Cyberfactory#1, Webinar 15.2.2022

Development of Cybersecure Architecture to improve Cyber Resilience - Practical examples

Jari Partanen, Bittium

Cyber-resilience capabilities – Introduction of the approach in Cyberfactory #1

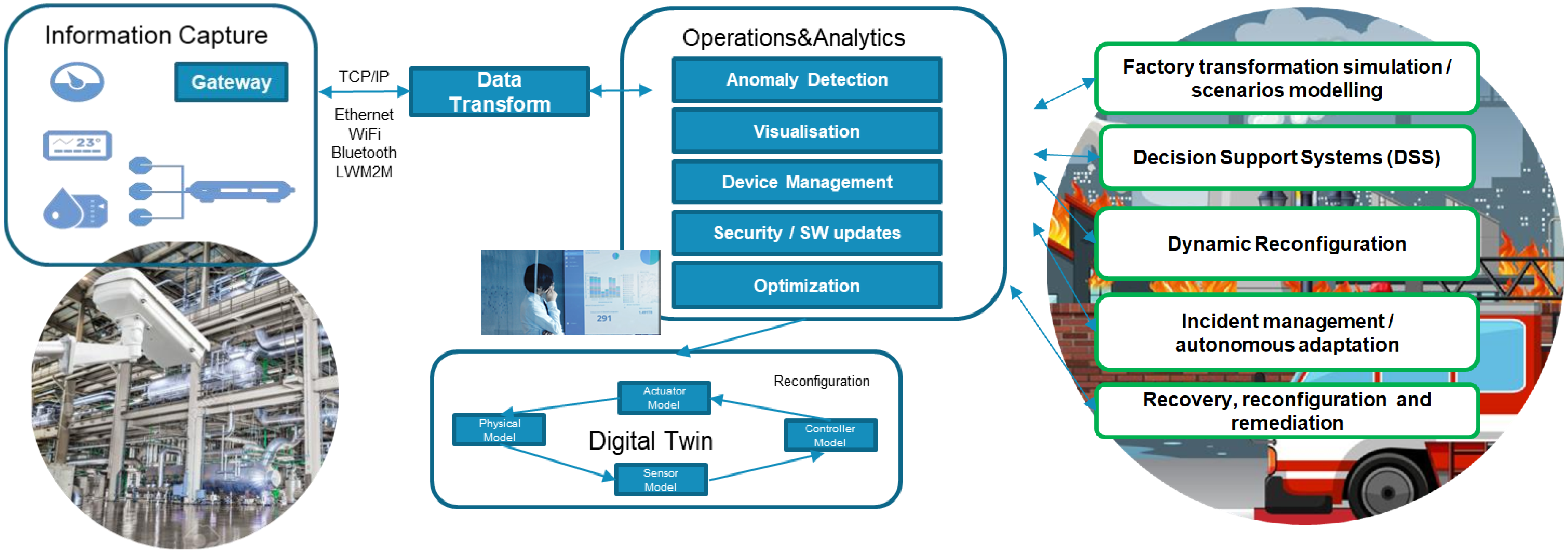
The development of Cyber-resilience capabilities goes beyond risk management and tactical technical solutions, requiring a holistic view of systems and processes to prepare for the reality of cyber incidents.

These principles are applied in the FoF environment.

Factory Data

Information Consolidation and Analytics

Cyber Resilience Activities



Information Capture

Gateway

TCP/IP

Ethernet
WiFi
Bluetooth
LWM2M

Data Transform

Operations&Analytics

Anomaly Detection

Visualisation

Device Management

Security / SW updates

Optimization

Actuator Model

Physical Model

Sensor Model

Controller Model

Reconfiguration

Digital Twin

Factory transformation simulation / scenarios modelling

Decision Support Systems (DSS)

