ETSI
The Standards People

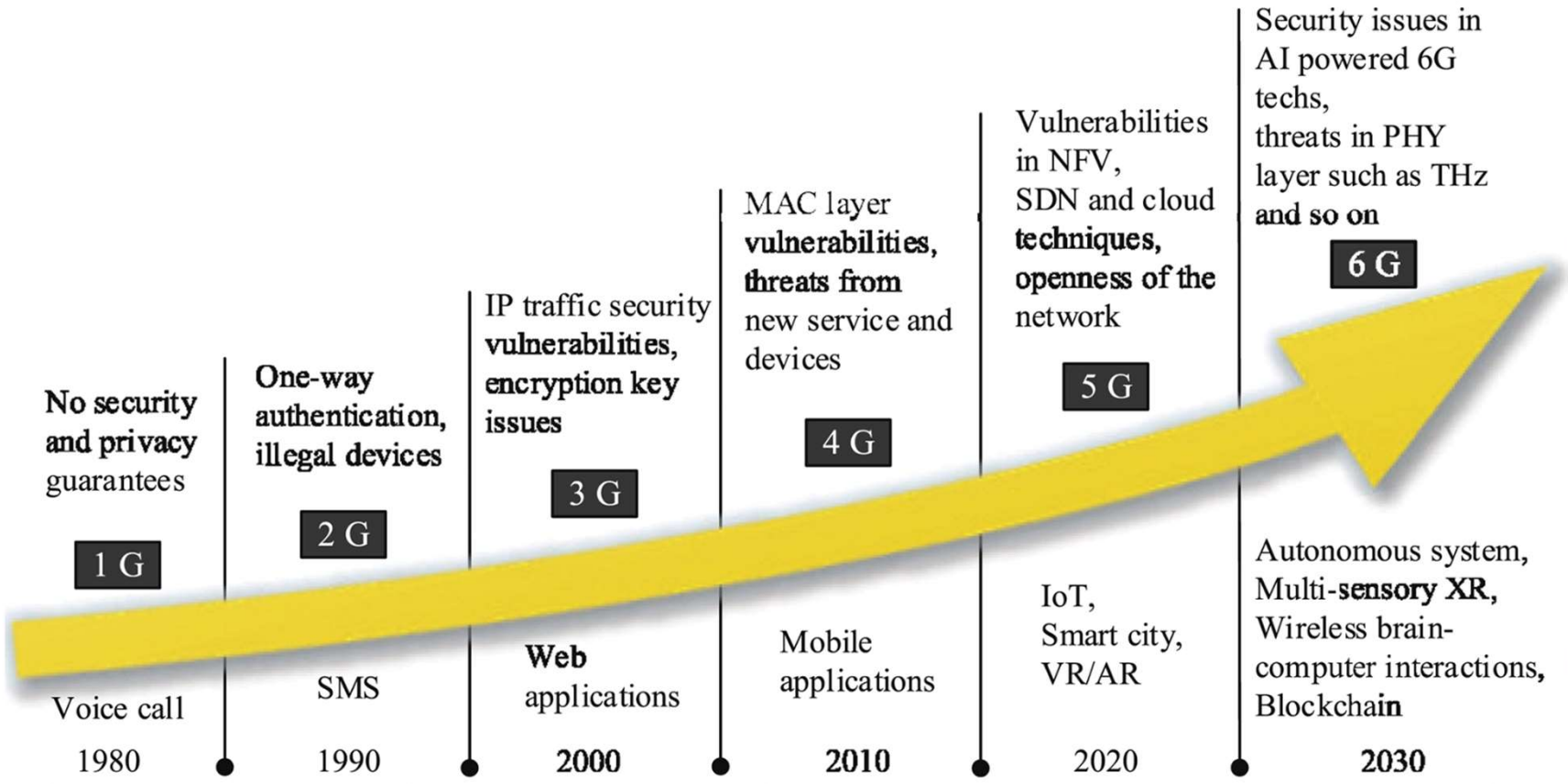
Security Conference

ZTA - The Inevitability … or is it NOT?

