Beneath the Surface: Navigating the Unseen Dangers of Connected “OT” Products

Wei-Cheng Tian, PhD & EMBA
Product Security, Delta Electronics Inc.

Introduction of Wei-Cheng Tian

Wei-Cheng Tian

Delta Research Center

PHD in EECS from the University of Michigan, Ann Arbor

Executive MBA from the State University at New York at Albany (SUNY Albany).

Current Job & Affiliation in Delta Electronics

- Director of cybersecurity lab in Delta Research Center
- Executive member of Delta Electronics Product Security Steering Committee
- Co-director of the Delta-NTU Joint RD center in National Taiwan University
- Governance Board of Delta-NTU Corp Lab

Professional Experiences

- Steering committee of the Delta-NTU Corp Lab for Cyberphysical System (CPS) in Singapore Nanyang Technological University
- Associate professor in Dept. of Electrical Engineering, Graduate Institute of Electronics Engineering, Graduate Institute of Biomedical Electronics and Bioinformatics, National Taiwan University
- PI of GE Global Research Center

Product Security Milestones in Delta Electronics

2018

Established **Delta Product Security Center** of Excellence

2019

Built **Cyberphysical System Security Research** Team in Delta Research Center

2020

Created Corp-level **Delta Product Security Steering Committee**

2020

Received the **First IEC 62443-4-1 Certificate in Taiwan**

2022

Established **ISO 17025 Cybersecurity Lab**

2024

Starting to Serve **External Clients & Partners**

Today our clients are cross various domains in the following:
Industry automation, factory automation, building automation, information & communication technology infrastructure, energy infrastructure, electric vehicles system, power systems & solutions!

Outline

1. What is Product Security
2. Why we need Product Security
   - Market Drivers
   - Customer Pain Points
3. How can Product Providers Respond?
   - Delta Practice as an Example
4. Key Product Security Capabilities for Product Providers
5. Summary: Our recommendation

What is Product Security

IT Security vs. OT Security vs. Product Security

IT Security

CIO covers

OT Security[3]

"Below" IT-OT convergence

CIO/Factory DIO cover

Optimization

Enterprise Network

Management

Operation Network

Communication

Device Network

Sensing/Control

Device/Machine/Process

IoT Layer

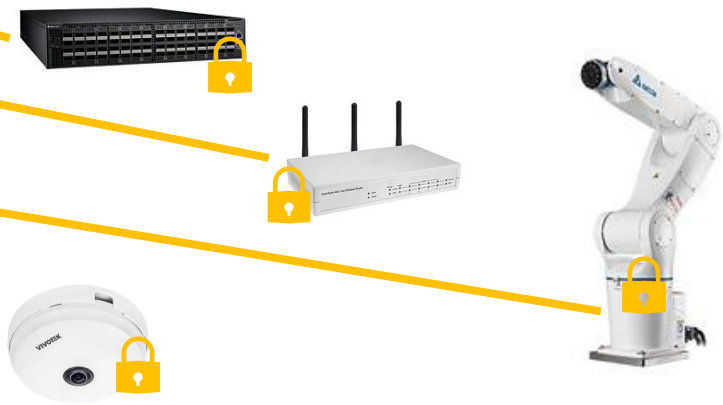
Our Point of View

To ensure the software programs embedded in Delta's and clients' products are SECURE with **free of security bugs** and equipped with **essential cyber security functions** in a **security-complied** product life cycle.

