How to remediate and recover from a cyber-attack

Jari Partanen

Director

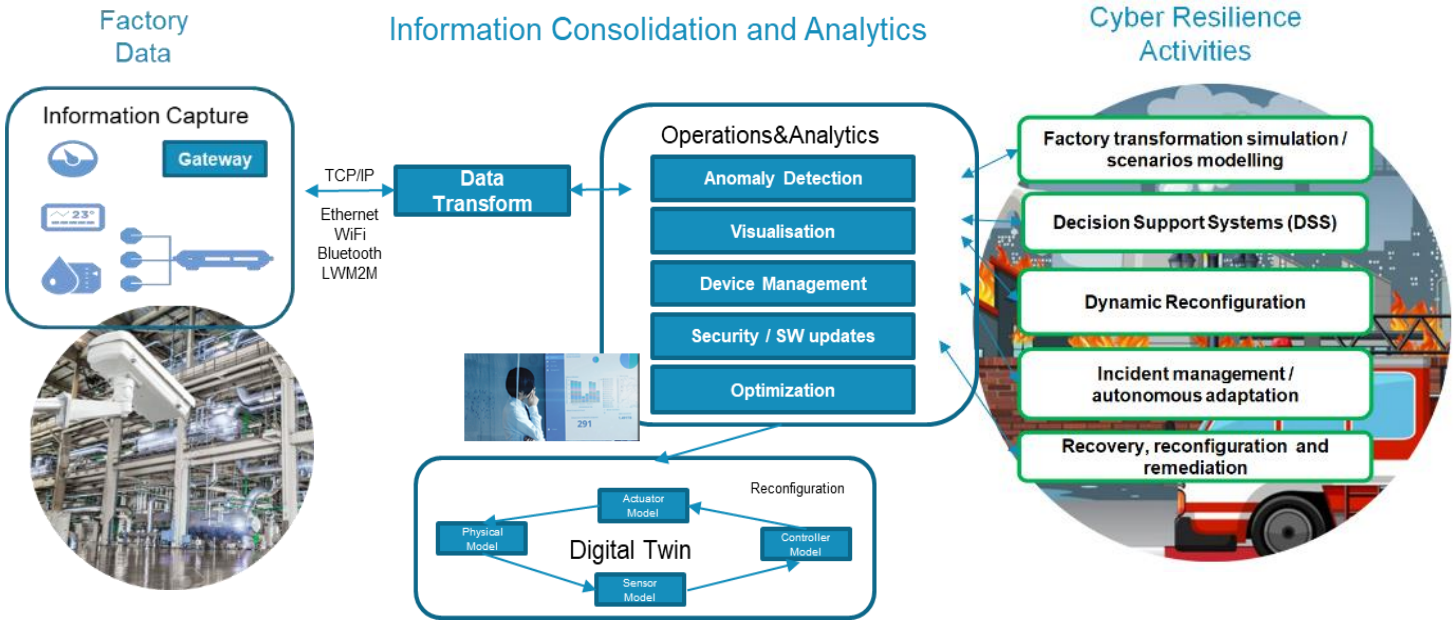
Head of Quality, Environment and Technology Management

Bittium

Prepare for Cyber Incidents with help of Cyber-resilience capabilities

The development of Cyber-resilience capabilities goes beyond risk management and technical solutions, requiring a holistic view of systems and processes to **prepare for the reality of cyber incidents.**

These principles are applied in the FoF environment.

