Securing OT Assets



Davy Cavens
OT Security Architect

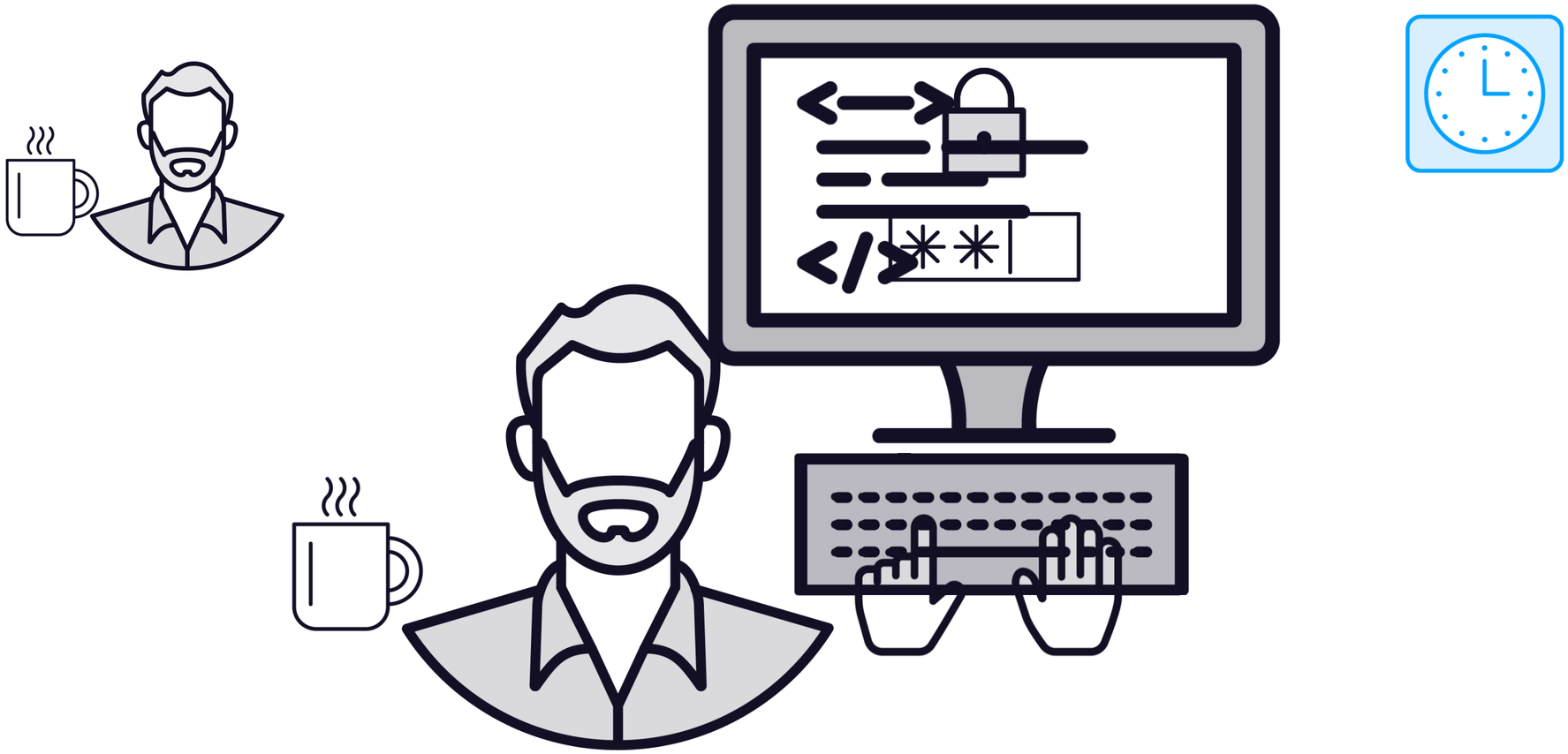
linkedin.com/in/davycavens/

Basic IT Policies





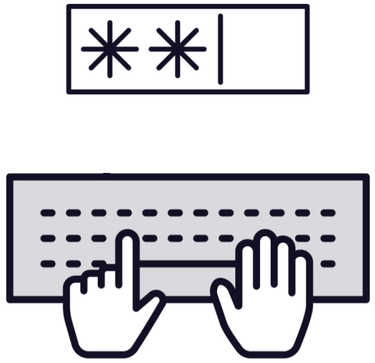
Basic IT Policies



Basic IT Policies



Idle Timeout



Password Policy



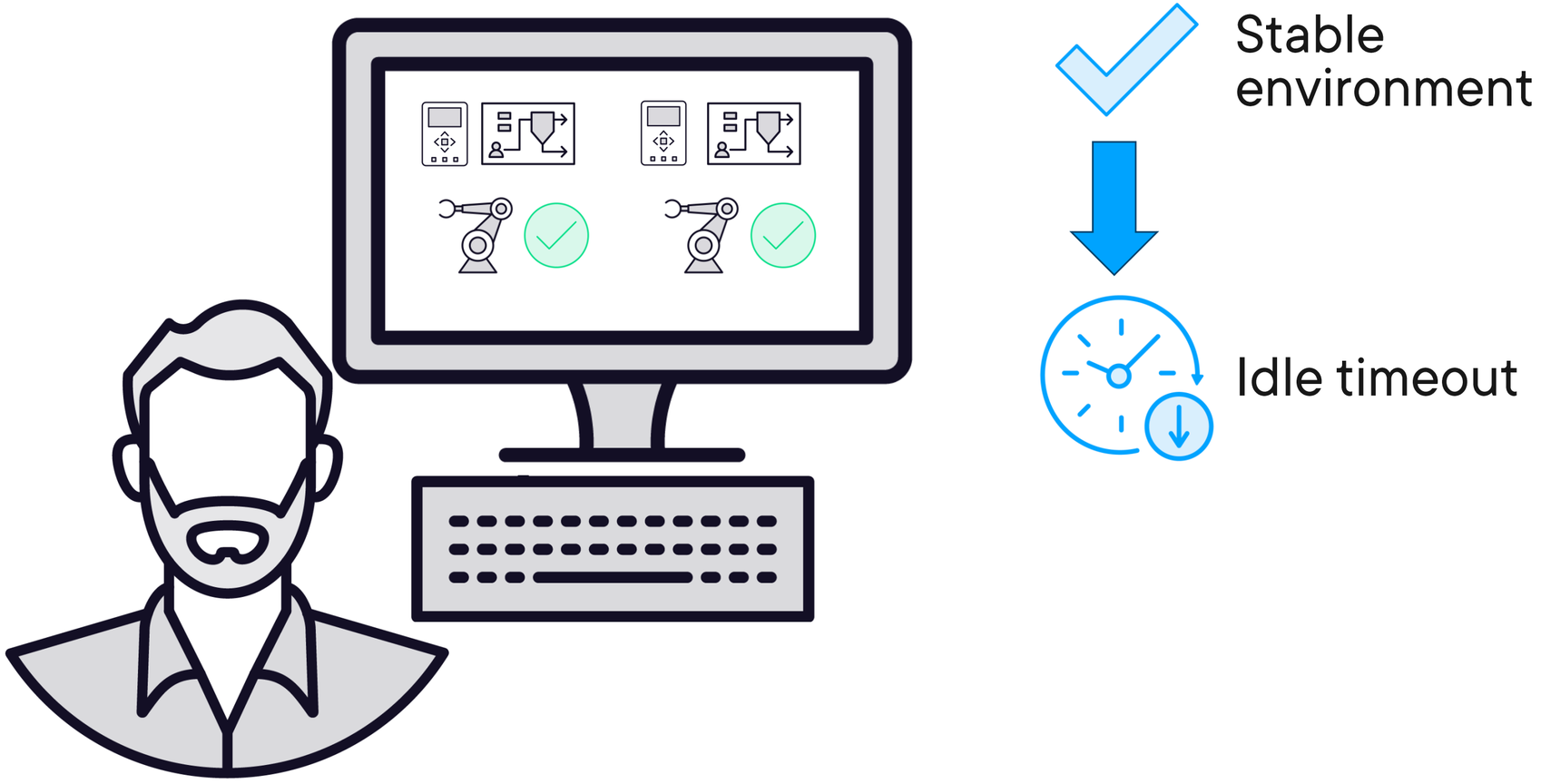
Lockout Policy

OT Operator

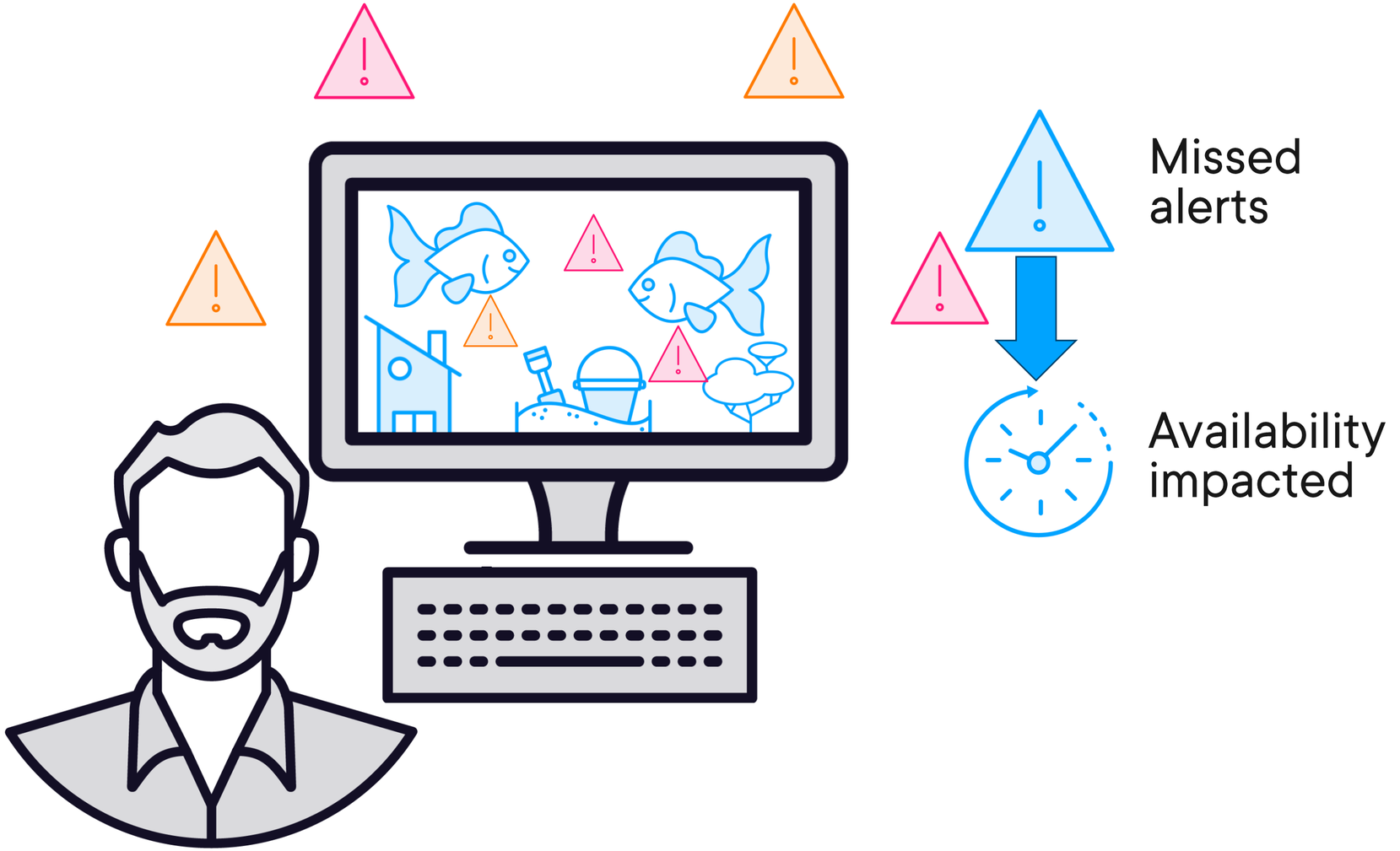


24/7

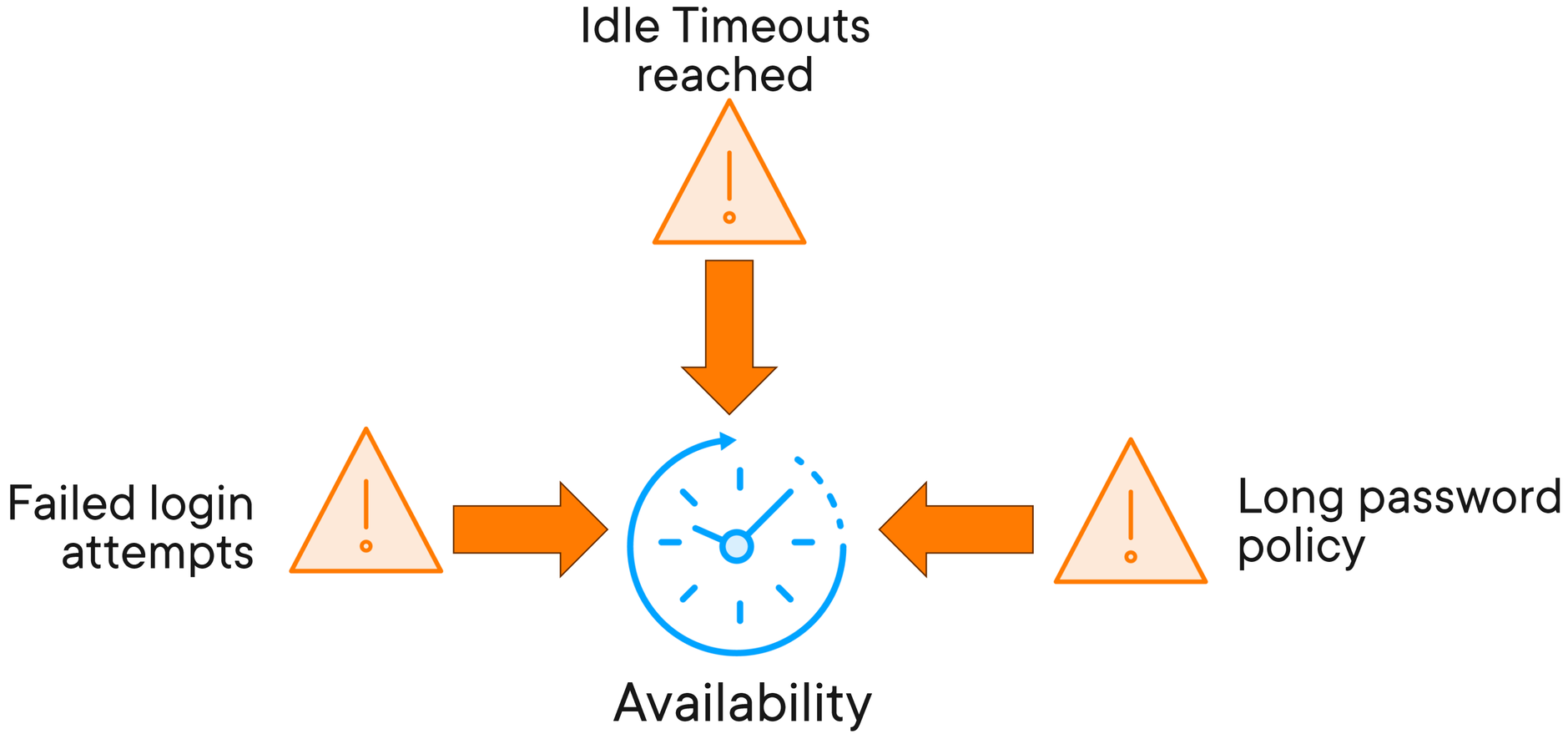