Target Audience

Product (component and system) providers

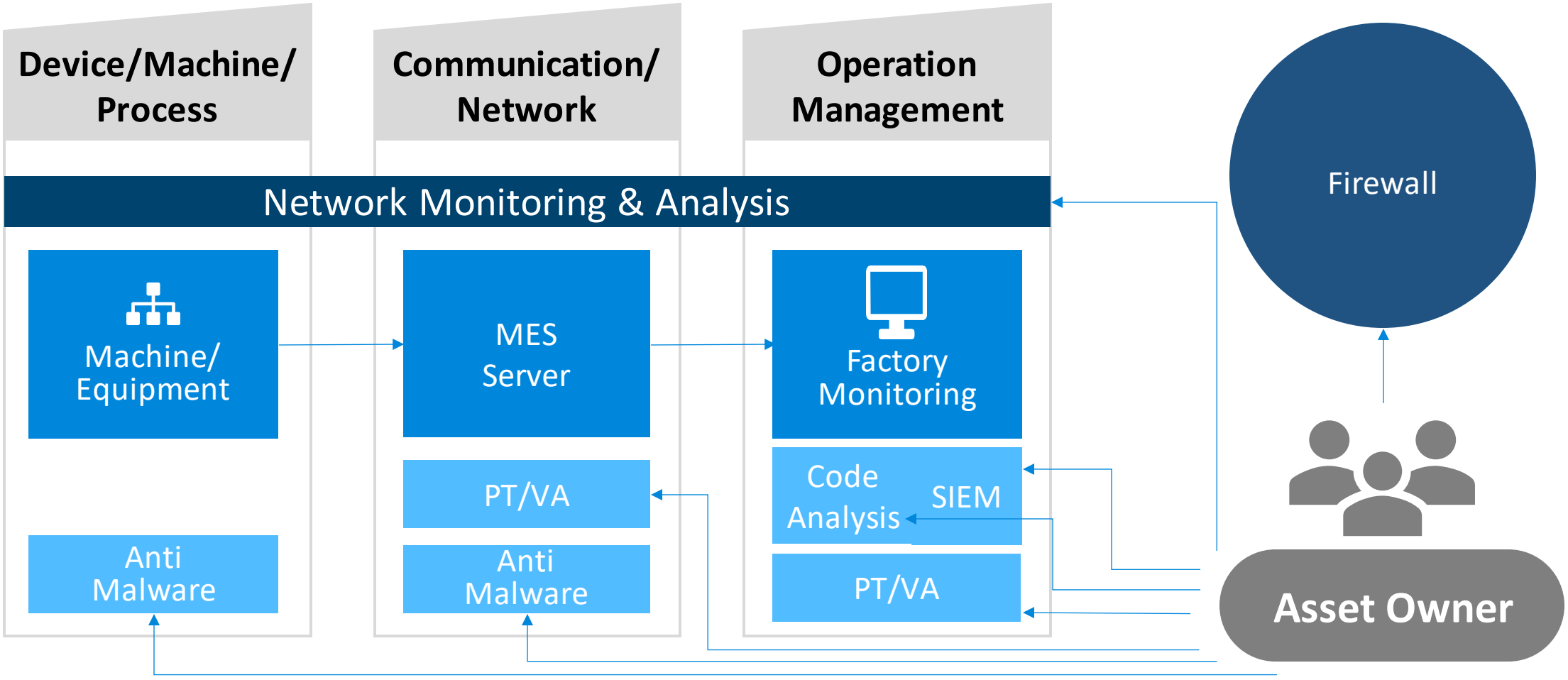
Product Security[1] within OT Products



[1]https://www.iec.ch/blog/understanding-iec-62443
[2]https://www.checkpoint.com/cyber-hub/network-security/what-is-industrial-control-systems-ics-security/
[3]https://www.gartner.com/reviews/market/operational-technology-security

Why conventional OT Security is not Sufficient for Asset Owner?

