Practical Autonomous Cyberhealth for resilient Micro, Small and Medium-sized Enterprises

Evangelos Mantas*, Dimitris Papadopoulos*, Carolina Fernández‖ , Nil Ortiz‖, Maxime Compastié‖, Antonio López Martínez††, Manuel Gil Pérez††, Akis Kourtis[xi], George Xylouris[xi], Izidor Mlakar[xiii], Stylianos Tsarsitalidis¶, Dimitrios Klonidis¶, Ignazio Pedone**, Daniele Canavese**, Gregorio Martínez Pérez††, Davide Sanvito[xii], Vangelis Logothetis‡, Diego Lopez[xiv], Antonio Pastor[xiv], Antonio Lioy**, Ludovic Jacquin[x], Roberto Bifulco[xii], Angeliki Kapodistria†, Athanasios Priovolos†, Georgios Gardikis†, Ioannis Neokosmidis‡, Theodoros Rokkas‡, Nikolaos Papadakis§, Dimitris Paraschos§, Primoz Jeran[xiii], Antonis Litke*, George Athanasiou‡‡

*Infili Technologies PC, Athens, Greece — ‖i2CAT Foundation, Barcelona, Catalonia, Spain
††University of Murcia, Murcia, Spain — [xi]ORION Innovations PC, Athens, Greece — [xiii]Sfera IT, Maribor, Slovenia
¶UBITECH Ubiquitous Solutions, Athens, Greece — **Politecnico di Torino,Turin, Italy
[xii]NEC Laboratories Europe GmbH, Heidelberg, Germany — [x]Hewlett Packard Enterprise, Bristol, United Kingdom
[xiv]Telefonica I+D, Madrid, Spain — ‡inCITES Consulting SA, Strassen, Luxembourg — †Space Hellas, Athens, Greece
§Stratotiki Sxoli Evelpidon, Vari, Greece — ‡‡DBC Europe SA, Brussels,Belgium

***Abstract*—The EU-funded PALANTIR project proposes a cybersecurity framework combining privacy assurance, data protection, incident detection and recovery aspects under the same platform. The project main focus is on cyber-resilience of SMEs and compliance with the relevant data privacy and protection regulations. The outcomes of the project will be validated in diverse application areas (eHealth, eCommerce, 5G-MEC) and will provide enterprises with security tools that will boost their resilience at a reasonable cost to protect their assets in the ever evolving cyber threat range.**

I. Introduction

The threat landscape of the cyber world changes every day and it is important that organisations acquire the necessary tools to protect themselves. From Denial of Service (DoS), phishing campaigns designed to deliver malware to sophisticated Advanced Persistent Threats (APTs), the operations of an organisation can be disrupted as a result of a cybersecurity attack. From the words of John Chambers, "There are two types of companies: those that have been hacked, and those who don't yet know they have been hacked" [1], a cybersecurity related incident seems unavoidable, and enterprises and organisations have to prepare themselves before disaster strikes. The unprecedented COVID-19 pandemic outbreak challenged cybersecurity even further due to the adoption of teleworking schemes, distance learning and teleconferencing, with new attack vectors and exploitation of the lack of enterprises' preparation to quickly adapt to the new normality. According to ENISA incident report for 2020 [2], "health has become one of the most critical sectors to protect against cyberattacks", a use case identified under PALANTIR and highly prioritised due to the sensitivity of a potential security breach. There is currently a big number of products and solutions to mitigate the ever-evolving cyber threat but most are not economically feasible for Micro, Small and Medium-Sized Enterprises (SMEs) that lack the necessary sources and knowledge to recover from such events. To this end, PALANTIR provides an evolving, expandable and unified framework, tailored to the individual needs of every SME, reducing the complexity level of usual security tools while being affordable and attractive for adoption.

The paper is organised as follows: Section II provides an overview of the related work while Section III gives the main lines of the approach by illustrating the PALANTIR concept, assets and delivery modes. Section IV presents the PALANTIR architecture followed by a high-level description of its components. Finally, Section V describes the Use Cases serving in validation and evaluation, while Section VI elaborates on the project research beyond state-of-the-art to address challenges that are hindering cyber-resiliency for SMEs, followed by closing remarks (Section VII).

