CRYPTO

How to: Secure data transfers between OT and IT environments with the DataDiode

Knowing what's happening with your critical infrastructure and operational technology is essential. But when you transfer your OT data into your IT environment, you need to be absolutely certain that external parties cannot use this data transfer to get into your OT environment.

Our DataDiode solves this issue by ensuring a unidirectional data flow at the highest security level. By blocking any data from moving into your OT environment via reverse data paths, you can prevent any external threats from entering the OT network. This way, your organization can safeguard the OT environment while allowing secure data transmission to your IT environment.

The challenge

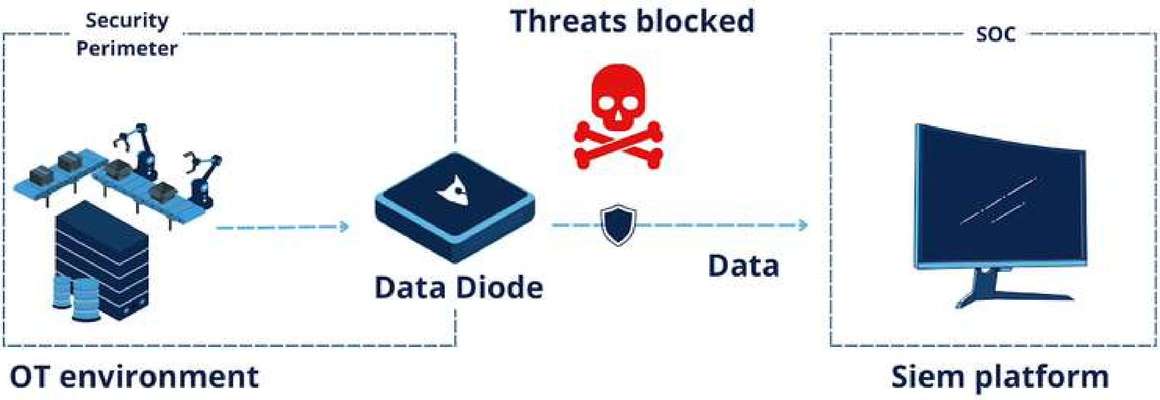
Data from OT networks to Security Information and Event Management (SIEM) systems in IT environments must be transferred securely. These SIEM platforms provide continuous monitoring and analysis, turning raw data into actionable intelligence, which is crucial for effective 24/7 threat detection and response.

The key challenge lies in securely transmitting data from OT networks to SIEM systems without introducing vulnerabilities. Traditional firewalls, once the primary defense, are increasingly inadequate against sophisticated cyber threats, often exposing the OT network to potential risks instead of protecting it.

The solution

Rather than relying on traditional firewalls, the hardware-enforced DataDiode ensures a unidirectional data flow. This way, you can safely transfer your OT data into your monitoring platforms, without the risk of unwanted reverse data transfers.

How it works



Step 1
Identify the critical OT systems and data that need to be monitored and analyzed by the SIEM platform.

Step 2
Install the DataDiode between the OT network and the IT network, connecting the outbound data flow to the SIEM platform.

Step 3
Configure the SIEM system to receive and process the data sent from the OT network for real-time threat monitoring and analysis.

Step 4
Verify the unidirectional flow by testing the setup to ensure that no data or threats can enter the OT network from the SIEM system.

Step 5
Regularly monitor and maintain the DataDiode and SIEM integration to ensure ongoing security and compliance with regulatory standards.

The benefits

- **Secure, real-time threat monitoring:** the DataDiode allows continuous data flow to SIEM systems for immediate threat analysis and response.
- **Operational continuity:** the DataDiode protects the integrity of the OT network, ensuring that critical systems remain unaffected, available and operational.
- **Compliance with regulations:** The DataDiode Ruggedized meets stringent security requirements for critical infrastructure protection, and is certified up to EAL7+.

Interested? Talk to an expert!

✉ internationalsales@foxcrypto.com

CRYPTO