It's very difficult & complex for asset owners to implement OT security

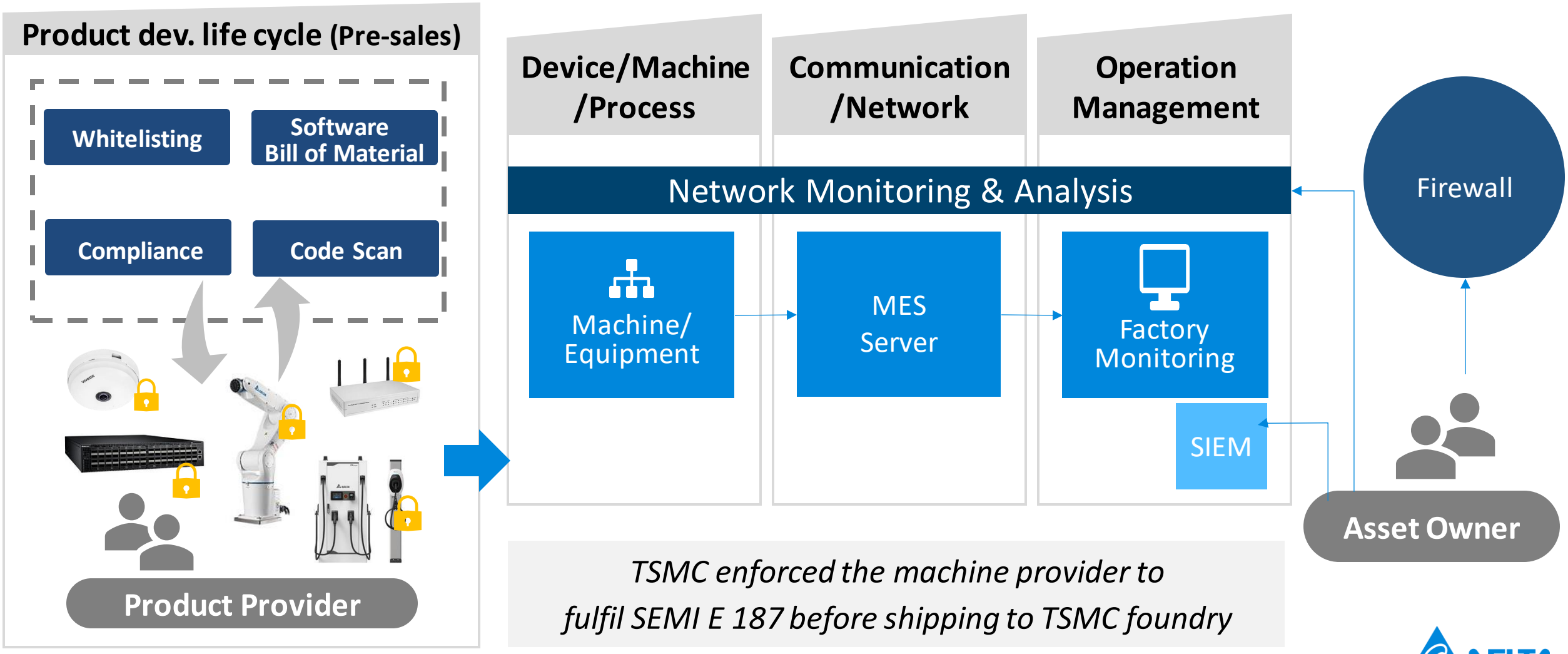


MES: Manufacturing Execution System
PT: Penetration Test
VA: Vulnerability Test
SIEM: Security Incident Respond System

Our Clients' production lines fail to implement security in their machines in OT field due to a) cost; b) Implementation complexity

How can Product Provider Offer Values from Product Security?

Product provider needs to be responsible for product security, to lessen the OT security burden from asset owners

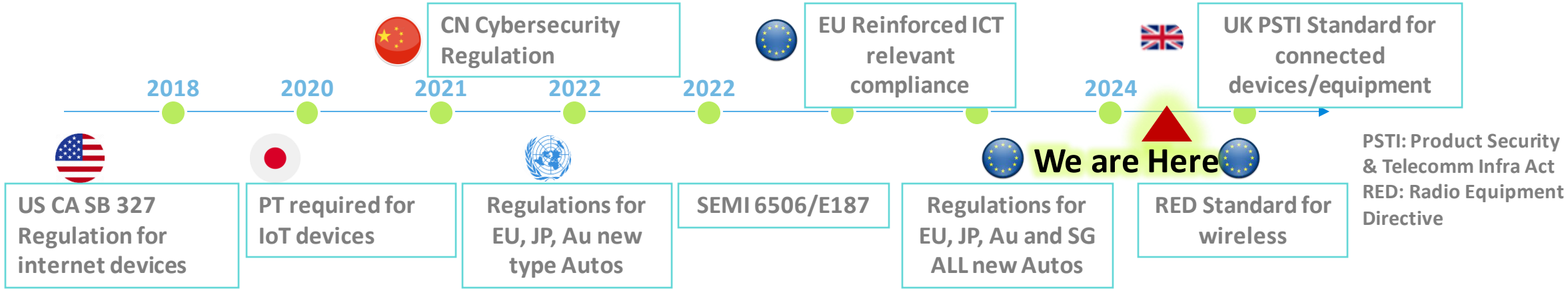


TSMC enforced the machine provider to fulfil SEMI E 187 before shipping to TSMC foundry

