DIFENDA

5 Immediate Steps to Enhance Your OT Security:

A Guide for Technical Security Leaders & CISOs

As an enterprise, the importance of Operational Technology (OT) security is a long-established truth. Recently, however, these OT environments have become a significant concern for Technical Security Leaders & CISOs. Given the vulnerable nature of OT networks — which often involve legacy systems and are commonly interconnected with IT networks — these environments present lucrative targets for threat actors. Layering in the potential for cyber breaches to cause serious operational consequences--from downtime and dangerous explosions to product deficiencies--the need to fortify your OT security has never been more crucial.

1 CONSTRUCT A MATURITY MODEL AND RISK REGISTER FOR OT:

The establishment of a maturity model is the bedrock of any cybersecurity program, including OT. Existing ad-hoc controls might provide some level of security to your OT environments; however, an effective OT security program is contingent upon maturity modeling. There are many free OT security models available online. Energy.gov is our favorite. This model can be leveraged to

- gauge existing controls
- benchmark against peers
- identify bottlenecks
- measure progress on security initiatives

This helps to pinpoint any gaps or weaknesses, thereby enabling the development of an enhanced security plan.
Once the maturity model is in place, you can use the insights gained to formulate a comprehensive risk register. This aids in laying out a roadmap to prioritize security initiatives.

2

"You can't secure what you don't know"

DEVELOP AN OT ASSET INVENTORY AND IMPROVE NETWORK VISIBILITY:

Documenting OT assets bridges the gap between high-level security initiatives and deployment to OT. It offers unparalleled visibility into your OT network, its functionality, access points, redundancy capabilities, points of entry and more.

Network security is a good place to start when implementing technical controls to secure OT environments because robust network security mechanisms prevent unauthorized access, misuse, malfunction, modification, and destruction, thereby safeguarding valuable OT assets.
Automation technologies, such as Defender for IoT, can expedite this process through passive network monitoring, saving resources compared to manual collection and analysis.

We have a maturity model, risk register, OT asset inventory, and some visibility on the OT network, what next?

3 FORMULATE AN INCIDENT RESPONSE PLAN:

Tailor an incident response plan that suits your environment and needs, outlining roles and responsibilities, escalation steps, and response actions.

There are numerous sources for and examples of incident response plans on the internet, and while we could provide some examples it's important to note that it must fit your environment and needs. Importantly, you also need regular simulated tests help fine-tune your response capabilities. Third-party assessments can provide unbiased results and prepare you for unexpected events.

4 IMPLEMENT ACCESS CONTROLS FOR OT NETWORKS AND ASSETS:

> **One of the most common vulnerabilities within the OT environment that often flies under the radar is related to access controls and permissions. We encounter situations where former employees still have access to critical systems or anomalies tied to an individual user account, which can lead to unauthorized and potentially harmful activities. For instance, we once found a terminated developer who had written a script to query certain bits of data from HMIs.**
>
> **—Chase Applegate**

Tight access controls prevent most OT attacks originating from the corporate network. Only critical business-justified access should be allowed, using secure protocols and technologies for remote access.

5 INSTALL OT SECURITY MONITORING SOLUTIONS AND BUILD OT SECURITY OPERATIONS:

Passive security measures are generally preferred in OT due to the implications of denying availability to OT assets.

Our experts recommend Defender for IoT or a comparable solution to read and analyze layer 2 traffic from the operations network. Later, integration with your SIEM is essential for effective monitoring and response.

Defender for IoT integrated with Microsoft Sentinel is our preferred choice, as the technologies work in harmony with one another, and are an unparallelled solution for companies that have already invested in Microsoft technologies.

Following these strategies will provide the best first steps at securing your OT environment and the IT/OT integration. Tied to your organization's overall security posture, addressing these 5 key elements o OT security can complement the business's efforts in compliance, risk mitigation, and technical safeguards against cyber threats.

Looking to lighten the load on your internal team? Contact Us to get the ball moving with a comprehensive OT Environment Assessment

CONTACT US | VIEW SAMPLE