PALANTIR

Newsletter Issue #2

Editorial

Welcome to the 2nd PALANTIR newsletter, an EU funded Innovation Project. We summarise the first version of the architecture, design and technical considerations on the Security-as-a-Service (SecaaS) approach followed in the project. There, virtual security instances (Security Capabilities) are semi-automatically deployed in the network to mitigate attacks identified by the PALANTIR platform. This targets several scenarios for SMEs and MEs and aims at simplicity of operation.

Introduction

Thanks to AI models, the PALANTIR platform identifies attacks to the protected environment. Based on the available Security Capabilities, the platform proposes the best solution so that the environment operator can decide whether to deploy these mechanisms or not. The deployment and proper configuration of these security services must be done in a way that it can properly mitigate the attack in the specific part of the network.

Key benefits

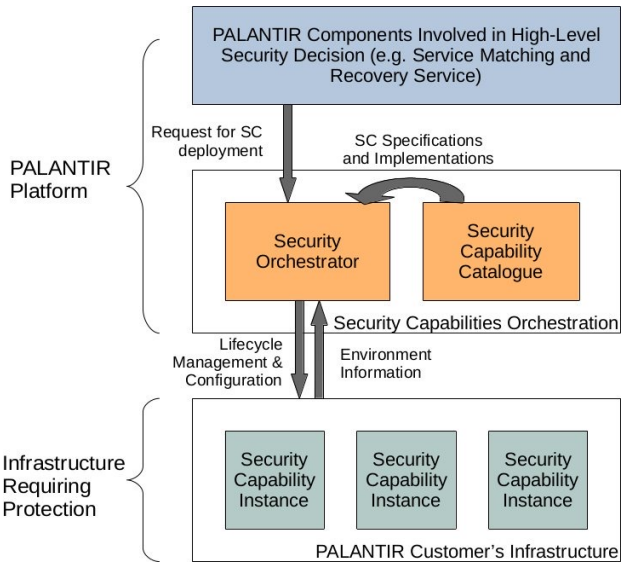
- Provide hardening virtual services to secure the entire SME.
- Automatically run, reconfigure and delete security services upon identified events.
- Easily store and search for the most adequate security services.

Architecture

PALANTIR offers Security Capabilities based on the attack to mitigate. Techniques like IDS, DPI or FW are covered, among others. These are stored in a Catalogue, or collection of Security Capabilities. The operator can easily retrieve their information and search for specific capabilities. Furthermore, the operator can evaluate their protective power, their fees, and their implication on customer privacy.

All PALANTIR components (including the Orchestrator, transparent to the SME operator) interrelate to decide which security service to roll out, where in the network, and how to configure it. Environment information is collected by the Orchestrator to be used by both the platform and the operator.

The components of the PALANTIR platform here described relate to the Secure Services Ecosystem; highlighted in blue in the figure and documented in the D3.1 deliverable - soon available under the project website (https://www.palantir-project.eu/documents/project-deliverables/).



Use cases

Apart from the architecture, PALANTIR develops three deployment models: Cloud, Edge and Lightweight with Customer Premises Equipment (CPE). These differentiate on the location to instantiate the Security Capabilities and on particular requirements for each mode.

To prove each mode delivers correctly, PALANTIR covers three use cases with different scenarios. Each scenario is designed with the elements needed for each deployment mode. The first one is a medical environment protected with Lightweight SecaaS, due to the private character of this scenario. The second implements an uninterrupted electronic commerce with Cloud SecaaS, since this business is very related with the cloud environment. The last one creates a large-scale Edge scenario with live threat intelligence sharing, implementing the Edge mode to bring capabilities near of the information source. All scenarios here presented will help to the implementation of all PALANTIR components, as well as the identification of interactions needed between components.

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.