Digital Twin for Industrial Cybersecurity Simulations

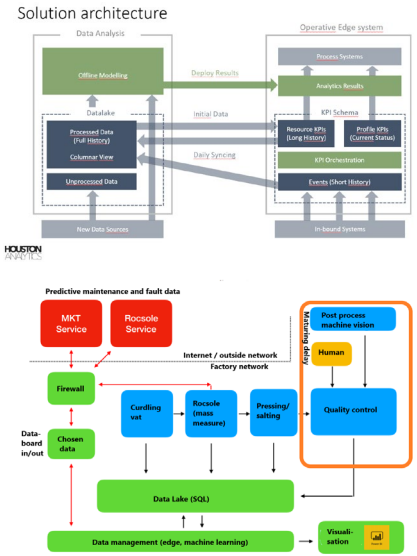
15/02/2022 VTT – beyond the obvious

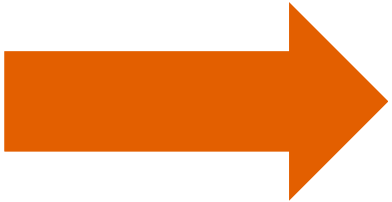
Good eyes, congrats

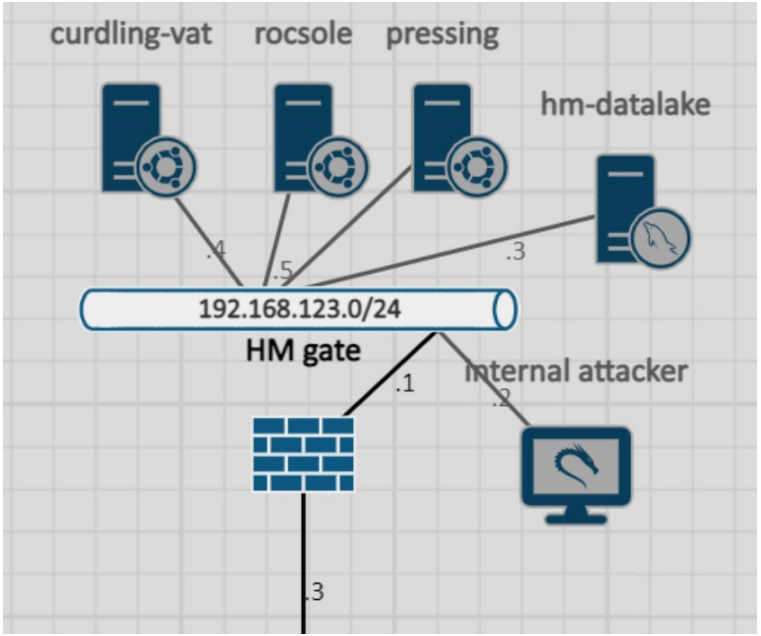
Digital twins for cybersecurity?

- What?
  - Simulation of system(s) for cyber security testing.
  - May have multiple levels of detail (e.g. Network, Protocol, Host – service/program, Host – settings) depending on purpose
    - From "full copy" to copy of address space and networked services
- How?
  - Copying virtual images, containers, virtual networks, architechtures, etc.
    - Airbus Heracles Cybersecurity Simulation Platform used in Cyber Factory#1 project
  - The original cyber object is copied to the selected platform in **suitable level of detail**.

