FIIF EVENT:
CYBERFACTORY#1 DISSEMINATION EVENT

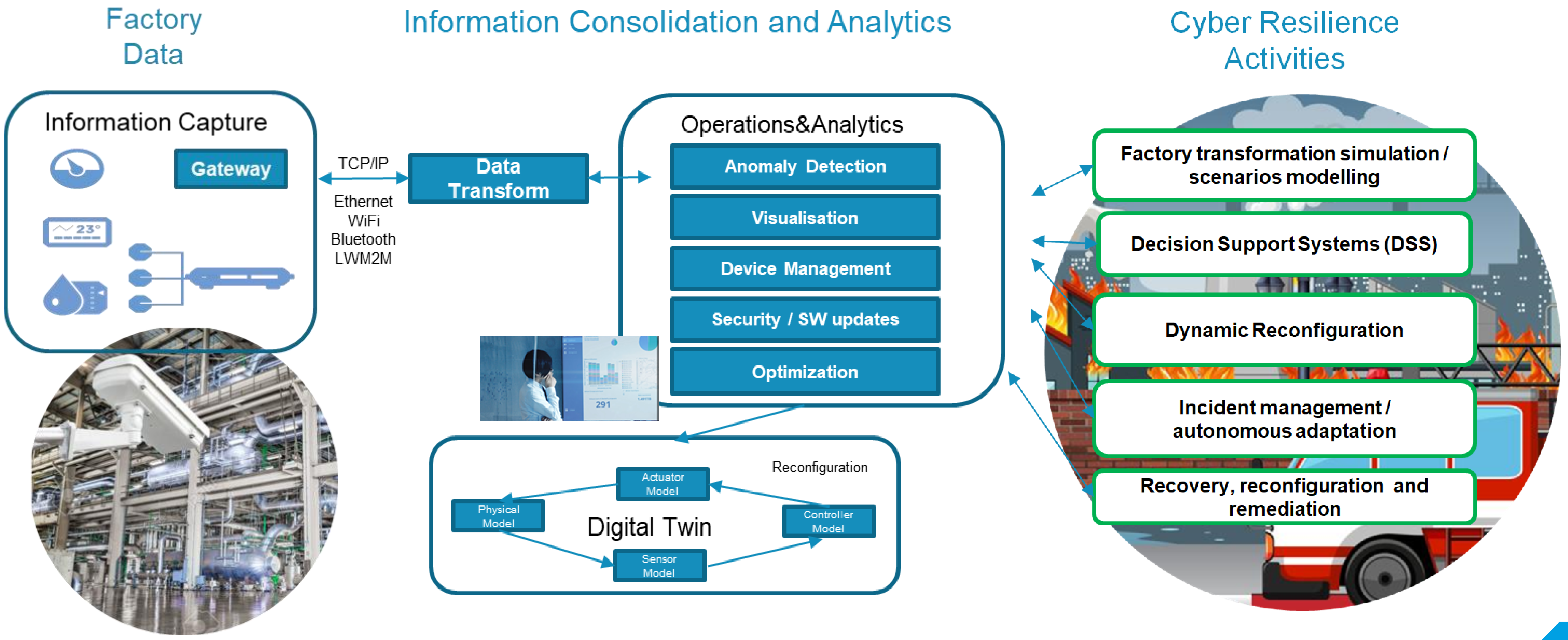
Development of Cybersecure Architecture to improve Cyber Resilience, Case Bittium

Jari Partanen

What are Cyber-resilience capabilities ?

Approach taken in Cyberfactory #1 project

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.



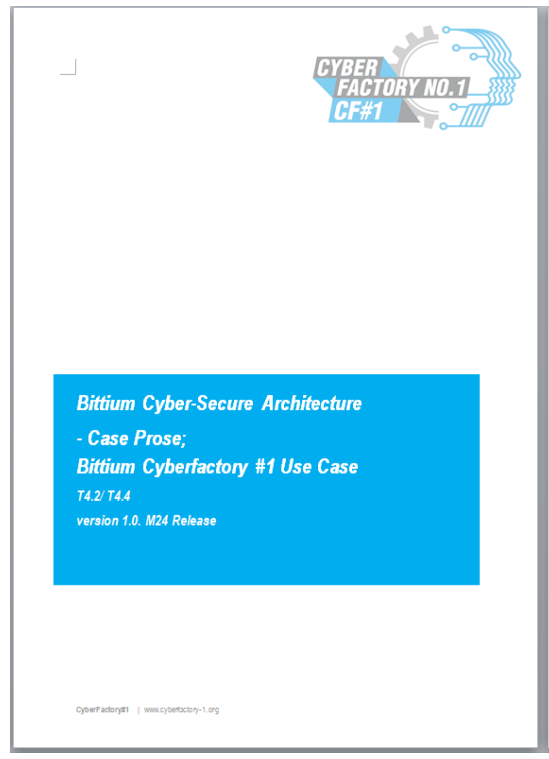
Cyber-secure networked supply chain and information architecture

Overview of Bittium Use Case in Cyberfactory#1

Goal was to create:

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

which support digital partnered manufacturing and deliveries.



