Practical Autonomous Cyberhealth
for resilient SMEs & Microenterprises

PALANTIR PILOT

The case of a complex cybersecurity attack mitigation within a medical practitioner environment

George Xilouris (ORION)
6.07.2023

PALANTIR Pilot

- Present a comprehensive cybersecurity framework designed to safeguard the health environment
- Delve into the critical issue of ransomware attacks and explore their significant impact on the health ecosystem.
- Highlight potential strategies to mitigate the risks associated with these malicious attacks.

The cost of Cyberattacks

How cyberattacks affect SMEs

BUSINESS RISKS AND COST OF CYBER ATTACKS

$7.5 MILLION

The average cost of a data breach rose from **$4.9 million in 2017 to $7.5 million in 2018.**

$1.745 TRILLION

In the **Asia Pacific** alone, a **Microsoft and Frost & Sullivan** estimated that the potential economic loss can hit **US$1.745 trillion**, which is more than **7% of the region's total GDP** of US$24.33 trillion.

$34,606

The average cost of cybersecurity incidents in a year for SMEs costs a **minimum of US$34,606** while that figure estimates at a minimum of **US$1.05 million** for large organizations.

WHY DO SMEs NEED TO WORRY?

YES, they do need to worry!

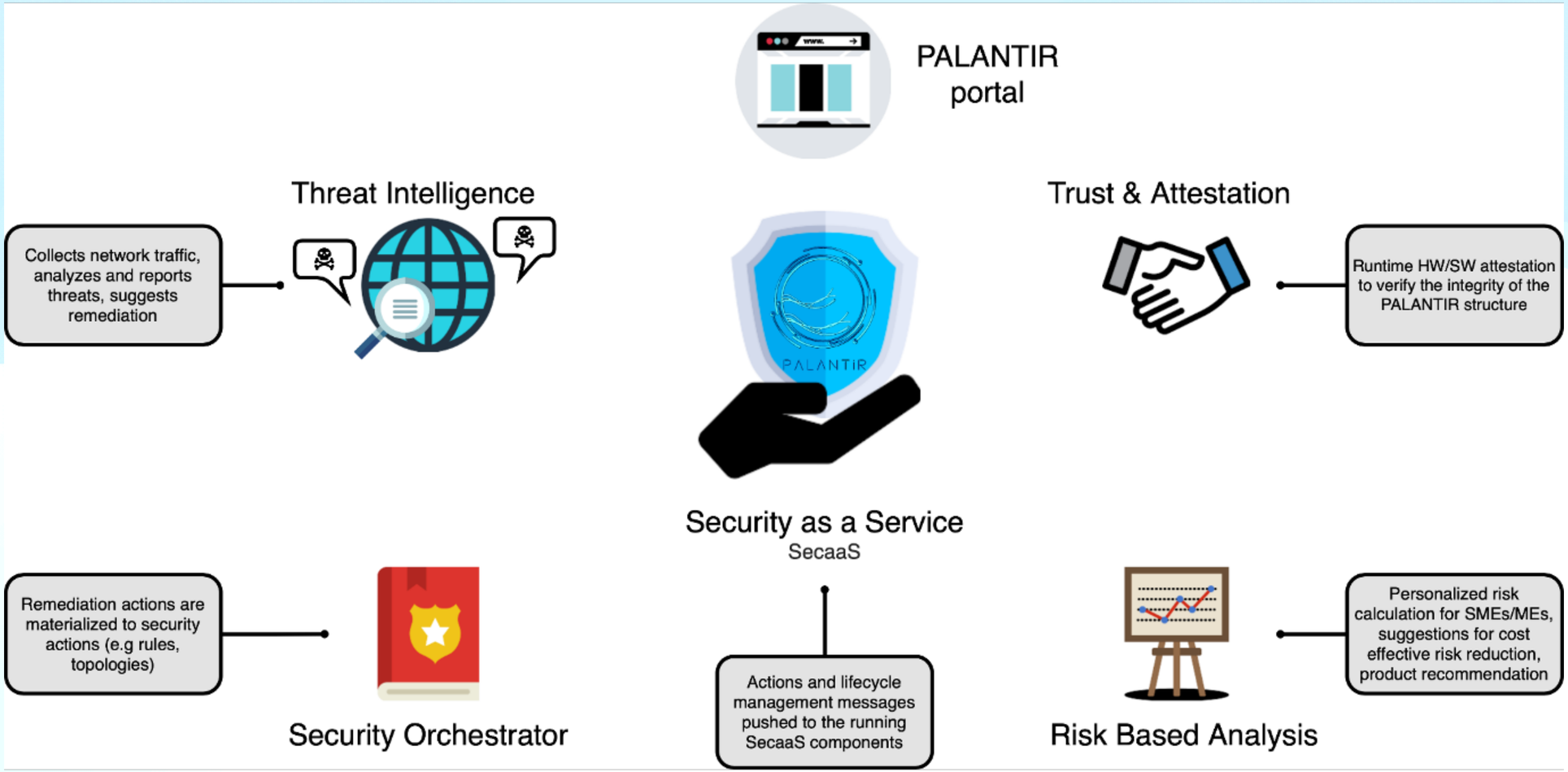
70%

of the attacks that occur are targeted at SMEs. There had been an overall sharp increase in cyber attacks through methods such as **ransomware attacks, business email compromise** (BCE) attacks and **spear-phishing attacks** in companies in 2018

47%

of **SMEs** had experienced at least one cyber attack in a single year and of those, **44%** experienced more attacks.

