PHOENI2X

Transport

Pilot Description

Rail infrastructure needs sensors to monitor safety parameters to ensure safe operations. The sensors report to an integrated OT solution which might be target of cybersecurity attacks.
The testbed for the use case includes the end-to-end OT solution for safety monitoring parameters in the Rail infrastructure operator.

Incident Scenarios

Phase	Highlighted events	Key PHOENI2X components in action
Prevention & Preparedness	Continuous data and meta-data collection for event anomaly detection, cyber hygiene procedures, threat information reception, digital forensics, training.	**CMT** shares to **PMEM** IoT devices data, network and server metadata for anomaly detection. **DS_Testing** allows the cybersecurity team to request a vulnerability assessment on the OT infrastructure, **CTI** receives threat information from 3rd party OES, Digital Forensics ensures all digital evidence are available at **FVT**, while **Serious Games** provide training on cybersecurity awareness.
Scenario 1 **Data Tampering**	An abnormal value is received from a safety sensor aiming at blocking normal operation of the rail infrastructure. Identification of possible tampering of data.	**PMEM** identifies an abnormal value, which deviates from the predicted expected values, and triggers a suggested response playbook. **ROAR** executes the playbook, notifying **FVT** who creates an incident case at **SMIR** and notifies the operator of the incident. The operator will use other monitoring solutions to validate or discard the abnormal value received.
Scenario 2 **DoS Attack**	The server platform supporting the OT system is exposed to a Denial of Service attack. Identification of the attack is performed through the analysis of use of resources of the server.	**PMEM** detects an increase in the use of resources of the server, triggering a suggested response to **ROAR**. The relevant playbook is executed notifying **FVT**, creating the incident case at **SMIR** and notifying the operator. **ROAR** will also execute an automatic remedial action. **SMIR** will generate a report for the cybersecurity team to assess the situation and close the incident.
Scenario 3 **Privilege Escalation**	One of the services of the OT platform has been exposed and there is a privilege escalation attack.	**NDR** will detect the event at the service, reporting it to **SIEM**, and forwarded to **FVT**. A playbook will be triggered at **ROAR**, creating an incident case at **SMIR**, notifying the operator and executing an automatic remedial action. **SMIR** will generate a report for the cybersecurity team to assess the situation and close the incident.
Post Incident	Business Continuity, reporting and training.	**ROAR** triggers the business continuity playbook to provide all logs and relevant documentation to the cybersecurity team from the monitoring solutions (CMT application, NDR, SIEM) to ensure proper management of the situation presented and generate a final report with required information. **SMIR** produces an incident report that is validated by the cybersecurity team to be later shared to the regulatory bodies through **CTI. Resilience CR** will be used to train the operational team regarding the cyber-threats presented.

PHOENIIX

PHOENI2X Solution

- **Improved Data Integrity** PMEM prediction models allow the identification of abnormal values on IoT solutions for critical infrastructures boosting knowledge on data integrity.
- **Enhances IoT/OT solutions stability** - PMEM, NDR, SIEM allow detection of cyber threats, and early response through pre-defined playbooks.
- **Provides OT cybersecurity visualisation** - FVT facilitates the visualisation of cyber threats to OES control rooms, while ROAR allows the integration of playbook actions to the operators easily through API.
- **Resilience Automation, Orchestration & Response (ROAR)** - Orchestrated playbooks span cyber (DDoS mitigation, malicious host isolation) and physical (link fail over) events, ensuring seamless Business Continuity, Recovery and Incident Response while every action is case managed in SMIR.
- **Operator Preparedness** - The Resilience Cyber Range (RCR) together with Serious Game modules, deliver immersive exercises tailored to the Rail sector and personalised feedback, continually increasing the security awareness and readiness of the employees.
- **Timely, Standards Based Information Exchange – SMIR** auto generates structured reports (STIX/TAXII, ISAC formats) that flow between the Operator of Essential Services, National Authorities and EU actors.

As a result, the pilot through PHOENI2X is able to improve security and resilience of the OT infrastructure a Rail operator uses to collect safety sensor data - predicting attacks, automating defense, training people, and reporting outcomes - in one integrated, AI assisted framework.

Consortium

University of Patras
Sphynx
Universitat Politècnica de Catalunya BarcelonaTech
OTE Group of Companies
FGC Ferrocarrils de la Generalitat de Catalunya
AEH
World Sensing
AEGIS IT Research
Social Engineering Academy
Eunomia Ltd. Consulting Services
Atos
APIROPLUS SOLUTIONS
Nodalpoint
UiO : University of Oslo
National Cyber Security Authority GR
National CSIRT-CY

phoeni2x.eu/ @Phoeni2xProject @Phoeni2xEUProject @Phoeni2x