Dynamic Reconfiguration

Incident management / autonomous adaptation

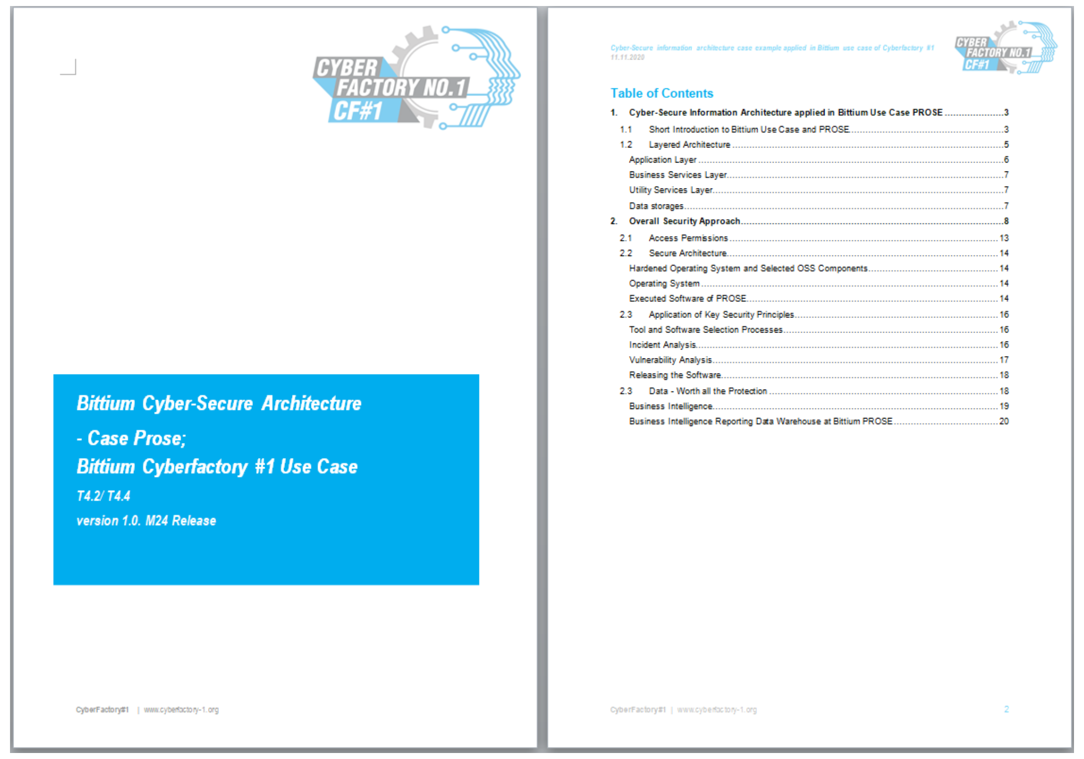
Recovery, reconfiguration and remediation

Overview of Bittium Use Case in Cyberfactory#1

Goal is to create:

- consistent and secure information architecture,
- processes and information tools,

which support digital partnered manufacturing and deliveries.



Bittium Cyber-Secure Architecture

- Case Prose;