II. Related Work

New paradigms and methods for the development of adaptive and reliable security frameworks are constantly emerging, relying on a wide range of technologies. For example, AI4HEALTHSEC [3] and CUREX [4] propose analytics-based platforms for forensics, risk awareness and data exchange, tailored for the healthcare industry. PUZZLE [5] focuses on blockchain-oriented technologies for threat sharing between SMEs, while C3ISP [6] considers confidential information sharing through standardized policy enforcement on encrypted data. CyberKit4SME [7] enables risk monitoring and forecasting through a series of risk modelling tools, supporting regulatory compliance analysis, while SECONDO [8] targets the optimization of cybersecurity investments for SMEs. Other proposed methodologies (ANASTACIA [9], SHIELD [10]) exploit NFV for adaptive monitoring of IT infrastructure. Our project, combines most of the aforementioned approaches

(NFV, machine learning, risk analysis, trust and attestation, threat sharing) offering a holistic protection for SMEs, acknowledging their lack of systematic approach for ensuring digital security.

III. The PALANTIR concept

PALANTIR aims at bridging the gap between large enterprises and SMEs by providing multi-layered, infrastructure-wide threat monitoring, cyber-resiliency and knowledge sharing in a heterogeneous ecosystem, while at the same time being able to market these services to third parties in the form of Security-as-a-service (SecaaS). The project will implement a coherent privacy assurance, data protection, incident detection and recovery framework, focusing on highly dynamic service-oriented systems and networks and taking advantage of their inherent programmability features and abstractions. PALANTIR also focuses on cyber-resiliency leveraging the features of service-oriented systems by a) applying and exploiting Network Functions Virtualisation (NFV) and Software-Defined Networking (SDN) technologies; b) considering emerging paradigms such as scalable Artificial Intelligence, standardisation and threat-sharing techniques to risk analysis, network operation, monitoring and management and c) ensuring the SME's compliance with relevant data privacy and protection regulations in the data breach age, implementing the "Privacy by Default" principle on how personal data is collected, used, transferred and stored between 3rd-party entities.

PALANTIR will implement three delivery modes, namely, the **Cloud SecaaS**, following the hosted Managed Security Services model (MSS), **Lightweight SecaaS**, following the virtual Customer Premises Equipment (vCPE) MSS model and **Managed Edge SecaaS**, following the Multi-access Edge Computing (MEC) model.

IV. PALANTIR System Architecture

The PALANTIR SecaaS approach consists of the deployment of security capabilities on-demand, with personalised characteristics associated with the client. Figure 1 exposes a synthetic representation of the main building blocks comprising its architecture.

*a) **Security Capabilities Hosting Infrastructure**:* This building block involves the underlying elements of the infrastructure, which are used to host and manage the SecaaS capabilities. It exposes the available physical resources in different ways, thanks to different virtualisation and optimisation techniques [11] (e.g., specific hypervisors, containers, pass-through, Enhanced Platform Awareness); serving the SecaaS capabilities. The SecaaS Capabilities can be deployed into Virtualised Network Functions (VNFs), which consist of one or more nodes running custom logic and leveraging different virtualisation techniques (e.g., VMs, containers). The Security Capabilities can also be implemented as a set of SDN flows or security configurations, depending on the capability being implemented and the hosting platform's features.

*b) **Security Capabilities Orchestration (SCO)**:* The SCO manages and enforces the different security capabilities, including their onboarding and registration of resources and metadata, the actual orchestration of security services and, in general, enactment of security controls. The main capability in use is that of a security service in the form of VNF and NS packages, where the later is handled by an ETSI MANO NFVO [12]. This component contains i) the *Security Capabilities Catalogue (SCC)*, which hosts the definitions of the security capabilities, along with their security, privacy and possibly deployment-related metadata; and ii) the *Security Orchestration (SO) and Capability Management*, which retrieves the security capabilities from SCC to manage their lifecycle and configuration (to enact specific security controls and apply particular security policies on them), as well as to monitor related resource usage and the health of the instantiated capabilities (for billing and SLA purposes, respectively). The SCO interacts both with the underlying infrastructure, to instantiate and enforce each capability, and with the components of the PALANTIR architecture, namely with i) the Threat Intelligence (TI) to obtain Machine Learning (ML) based recommendations which are then applied by enforcing the capabilities; with ii) Trust, Attestation & Recovery (TAR) that determines whether a node is untrusted (potentially compromised) and with iii) the Portal to expose available SecaaS capabilities, its operational status as well as billing and SLA-related information.