Building the cyber digital twin in CF#1







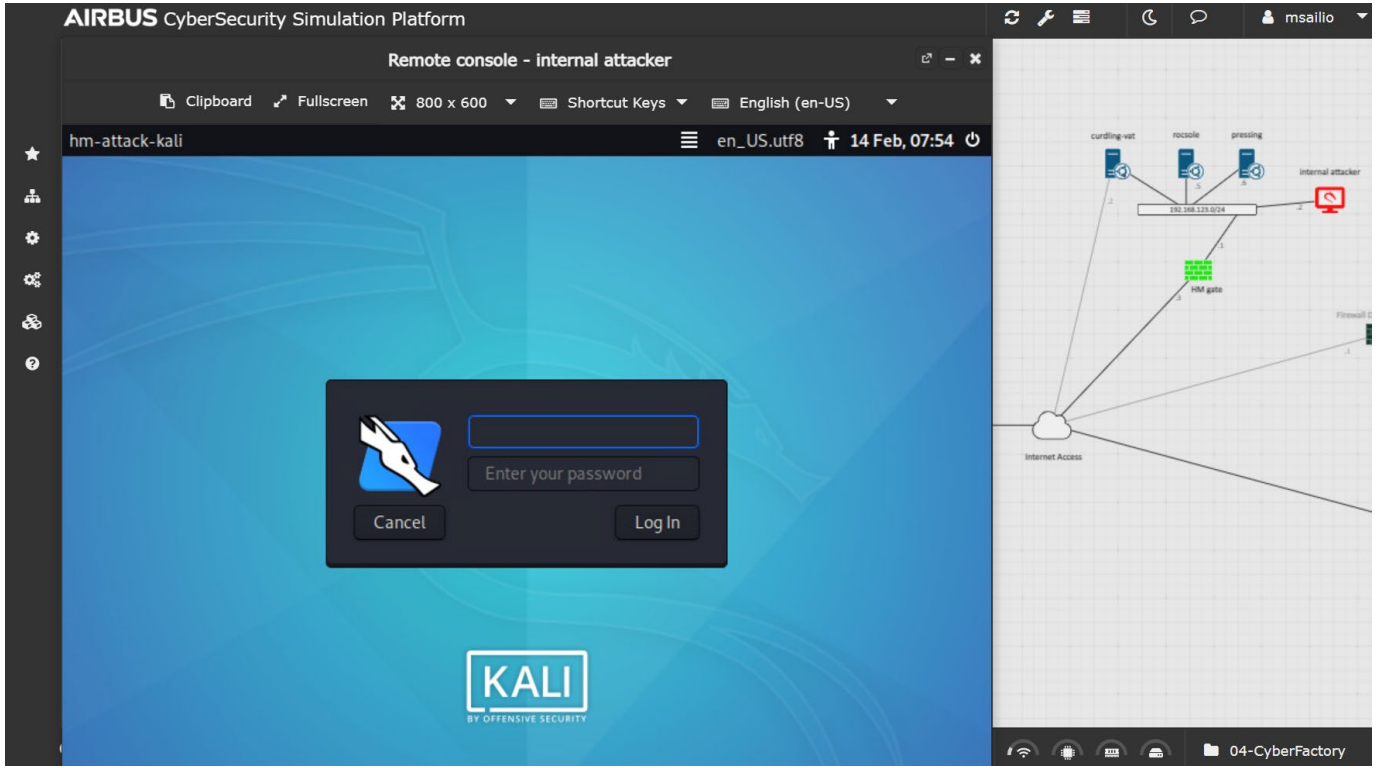
Usecase: Cyber incident affecting health and safety

- **Traceability incident affecting health and safety**
  - This misuse-case comprises industrial sabotage done by either an employee or a malicious third party with the intention of disrupting the production line and causing production delays. In case the product ends up in the market shelf, this incident - when discovered - results into the need of pulling an entire product batch off the market, which is costly, but causes also critical harm to the company brand.
- In the scenario, a cyber incident disables or modifies the sterilization phase of the cheese robot process. The resulting cheese would be potentially dangerous for humans.
- If the change was detected in normal quality control phase, the whole batch, and perhaps multiple batches would be lost

Collaboration

- Infrastructure on Airbus Cyber Simulation Platform
- Digital Twin based on cheese maker system architechture (High Metal)
- Traffic Monitoring (VTT, Rugged Tooling)
- Machine learning decision making (VTT) from Siem input

Platform


AIRBUS CyberSecurity Simulation Platform
msailio
Remote console - internal attacker
Clipboard
Fullscreen
800 x 600
Shortcut Keys
English (en-US)
hm-attack-kali
en_US.utf8
14 Feb, 07:54
Enter your password
Cancel
Log In
KALI
BY OFFENSIVE SECURITY
curdling-vat
rocsole
pressing
internal attacker
HM gate
Internet Access
04-CyberFactory

Attack simulation

- Attacker has gained access to network, in simulation we use "Internal attacker" in network graph
- Attacker sees network broadcast traffic used by S7 protocol, and starts going through the systems to detect vulnerable systems
- In our scenario, the administrator of the system has not changed the default username/password combination, and the attacker uses this to gain access to the system
  - Metasploit module: auxillary/scanner/ssh/ssh_login
- Rocsole system gives remote access to the attacker, and after a short while, the attacker changes the sterilization temperature settings to about 35°C

Simulation – Detection - Recovery

- Detection focuses on abnormal network activity, as remote access enabled on the roscoe control system.
  - Abnormal general network activity, using Zeek (VTT)
  - Abnormal connections (Rugged Tooling)
- SIEM system combines events from different tools
  - Logs from failed Rocsole log-in attempts
- Cybersecurity incident is now detected, and will be resolved (out of scope)
  - Attack simulation helps identify important logs and data sources for incident management
  - Identify weaknesses and priorities for improvement of original system
  - Likely future research using AI/ML techniques
- After the attack, the system is reverted back
  - Roscole image reverted to certified clean state from backup
  - Attacker image reverted to original state

Conclusions

- What did we do?
  - Generated Cyber Digital Twin based on High Metal novel cheese platform
  - Simulated a hacking attack against the cyber digital twin, to detect attacks able to compromise the quality and safety of the process result (the cheese)
  - Combined tools from different project partners to enable increased accuracy and reliability
  - Identified requirements for optimal resource cyber digital twins for future applications

Questions?

- Now or email to **mirko.sailio@vtt.fi**

Thanks!