Implement new OT architecture** – Once new architecture is in place, the new OT environment can be built.