*c) **Threat Intelligence (TI)**:* The TI component complements the protection provided by the SecaaS Capabilities with advanced analytics mechanisms based on ML/Deep Learning (DL) techniques on different modalities of data from heterogeneous sources. By adopting a hybrid approach, analytics-based methods are combined with traditional signature-based IDSs to detect complex attacks [10]. TI communicates mainly with the deployed SecaaS and the SCO, creating a control loop. Its Distributed Collectors & Preprocessing module traces traffic from the network. The Multi-modal ML subcomponent analyses it for signs of malicious activity and outputs the detected threats to the Remediation & Recommendation module. The reactive measures to the cyber threats are then sent to the SCO for the enforcement of mitigation actions. TI communicates also with the PALANTIR Portal in order to share with other SecaaS clients the threat findings and the remediation policies (using STIX [13] and MSPL/HSPL formats [14], respectively).

*d) **Trust, Attestation & Recovery (TAR)**:* The TAR component works in collaboration with most of other main components in the PALANTIR architecture, either to attest or leverage them for fault management and to retrieve the expected state of the attested components. The TAR interacts with the hosting infrastructure's devices mostly to run the remote attestation, retrieving the attestation proof from the Root of Trust (RoT) as described in [15]. In PALANTIR, attestation of UEFI measured boot in [16], the shim in [17] and Grub2 in [18] bootloaders and Linux IMA in [19] is complemented with hardware attestation using Trusted Computing Group (TCG) Platform Certificates in [20] and runtime monitoring of the