Bittium Cyber-Secure Architecture

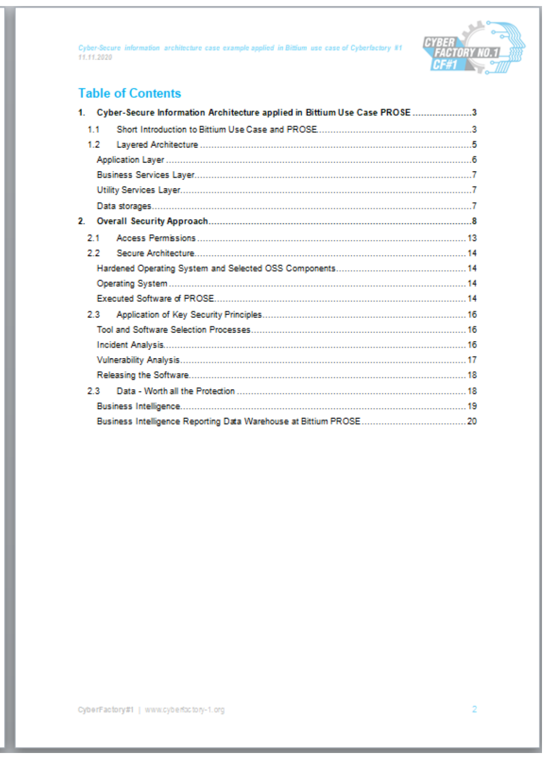
- Case Prose;

Bittium Cyberfactory #1 Use Case

T4.2/ T4.4

version 1.0. M24 Release

CyberFactory#1 | www.cyberfactory-1.org

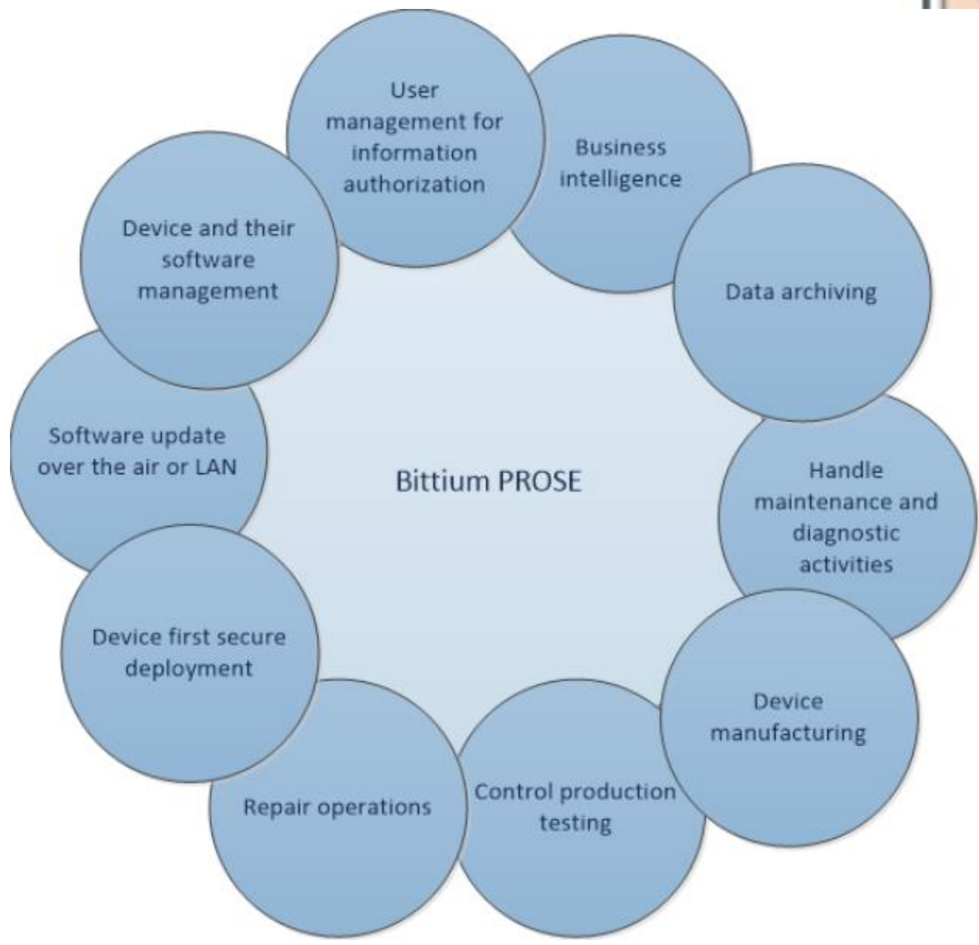


Cyber-Secure information architecture case example applied in Bittium use case of Cyberfactory #1

