Secure Remote Access in OT

with

Privileged Access Management

ot • security by WALLIX

PAM4OT

Securing Industrial Performance

Industrial Cyber Security

10 oktober 2023 | Congrescentrum 1931, den Bosch

ACTEMIUM

ot • security by WALLIX

Remote Access in OT

Some challenges we face

Remote Access saves a lot of time and money

- Maintenance & Support technicians
- Vendors
- System integrators
- Equipment manufacturers

But… for security reasons, we don't like

- Weak authentication mechanisms like 1-FA
- External remote users connecting at any time without prior notice
- Backdoors like unmanaged/ wireless phone-home systems
- Remote users performing actions behind the scenes
- Share (admin) passwords
- Every remote user can reach everything with any protocol
- Remote users making unauthorised lateral movements (RDP and free…)

PAM4OT can help!

Authentication
suppliers

Control
Sessions

Traceability
Activities

Secure
Passwords & Behaviors

Hardening
User rights

Who
Multi-Factor Authentication

Why
- Approval workflow
- Protocols rupture

When
- Session traceability
- Session recording

What
- Password Security
- User Behavior Analysis

How
- Principle of Least Privilege
- Full Endpoint Hardening

MFA / SSO

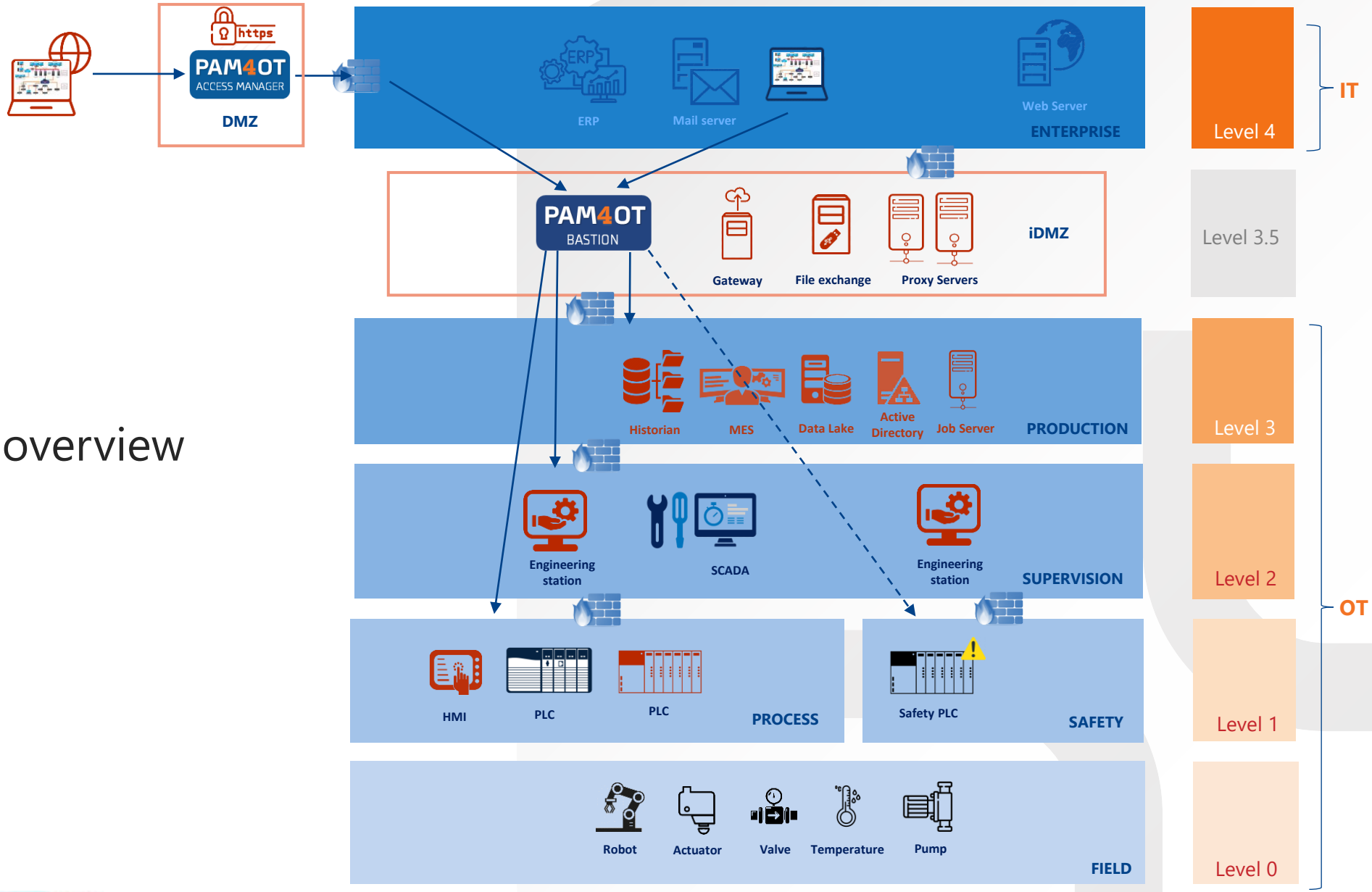
Control, Visibility, Traceability

Endpoint security

Let's see how PAM4OT mitigate our risks!

- ☑ Single point of entrance, managed accounts
- ! Weak authentication mechanisms like 1-FA
- ! External remote users connecting at any time without prior notice
- ! Remote users performing actions behind the scenes
- ! Share (admin) passwords
- ! Any remote user can reach everything
- ! Remote users making unauthorised lateral movements (RDP and free…)

Architecture overview (example)

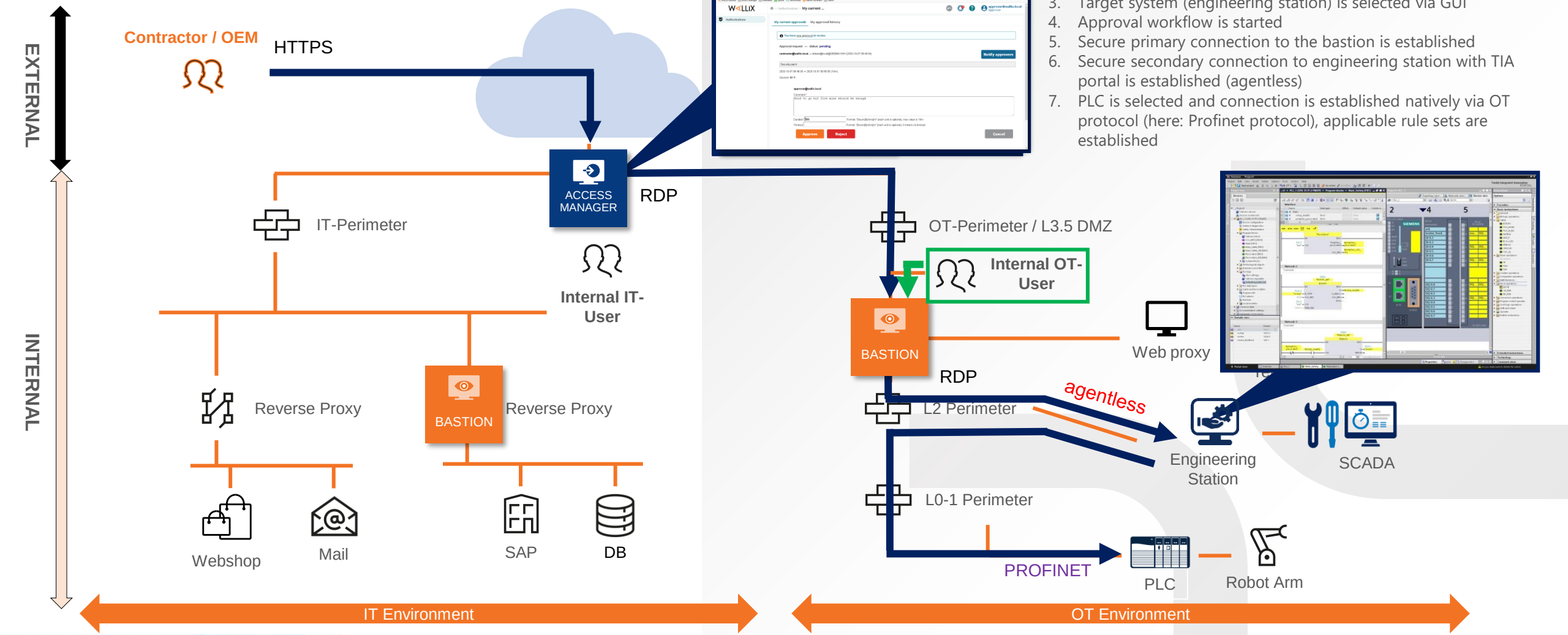


Let's see how PAM4OT mitigate our risks!