PALANTIR Concept



What is a Ransomware attack

Definition and context

- Ransomware attacks involve malicious actors gaining unauthorized access to computer systems and encrypting sensitive data, holding it hostage until a ransom is paid.
- These attacks have increasingly targeted healthcare organizations due to the high value and sensitivity of patient data, the criticality of health services, and potential financial incentives

What is a ransomware attack

The impacts within Health Environment

- **Patient Safety:** Ransomware attacks can disrupt critical health services, such as electronic health records (EHR) systems, medical devices, and communication channels
- **Data Breaches:** Healthcare facilities hold vast amounts of personal and medical information, making them prime targets for data breaches
- **Financial Losses:** Organizations affected by ransomware attacks may incur significant financial losses
- **Loss of Trust:** Patients and stakeholders may lose trust in healthcare providers' ability to protect their personal information and ensure the confidentiality, integrity, and availability of critical health services.

What is a ransomware attack

Vulnerabilities in a Health Environment

- **Legacy Systems:** Many healthcare institutions still operate on outdated software and infrastructure
- **Human Factors:** Employees' lack of cybersecurity awareness and training
- **Third-Party Risks:** Health systems often rely on third-party vendors for various services

PALANTIR offering

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

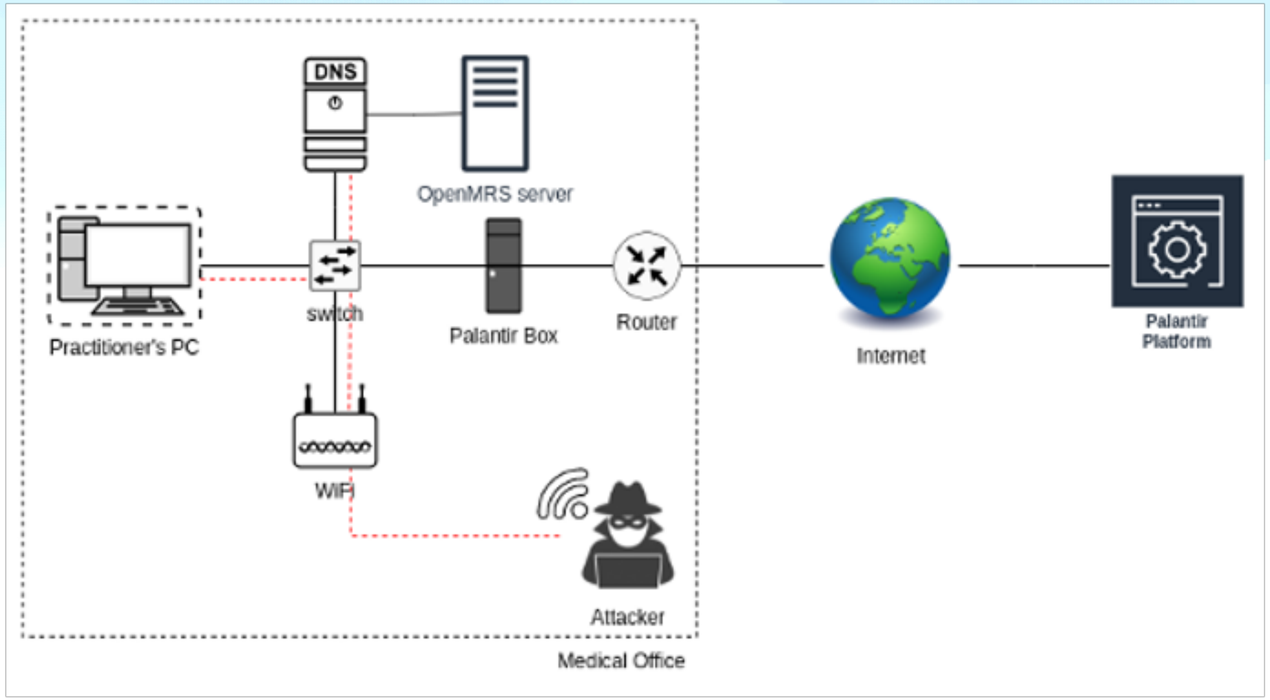
Provide novel hybrid incident detection with live threat intelligence sharing

PALANTIR SecaaS is leveraged to detect ransomware activity using flow-level features and isolate and remediate the attack.

PALANTIR Pilot

The PiaB deployment

- Exploit the Palantir-In-a-Box deployment flavour
- Use an on-premises lightweight deployment
- Easy to install and use



The Pilot

Outline

- Introduce the ransomware* attack without Palantir
- Attack targets the OpenMRS server that locates patients sensitive and private data
- Attack manages to gain access and encrypt database contents making OpenMRS operation impossible
- Initiate PALANTIR baseline service on Palantir-in-a-Box delivery mode
- Re-enact the ransomware attack
- Demonstrate Palantir detection and attack remediation

The Pilot

The multi-stage ransomware attack

- Accessing local network and staging the Man-in-the-middle setup
- Login account hacking (credentials)
- Remote Code Execution
- Reverse Shell (enable remote shell access)
- Privilege escalation (elevate permissions to root)
- Retrieve database credentials from the local filesystem
- Access database
- Encrypt database

PILOT Demonstration

Check out the PALANTIR Questionare

https://shorturl.at/xAFO9

Thank you for providing your feedback!

https://www.palantir-project.eu/

Thank You

The PALANTIR Consortium