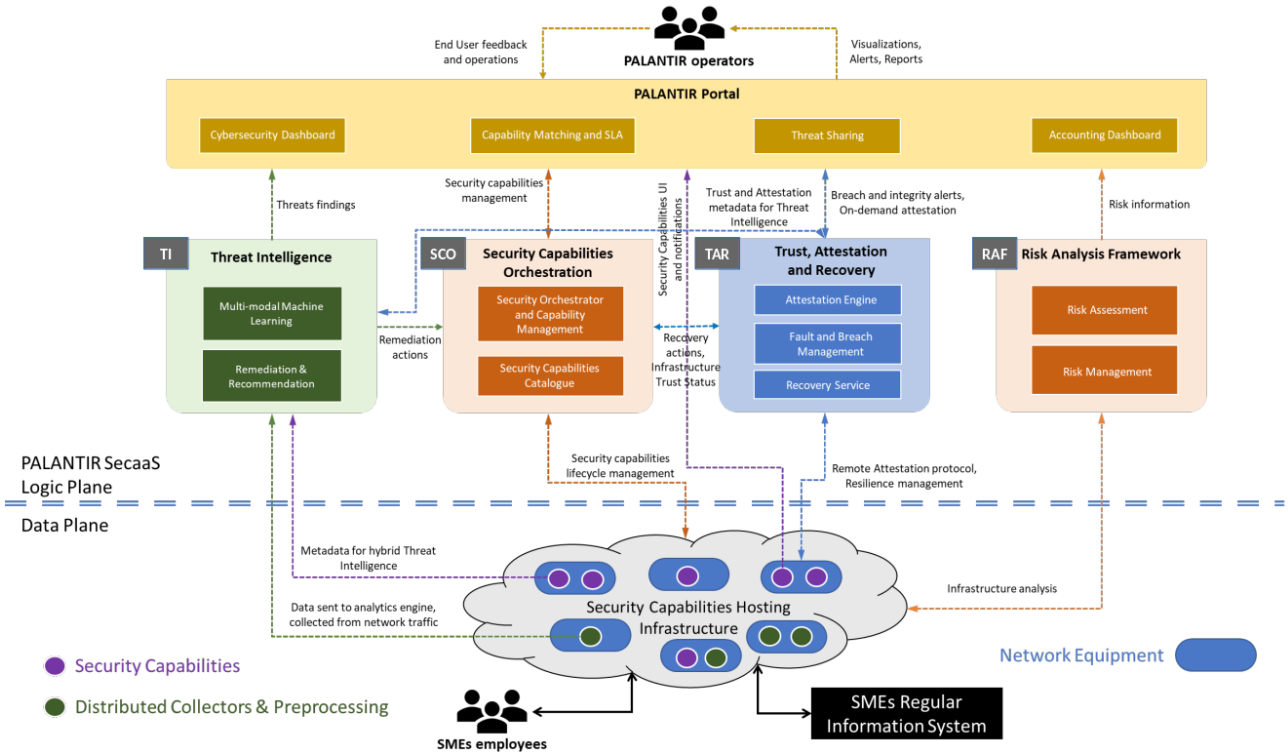

Fig. 1. PALANTIR architecture

OS' and its security critical services' memory.

*e) **Risk Analysis Framework (RAF)**:* PALANTIR provides a risk-based assessment similar to the ENISA SME framework [21], which allows the client to know the risks associated with its information systems, network, components, architecture, etc. RAF incorporates four phases to design and implement different risks profiles, adapted to client needs: i) Risk Profile Selection, ii) Critical Assets Identification, iii) Controls Selection and iv) Implementation and Management. The Risk Profile Selection is joint to the Critical Assets Identification, the unique step with more human interaction, since the client should enumerate the assets found in its organisation. The last two phases will be automated with the help of NIST tools, which offer interesting functionalities including vulnerability tests, security services deployments, customised security settings and lifecycle management.

*f) **PALANTIR Portal**:* The Portal consists of dashboards, each presenting the end-user with different views of data originating from most PALANTIR components, including data related to the deployed Security Capabilities. Such views depend on the user's role. As such, very basic monitoring views, such as accounting/billing for the enforced capabilities or generic security status indications, are provided for members of a client organisation. The network operators, on the other hand, have access to more in-depth security-related data, including security metrics, asserted threats and potential security breaches, as well as operational monitoring data. The view of each section in the dashboard is tailored to the purpose of the different components, whose features and information are being exposed. The Portal also provides mechanisms for knowledge sharing regarding threats, attack patterns and defence strategies, by exposing Indicators of Compromise (IoC). The IoC database is used along with a correlation mechanism to discover relationships between attributes, providing useful information on threats and remediation actions when similar events occur in different client organisations. The Portal visualises important and relevant security data to the user, while providing access to the management of the security capabilities deployed through SCO.

V. Validation & Evaluation use cases

To demonstrate the different operations of the PALANTIR platform, the following target scenarios have been identified:

*a) **eHealth: Securing private medical practices with Lightweight SecaaS**:* Private medical practices are prime examples of SMEs with high security and data protection needs as they frequently suffer from critical data breaches and the staff is usually not in the position to handle a cyber-attack. According to 2016 results from Ponemon [22], criminal attacks have "increased by 125% since 2010 and now represent the leading cause of healthcare data breaches". Medical devices store patient data but without the inherent protection of a computer (e.g. firewall, antivirus etc.). Besides, while laptops, PCs, smartphones receive regular updates and are often changed every 3-4 years, medical devices are usually kept for more than a decade and are rarely upgraded or hardened against new threats. PALANTIR will showcase the

prevention of attacks to a medical server that could lead to the leakage of sensitive personal data. Given that healthcare relies on uninterrupted access to patient data, it is particularly vulnerable to ransomware attacks, delivered by vectors like worms or phishing emails. In the case of a small practice, a ransomware attack can threaten business continuity and the victim can succumb to the financial demands of the attacker. To this end, the PALANTIR Lightweight SecaaS will detect the attacker's malicious activity as an anomaly and issue an alert to the healthcare practitioner, while also registering the event for the system administrator. A remediation action to block the malicious connection will be suggested and enforced by the SecaaS components, leading to the disruption of the data leakage attempt.