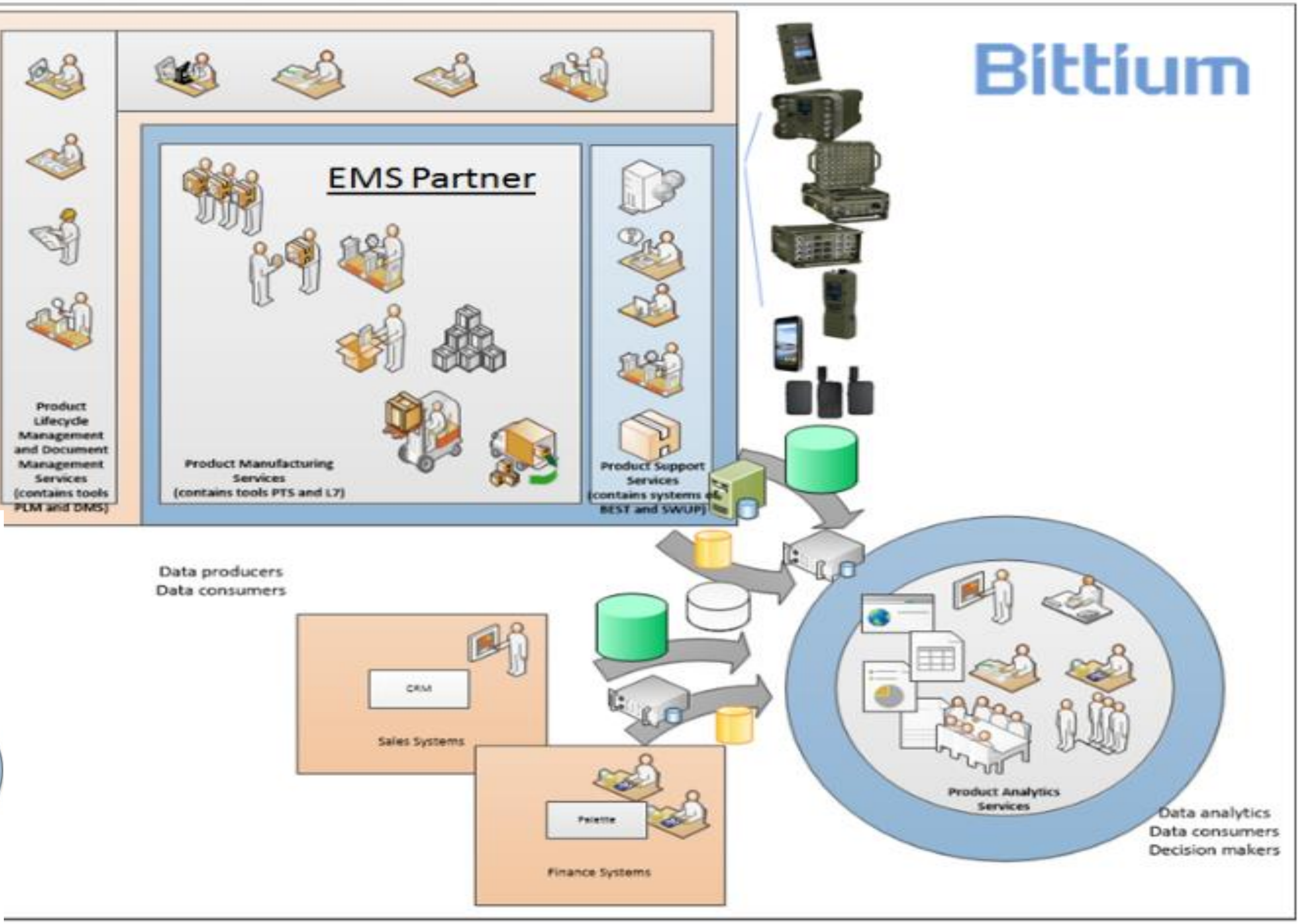
11.11.2020

Table of Contents

CyberFactory#1 | www.cyberfactory-1.org

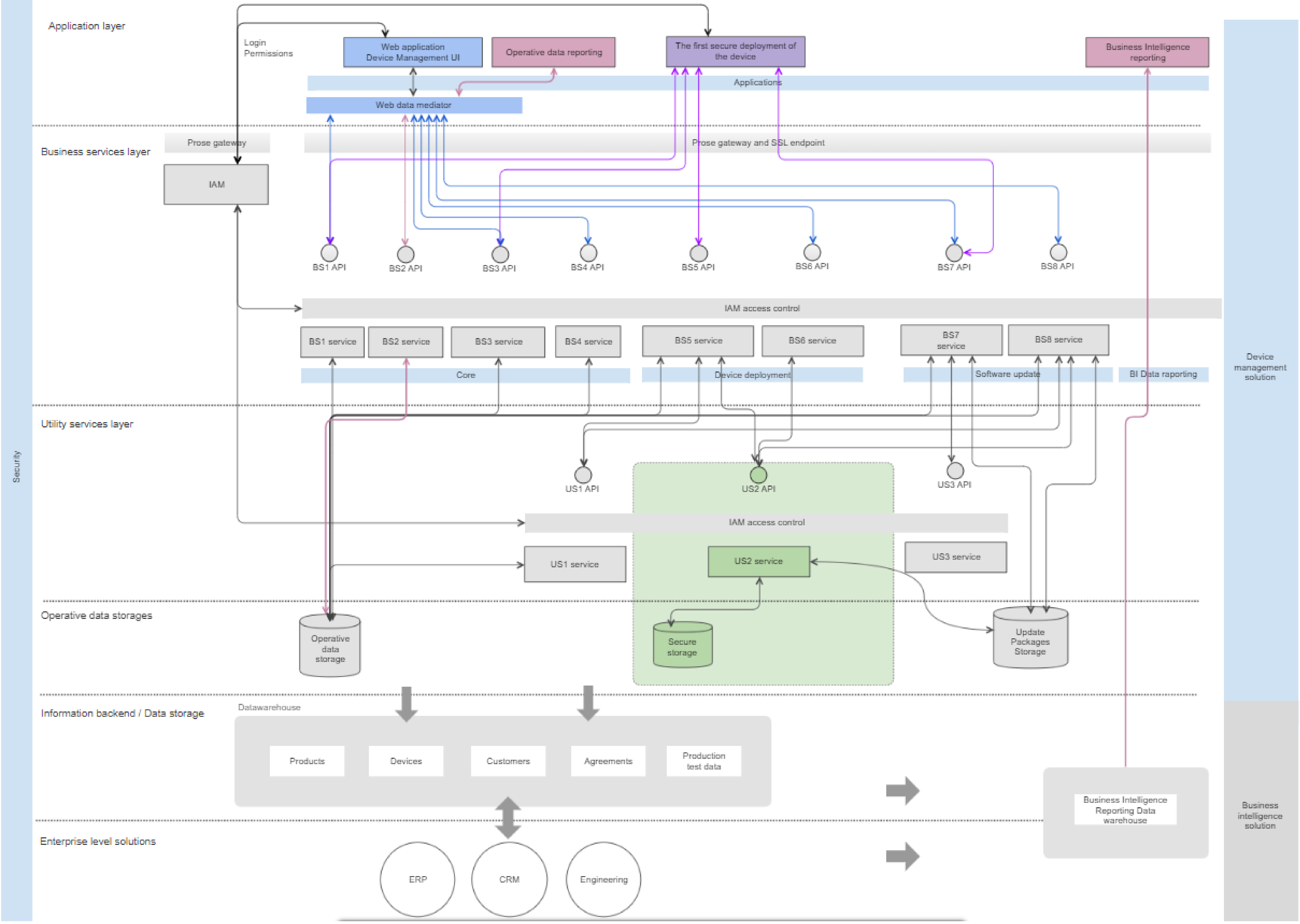


Bittium PROSE
User management for information authorization
Business intelligence
Data archiving
Handle maintenance and diagnostic activities
Device manufacturing
Control production testing
Repair operations
Device first secure deployment
Software update over the air or LAN
Device and their software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

Bittium PROSE cyber secure architecture in a nutshell



- 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.

Exploitation of the capabilities for Manufacturing Optimization

CAP41-Real time sensing & tracking

- Development of Asset management and tracking to enable ***real-time transparency*** throughout the delivery chain

CAP42-Manufacturing data-lake exploitation

- Use case architecture was developed towards concept where data lake information is collected consistently with help of ETL (Extract-Transfrm-Load) to data lake

=> ***Continuous and transparent nearly real-time reporting from Virtual Delivery Chain***

CAP44-Distributed Manufacturing

- Developed a concept which helps to recognize effect of failures in the data to the system. Data generated to include a set of different failures, threats, missing data and data anomalies => ***BI reporting and justification of manufacturing capacity***

Exploitation of Cyber-Secure Architecture Capabilities

CAP51-Human/Machine access & trust mgmt

- Deployment of ***Identity and Access Management*** solution architecture.