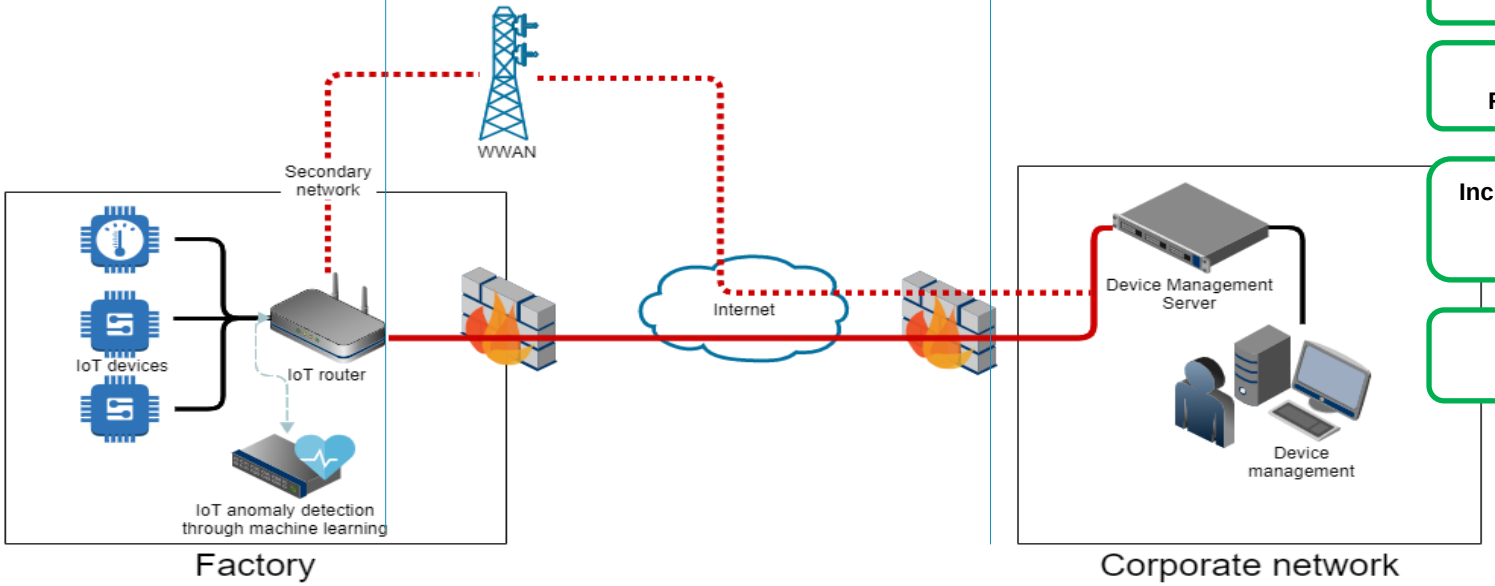


Example for Remediation of Cyber Attack: Case

Edge Tier
(Control Domain)

Platform Tier
(Operations + Information Domain)

Enterprise Tier
(Application + Business Domain)

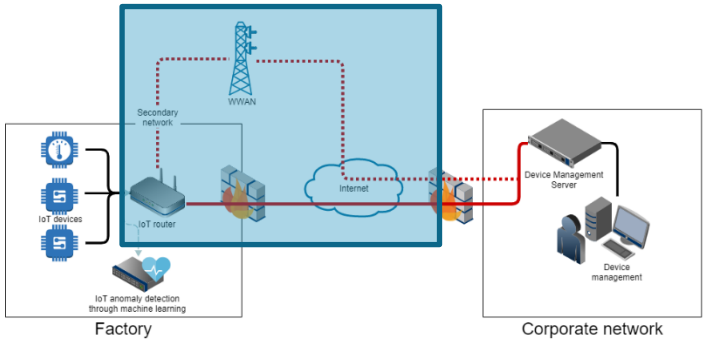


- **Decision Support**
- **Dynamic Reconfiguration**
- **Incident management & autonomous Adaptation**
- **Recovery and Remediation**

Address Resilient Communications

- A key resilience function in FoF systems, including IIoT devices is the **ability to maintain constant connectivity** to industrial control systems and other system on a continuous basis
- Single network may not provide sufficient reliability in critical manufacturing systems
- In order to build resilient manufacturing systems, a **seamless network failover is relevant**