OT Operator



OT Operator



Considerations

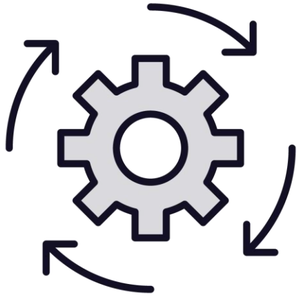


Striking a Balance



Security





Usability

Mitigations

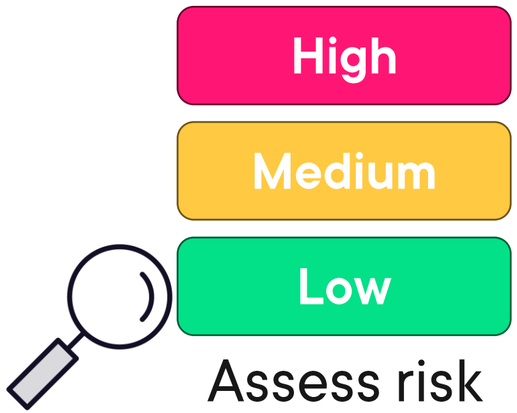


Longer
idle timeout

Transparent
lockscreen

Badge or
Smart Card

Methodology



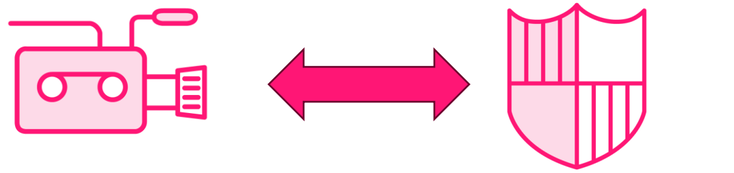
Assess risk



Define mitigations



Involve stakeholders

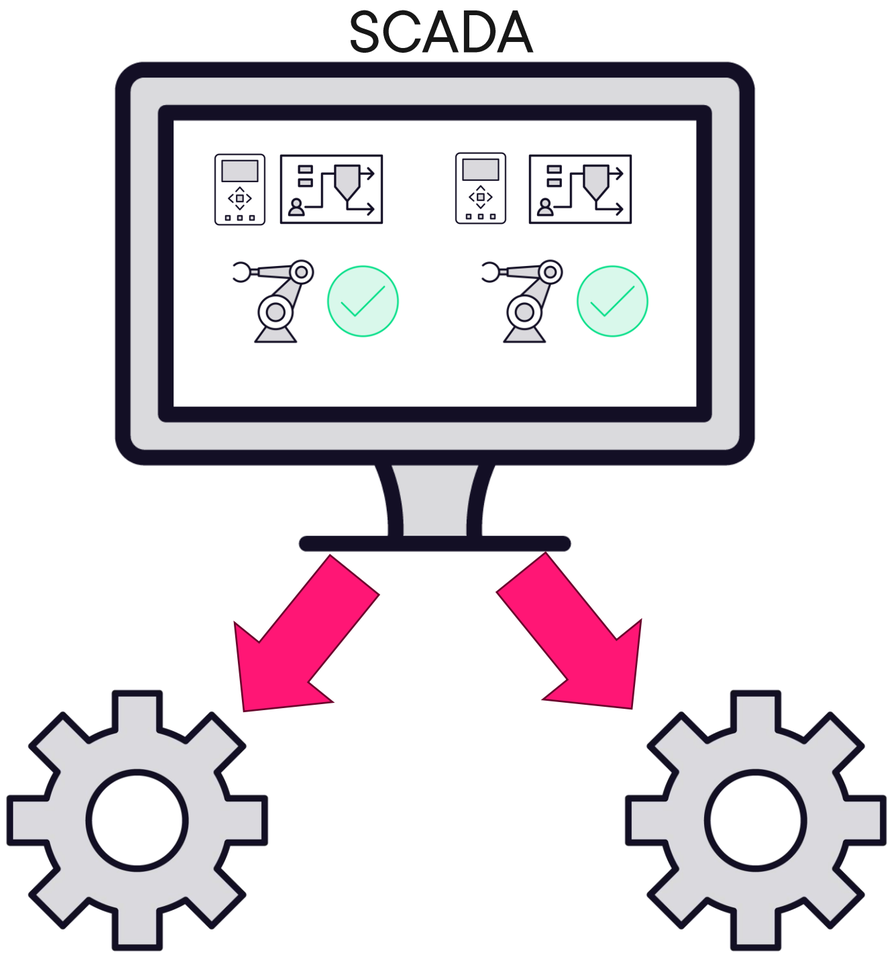


Physical controls

