PALANTIR

Newsletter Issue #1

Editorial

Dear Reader, welcome to the first newsletter of PALANTIR, an EU funded Innovation Project. This first issue provides a brief introduction to the project, an overview of the Architecture definition, and the Threat and Attack Surface analysis conducted in the first months of our project. More project news is to follow while comments and suggestions are always welcome.

Introduction

The increasing importance of cybersecurity, resulting from the sustained digitalization of almost every aspect of everyday life, is undeniable. SMEs and MEs now share similar needs with larger enterprises in terms of digital security but often lack the resources or expertise to fulfil them. PALANTIR project proposes a cybersecurity framework combining privacy assurance, data protection, incident detection and recovery aspects under the same platform, focusing on cyber-resilience of SMEs and compliance with the relevant data privacy and protection regulations.

Objectives

- Provide SMEs/MEs with a practical framework to assess and manage cybersecurity risks and define their cybersecurity needs.
- Provide affordable Managed Security Services, in multiple delivery modes.
- Provide novel hybrid incident detection with live threat intelligence sharing.
- Ensure the financial sustainability of PALANTIR cyber defence while disrupting the economic benefits of the attacker.

Architecture

During the early stage of the project, the consortium elicited the project's requirement through a technical survey of subject matter experts and a business questionnaire for PALANTIR business's stakeholder. Then, the partners refined the Conceptual solution into the technical architecture that drives the implementation. An overview of the architecture is available online at: https://www.palantir-project.eu/architecture/

The architecture embodies the core features that PALANTIR aims to offer to its users, namely an as-a-Service business model for flexible and dynamic Cybersecurity protection, enhanced with Machine Learning-based and attestation-based detection capabilities, and complemented with a risk analysis to quantify the impact of security or privacy vulnerabilities. Furthermore, PALANTIR leverages policy-based remediation and recovery to automate security incident management.

Deliverable 2.1. Requirements & High-Level Design – Interim, which will be available later on the project website (https://www.palantir-project.eu/documents/project-deliverables/), is the PALANTIR document that defines the architecture, presents the inter-component interaction to explain the project's solution. The Reader will also find the set of standards and open-source tools being considered by the partners.

Threat Analysis

Threat analysis and sharing holds an important role in the PALANTIR ecosystem. PALANTIR's AI powered architecture and mechanisms focus on developing a real time early detection system for threats in the SME ecosystem. In a typical Information and Communication Technology system (ICT), assets can be: (a) hardware, software and communication components; (b) communication links between them; (c) data that control the function of the system, are produced and/or consumed by it, or flow within it; (d) the physical and organizational infrastructure within which the ICT system is deployed, and (e) the human agents who interact with the system and may affect its operation (e.g., users, system administrators etc.).

Follow us:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883335. The information contained in this newsletter reflects only the authors' view. EC is not responsible for any use that may be made of this information.