CAP53-Human/Machine behavior watch

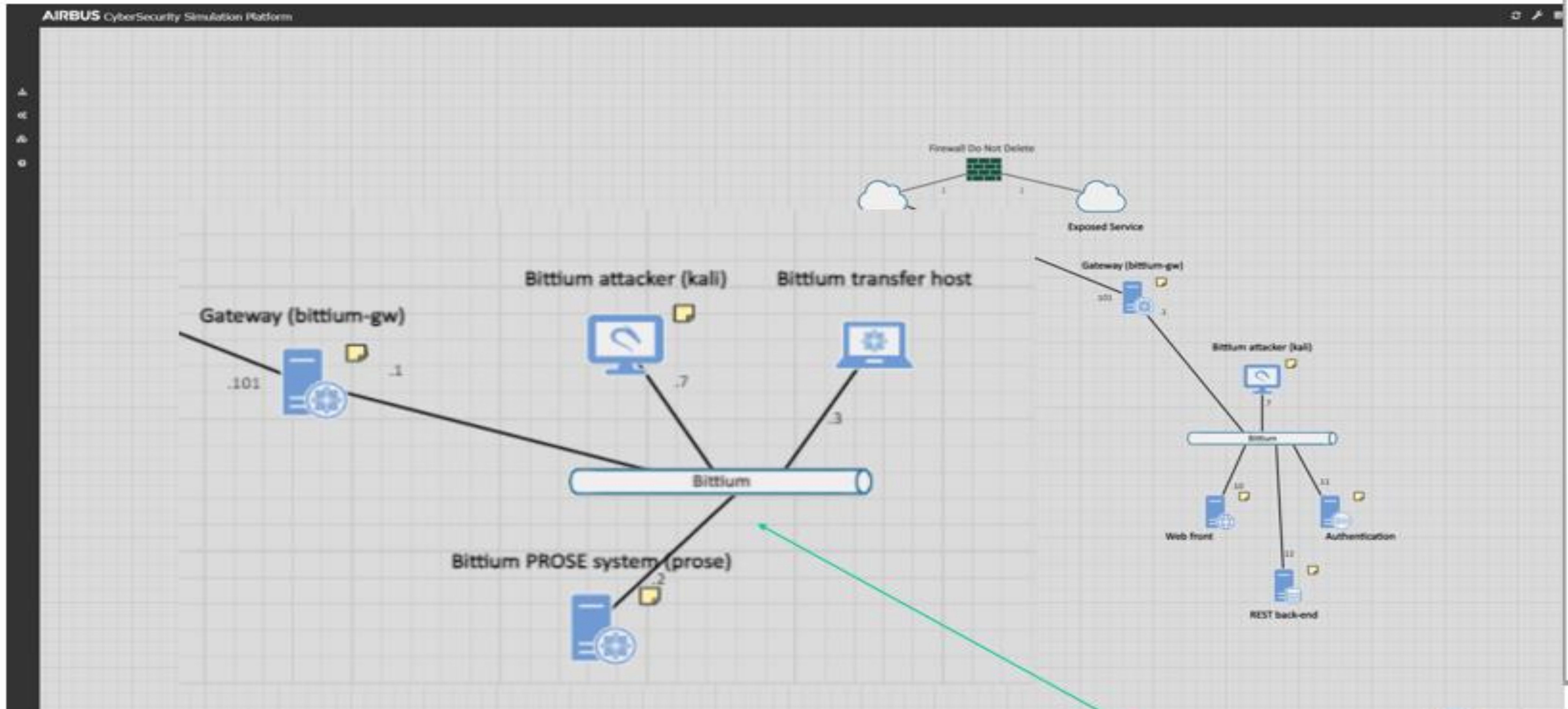
- Deployment of ***incident analysis, vulnerability management*** and applicable ***anomaly detection*** and ***SIEM functionalities***.