Cybersecurity controls

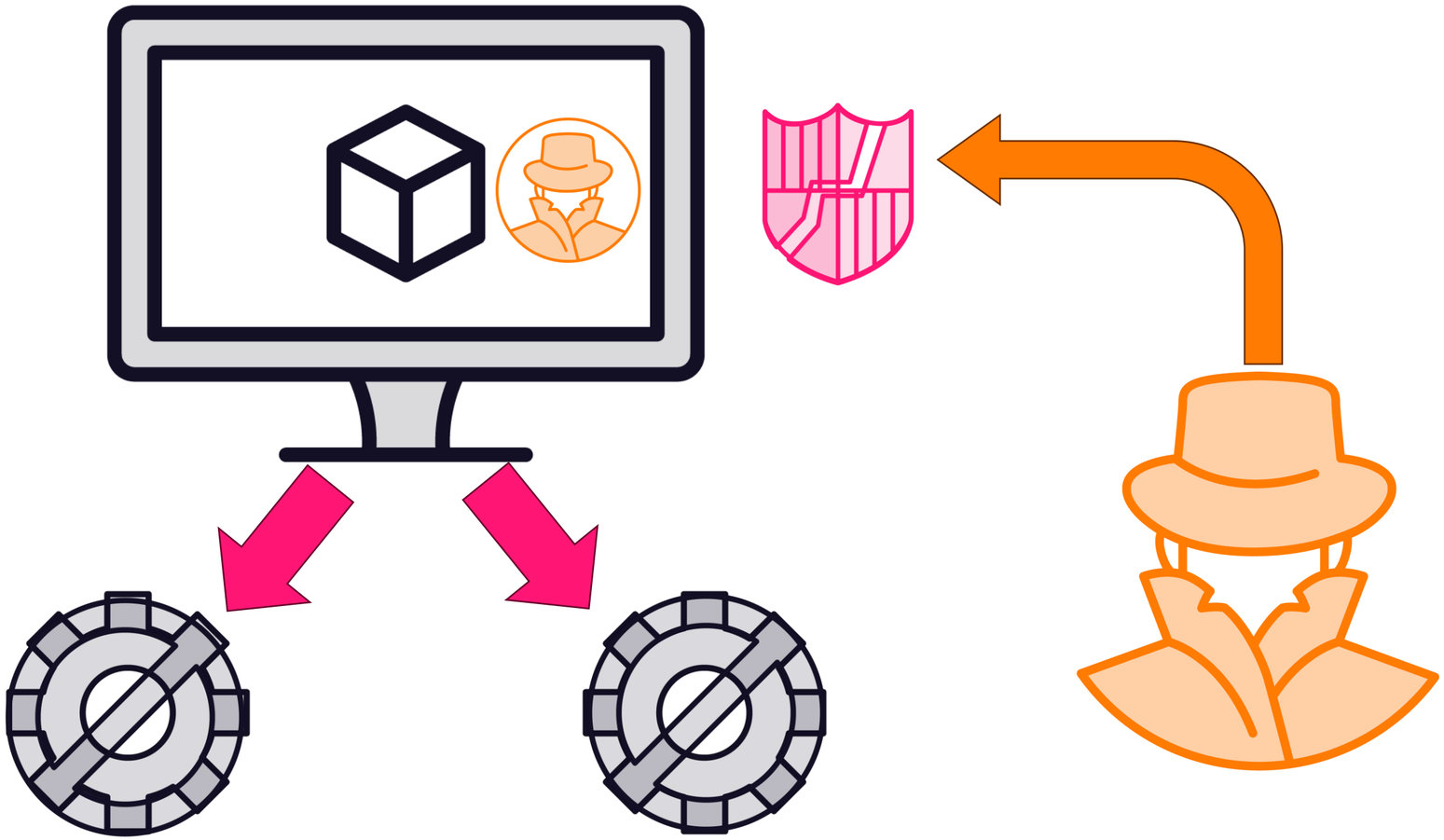
Supply Chain Control

Common Scenario



Common Scenario

Log4J



Responsibilities of the Product Supplier



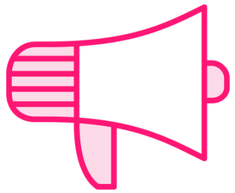
Supplier



Providing patches



Providing mitigations

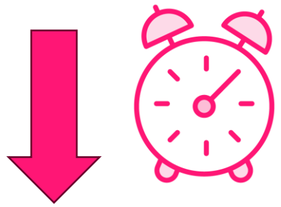


Reporting vulnerabilities

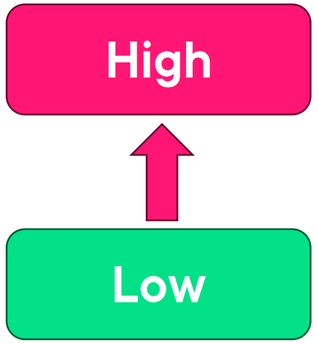
Responsibilities of the Product Supplier



