PALANTIR

Newsletter Issue #3

Editorial

Welcome to the 3rd PALANTIR newsletter, an EU-funded Innovation Project. In this issue, we delve into the threat management process and describe how our components interact to enact the innocuity of customer assets. We showcase the security dashboard and the involvement of an operator, the incident response and recovery services coordinating the mitigating measures, the service matching selecting adequate Security Capabilities and the attestation engine leverages their self-protection.

Introduction

PALANTIR platform relies on a set of sensors and AI models to detect and classify an ongoing attack and multiple actuators, called Security Capabilities (SCs), to enforce mitigation. However, preparing a comprehensive response requires analysing the context and the coordination of the rightful enablers. In PALANTIR, this process is referred as threat management. The work package 4 leads its design and implementation by emphasising four objectives: (i) the flexibility to cope with different threats (including the ones affecting the security capabilities themselves) (ii) the automation to limit the vulnerable timespan, and (iii) the attractiveness to involve decision makers when requested.

Key benefits

- Accessible security management interface addressing multiple user profiles in SMEs
- Flexible management of the threat mitigation lifecycle through novel FSM techniques
- Automated and cost-efficient selection of adapted mitigation actuators
- Self-protection through integrity monitoring of the deployed security enablers

Architecture

When an attack is detected and classified, the incident response (IR) component controls the remediation. It instantiates a finite state machine (FSM) that guides the establishment of the adapted countermeasures in finely tailored fashion by coping with the peculiarities of the customer information system. The nature of FSMs allows a stateful management accounting for the enactment of all needed measures while supporting complex scenarios.

Addressing an attack may necessitate additional features provided by unsubscribed SCs. These pieces of software are available off-the-shelves from the PALANTIR catalogue and come with their own technical requirements and fees. The service matching (SM) component intervenes to analyse the customer's environment to pinpoint the compatible enablers to utilise. The pricing is also optimised based on supported billing models. If the SME accepts to purchase the proposed security capabilities, the order is submitted to the orchestrator for deployment.

All along the remediation, an operator can proceed with the follow-up of the process through the security dashboard (SD). This user interface exposes at glance the status of PALANTIR platform, inspects the situation of protected assets, and permits to interact with the threat mitigation. The portal is composed of views addressing different levels of technicity:

1. SME Manager having access to business-oriented features but few technical details. This role is adapted for executives in PALANTIR's subscribers.
2. Network operator and Platform administrator, completely overseeing the technical aspects of the mitigation. These roles fit the main users from PALANTIR service providers and the executives from this organisation.
3. Security capability developer, provisioning the catalogue and accessing a financial follow-up. This profile tailors the software engineers willing to conceive and commercialise SCs for the PALANTIR platform and monitoring their revenues.

When the remediation process completes, the integrity of deployed SCs is continuously monitored by the Attestation Engine (AE) component. A set of reference metrics are measured whenever a new security capability is registered in the PALANTIR platform. During their operation, they serve as indicators to identify tampered instances.

When such an instance is found, the AE triggers the Recovery Service (RS) for the platform self-protection. This component controls the restoration according to policies specified by the operations. The possible actions range from basic re-instantiation to infrastructure isolation for forensic purpose. Similarly to the IR, the RS exploits FSMs for the same qualities.

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.