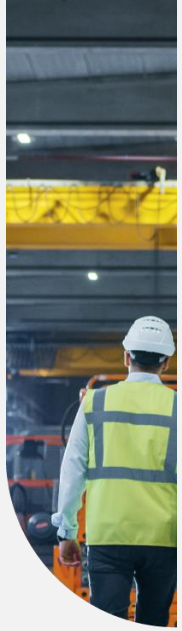


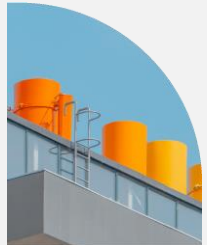
FORTINET

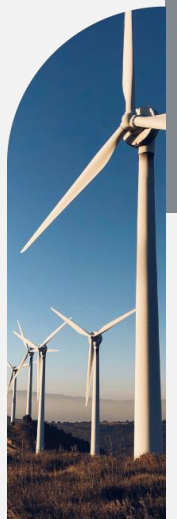
OPERATIONAL TECHNOLOGY
SYMPOSIUM 2021

Securing manufacturing's digital infrastructure using Fortinet

Dee Kimata

Schneider Electric





Agenda

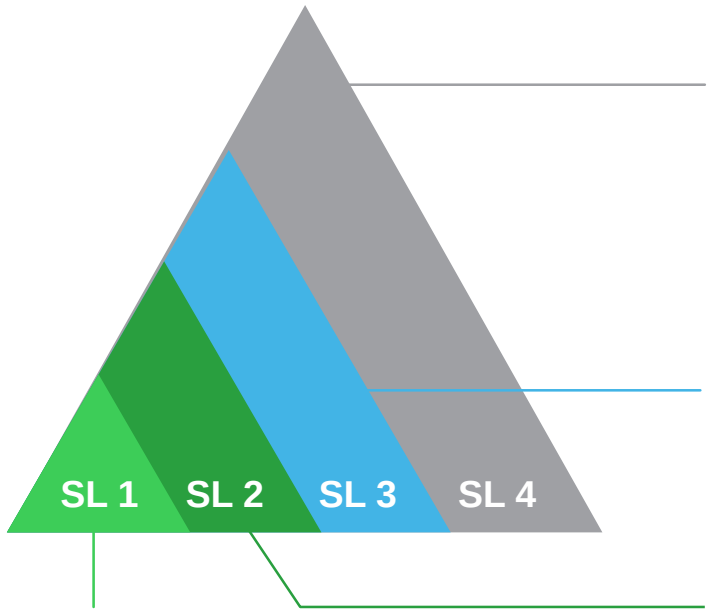
Schneider Electric utilizes Fortinet products with customers and internally

- Cybersecurity requirements in manufacturing
- Fortinet leveraged in standard architectures
- Usecase 1: Customer Example
- Usecase 2: Customer Example
- Usecase 3: SE Example

Life Is On Schneider Electric

Cybersecurity requirements for manufacturing

Standard alignment – IEC 62443 framework



Protection against intentional violation using sophisticated means with extended resources, system specific skills and high motivation.

Protection against intentional violation using sophisticated means with moderate resources, system specific skills and moderate motivation.

Protection against intentional violation using simple means with low resources, generic skills and low motivation.

Protection against casual or coincidental violation.

Key requirements / best practices

Objective: Secure data transfer to enable digitalization

Security level 1 requirements:

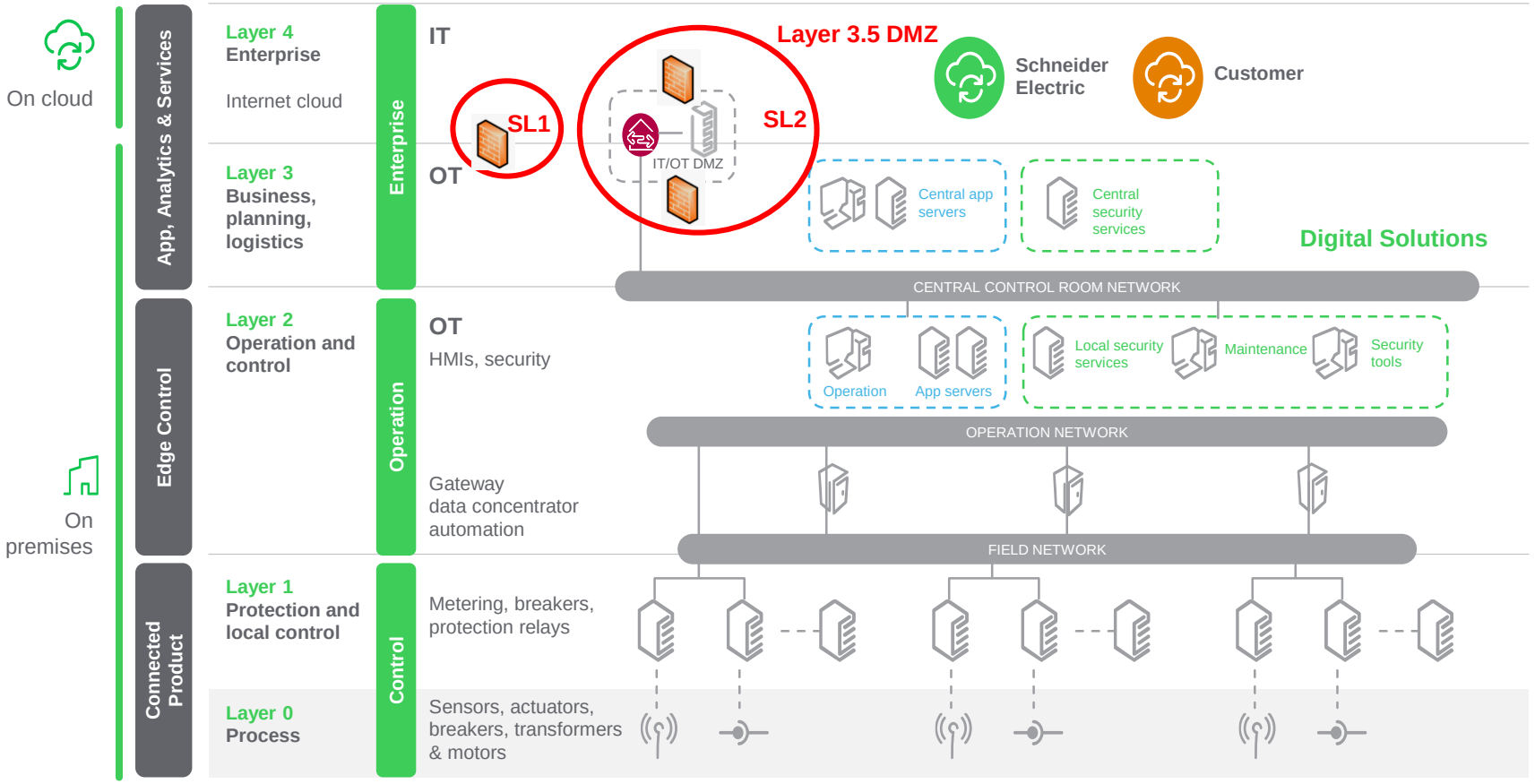
- Defined network layers and with at least one firewall
- Create a DMZ (level 3.5)
- Ensure that data doesn't bypass network layers while in transit
- Support the confidentially of the data at rest and in transit

Security level 2 + requirements:

- Ensure management of north and south firewalls are independent (different manufacturers)
- Create north and south firewalls around the DMZ

Life Is On Schneider Electric

Fortinet leveraged in standard architectures



- Fortinet Firewalls built into Schneider reference architecture
- Structure allows for the secure data transfer to support digital and cyber security solutions
- Enterprise never connects directly to the DCS system but required data can be transferred.
- Network segmentation required prior to implementing digital solutions (to algin to best practices)

Life Is On Schneider Electric

Use Case 1 – Implementing cyber monitoring solution

Customer profile: Chemical plant, multi-plant implementation

The CHALLENGE: The advanced network monitoring solution required sensitive data to go offsite. If the data was compromised, the malicious actor could have a digital footprint for what the plant looks like – presenting a risk for the customer.

- Customer intended to implement the network monitoring solution at many sites and needed a standard solution to implement across the board.
- Customer had separate teams (IT vs. OT) to manage the enterprise and operations network.

The SOLUTION: Leveraged a Fortinet firewall as part of the recommended reference architecture. Leading to the following benefits:

- Singe firewall used to run OT traffic; single point of exit for the data in transit.
- Firewall fully managed by OT team with focus on operations.

Use Case 2 – Increased visibility to level 2 data

Customer profile: Standard configuration for network monitoring solutions

The CHALLENGE: Customer was experiencing limited visibility to the mesh network (level 2 network) but required the data from the mesh network switches to feed their network monitoring solution.

- The mesh network collects valuable information from PLC/Controllers.
- Within the mesh network, there is only direct communication to the control stations.

The SOLUTION: Installed a management firewall between the level 2 (mesh network) and level 3 (process control network (PCN)) to provide security and enable secure data transfer.

- This firewall implementation gave the ability to feed data from the mesh switches into network monitoring solutions, allow for remote access, etc.

Use Case 3 – Leveraging information for remediation

Customer profile: SE product security group

The CHALLENGE: While cyber security vulnerabilities are discovered frequently, a wholistic view of vulnerabilities is a challenge. Manufacturers want to be notified so corrective patches or fixes can be issued.

- Need both a tool and process to effectively share vulnerabilities, report issue, and create a resolution.
- Multiple channels/information sharing is critical to support these efforts.

The SOLUTION: Collaboration with Fortinet's R&D team created an information flow between both teams.

- Identified vulnerabilities are communicated, triaged and joint communication is sent to customers.
- Typically identified a remediation/resolution to risk by time release/notification is sent out.

Q&A

Thank You.

Dee Kimata

OPERATIONAL TECHNOLOGY SYMPOSIUM 2021