Why we need Product Security

Market Drivers for Product Security

Regulatory landscape



Increasing cyberattacks, causing significant loss

89% companies reported some form of attacks.

TrendMicro 2022

USD $2.5M loss as a median number for enterprises.

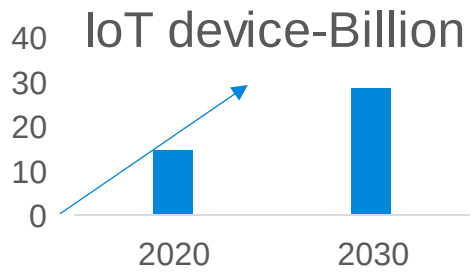
EY (安永) 2023

3+ vulnerabilities each hour (total 26,447 in 2023)

Qualys Security Blog

Connectivity introduce more attack surface

100% increased of IoT devices from 2020 to 2030



Demands & Pain Points on Doing Product Security

Target Clients

Product Providers /OBMs

Pain Points

Limited product security experts

- **Costly** to build & maintain security capability

Don’t know how to choose security solutions/services across the product development cycle:

- IT security companies less focus on **product security**

Don’t know how much to invest:

- Companies planned 7+% IT budget on cybersecurity in 2023 but struggle on the **cost performance/cost of ownership** when incorporating product security

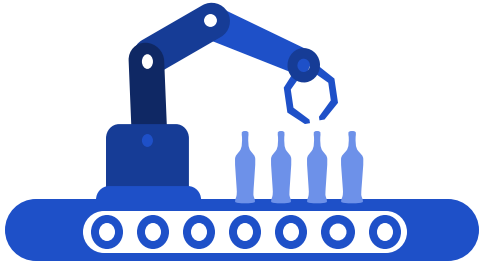
Clients Demands

“Security’ as differentiators; Choose **essential security solutions**
Design with **best practices and Cost-effective** solutions and services

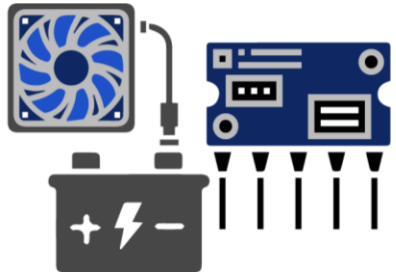
How can product provider respond?

Using Delta Electronics as an Example

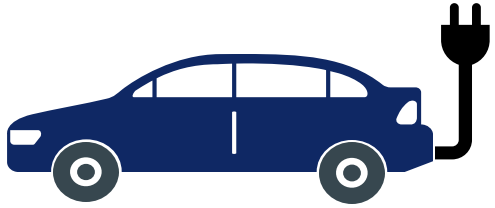
Infrastructure Business



Automation Business



Power Electronics Business



Mobility Business

- Identify product security provider
- Allocate dedicated resource
- Identify the relevant standards and partner with third party for compliance certification

GE ACC Level 2 Controllers

IEC 62443-3-3 Energy System

IEC 62443-4-2 Embedded Device

IEC 62443-3-3 Energy Solution

ISO 21434 For EV

Application Whitelisting (AWL) Solution Certified by CHT Cybersecurity

AWL was Added to Gartner Cybersecurity Product List

VPC: Voluntary Product Certification

The Growing Trend of EV Charger Attack

Trend 1

Vulnerability

CVE-2024-26288
CVE-2024-25999
CVE-2023-21824
CVE-2022-22807
…more
[REF:CVE® List]