Presented by:

Galina Pildush, PhD,
Global Sr.Consulting Engineer, xG Security, Palo Alto Networks

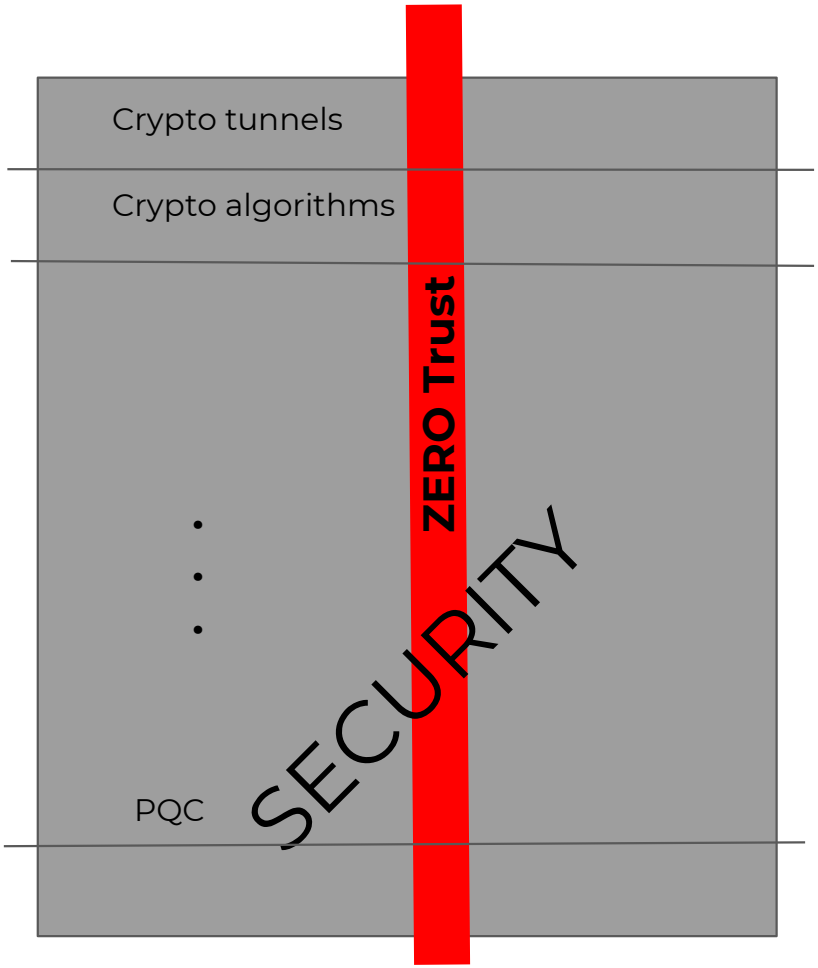
Evolution of Security … xG…



source: https://civils.pteducation.com/

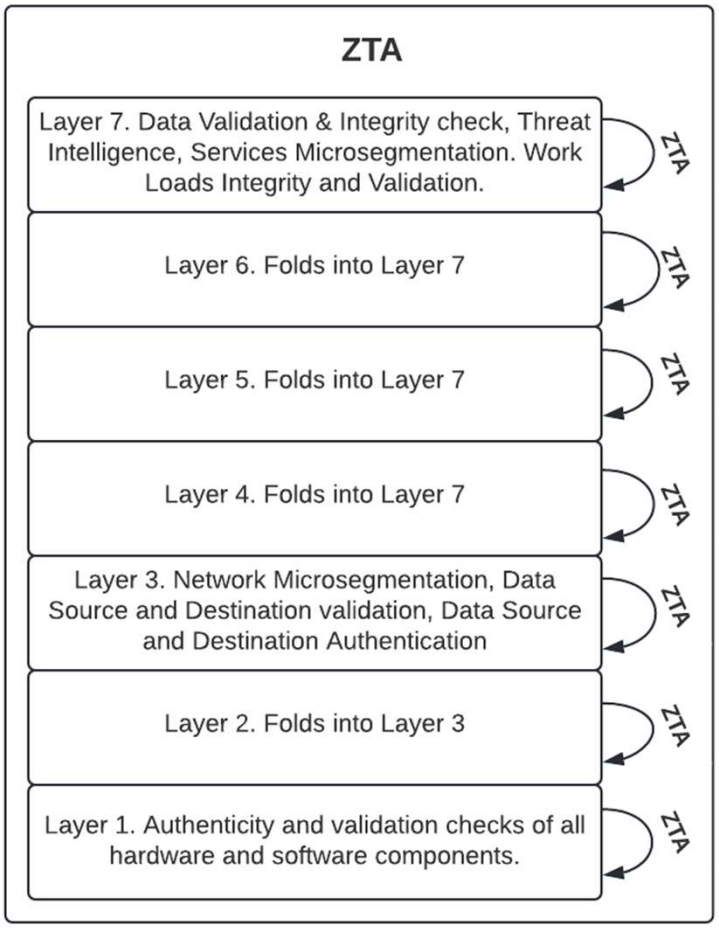

TRUST

Defining Zero Trust



Zero Trust is a security strategy designed to prevent breaches by eliminating trust in the digital world while consistently verifying all users, devices, and applications across all locations.