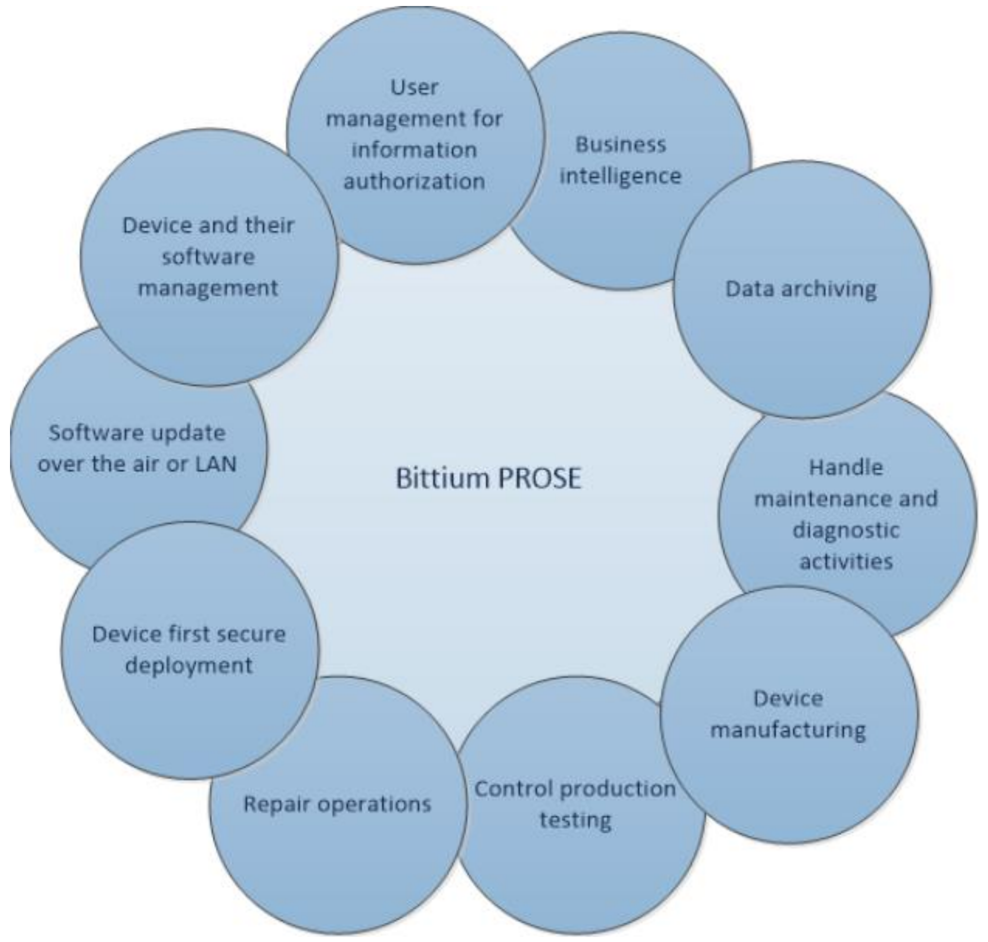
Bittium Cyberfactory #1 Use Case

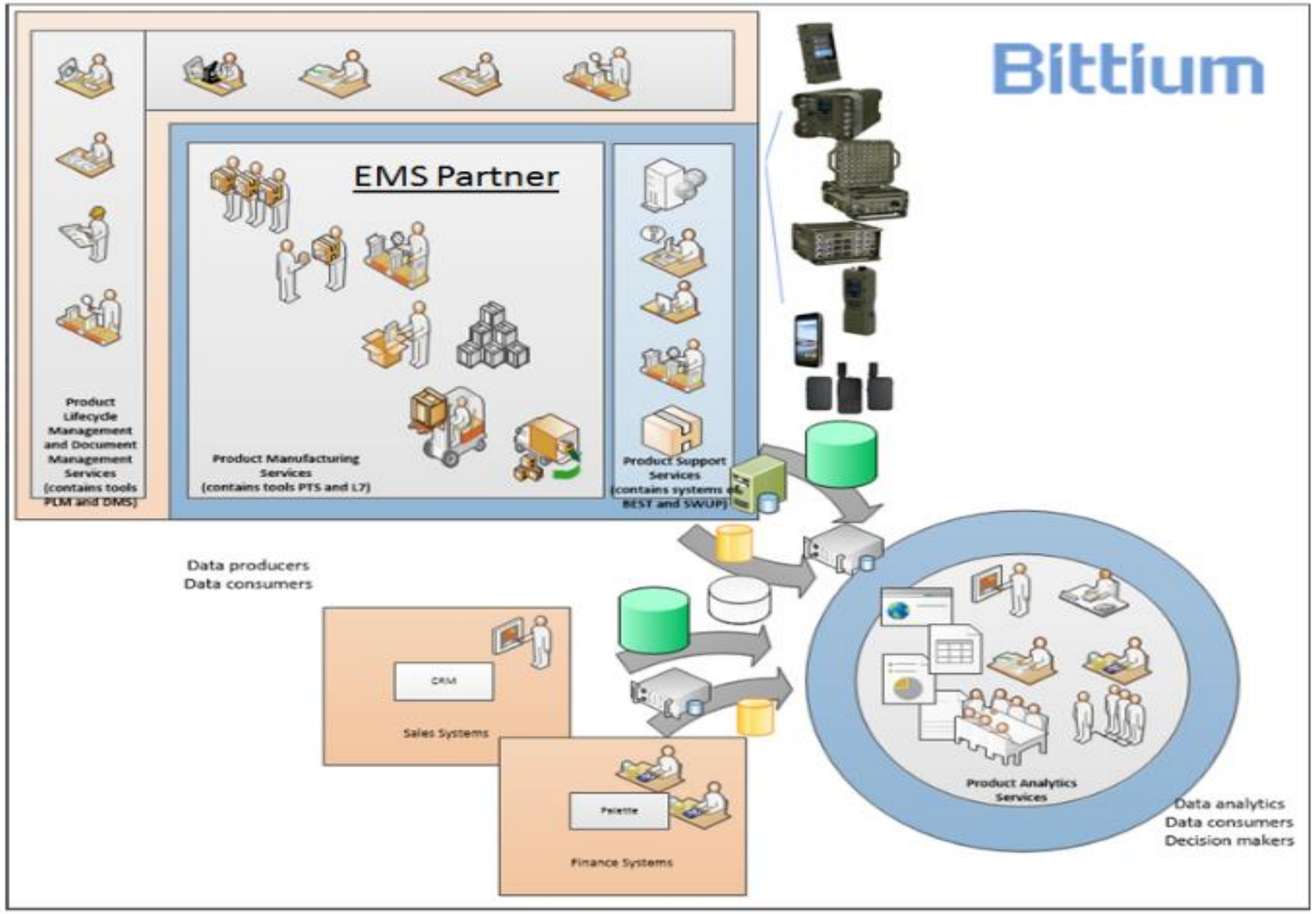
T4.2/ T4.4

version 1.0. M24 Release

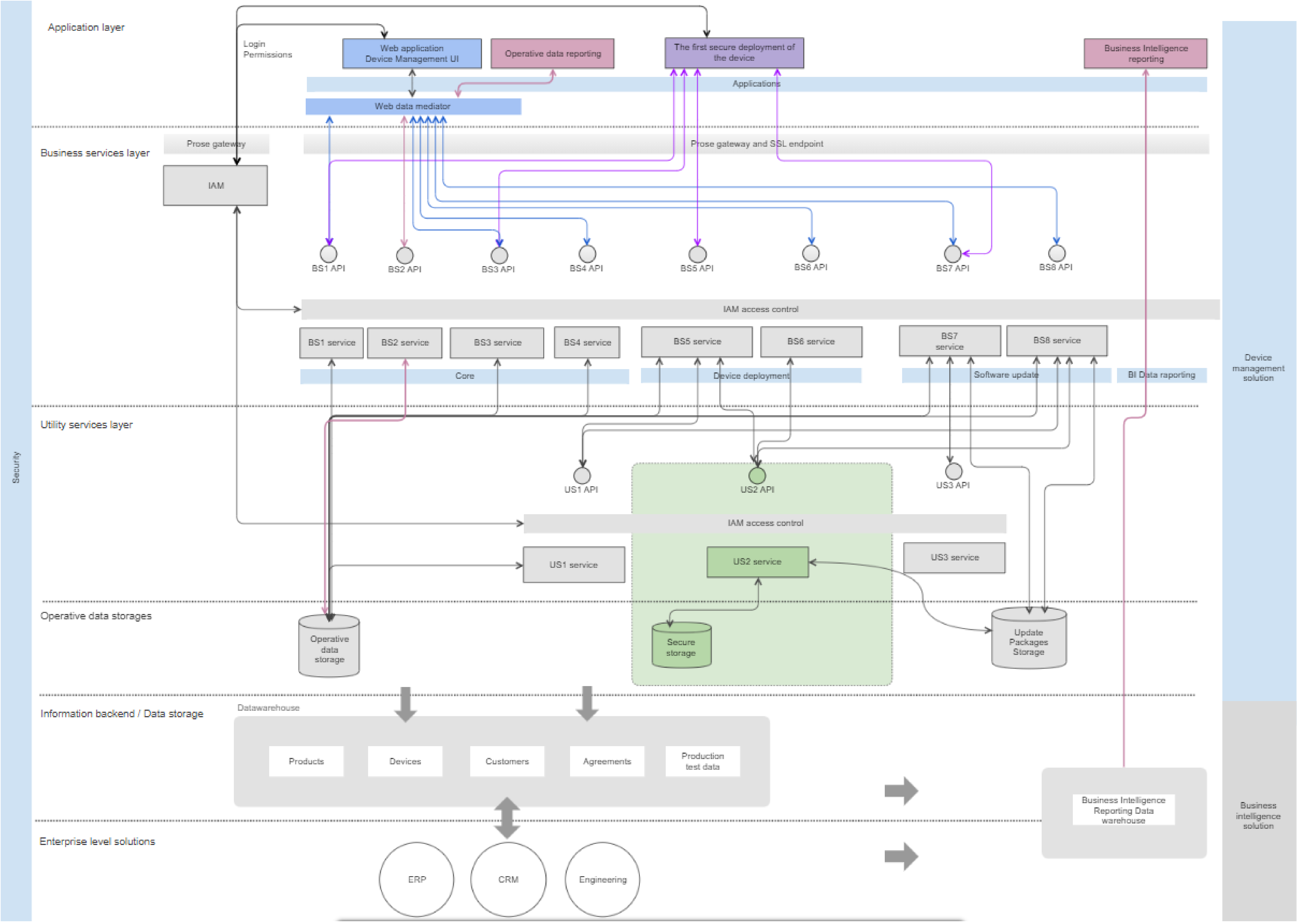
CyberFactory#1 | www.cyberfactory-1.org

Cyber-Secure information architecture case example applied in Bittium use case of Cyberfactory #1
11.11.2020


Bittium PROSE
User management for information authorization
Business intelligence
Data archiving
Handle maintenance and diagnostic activities
Device manufacturing
Control production testing
Repair operations
Device first secure deployment
Software update over the air or LAN
Device and their software management


Bittium
EMS Partner
Product Lifecycle Management and Document Management Services (contains tools PLM and DMS)
Product Manufacturing Services (contains tools PTS and L7)
Product Support Services (contains systems of BEST and SWUP)
Data producers
Data consumers
CRM
Sales Systems
Palette
Finance Systems
Product Analytics Services
Data analytics
Data consumers
Decision makers

Overview of Bittium PROSE architecture – Simplified View



- Bittium PROSE (Product Services) is a solution for Device Life Cycle Management.
- Bittium PROSE is an eco-system: with PROSE it is easy to manage devices and their software, handle maintenance and diagnostic activities, control manufacturing and production testing and test events in repair operations.
- PROSE handles business intelligence level and operative level reporting.
- It contains user management for information authorization.
- Also the first secure deployment of devices, commissioning, is possible with help of PROSE.

Aspects to Build Cyber Resilience in the Use Case Information Architecture

IAM Controls

- Access & Trust Mgmt; Build Identity and Access Management solution architecture.