b) ***e-Commerce: Uninterrupted Electronic Commerce with Cloud SecaaS****:* Small businesses with e-commerce operations are increasingly leveraging cloud services along with local infrastructure for expense savings, yet they do not always ensure that these services use strong online security measures. Once a company has violated a customer's trust, it is difficult to restore it. In 2017, Verizon's Data Breach Investigations Report [23] found that more than 75% of the data breach victims they studied were small businesses. The strong reliance to online customer services and the lack of security breach technology safeguards provides hackers the opportunity to easily access streams of sensitive corporate and personal data. PALANTIR will protect the infrastructure of a typical retail and service-oriented SME maintaining an e-commerce platform that comprises 3 offices located in different cities that manage real customer and corporate data on a daily basis. The SMEs' IT background is limited and focused on offering goods and services both online and offline. In addition to an e-commerce web site, the business also uses a hybrid, local+cloud-based CRM solution which includes billing, payments, electronic cashiers, Point of Sale terminals, etc., all connected to the internet. For the purpose of day-to-day operations, it involves several PCs, smartphones and tablets connected to the same network. PALANTIR is expected to provide a holistic cybersecurity protection to the ME, protecting the link between internal company's servers (internal network) and external network (routers, remote desktops, VPN service). Moreover, it will provide a service supporting risk assessment framework, enabling the detection of data breach attempts by analysing the collected network traffic, thus providing visibility on threats and levels of risk, or compliance towards certain established regulations (GDPR) for the customer. The scenario will include the execution of numerous attack vectors with the focus on data breach through the theft of digital identity, including spyware/ransomware, targeting the corporate infrastructure and precursors such as phishing and pharming. PALANTIR will exploit its trust and attestation capabilities to verify the integrity of the enterprise's infrastructure, will detect the incoming threats using its analytics framework and will propose relevant countermeasures to mitigate these threats from the SecaaS catalogue along with useful contextual information to the user.

c) ***5G-MEC: Live Threat Intelligence Sharing in a large-scale Edge scenario****:* PALANTIR provides an ideal foundation to leverage collective use of live threat intelligence by i) enabling the PALANTIR provider to jointly analyse data from multiple clients (rather than individually) and ii) allowing the provider to publish and retrieve anonymised cyber threat intelligence information to and from diverse knowledge sharing infrastructures (e.g., MISP instances). The service provider should be able to i) jointly analyse information from multiple clients to detect incidents which would remain unnoticed if each client was treated individually and ii) exploit the live threat intelligence feedback regarding propagating security threats to insert appropriate security-oriented functionalities directly into the local network of the user, through its provided gateway or in the network infrastructure. Using centralised security analytics to contextualise large flows of network traffic will allow to determine which types of evolving threats are targeting certain industries, so as to deploy tailored cybersecurity measures. The knowledge sharing capabilities of PALANTIR will be evaluated in realistic simulations of spreading attacks, leveraging two 5G testbeds that can emulate traffic from multiple SecaaS clients on their edge network as well as parallel complex attacks, in large scale Multi-access Edge Computing (MEC) scenarios. The use case will rely on virtual network and SDN/NFV infrastructures, comprised of high-performance servers to run NFV management software and SDN controllers. The PALANTIR components will be deployed on various levels of virtual networks, and realistic simulated cyberattack scenarios of propagating attacks will be simultaneously directed to multiple PALANTIR clients. In this context, we expect PALANTIR to i) detect the common threat addressed to multiple clients, ii) publish the incident to a knowledge sharing platform (e.g. MISP), iii) retrieve relevant threat intel information in order to produce an appropriate mitigation plan, and iv) relay high-level mitigation policies through the PALANTIR provider to other SecaaS clients.

VI. Beyond the State of the Art

By achieving cyber-resiliency for SMEs, PALANTIR is aligned with current issues in the detection and remediation of threats affecting their resources. In this section, we detail the challenges tackled by the project, and how the PALANTIR architecture addresses them.

a) ***Knowledge Sharing in Threat Intelligence****:* Threat intelligence is a vital process for organisations to anticipate and prevent attacks. The traditional approaches collect threat information from well-recognised entities (such as CERTs) and interpret operational recommendations. However, the proliferation of cyber-threats confronts organisations to attacks that have not been analysed beforehand by competent entities. Sharing threat intelligence permits the organizations to contribute to the knowledge of cyber-threat while relieving them from the burden of conducting alone their analysis.

However, sharing threat intelligence across multiple organisations faces multiples challenges. According to [24], unreasoned integration of threat intelligence sources worsens

data quality while making relevant intelligence harder to be found. PALANTIR tackles this issue by becoming a trust party, refining the shared intelligence to improve the quality of shared data while ensuring anonymisation. Besides, each PALANTIR's customer can control the nature of the intelligence to receive, in line with its own protected resources and the chosen deployment model. Another challenge is to well-balance the technical coupling of threat intelligence data, since information tightly bound to the technical context of an organisation may harden its interpretation by another.