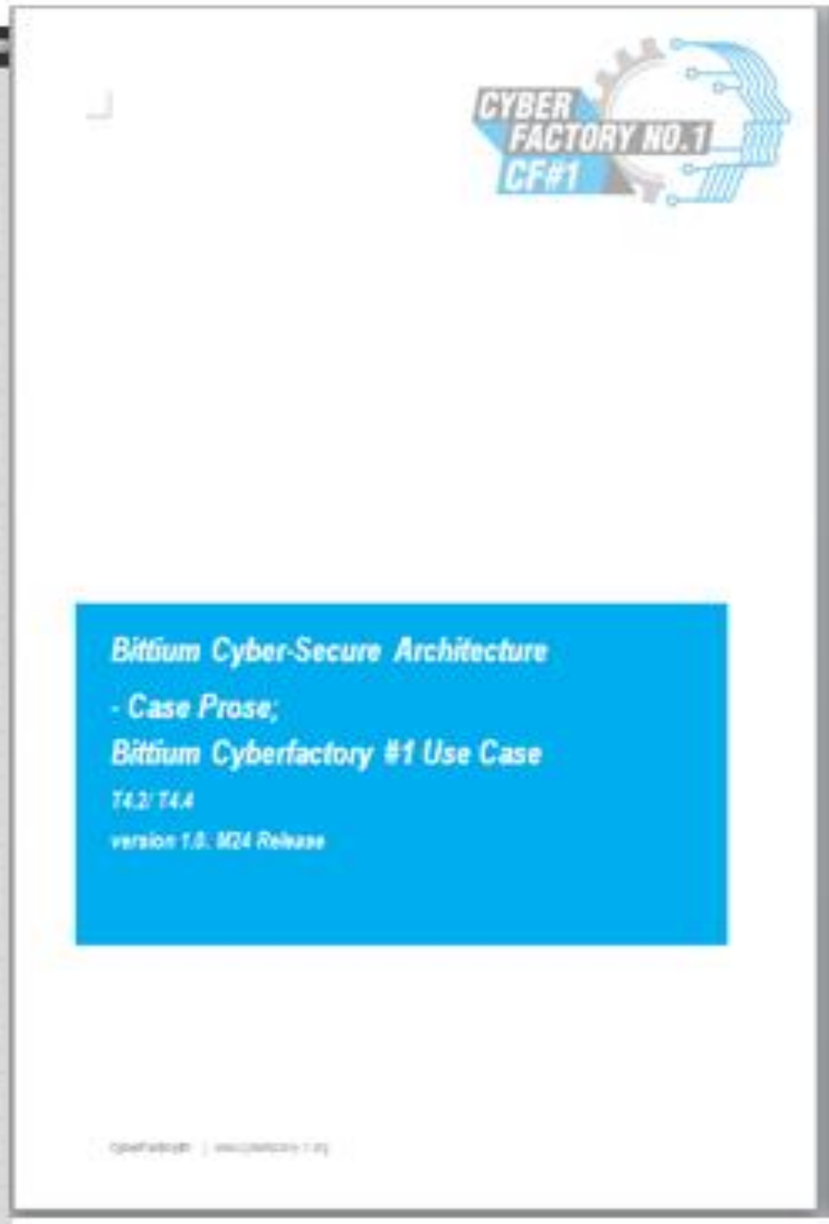
CAP54-Cyber-resilience mechanisms

- ***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.
- Creation of ***large number of cyber security simulation test cases*** e.g. MITRE Attack scenarios

Improvement of Cyber Resilience capabilities

Simulation of cyber attacks with help of Airbus CyberRange





Bittium Cyber-Secure Architecture

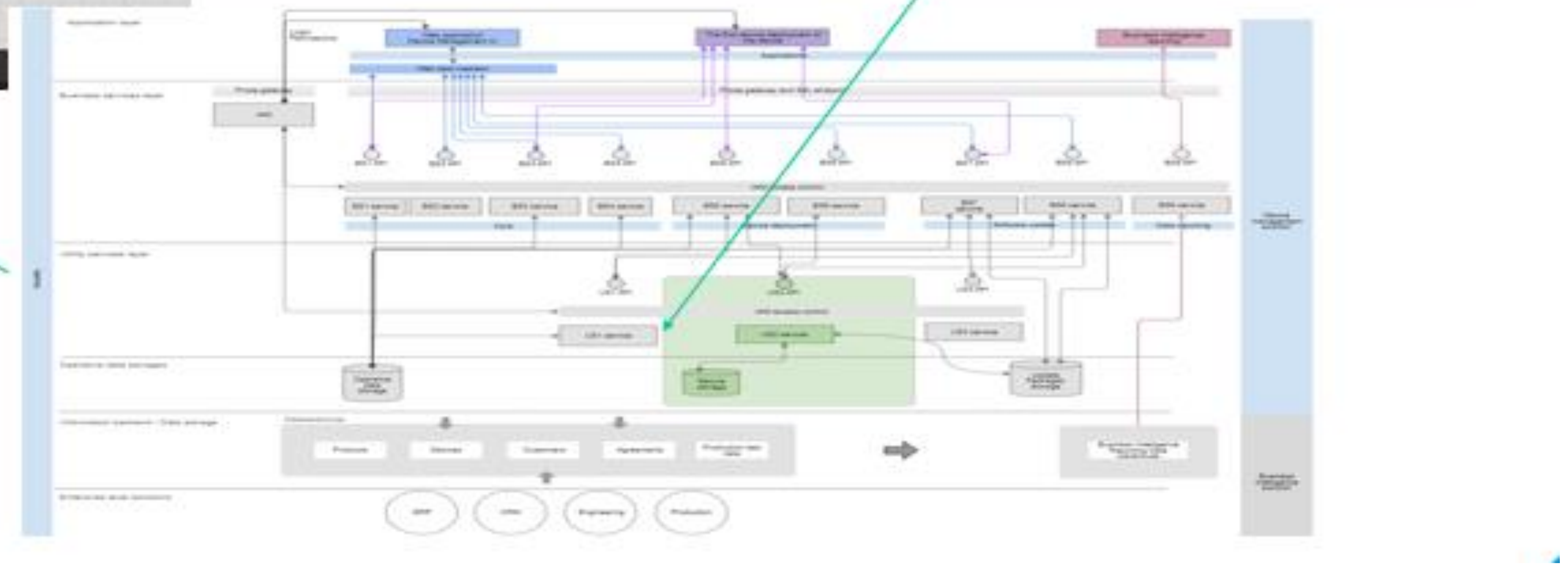
- Case Prose;