Supplier

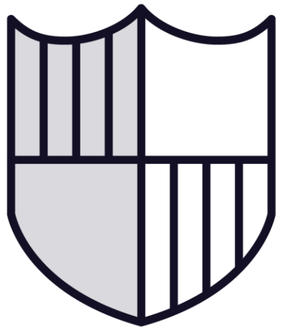


Response time

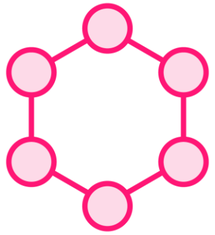


Risk increase

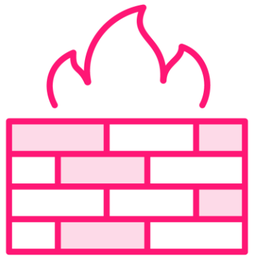
Mitigation Techniques



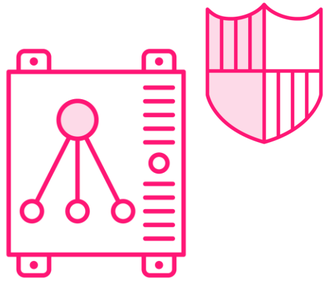
Technical controls



Segmentation



Firewalling



WAF

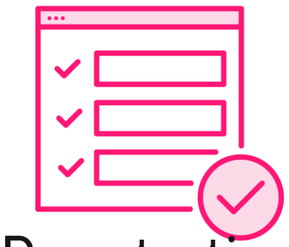
Mitigation Techniques



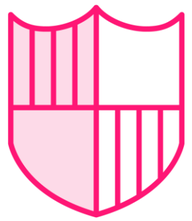
Technical controls



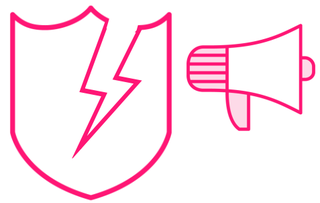
Vendor assessment



Penetration testing



Security assessment



Reporting procedures

Mitigation Techniques