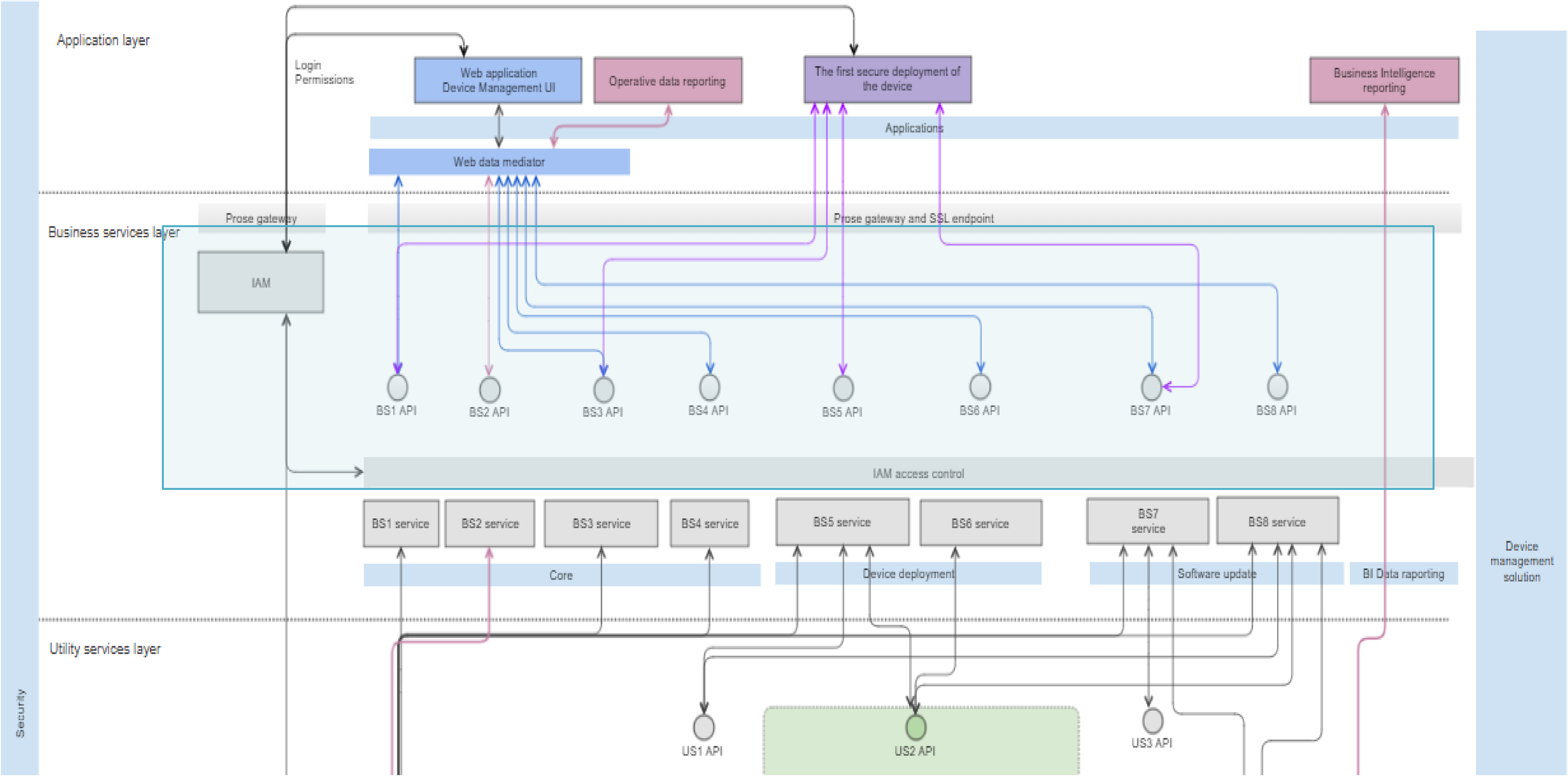
Behaviour Watch Principles

- (Human/Machine) Behavior Watch; Deploy Incident analysis, Vulnerability Scanning, Anomaly Detection and applicable SIEM functionalities.