- [x] Single point of entrance, managed accounts
- [x] Apply two-factor authentication
- [x] External remote users (where needed) require approval prior to connect
- [x] Remote sessions are recorded – bookmarked actions can quickly be reviewed
- [x] Hide & rotate (admin) passwords in vault, central user management
- [x] A remote user can connect permitted targets using preconfigured protocols
- [x] Enforce restrictions on authorised targets, blocking illegal commands, lateral movement

USE CASE 1: Access of external users (standard workstation) to engineering station

1. Connection via browser is established
2. User is authenticated
3. Target system (engineering station) is selected via GUI
4. Approval workflow is started
5. Secure primary connection to the bastion is established
6. Secure secondary connection to engineering station with TIA portal is established (agentless)
7. PLC is selected and connection is established natively via OT protocol (here: Profinet protocol), applicable rule sets are established



Securing Industrial Performance

Industrial Cyber Security

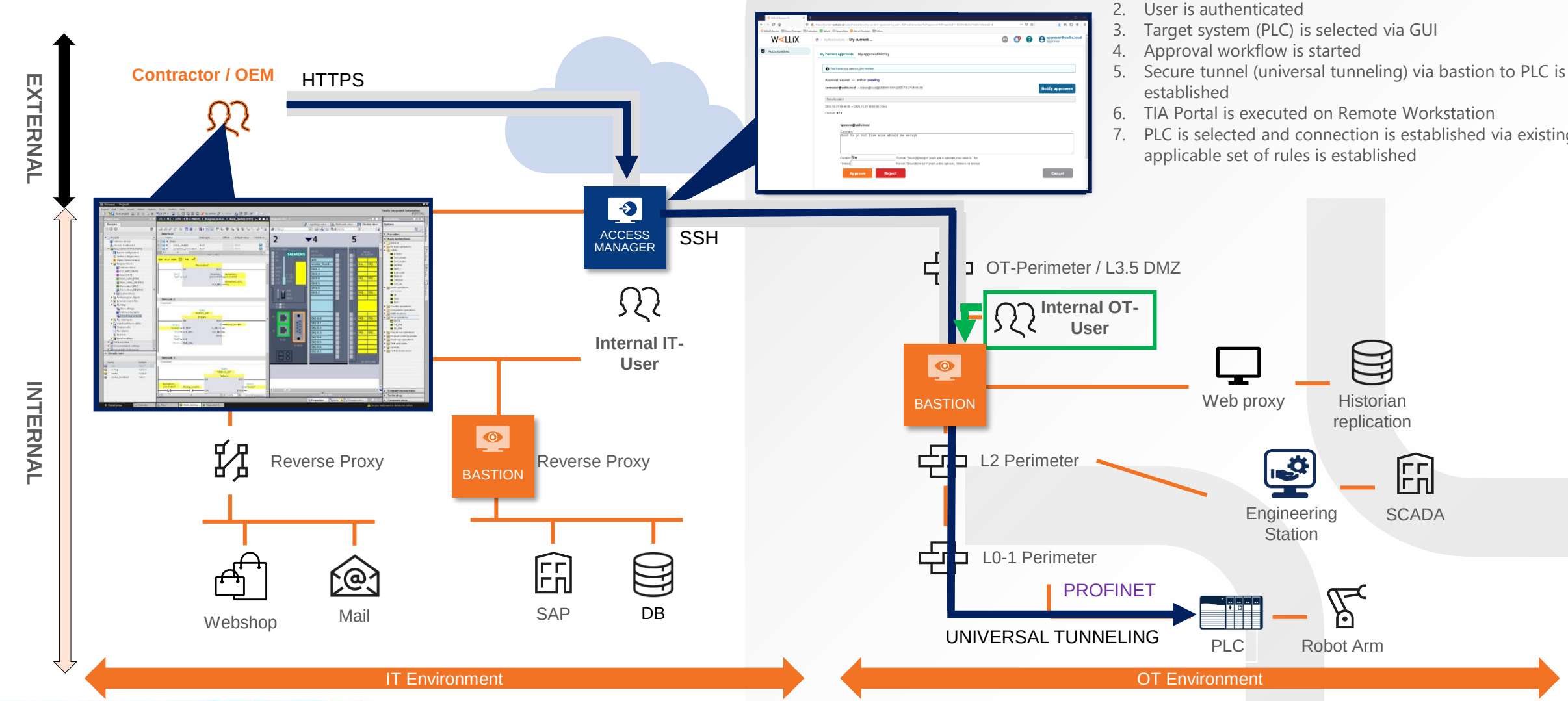
10 oktober 2023 | Congrescentrum 1931, den Bosch