To that extent, PALANTIR supports a hybrid threat intelligence approach and exploits multiple data sources to deliver context-agnostic technical indicators. Standardised formats such as STIX [13] are under consideration for this purpose, while remediation actions are expressed as high-level specifications structured in MSPL/HSPL [14] policies. Once a threat and the corresponding remediation actions are identified, the attack time window may remain open for SMEs, as their limited skills may prevent them from timely deciding and enforcing a remediation measure. PALANTIR addresses this issue by providing automatic notifications for newly undisclosed threats. The remediation can be either automated, to enact an unmanned protection, or semi-automated to leave the the customer in control.

b) ***Security Orchestration****:* A Security Orchestrator manages the enforcement of security configurations in an environment while considering extra information, e.g., for security checks and proper scheduling for their deployment. When modelled as resources (*capabilities* in PALANTIR), like network services (SecaaS) or security-related configurations (for network, HW or SW) their lifecycle can be managed. The security enforcement can be carried out through heterogeneous approaches: it can be either thought as a complementary mechanism on top of an already existing virtualised environment running network services [25] or as a mean in itself, where security capabilities are enforced to protect the infrastructure. This enforcement can be defined to extend low-level data models (e.g., the VNFD [26] used by the NFVO) with specific parameters or either add separate security-related data models. In PALANTIR we follow the latter approach (direct protection of the infrastructure and separate security-related data models), since this approach permits decoupling both the aim of the infrastructure and of the default network services from the PALANTIR platform, without modifying the current state. Finally, the orchestration leverages appropriate underlying network and systems setup, so as to optimise resources and time and increase flexibility and visibility. Some examples are the SDN approach, which allows a shared view of the network and the propagation and sync of network configurations; while the NFV approach enables a general view of the network service capabilities along with its reconfiguration and scaling. The SDN approach has been explored for security enforcement for cloud environments [27], yet its combination with the NFV architecture and tools brings further benefits.

c) ***Value Chain in Cyber-Resilience****:* When considering the protection of an information system, one of the biggest challenges relates to the correct assessment of the threats to mitigate, and the selection of the right security appliances to deploy. For an SME with limited cybersecurity expertise, insufficient or redundant protections are easy pitfalls to fall in. PALANTIR offloads this complexity from customers by providing a novel risk assessment framework to identify security needs, collaborating with the SCO for matching a given risk with a relevant security appliance.

As the landscape of cyberthreats is continuously evolving, ensuring its constant monitoring is a strict requirement to maintain the protection of an information system. Although cyber-threat intelligence is sustained by open identified threat databases (e.g. CERTs security advisories), interpreting and enforcing protective measures requires time and skills that SMEs may be missing. PALANTIR leverages a shared Threat Intelligence to identify and prioritise emerging threats, and to distribute this knowledge among PALANTIR's customers, consequently reducing the attack's time window on undisclosed threats.

The limited cybersecurity skills of SMEs also rebound on the deployment of cybersecurity appliances: their appropriate configuration requires both expertise and perfect knowledge on the assets to be protected. This results in error-prone management actions, likely to undermine the protection. In contrast, PALANTIR handles the management and the security configuration of applications through the security orchestration, also leveraging tailored delivery models.

One last aspect regards the financial cost of the protection is that addressing a wide spectrum of threats involves relying on different type of security products coming with their specific pricing and SLA. The variability of the infrastructure environments to be deployed (cloud, on-premise through CPE, Edge) complicates further the cost assessments of a protection. PALANTIR proposes to unify the subscription by providing an homogeneous billing and SLA for the delivered security capabilities. Such information is encoded in the Service Catalogue and is available to the user before the subscription. Also, the threat assessment and the virtualisation of CPE are important levers provided by PALANTIR to minimise the operational expenditure of the protection.

d) ***Threat Detection****:* As the number and complexity of cyber-attacks grows, the vast number of SIEM and Threat Intelligence solutions fails to properly detect novel threats, due to the fact that they leverage a very limited spectrum of information. According to ENISA, [28], such systems more often end up as "data warehouses" and the data that reach an expert responder are "too voluminous" and their relevance cannot be determined. When even experts are expected to remove the "signal from noise", non-experts will be faced with insurmountable difficulties in interpreting threat intelligence. Modern cybersecurity requires not only high detection rates but also a new, flexible threat scoring system.