Cyber Resilience Capabilities

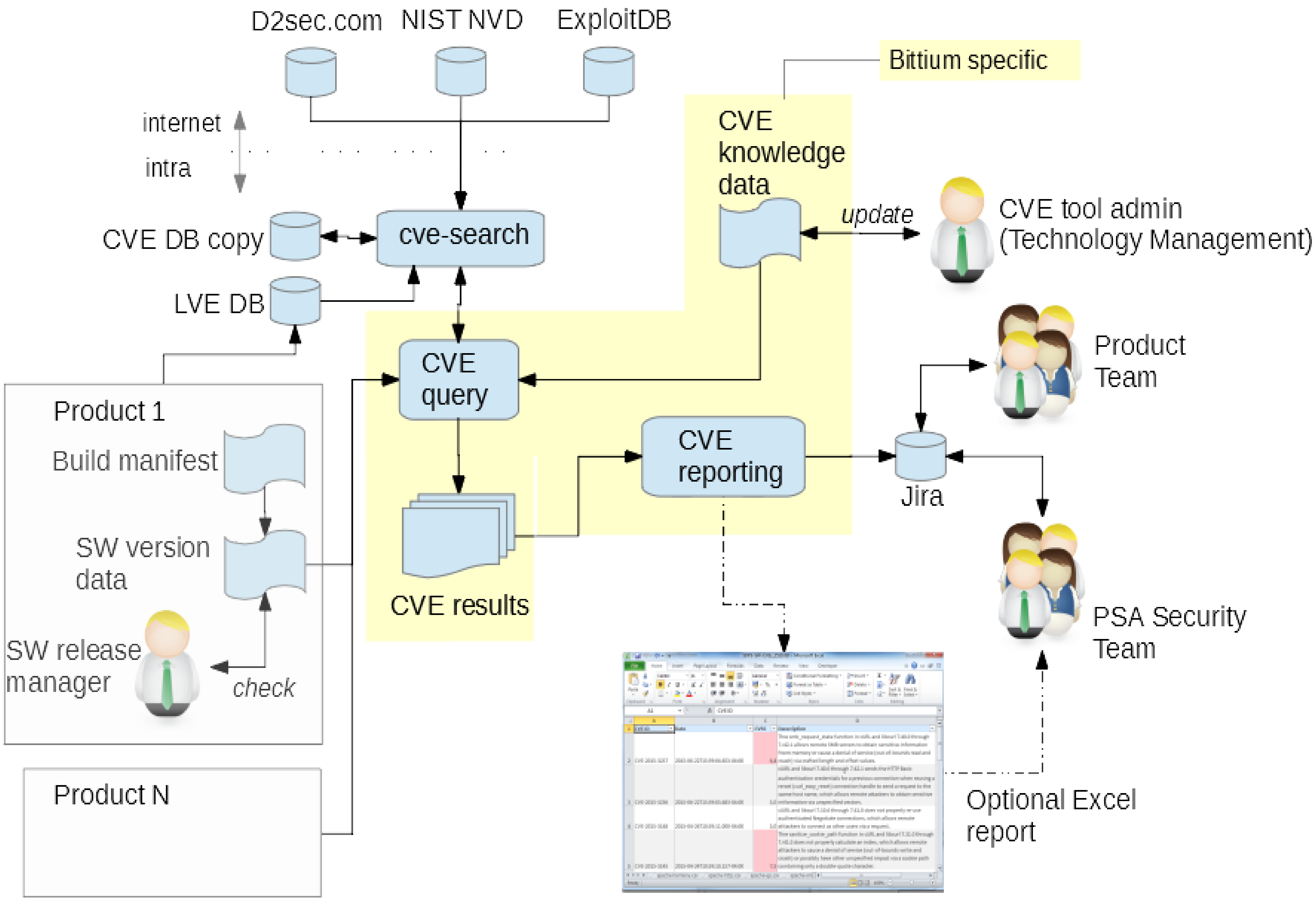
- Connection of the architecture, digital twin of the system and simulation environment (with help of Airbus CyberRange in CF#1) - Simulation of the weaknesses, capabilities with help of various Cyber frameworks.