ACTEMIUM

ot security by WALLIX

USE CASE 2: Access of external users (remote workstation) to OT component

1. Connection via browser is established
2. User is authenticated
3. Target system (PLC) is selected via GUI
4. Approval workflow is started
5. Secure tunnel (universal tunneling) via bastion to PLC is established
6. TIA Portal is executed on Remote Workstation
7. PLC is selected and connection is established via existing tunnel, applicable set of rules is established



Questions

Contact details

Gert Ippel

Industrial Cybersecurity Consultant

Actemium

gert.ippel@actemium.com

+31 640 486 566

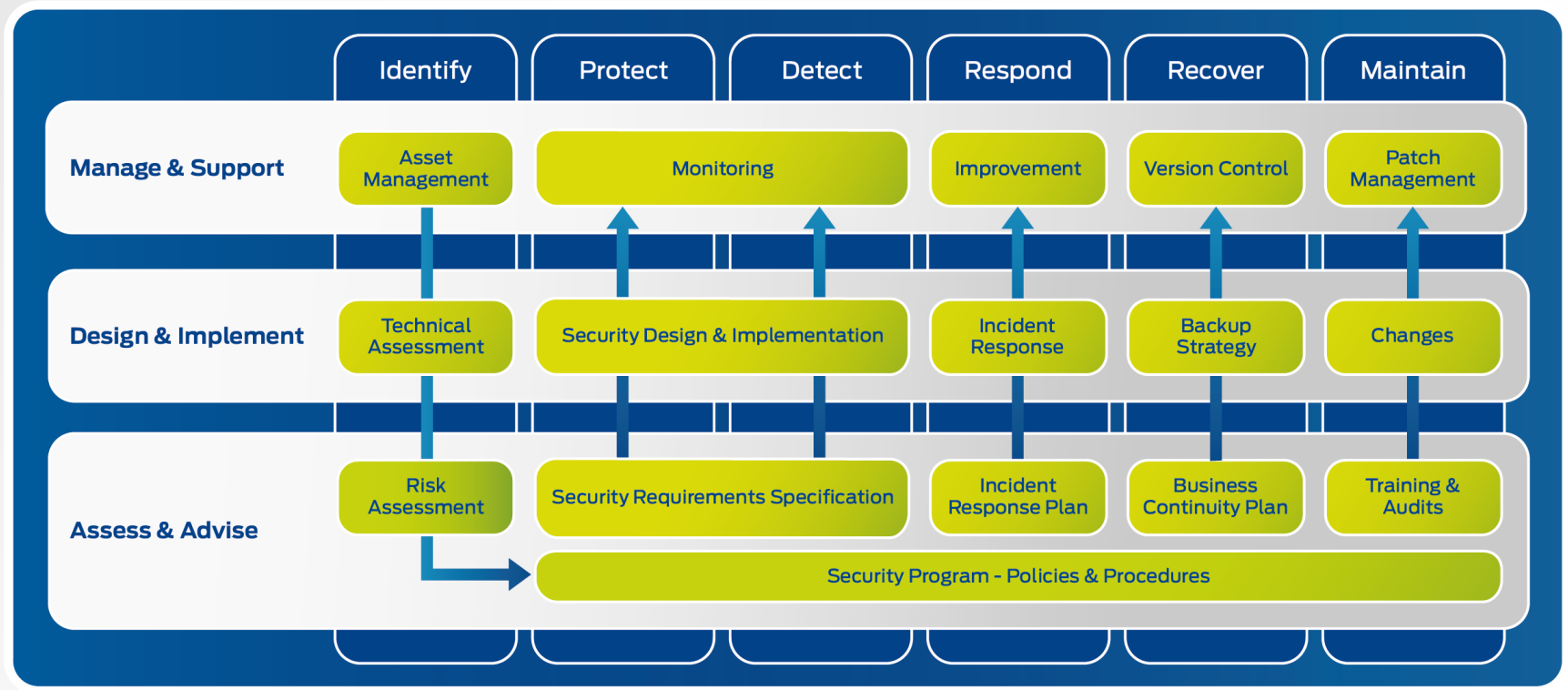
Vincent VANBIERVLIET

PreSales Manager

Wallix

vvanbiervliet@wallix.com

+32 479 214 710



Actemium Cybersecurity Services. A risk-based approach