Bittium Cyberfactory #1 Use Case

T4.2/ T4.4

version 1.0, M24 Release

Table of Contents

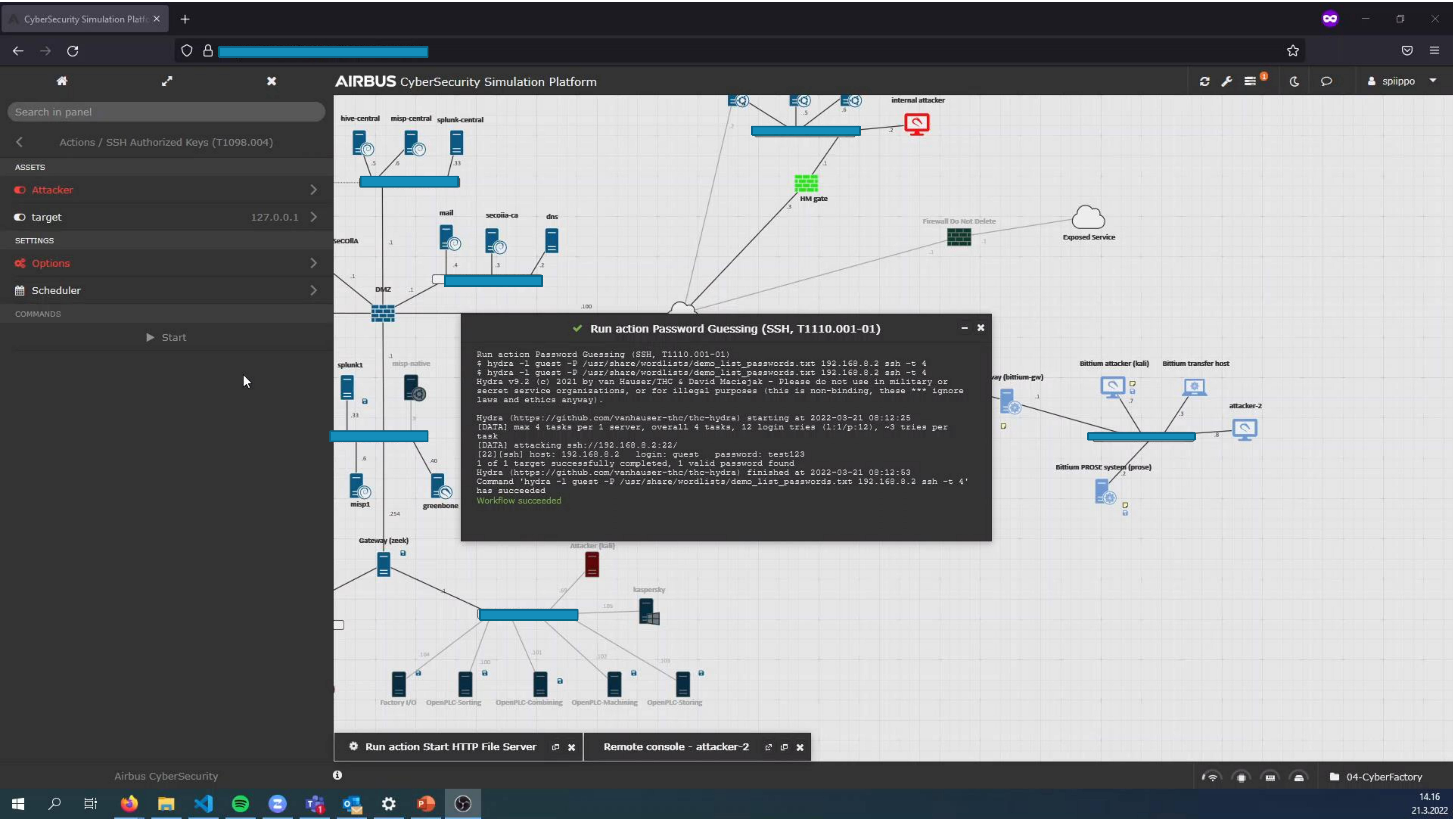


Use of e.g. MITRE & OWASP etc. as Cyber Security frameworks.

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

CyberRange Demo

Persistence



✓ Run action Password Guessing (SSH, T1110.001-01)

```
Run action Password Guessing (SSH, T1110.001-01)
$ hydra -l guest -P /usr/share/wordlists/demo_list_passwords.txt 192.168.8.2 ssh -t 4
$ hydra -l guest -P /usr/share/wordlists/demo_list_passwords.txt 192.168.8.2 ssh -t 4
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or
secret service organizations, or for illegal purposes (this is non-binding, these *** ignore
laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-03-21 08:12:25
[DATA] max 4 tasks per 1 server, overall 4 tasks, 12 login tries (l:1/p:12), ~3 tries per
task
[DATA] attacking ssh://192.168.8.2:22/
[22][ssh] host: 192.168.8.2   login: guest   password: test123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-03-21 08:12:53
Command 'hydra -l guest -P /usr/share/wordlists/demo_list_passwords.txt 192.168.8.2 ssh -t 4'
has succeeded
Workflow succeeded
```

Business Exploitation Summary 1 (2)

Business Aspects

- All the developed functionalities are **applied in all Bittium Product Deliveries**.
- Bittium PROSE is **increasingly used by Bittium customers**, who are managing e.g. their secure devices life-cycle with help of the system.
- Bittium SafeMove products will also be enhanced with some of the **recognized & learned capabilities** as outcome of Cyberfactory#1.
- The developed MITRE and OWASP cyber security **simulation, attack and testing scenarios will be enhanced** with additional cyber testing frameworks, and also **partially offered also to customers**.