Technical controls



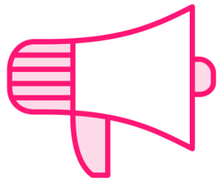
Vendor assessment



Contractual agreement



SBOM

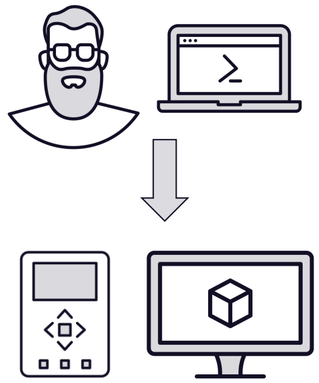


Vulnerability reporting

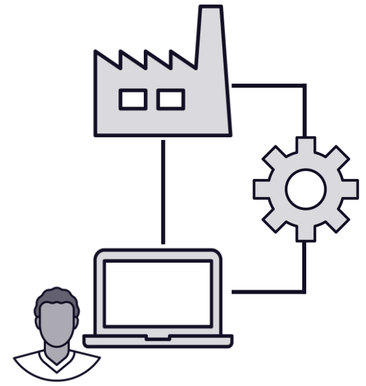


Incident reporting

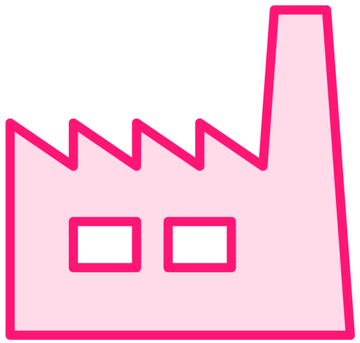
The Digital Supply Chain



Suppliers



System integrators



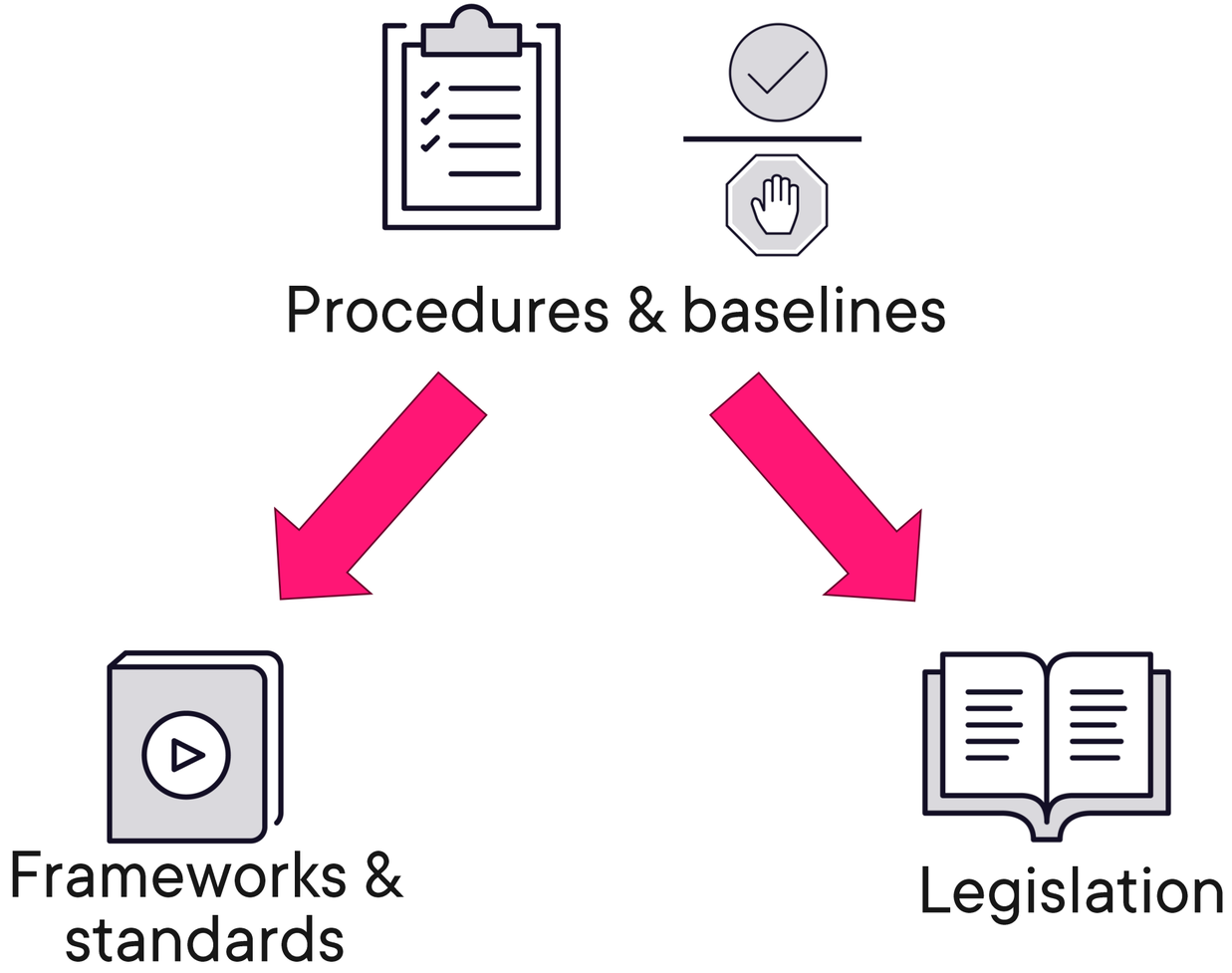


ICT service management

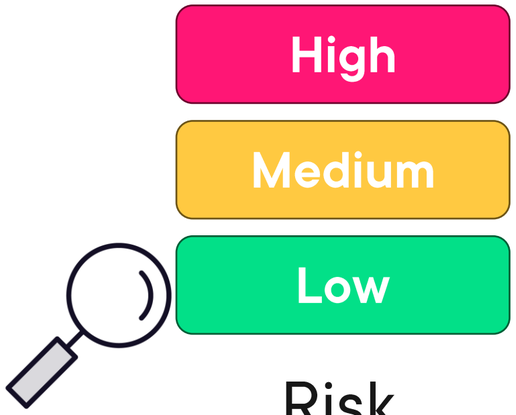


Digital service providers

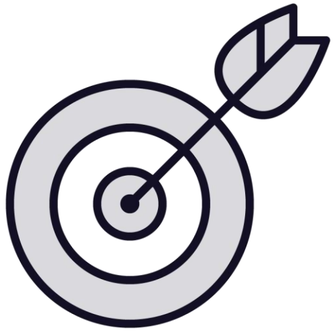
Getting Started



Methodology



Risk assessment