Trend 2

Exploit

Memory

1. Malware Injections
2. Man-in-the-Middle (MITM)
3. Denial of Service (DoS)
4. False Data Injection
5. Physical Attack

[REF:Cybersecurity Risk Analysis of Electric Vehicles Charging Stations]

Trend 3

Impact

1. Spread Malicious information

2. Charging point hijacking

3. Data Leak

Selected Examples of Exploit and Defense Method:

Using OCPP 1.6 as an Example

	Case 1	Case 2	Case 3
Exploit Design	Hackers used MITM to modify firmware update process in order to exploit Log4Shell to gain root access to the EVSE	Hackers can terminate the charging session with MITM	A malicious firmware could be loaded during the update process with the code injection attack
Defense Method	• Using OCPP 1.6J with TLS • Using SFTP, FTPS or HTTPS to transfer files	• Using OCPP 1.6J with TLS	• Using OCPP 1.6J with TLS • Using whitelisting, Hash or Digital Signature to check the integrity of a downloaded file

Key Product Security Capabilities for Product Providers

What capability needed for product security?

Before Shipment

Services, SW Tools
Cyber security
Components

Product Provider

Product Development

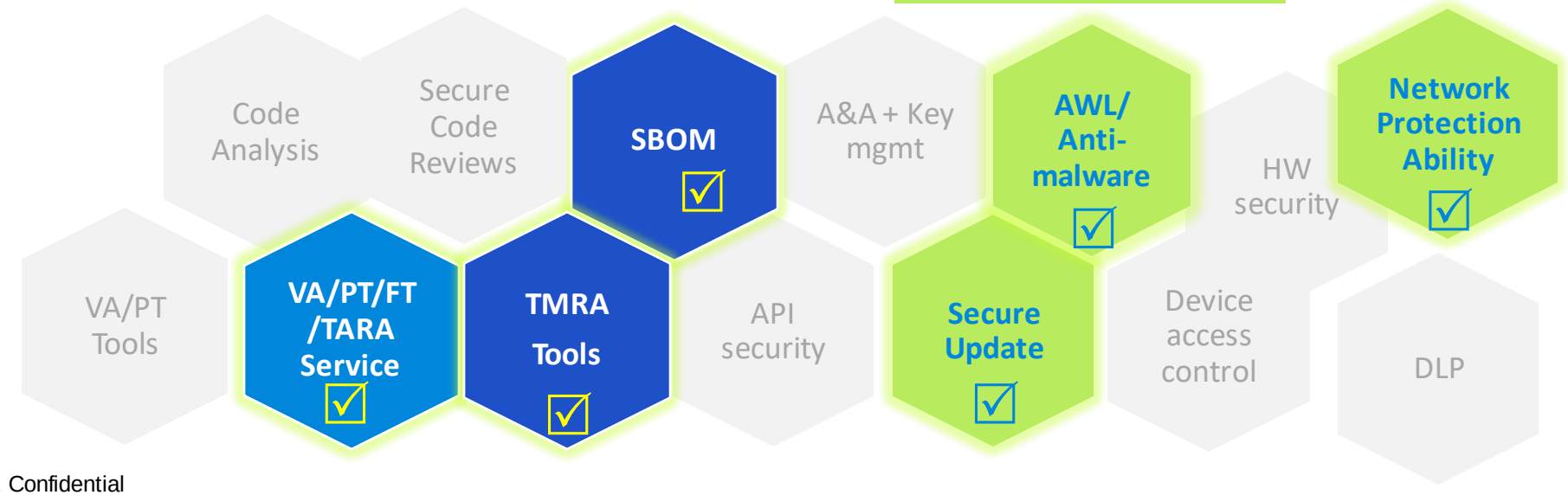
Compliance & Testing Service

Security SW Dev. Tools

Security SW & Components

Distributors Agents

Asset Owners:
- **Factories**
- **Foundry**
- **Any OT fields**



VA: Vulnerability Analysis
PT: Penetrate Test
FT: Fuzzing Test
TARA: Threat Analysis & Risk Analysis