ETSI ISG ETI (Encrypted Traffic Integration) Group Report on ZT



First, validate, and only then, encrypt

source: https://www.etsi.org/deliver/etsi_gr/ETI/001_099/002/01.01.01_60/gr_ETI002v010101p.pdf

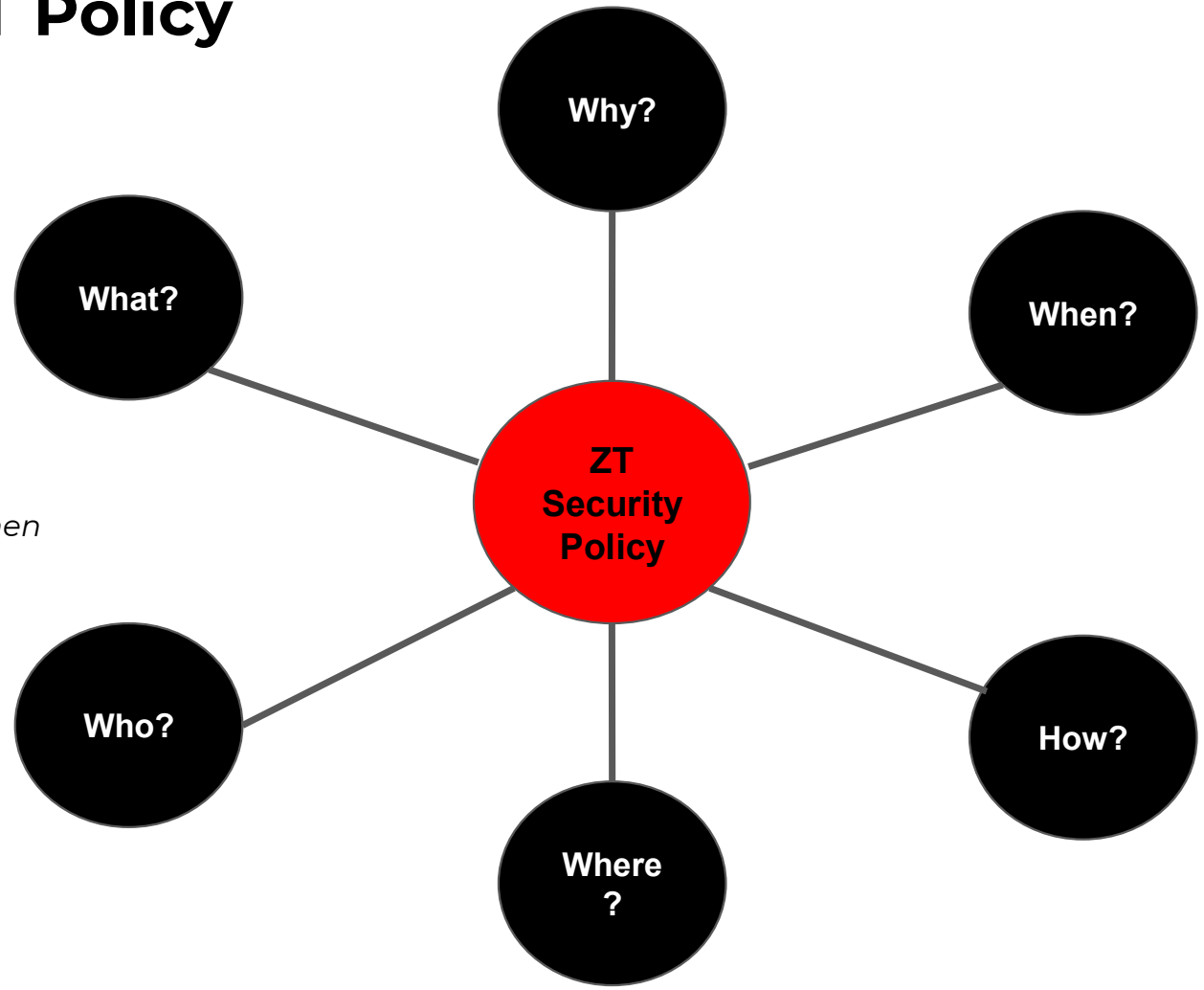
Best Practices Deploying Zero Trust Networks

- Zero Trust augments your existing network
- The Zero Trust network is interconnected with your existing network to take advantage of the technology you already have
- By following a five-step methodology deployment of your Zero Trust network can be accomplished with relative ease

What is ZT policy?