PALANTIR addresses these problems by introducing data analysis in two discrete dimensions (i.e., anomaly detection and threat classification) [29] through the use of machine learning. It employs memory-based neural networks such as

Recurrent, Convolutional Neural Networks and AutoEncoders to exploit temporal correlations often found in network data. These architectures will be able to extract knowledge not only in a per-flow basis, but also detect anomalous behaviour from the temporal evolution of hosts' conversations. Further, PALANTIR embeds Multi-modal Learning that will drastically improve the accuracy of the implemented methods by enriching the flow data with three other types of information: a) analysis data provided by the security-related services that perform operations like DPI, b) with information of the topology of the network, and c) the hardware and attestation information. To this end, the Threat Intelligence component will exploit the great momentum of deep learning, in conjunction with the reliability of virtualised, signature-based intrusion detection systems, to provide an aggregated threat score, aiming towards a universal, hybrid cybersecurity solution.

VII. Conclusions

In this position paper we describe the novel approach adopted by the PALANTIR project to protect the information systems of SMEs as well as providing a detailed, preliminary architecture. We also document a survey on related work and a more detailed analysis on the expected contributions beyond the SotA in Section VI.

The PALANTIR platform has presented here the architecture and is currently under development. It will be designed and evaluated with the use-cases presented in Section V. Specifically, we will review them through an industrial-grade threat analysis, so as to align the specification of PALANTIR platform with real-world requirements and validate its contribution to cyber-resilience against realistic threats.

VIII. Acknowledgement

This work has received funding by the European Union Horizon 2020 research and innovation programme, supported under Grant Agreement no. 883335. Part of this work, on NFV and SDN, is also supported by the Spanish Government under Grant TEC2017-84423-C3-3-P. The content of this article does not reflect the official opinion of the European Union or any other institution. Responsibility for the information and views expressed therein lies entirely with the authors.

References

[1] Cisco, What are the most common cyber attacks?, https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html (2018).

[2] C. Douligeris, O. Raghimi, M. B. Lourenço, L. Marinos, A. Sfakianakis, C. Doerr, J. Armin, M. Riccardi, M. Wim, N. Thaker, P. Stirparo, P. Samwel, P. Paganini, S. Adachi, S. Lingris, T. Hemker, From January 2019 to April 2020 Main incidents in the EU and worldwide ENISA Threat Landscape, Tech. rep., ENISA (2020).

[3] AI4HEALTHSEC, A Dynamic and Self-Organized Artificial Swarm Intelligence Solution for Security and Privacy Threats in Healthcare ICT Infrastructures, https://www.ai4healthsec.eu/.

[4] CUREX, Secure and Private Health Data Exchnage, https://curex-project.eu/.

[5] PUZZLE, Towards a Sophisticated SIEM Marketplace for Blockchain-based Threat Intelligence and Security-as-a-Service, https:puzzle-h2020.com/.

[6] C3ISP, Collaborative and Confidential Information Sharing and Analysis for Cyber Protection, https://c3isp.eu/.

[7] CyberKit4SME, Democratizing a Cyber Security Toolkit for SMEs and MEs, https://cyberkit4sme.eu/.

[8] SECONDO, A Security ECONomics service platform for smart security investments and cyber insurance pricing in the beyonD 2020 netwOrking era, https://secondo-h2020.eu/.

[9] ANASTACIA, Advanced Networked Agents for Security and Trust Assessment in CPS / IOT Architectures, http://www.anastacia-h2020.eu/.

[10] H. Attak, M. Casassa-Mont, C. Dávila, E.-C. Davri, C. Fernandez, G. Gardikis, B. Gastón, L. Jacquin, A. Lioy, A. Litke, N. K. Papadakis, D. Papadopoulos, J. Núñez, E. Trouva, SHIELD: Securing Against Intruders and Other Threats Through an NFV-Enabled Environment, 2017. doi:10.1007/978-3-319-64653-4_8.