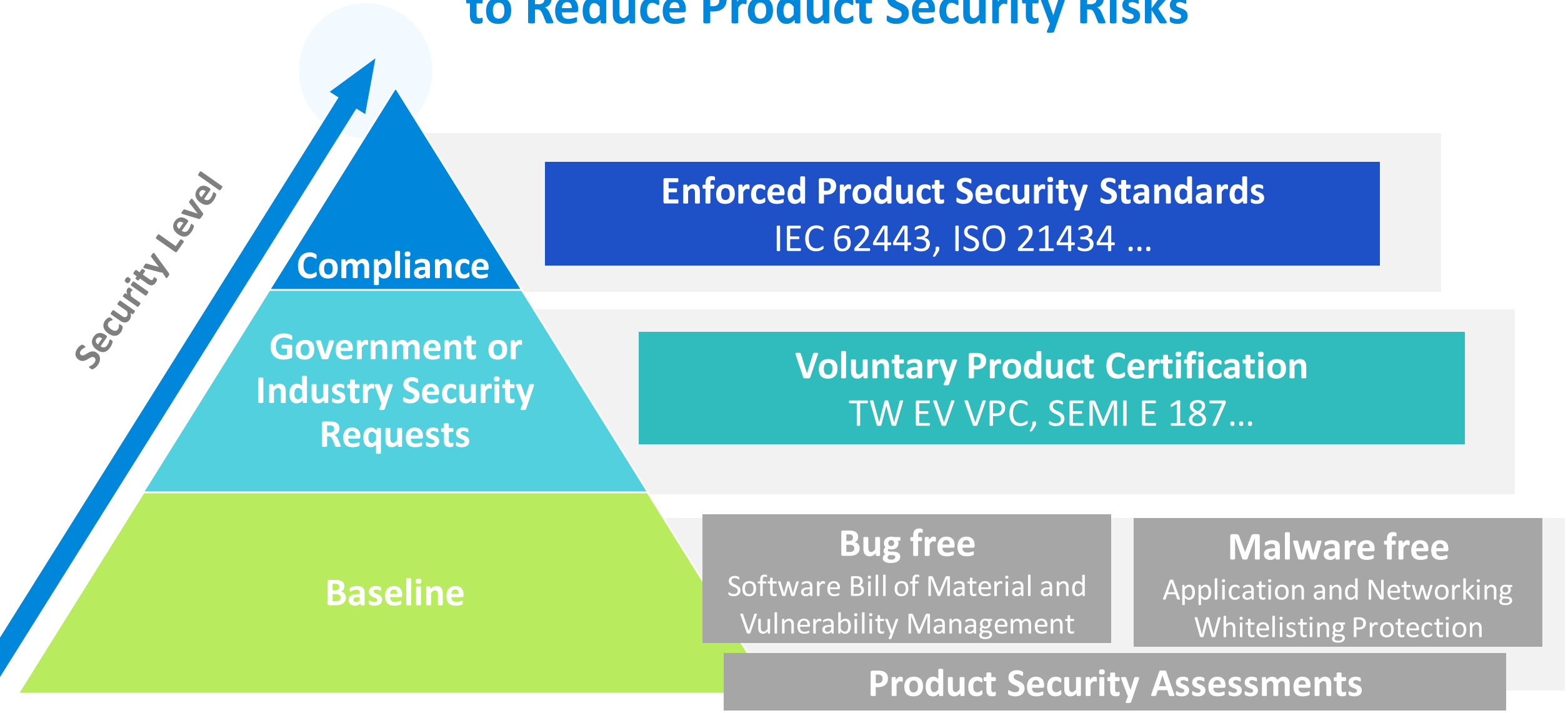
SBOM: SW Bill of Material
TMRA: Threat Modeling & Risk Analysis

AWL: Application Whitelisting

A&A: Authentication & Authorization
DLP: Data Leakage Protection

Summary: Our recommendation

Delta Cybersecurity's Recommendation to Reduce Product Security Risks



Build & Conduct a Secure SW development Life Cycle

Smarter. Greener. Together.

Wei-Cheng Tian
wc.tian@deltaww.com
https://tw.linkedin.com/in/wei-cheng-tian-25b1a427