Seamless connectivity

Centralized & Device management

Analytics

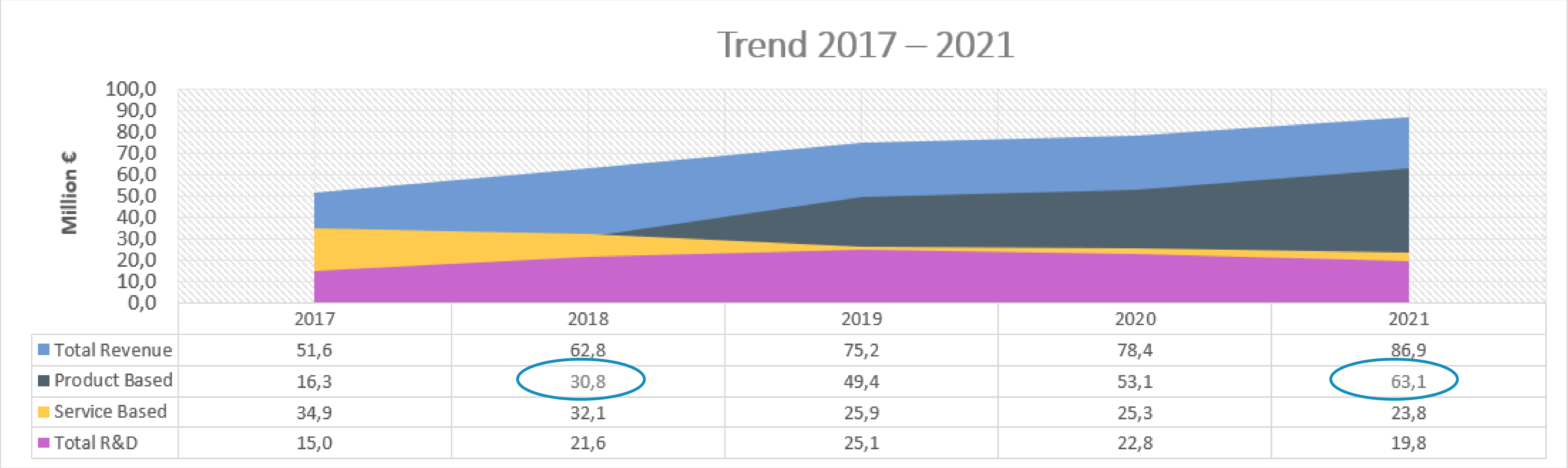
Business Exploitation Summary 2 (2)

Opportunities for further exploitation & research

- Further development of the Bittium PROSE system to be able cover real-time MES system functionalities required by ever increasing traceability requirements raised by **Regulated Operations** (like Medical or Defense & Security).
- The developed cybersecurity architecture will be further exploited also in the other Bittium systems and domains for example to cover the challenges addressed various **Cyber challenges for Medical systems**.
- Bittium is also contributing to the Horizon 2020 project **iDUNN** (https://www.idunnproject.eu/), which focuses on adding the trust ingredient to any business by making its ICT systems resilient to cyber-attacks.

Evidence (KP1 and KP2)

KPI1: Productivity rate improvement by 40% in 4 years



	2017	2018	2019	2020	2021
🟦 Total Revenue	51,6	62,8	75,2	78,4	86,9
⬛ Product Based	16,3	30,8	49,4	53,1	63,1
🟨 Service Based	34,9	32,1	25,9	25,3	23,8
🟪 Total R&D	15,0	21,6	25,1	22,8	19,8

Justifications

- **Virtual factory; amount of product delivery related personnel has grown by 15 %.**
- **Products related revenue 2 x (2018 – 2021), note delivery volume (pcs) grown even more.**

KPI2: Cyber security related analysis and testing coverage increase by 50% in 4 years

Justifications

# of New cybersecurity attack scenarios built / tested (single number)	Original value (2018)	Current Value (2022)
MITRE attack scenarios (separate) (test cases)	Not in use	*>> 270*
OWASP (test cases)	Basic	*70*
Airbus CyberRange	Not in use	*Several attack scenarios with Digital Twin*
Vulnerability Management	Not consistent	*Automated*

Cyberfactory # 1: Review of the Goals and Objectives, Bittium

KPI	Historical Reference Value	Target Reference Value	Status May 2022 (2018 vs. 2021)
- Productivity rate improvement by 40% in 4 years (1).	~ 1.0	1.4	~ 1.8
- Cyber security related analysis and testing coverage increase by 50% in 4 years (2).	1.0	1.5	>> 1.5

(1) Amount of Product Sales(M€) /# of Delivery Personnel

(2) # of Tests, including e.g. vulnerability scans and various penetration tests. Also test coverage will be measured.

Thank You!

Any Questions?

More information Jari.Partanen@bittium.com