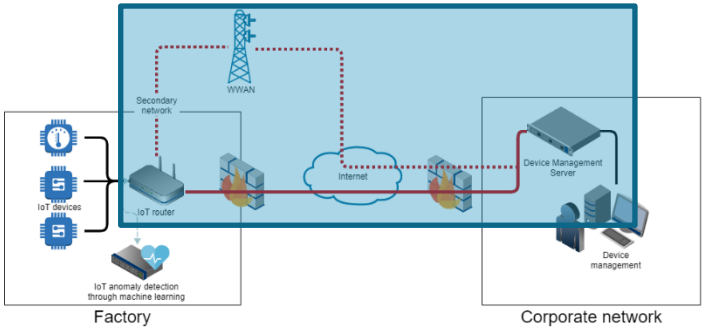
=> *Resilient communications*



Incident management & autonomous Adaptation

Update FoF assets for Recovery and Remediation

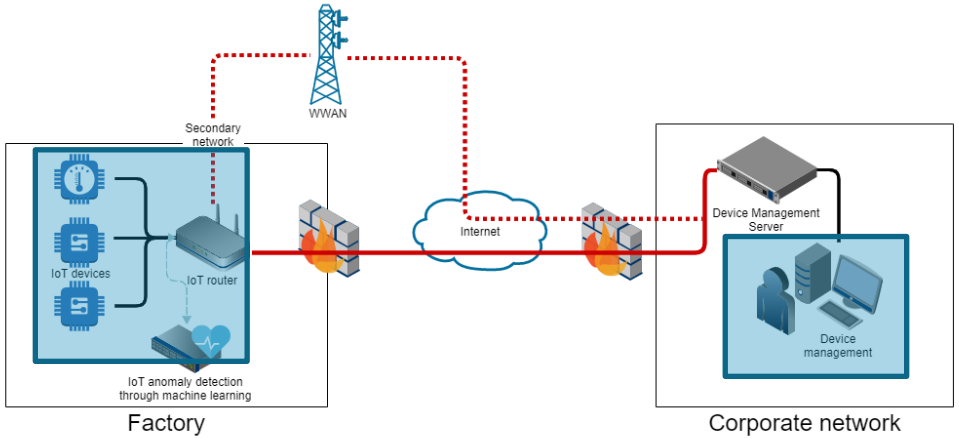
- A common flaw in FoF or e.g. IIoT systems is the **cumbersome or non-existent update system**
- Administrator is provided with *insight on the current rate of deployment of up-to-date and outdated FoF resources*
- Administrator can *monitor the update progress in real-time* using the FoF resource management console dashboards
- *The scenario enables Recovery and Remediation of the Attack*



Recovery and Remediation

Reconfigure Dynamically FoF resources

- *Dynamic security policies* are an important enabler for resilience of FoF resources e.g. IIoT systems
- Based on *FoF equipment produced data* (and changes in certain data points) the *security policy of the equipment* get update from the management server
- ***Dynamic reconfiguration enables the recovery from incidents and disaster situations***



Decision Support

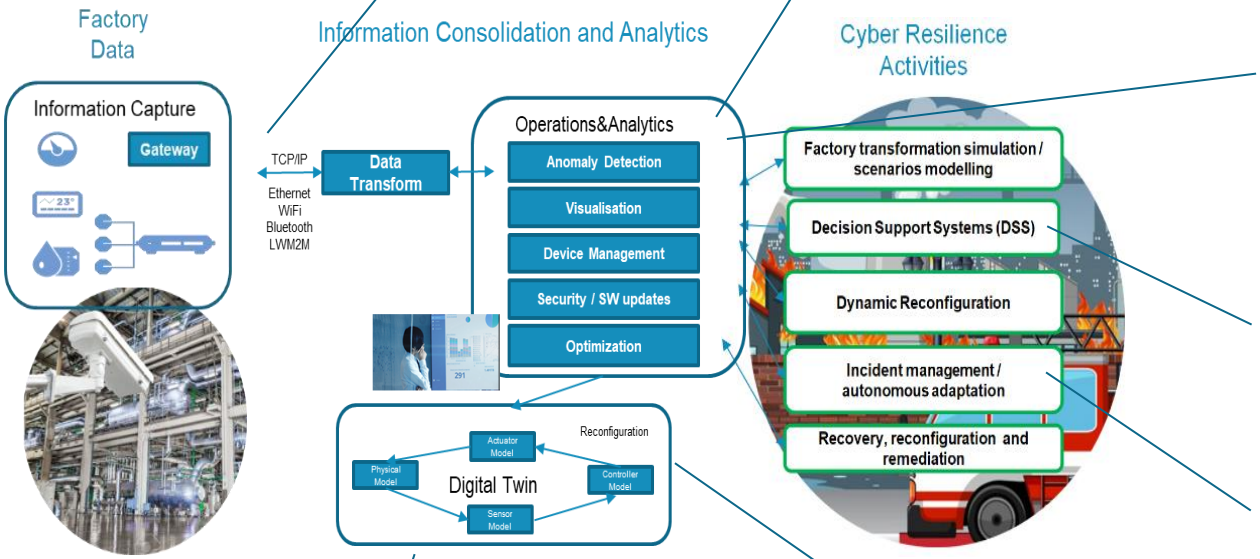
Dynamic Reconfiguration

Recovery and Remediation

Example Approaches for Cyber Resilience addressed in CF#1

Addition of Extra Layer of Security for Wireless Communications **(GOHM, Vestel)**

OT systems to report to Security operations system (SoC) Capability to collect, process, filter and forward information to SoC **(Lostar) Architecture with Vestel, GOHM**



Include to the "Virtual Assistant Agent" a module with notifications to different users **(Sistrade)**

Secure architecture for **implementation of Incident Management DSS Tool (Airbus DE)**

Description of a reconfiguration approach which is able to adjust individual robot behaviour at run time **(HTW)**
Show what reconfiguration concept shall prevent (OFFIS)

Simulation of Use Case Security Architecture with help of digital twin and Airbus CyberRange Tool **(Airbus FR, Bittium, VTT, Netox, Rugged Tooling, Houston)**

Secure Cheese Making Architecture (HighMetal, VTT, Houston Analytics)

Thank you!

Bittium

Jari Partanen

Jari.Partanen @bittium.com