PALANTIR

Newsletter Issue #5

Editorial

Welcome to the 5th PALANTIR newsletter, an EU-funded Innovation Project. In this issue, we describe the use cases of the project. Pilot 1 implements a Lightweight SecaaS deployment model for the protection of small businesses from data breaches, Pilot 2 implements a hybrid deployment model with Cloud SecaaS deployment and Pilot 3 uses 5G-enabled testbeds that can emulate traffic from multiple SecaaS clients on their edge network.

Introduction

PALANTIR provides a multi-layered, infrastructure-wide approach for threat monitoring, cyber-resiliency, and knowledge sharing in heterogeneous platforms. Infrastructure is built upon the features of Network Functions Virtualization (NFV), scalable Machine Learning (ML) towards hybrid Threat Intelligence, attestation techniques for secure infrastructure and trusted services, as well as standardization and threat-sharing methods to risk analysis, network operation, monitoring and management.

Key benefits

- PALANTIR covers 3 modes of deployment from Edge to Cloud to 5G
- Evaluates against different types of threats
- Leverages different cutting-edge technologies
- Applies threat sharing in a multi-modal scenario

Pilot 1: Medical SecaaS

Pilot 1 implements a Lightweight SecaaS for the protection of small businesses from data breaches and ransomware attacks. To this end, the PALANTIR platform will be leveraged in the scope of medical data protection, where relevant activities to safeguard patient data and prevent medical identity theft will be supported. In order to support such pilot and showcase the added value of PALANTIR components, a data leakage scenario will be developed and implemented in a medical practice office to replicate a real-world cybersecurity scenario. Various attack types will be investigated, as to their efficiency and applicability to real world conditions. The primary goal of this use case is to demonstrate a lightweight cybersecurity solution that can leverage both PALANTIR cloud platform modules that will run remotely, and the local edge modules that will perform the on-site operations, i.e., detection and remediation. Edge operations will receive periodically updated metadata in various forms (weights, models, etc.) that will maintain the platform's readiness in new attacks, and also provide an efficient lightweight SecaaS solution.

Pilot 2: Electronic Commerce with Cloud SecaaS

The PALANTIR solution in Pilot 2 provides a holistic cybersecurity protection for a ME in retail and service-oriented setting that uses on-premises equipment and a cloud-based solution that needs to be protected. The PALANTIR solution will be leveraged against attacks targeting disruption of business, getting access to private data of customers, and getting access to sensitive corporate information. In order to support such pilot and showcase the added value of PALANTIR components, diverse attack scenarios will be developed and demonstrated in collaboration with a subcontracted ME who will offer 3 offices located in 3 different cities in Slovenia all daily processing real customer and corporate data. In addition to a replica of local environments and operations, a replica of the e-commerce website and complete suite of cloud-based solutions used by the ME will be made available for replication. Various attack types will be investigated on the corporate infrastructure and the eCommerce platform as to effectiveness of the PALANTIR framework and its applicability to real world conditions.

Pilot 3: Live Threat Intelligence Sharing in a large-scale Edge scenario

This pilot experimentally demonstrates the operational capacity of PALANTIR solution in the 5TONIC and 5GENESIS testbeds. These 5G-enabled testbeds can emulate traffic from multiple SecaaS clients on their edge network as well as parallel complex attacks, in large-scale MEC scenarios. Pilot 3 will incorporate the virtual network infrastructure as well as SDN/NFV infrastructure comprised of high-performance servers for the execution of NFV management software and deployment of SDN controllers. The different elements of the testbed can be flexibly interconnected using OpenFlow switches. 5TONIC provides multi-site capability by incorporating infrastructure and equipment located at TID premises. A part of these labs is the Mouseworld, a configurable generator of labelled network traffic datasets, supporting dynamic network topologies (by means of an NFV infrastructure), experiment scheduling to configure and run predefined scenarios, and dataset labelling from the knowledge derived from the scheduled experiments. Pilot 3 investigates a large-scale 5G scenario Edge SecaaS, where the Communication Service Provider (CSP) deploys the SecaaS on the network edge, following the Multi-Access Edge Computing (MEC) paradigm, an essential building block of 5G deployments.

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.