[11] Network functions virtualisation (NFV); NFV performance & portability best practises, https://www.etsi.org/deliver/etsi_gs/NFV-PER/001_099/001/01.01.02_60/gs_nfv-per001v010102p.pdf (2014).

[12] Network functions virtualisation (nfv); management and orchestration, https://www.etsi.org/deliver/etsi_gs/nfv-man/001_099/001/01.01.01_60/gs_nfv-man001v010101p.pdf (2014).

[13] R. Struse, T. Darley, B. Jordan, R. Piazza, T. Darley, STIX™ Version 2.1, https://docs.oasis-open.org/cti/stix/v2.1/cs02/stix-v2.1-cs02.pdf (Jan. 2021).

[14] D. Montero, M. Yannuzzi, A. Shaw, L. Jacquin, A. Pastor, R. Serral-Gracia, A. Lioy, F. Risso, C. Basile, R. Sassu, M. Nemirovsky, F. Ciaccia, M. Georgiades, S. Charalambides, J. Kusijarvi, F. Bosco, Virtualized security at the network edge: a user-centric approach, IEEE Communications Magazine (2015) 176–186doi:10.1109/MCOM.2015.7081092.

[15] M. D. Benedictis, A. Lioy, Integrity verification of docker containers for a lightweight cloud environment, Elsevier Future Generation Computer Systems 97 (2019) 236–246. doi:10.1016/j.future.2019.02.026.

[16] TCG PC client specific platform firmware profile specification, pc client working group, https://trustedcomputinggroup.org/resource/pc-client-specific-platform-firmware-profile-specification/.

[17] Shim, a first-stage UEFI bootloader, https://github.com/rhboot/shim/blob/main/README.tpm.

[18] GNU GRUB measured boot, https://www.gnu.org/software/grub/manual/grub/html_node/Measured-Boot.html.

[19] R. Sailer, X. Zhang, T. Jaeger, L. van Doorn, Design and implementation of a tcg-based integrity measurement architecture, in: M. Blaze (Ed.), Proceedings of the 13th USENIX Security Symposium, August 9-13, 2004, San Diego, CA, USA, USENIX, 2004, pp. 223–238.

[20] TCG platform certificate profile, infrastructure working group, https://trustedcomputinggroup.org/resource/tcg-platform-certificate-profile/.

[21] ENISA, ENISA risk management approach for SME/MEs. (2009).

[22] Ponemon, 2016 cost of cyber crime study & the risk of business innovation (2016).

[23] Verizon, Verizon data breach investigations report (dbir) from the perspective of exterior security perimeter (2017).

[24] C. Sillaber, C. Sauerwein, A. Mussmann, R. Breu, Data Quality Challenges and Future Research Directions in Threat Intelligence Sharing Practice, in: Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security, WISCS '16, Association for Computing Machinery, 2016, pp. 65–70. doi:10.1145/2994539.2994546.

[25] Network functions virtualisation (nfv); security management and monitoring specification, https://www.etsi.org/deliver/etsi_gs/NFV-SEC/001_099/013/03.01.01_60/gs_NFV-SEC013v030101p.pdf (2017).

[26] M. Compastié, R. Badonnel, O. Festor, R. He, A tosca-oriented software-defined security approach for unikernel-based protected clouds, in: 2019 IEEE Conference on Network Softwarization (NetSoft), 2019, pp. 151–159. doi:10.1109/NETSOFT.2019.8806623.

[27] M. Compastié, R. Badonnel, O. Festor, R. He, M. Kassi-Lahlou, Unikernel-based approach for software-defined security in cloud infrastructures, in: NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium, 2018, pp. 1–7. doi:10.1109/NOMS.2018.8406155.

[28] ENISA, Exploring the opportunities and limitations of current Threat Intelligence Platforms, Report/Study (Dec. 2017).

[29] H. Attak, M. Combalia, G. Gardikis, B. Gastón, L. Jacquin, D. Katsianis, A. Litke, N. Papadakis, D. Papadopoulos, A. Pastor, M. Roig, O. Segou, Application of distributed computing and machine learning technologies to cybersecurity, Computer & Electronics Security Applications Rendezvous (C&ESAR), 19-21 November 2018 (2018).