Security Level Target



Set security requirements

Frameworks and Standards



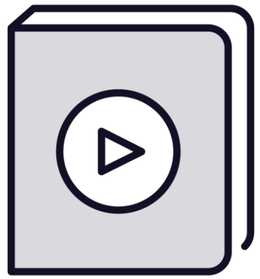
IEC 62443

3-3
System requirements

4-2
Component requirements

4-1
Vulnerability handling

Additional Frameworks



NIST SP 800-161

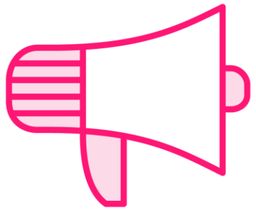


ISO 27000 series

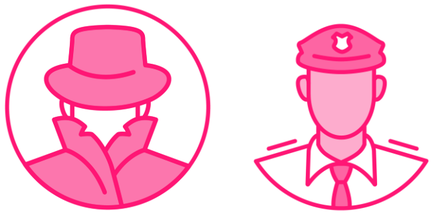
Legislation



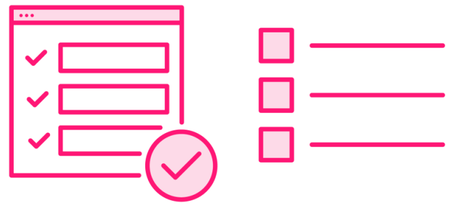
Cyber Resilience Act



Vulnerability reporting



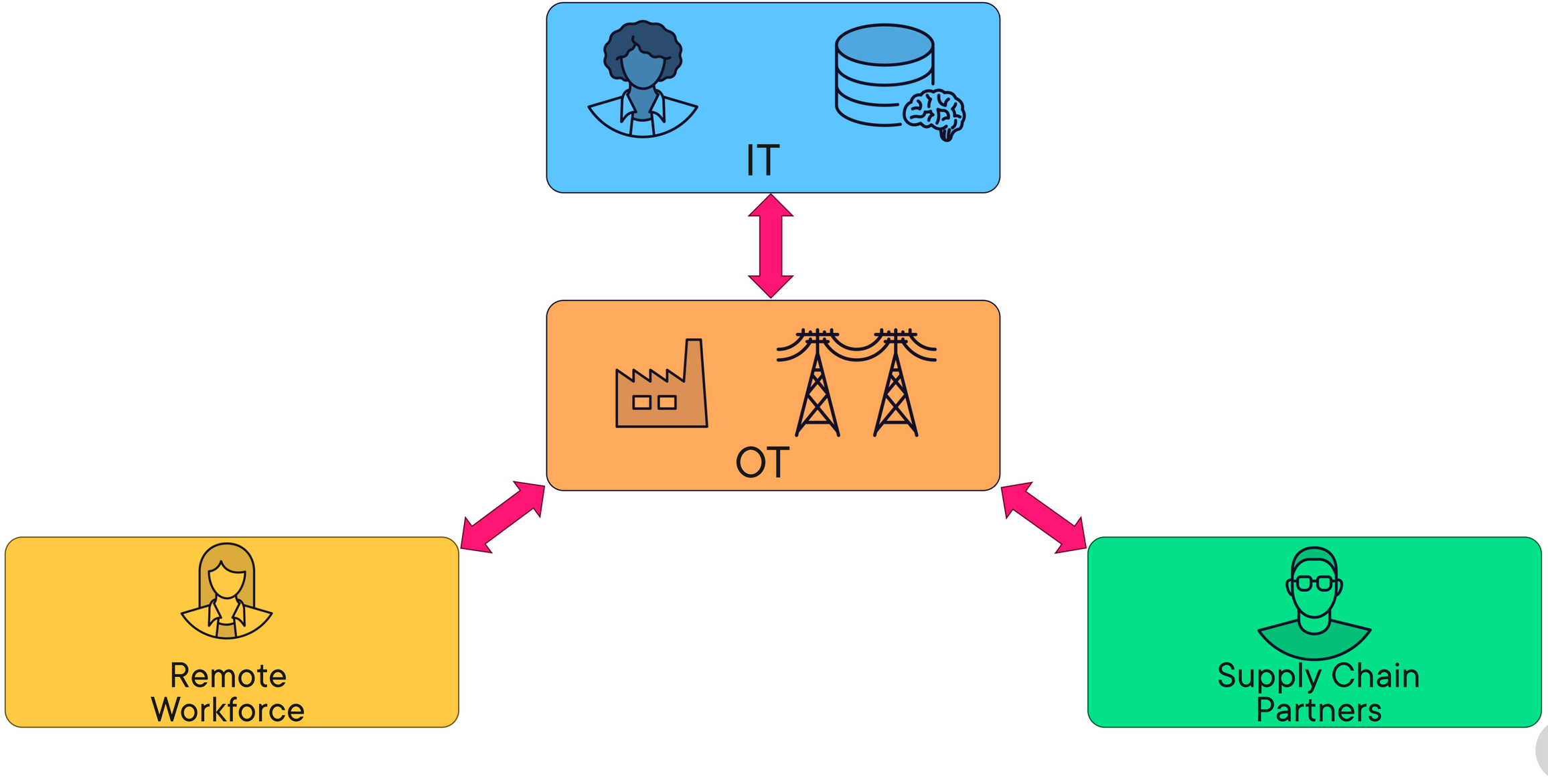
Incident reporting



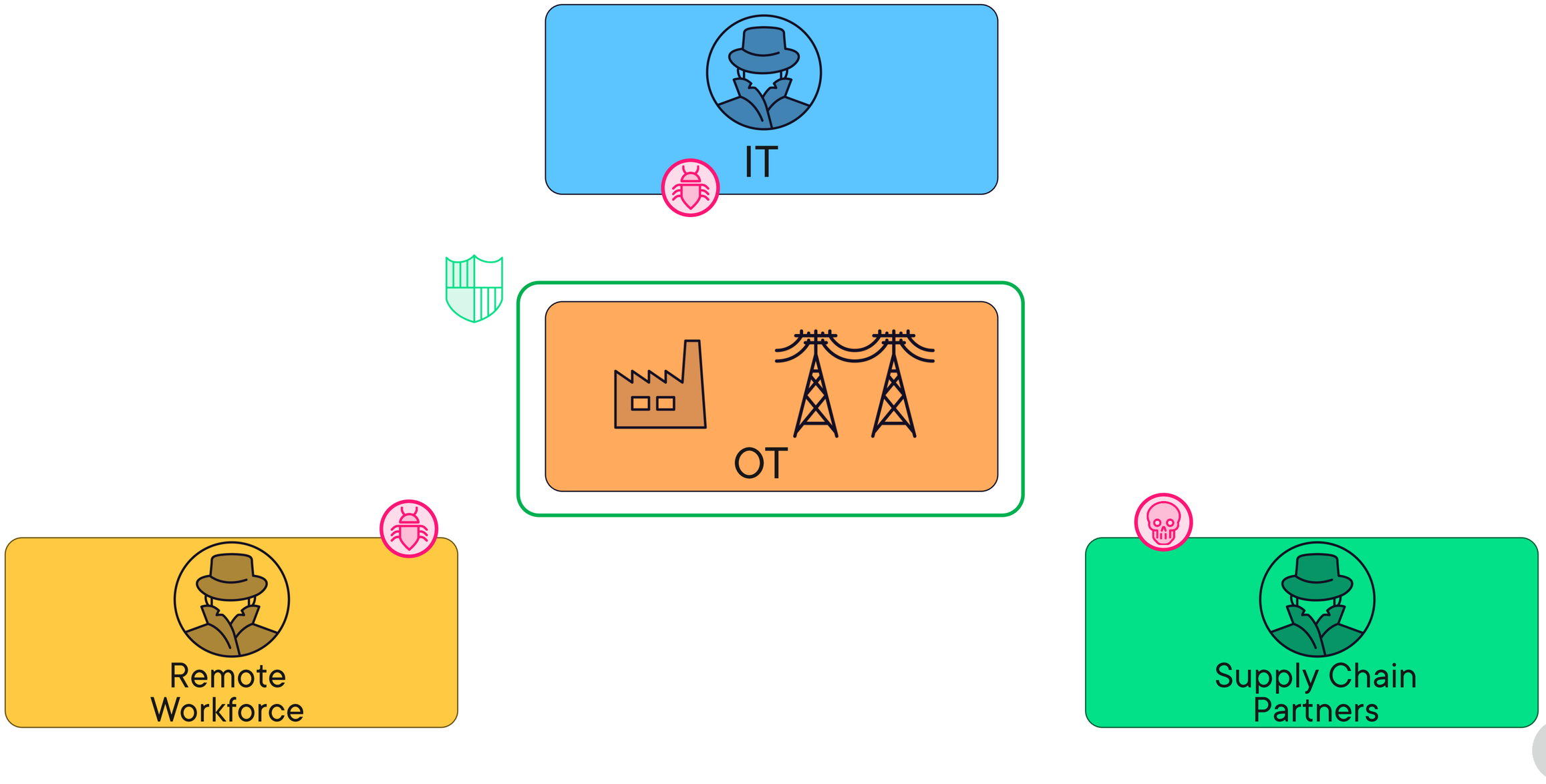
SBOM & Penetration testing