Human/Machine access & trust management – Identity and Access Management

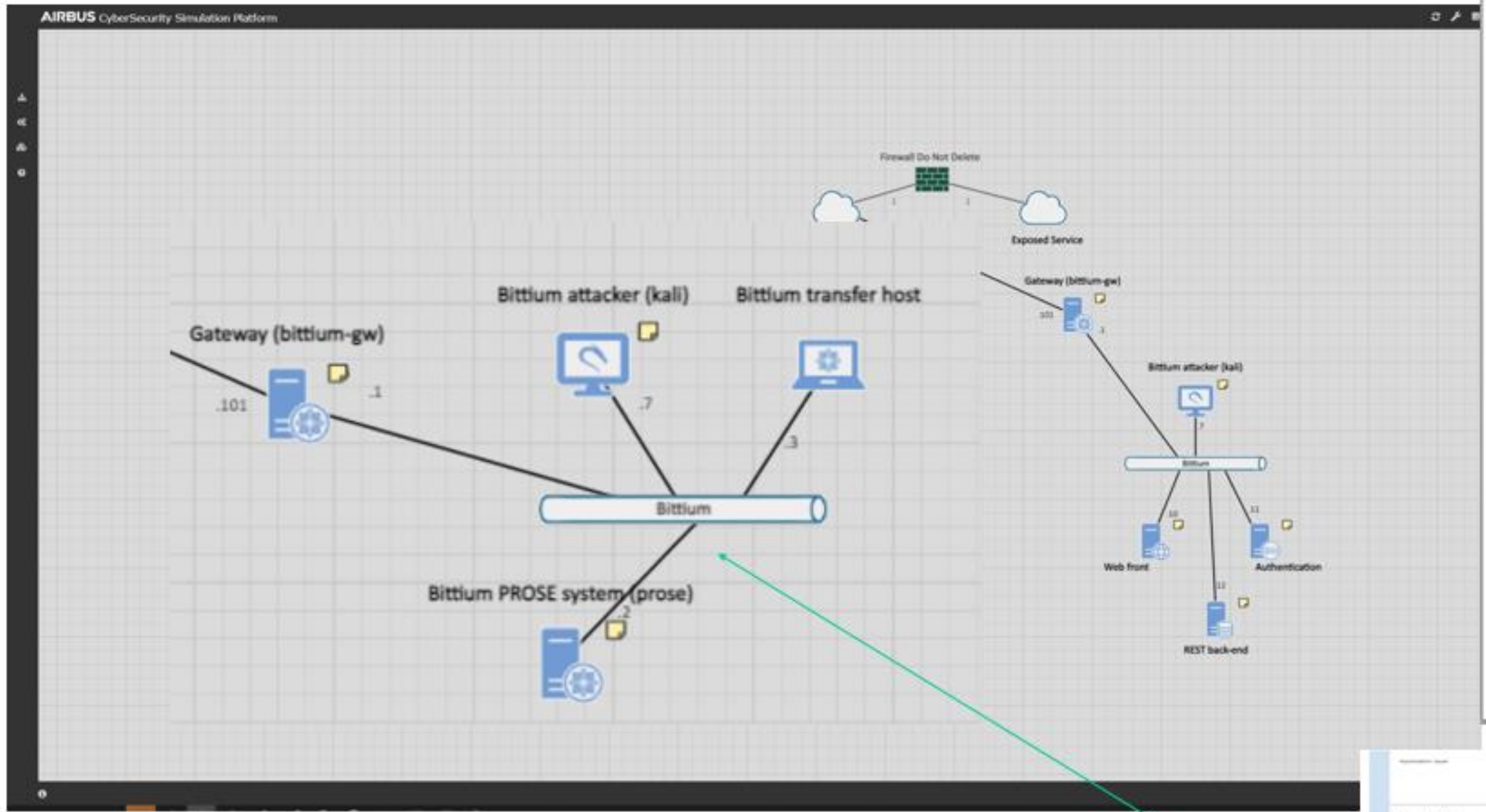


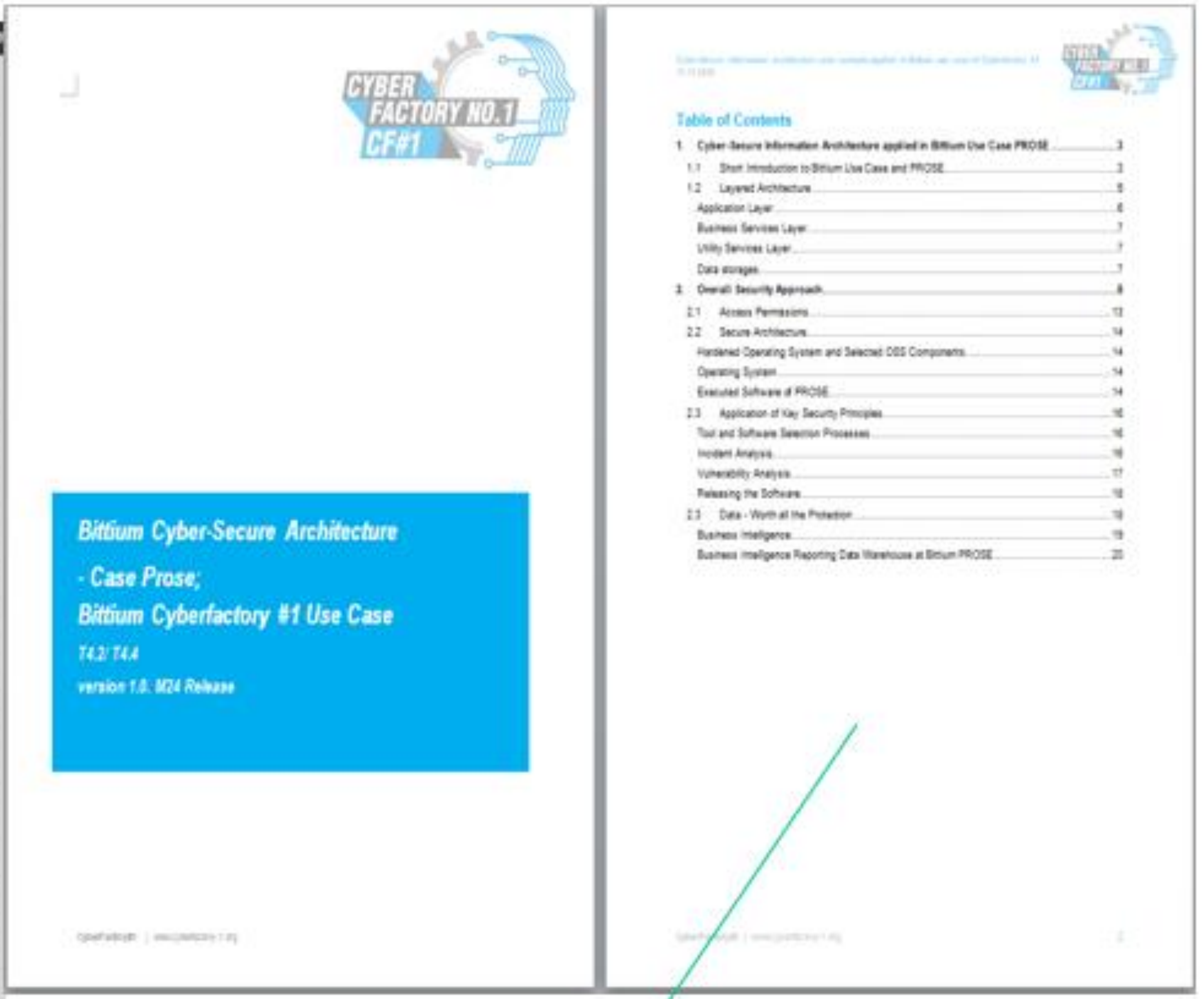
- Permission control is an integral part of Bittium PROSE service architecture.
- Each service checks the service API caller permissions from IAM based on the token obtained by the application before proceeding to call the services.
- Only the callers with correct permissions for executing the requested service call are served.
- All other calls are blocked, logged and error code is returned to the caller.

