PHOENIIX

Healthcare

Pilot Description

This pilot targets a key cybersecurity threat in digital healthcare: software supply chain attacks. It simulates and protects against such attacks by emulating the development environment of a national healthcare portal that delivers public health services and manages over €100 million in healthcare reimbursements monthly.

Incident Scenarios

Phase	Highlighted events	Key PHOENI2X components in action
Prevention & Preparedness	Continuous log collection from the development environment; threat intelligence-driven asset vulnerability assessments; secure coding and supply chain risk training for developers.	**UEBA** uses behavioural baselines to train models for detecting anomalies in user/system actions; **FVT** visualizes logs and activity; **SPA** uses imported dev environment assets to conduct vulnerability assessments; **ResilienceCR** delivers tailored developer training.
Scenario 1 **Unauthorized code commit**	A stolen developer token is used for unauthorized access to commit malicious the code. The attacker's abnormal patterns - off-hours login, unknown device, privilege escalation - are detected.	**UEBA** detects anomalies; **SPA** and **ROAR** block the attacker and prevent malicious code from being committed; **CERCA** calculates the risk dynamically;
Scenario 2 **Malicious Codebase Tampering**	An attacker attempts to delete a critical branch from the source code to disrupt operations.	**UEBA** detects anomalies; **SPA** and **ROAR** halt the deletion and restores code integrity while blocking the attacker; **CERCA** calculates the risk dynamically;
Scenario 3 **Vulnerable Dependency Injection**	A developer introduces a third-party library which post-deployment to production operations is found to be vulnerable.	**CTI** and **SPA** correlate external vulnerability alerts with deployed code assets; **ROAR** initiates incident response playbook and notifies the SOC to suspend operations.
Post Incident	Business continuity, threat mitigation, reporting and knowledge sharing	**SPA** and **ROAR** instruct rollback and orchestrate deployment of safe software version to production operations; **SMIR** generates NIS2-aligned reports for national authorities; **CTI** shares threat intelligence with other PHOENI2x instances

PHOENIIX

PHOENI2X Solution

- **End-to-end threat visibility:**
  Continuous monitoring via the Elastic Stack, FVT, and UEBA detects abnormal behavior, while SPA and CERCA assess and contextualize risk in real time.
- **Automated response and recovery:**
  ROAR executes standardized playbooks to contain attacks - blocking malicious activity, rolling back code, and guiding secure restoration.
- **Regulatory compliance and intelligence sharing:**
  SMIR ensures incident reporting meets healthcare regulations, and CTI distributes threat insights across trusted networks.
- **Resilience through training:**
  ResilienceCR builds long-term security awareness by training developers in secure coding and supply chain risk mitigation.

The pilot shows how PHOENI2X fortifies the digital healthcare supply chain: predicting risks, automating responses, training personnel, and securing services with a harmonized, AI-supported approach.

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