

OT Cyber-Physical Security Assessment

Observations and Recommended Mitigations or Improvements

Outline

- Purpose of Assessment
- Company background
- Observations & Recommended Mitigations or Improvements

Purpose of Assessment

- Assess XYZ because etc

Company Background

- Customer background
- Assessment Team background

Observations & Recommended Mitigations or Improvements

- OT Security Program, Risk Management & Governance
- Asset Inventory
- Configuration Management, Change Control, Management of Change
- Network and System Architecture
- Access Control (physical, logical, role based, least privilege etc)
- Third Party Risk and Supply Chain Risk Management
- Insider Threat Program
- RF & Wireless Security
- Portable, Mobile & Peripheral Devices (e.g. laptop, tablets, USB etc)
- Systems Security Engineering
- Business Continuity, DRP, COOP
- Incident Response and Recovery (e.g. OT SOC, threat hunting etc)
- Security Assessments & Penetration Testing
- Safety (e.g. HSE, EHS, HAZOP, LOPA, PHA, cyberPHA, SIS etc)
- OT specific cyber training, certifications and awareness

OT Security Program, Risk Management & Governance

Observation: describe findings (both negative and positive), background, history etc in a few sentence paragraph narrative

Recommendations:

- List up to 3-5 recommended mitigations or improvements or continuations of something already moving in right direction as relevant or possible to fit on the slide.

Asset Inventory

Observation: describe findings (both negative and positive), background, history etc in a few sentence paragraph narrative

Recommendations:

- List up to 3-5 recommended mitigations or improvements or continuations of something already moving in right direction as relevant or possible to fit on the slide.

Configuration Management, Change Control, Management of Change

Observation: describe findings (both negative and positive), background, history etc in a few sentence paragraph narrative

Recommendations:

- List up to 3-5 recommended mitigations or improvements or continuations of something already moving in right direction as relevant or possible to fit on the slide.

Network and System Architecture

Observation: describe findings (both negative and positive), background, history etc in a few sentence paragraph narrative

Recommendations:

- List up to 3-5 recommended mitigations or improvements or continuations of something already moving in right direction as relevant or possible to fit on the slide.

Access Control (physical, logical, role based, least privilege etc)

Observation: describe findings (both negative and positive), background, history etc in a few sentence paragraph narrative

Recommendations:

- List up to 3-5 recommended mitigations or improvements or continuations of something already moving in right direction as relevant or possible to fit on the slide.

Third Party Risk and Supply Chain Risk Management

Observation: describe findings (both negative and positive), background, history etc in a few sentence paragraph narrative

Recommendations:

- List up to 3-5 recommended mitigations or improvements or continuations of something already moving in right direction as relevant or possible to fit on the slide.

Insider Threat Program

Observation: describe findings (both negative and positive), background, history etc in a few sentence paragraph narrative

Recommendations:

- List up to 3-5 recommended mitigations or improvements or continuations of something already moving in right direction as relevant or possible to fit on the slide.

RF & Wireless Security

Observation: describe findings (both negative and positive), background, history etc in a few sentence paragraph narrative

Recommendations:

- List up to 3-5 recommended mitigations or improvements or continuations of something already moving in right direction as relevant or possible to fit on the slide.

Portable, Mobile & Peripheral Devices (e.g. laptop, tablets, USB etc)

Observation: describe findings (both negative and positive), background, history etc in a few sentence paragraph narrative

Recommendations:

- List up to 3-5 recommended mitigations or improvements or continuations of something already moving in right direction as relevant or possible to fit on the slide.

Systems Security Engineering

Observation: describe findings (both negative and positive), background, history etc in a few sentence paragraph narrative

Recommendations:

- List up to 3-5 recommended mitigations or improvements or continuations of something already moving in right direction as relevant or possible to fit on the slide.

Business Continuity, DRP, COOP

Observation: describe findings (both negative and positive), background, history etc in a few sentence paragraph narrative

Recommendations:

- List up to 3-5 recommended mitigations or improvements or continuations of something already moving in right direction as relevant or possible to fit on the slide.

Incident Response and Recovery (e.g. OT SOC, threat hunting etc)

Observation: describe findings (both negative and positive), background, history etc in a few sentence paragraph narrative

Recommendations:

- List up to 3-5 recommended mitigations or improvements or continuations of something already moving in right direction as relevant or possible to fit on the slide.

Security Assessments & Penetration Testing

Observation: describe findings (both negative and positive), background, history etc in a few sentence paragraph narrative

Recommendations:

- List up to 3-5 recommended mitigations or improvements or continuations of something already moving in right direction as relevant or possible to fit on the slide.

Safety (e.g. HSE, EHS, HAZOP, LOPA, PHA, cyberPHA, SIS etc)

Observation: describe findings (both negative and positive), background, history etc in a few sentence paragraph narrative

Recommendations:

- List up to 3-5 recommended mitigations or improvements or continuations of something already moving in right direction as relevant or possible to fit on the slide.

OT specific cyber training, certifications and awareness

Observation: describe findings (both negative and positive), background, history etc in a few sentence paragraph narrative

Recommendations:

- List up to 3-5 recommended mitigations or improvements or continuations of something already moving in right direction as relevant or possible to fit on the slide.