Example of CVE Process applied in the Use Case



Cyber-resilience capabilities Simulation of Cyber Attacks with help of Airbus CyberRange





Bittium Cyber-Secure Architecture

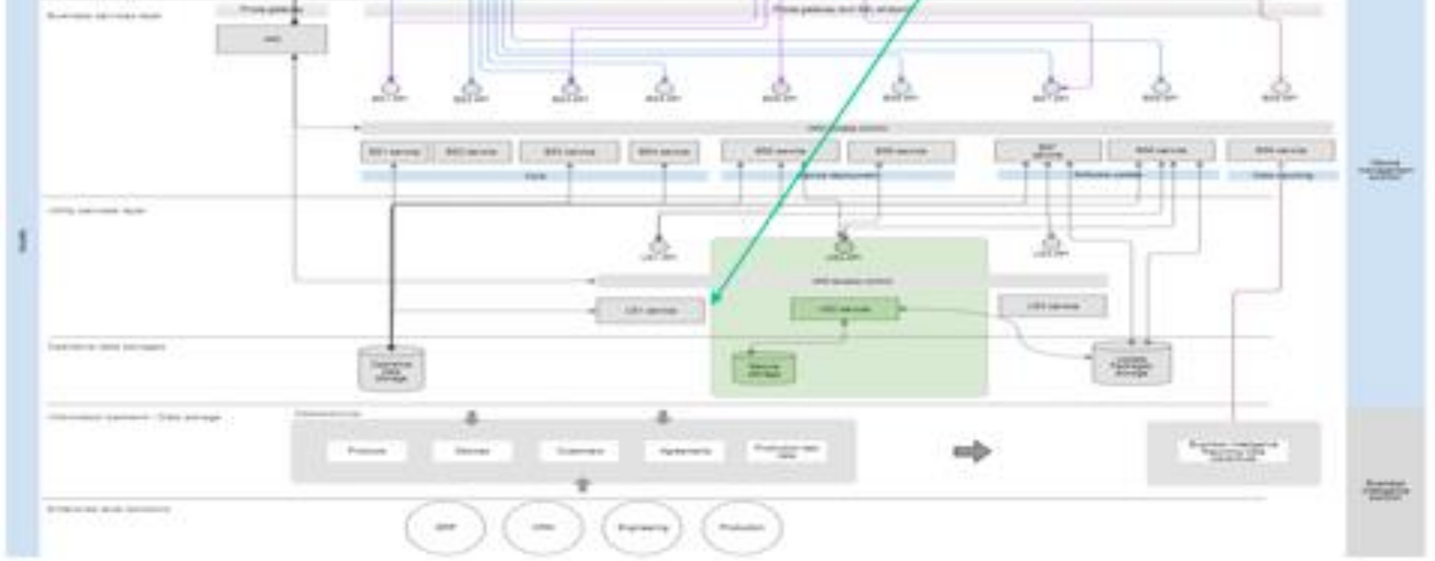
- Case Prose;

Bittium Cyberfactory #1 Use Case

T4.2/ T4.4

version 1.0. M24 Release

Table of Contents



Use of e.g. MITRE & OWASP etc. as frameworks.

Connection of the use case architecture, digital twin of the use case and simulation environment (with help of Airbus CyberRange).

Thank You!

Any Questions?

More information Jari.Partanen@bittium.com