Incident Response Examples

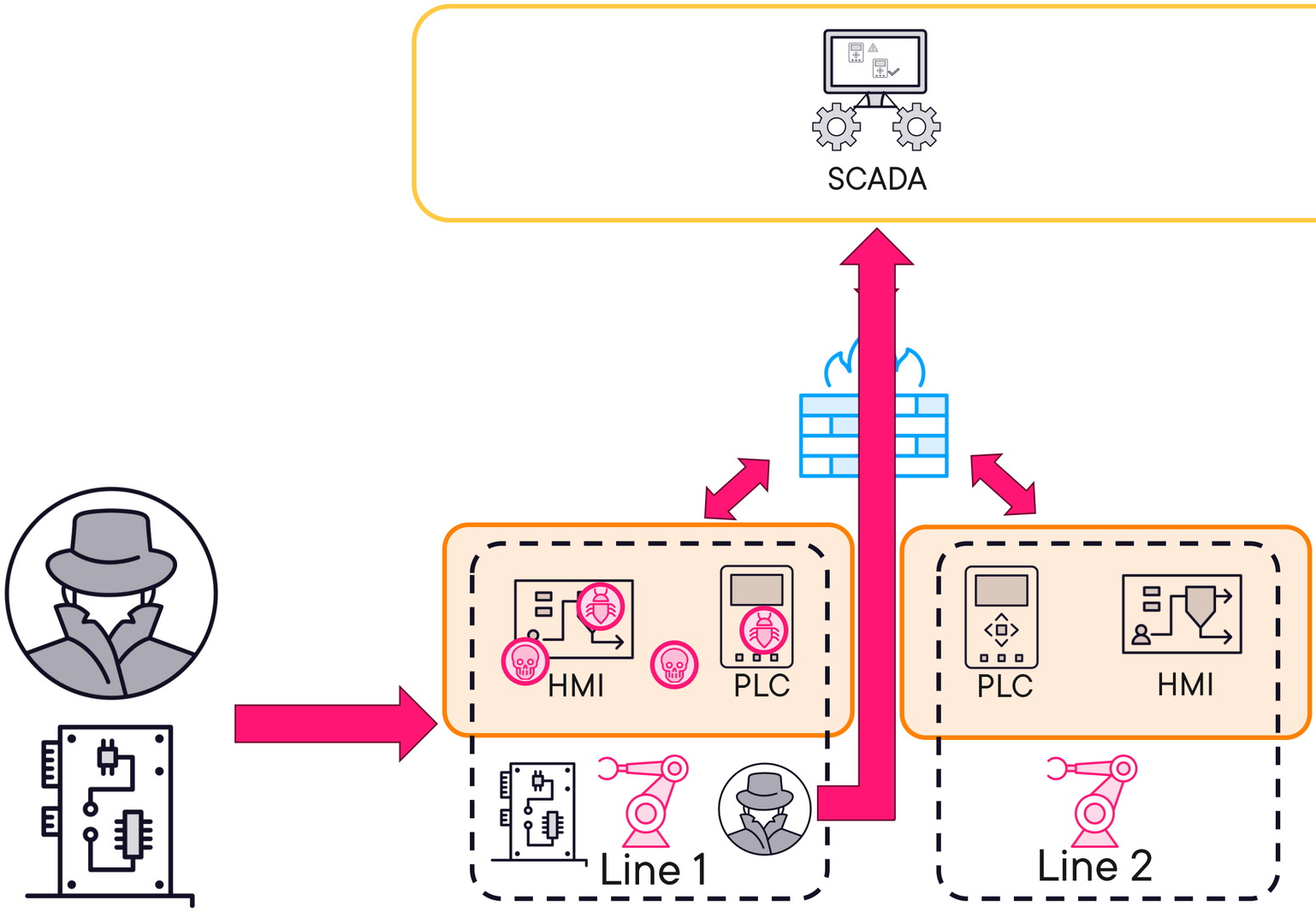
OT Bridges



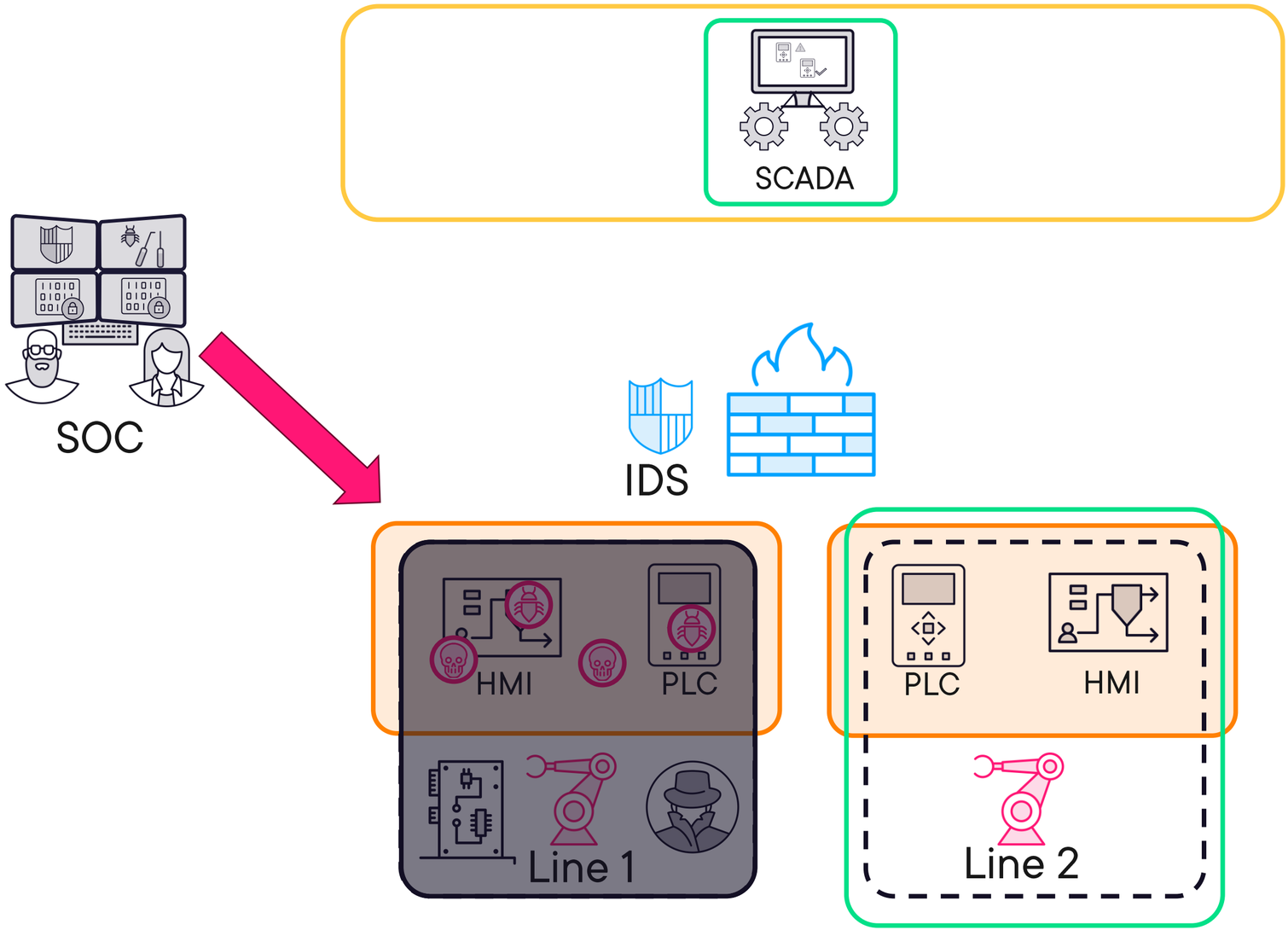
Island Mode



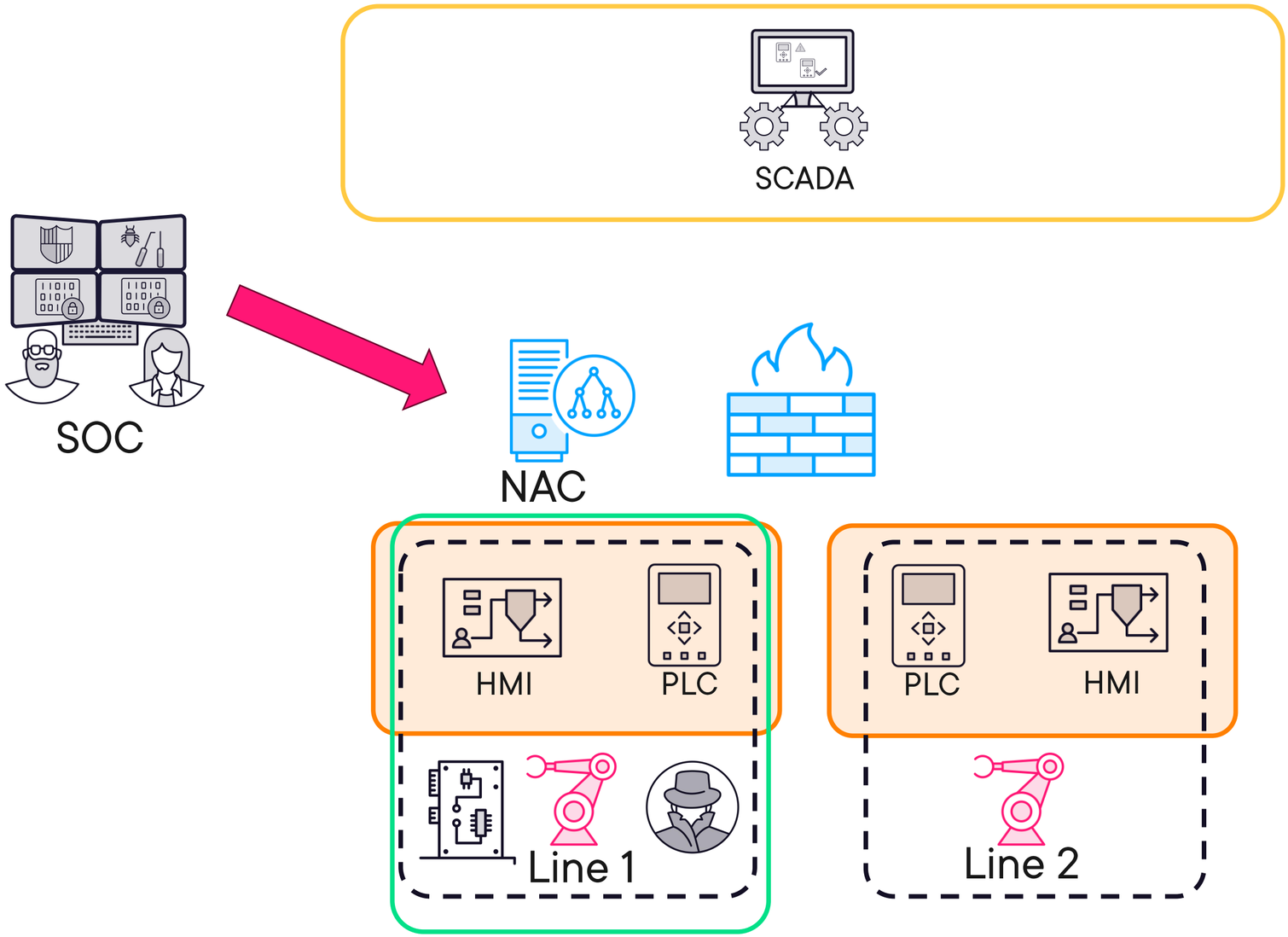
Island Mode



Island Mode



Island Mode



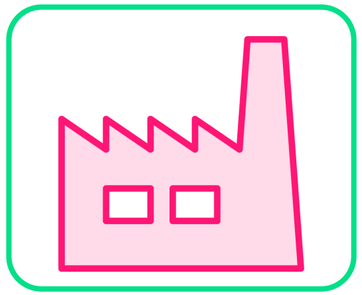
Tips and Tricks



Document procedures



Communication templates

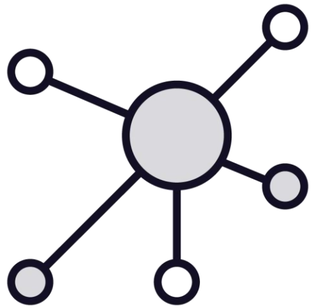


Isolation procedures

Tips and Tricks



Document procedures

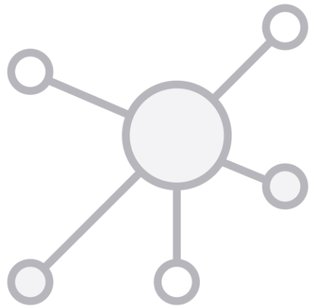


Map dependencies

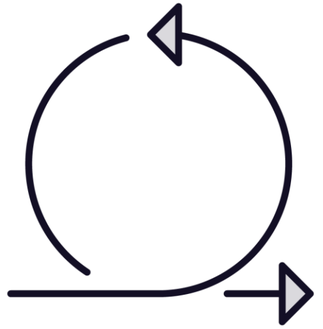
Tips and Tricks



Document procedures



