PALANTIR

Threat Management and Sharing

Threat Management proposal

PALANTIR proposes a technically and economically adapted remediation against cyber-threats hampering customers' assets and security enablers reinforced by intelligence sharing.

The PALANTIR innovation

PALANTIR capitalises on SecaaS-driven orchestration to conduct remediation through technically agnostic playbooks. They describe specific actions to enforce the policy specified by the operators and cover threats jeopardising both the subscriber's assets and the PALANTIR platform itself. This approach enables stakeholders to perfect strategies and exchange their work with the community while maintaining control over their budget.

Threat Management result

Active user awareness on the threat posture of his information system and expanse through a comprehensive user interface, and involvement in threat intelligence sharing.

Consistent and finely tailored remediation procedures against multifaceted threats ranging from cyberattacks to security enabler malfunction.

Selection of security enablers based on protection needs and cost containment, continuously accessed via billing follow up.

Extensive assessment of SecaaS service integrity for self-protection against subduction attempts against PALANTIR.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883335.