8 Practical Steps for Implementing SEMI E187 and E188 Cybersecurity Standards

in Smart Semiconductor Manufacturing

SEMI E187 and SEMI E188 are two forward-looking cybersecurity standards released in 2022 to secure the semiconductor manufacturing ecosystem.

SEMI E187

Focused on enhancing supply chain measures to prevent new, infected manufacturing equipment from entering and integrating into the foundry.

SEMI E188

Extends to existing equipment with a focus on mitigating risks for malware and protecting manufacturing facilities.

Practical implementation requires a systematic approach

1

Assessment and Gap Analysis

Identify potential vulnerabilities, gaps in compliance, and areas for improvement. This analysis will be the foundation for developing an implementation roadmap.

2

Establish a Cross-Functional Team

This team will oversee the implementation process, coordinate efforts across departments, and ensure alignment with organizational objectives.

3

Education and Training

Provide training and awareness programs to all employees on these cybersecurity standards, the implications, and how to comply.

4

Policy Development and Documentation

Develop and document SEMI E187 and E188-related cybersecurity policies and procedures and ensure they are accessible to all relevant stakeholders.

5

Technical Implementation

Implement technical solutions and controls, such as anti-malware, IPS, firewalls, and network monitoring tools that address specific SEMI E187 and E188 requirements.

6

Testing and Validation

Perform vulnerability assessments, penetration testing, and simulations of cyber attacks to identify any weaknesses or vulnerabilities that need to be addressed.

7

Continuous Monitoring and Improvement

Establish a process to monitor and enhance SEMI E187 and E188 compliance. Look for emerging threats and update policies and controls accordingly.

8

Create a Comprehensive Resiliency Plan

Plans should be based on the four fundamental cyber resiliency goals: anticipate, withstand, recover, and adapt.

Discover resources and tools to support your implementation of SEMI E187 and E188 standards at www.txone.com

About TXOne Networks

TXOne Networks offers cybersecurity solutions for ICS and OT environments, employing the OT zero trust methodology for Cyber-Physical Systems (CPS). We foster collaborations with leading manufacturers and infrastructure operators to devise effective defense strategies, addressing security vulnerabilities in industrial settings.

txone networks

txone.com