Map dependencies



Practice makes perfect

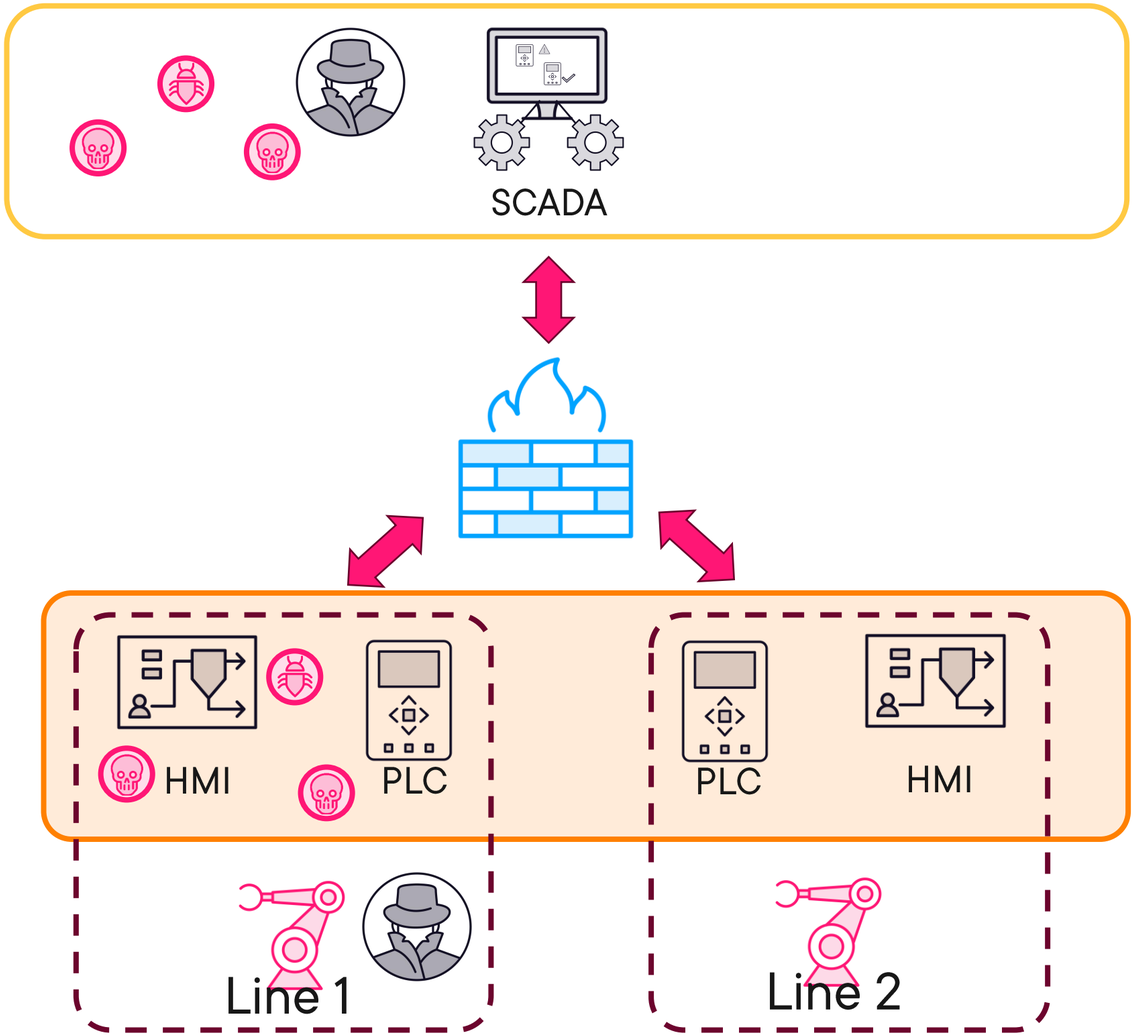


Tabletop exercises

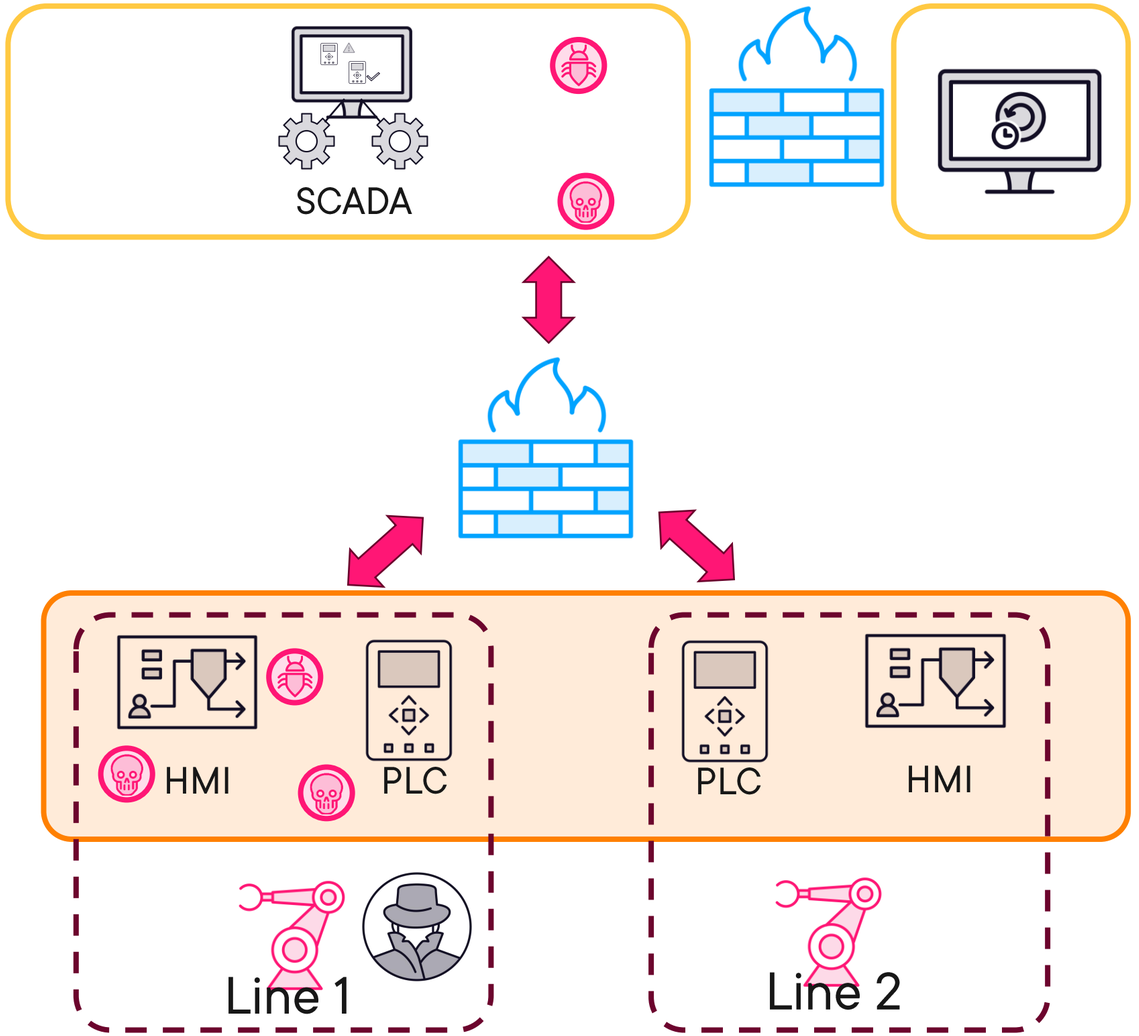


Dry-run procedures

Backup Isolation



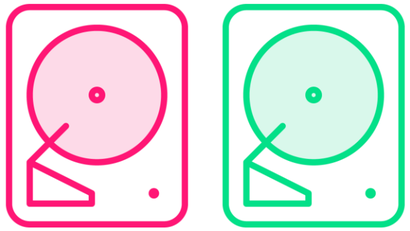
Backup Isolation



3 – 2 – 1 Strategy



3
Backups

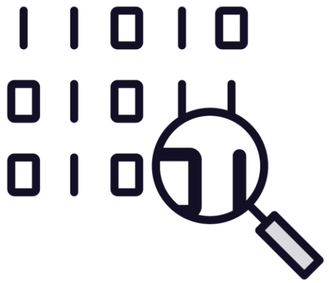


2
Storage media

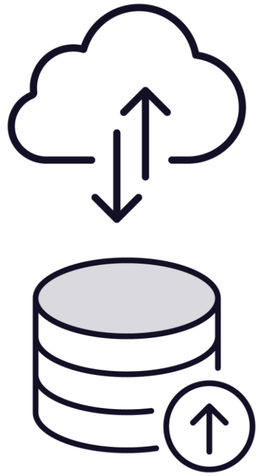


1
Off-site location

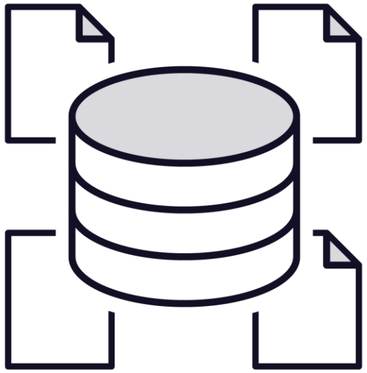
Key Considerations



Restore Data



Store off-site



Test restore procedure

Summary

Finding a balance

Supply chain control

Backups