DIFENDA

Microsoft Intelligent Security Association

Microsoft

Microsoft Solutions Partner
Security
Specialist
Cloud Security
Threat Protection

Case Study

VISIBILITY LEADS TO UNIFIED PROTECTION OF BUSINESS CRITICAL PRODUCTION SYSTEMS

At-A-Glance

Key Drivers & Customer Situation:

In 2021, Difenda was asked by a customer to run attack scenarios against their OT environment to determine potential risk and assist in demonstrating the benefits on a Microsoft Defender for IoT implementation. Due to the sensitivity of the OT environment, Difenda worked with one of our OT/ICS partners, IdeaWorks, to build a simulated lab environment, designed to replicate a small subset of the customer's environment.

The attack scenario developed by Difenda's Cyber Research & Response team was based on Industrial Controls Systems (ICS) attacks Havex and Triton, with the following attack tactics considered when developing with the attack strategy:

Reconnaissance | Persistence | Credential Access | Lateral Movement

During the exercise, the attack team leveraged 'live off the land' techniques to gather information about the OT network. As the attack progressed, information gathered allowed the attacker to connect directly to the engineering workstation and access core configuration files for a PLC on the OT network. This file was modified to tamper with key PLC settings designed to take down the OT environment and uploaded to an actual PLC, all completely undetected.

Solution

Enter Microsoft Defender for IoT and Difenda MXDR for OT

As part of the exercise, Difenda was able to assess the attack workflow and based on the instructional changes from the engineering workstation to the PLC, developed, implemented, and tested new detection rules within Microsoft Defender for IoT. The newly developed rule was enabled, and the attack was replayed. As the attacker moved to update the file on the PLC, Difenda's defensive team was able to detect the threat.

Knowing real-world OT / ICS environment attacks

+

Identifying risk within OT Environment

=

Protection of business critical protection systems

Win Insights

- Difenda was able to meet the customers needs
- Achieved full visibility with Difenda MXDR for OT
- Developed, implemented, and rested new rule detection that detected the threat

> *Our work with Difenda is part of an on-going effort to maintain operational safety and resilience, including the reduction of cybersecurity risks. The team helped us understand the security of our OT environments without disrupting our daily operations.*
>
> **Principal IT Security Engineer**