Kipling Method - ZT Policy

"I KEEP six honest serving-men
(They taught me all I knew);
Their names are What and Why and When
And How and Where and Who."
[Rudyard Kipling, Just So Stories, 1902]



Kipling Method for ZT is referred to in many standards and government documents. Here is one example - https://www.gsa.gov/system/files/Zero_Trust_Architecture_Buyers_Guide_v2_July_2022.pdf

Drilling Deeper Into Zero Trust Security Policies for xG Infrastructures

What?	What applications are been used to access? Identify/validate signaling and user plane traffic
Why?	Why is the packet trying to access the resource? Identify legitimate flows for signaling & user planes
When?	When is the resource been accessed? Predictable signaling/user plane traffic behaviours.
How?	How is the packet accessing the protected surface throughout this communication? Visibility into signaling & user planes.
Where?	Where is the packet source and destination? Specify the source/destination
Who?	Who should be connecting? Validate unique user IDs

WHO Needs ZT? WHY ?

IoT Devices / M2M

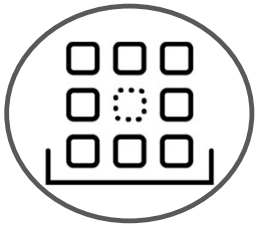
41 Billion IoT device to be connected by 2025

98% traffic is unencrypted, 57% of IoT devices are vulnerable. They are prone to Remote Code execution, firmware attacks, battery drain attacks etc

Edge Computing

75% of Enterprise data to be processed at edge by 2025

Prone to HW/SW injection, DDOS Attacks, Sniffing, Routing Information Attacks such as Black hole attacks, Logging Attacks etc



The Network Core

Aggregation point for signalling, auth, QOS etc

Risk of Signalling Attacks, Software and Virtualisation Security, Cloud Security, DDOS Attacks etc

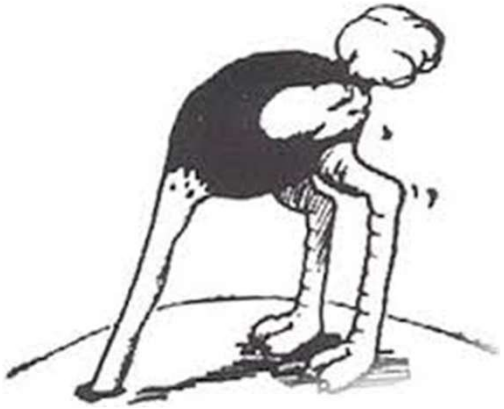
Full visibility and prevention across all locations and layers

Automated Security using ML & AI

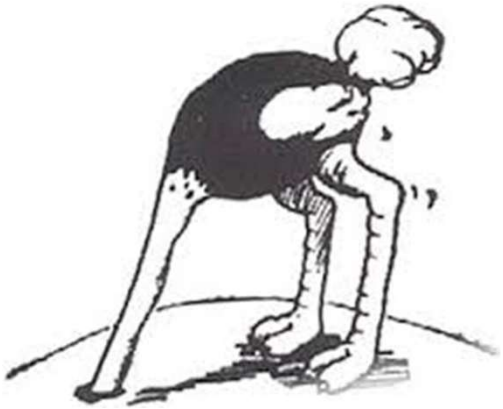
Zero-Trust

When Everyone Puts their Head in a Sand… What Happens?

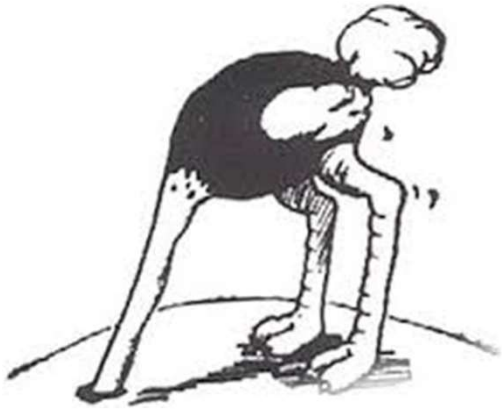
Mobile Service Provider



User



UE manufacturer



Accelerating Cyber Attacks Impact Every Vertical & Infrastructure

Security Camera Breach

150,000 Verkada cameras footage stolen affecting Tesla, Nissan, Schools, Hospitals and Jails

25% of cyber attacks involve IoT devices in organizations- Gartner

Hospital Cyber Attack

A ransomware attack disabled computers and medical equipment in 50+ NHS hospitals in the UK and US

82% of healthcare organizations have experienced a Cyber attack on medical devices in 2020/2023 - HIPAA Journal 2023

Colonial Pipeline Hack

Gas line shut off for 13 days. First complete shutdown in 57 year history, causing fuel and gasoline shortages

By 2025, cyber attackers will have weaponized OT environments to successfully harm or kill humans- Gartner

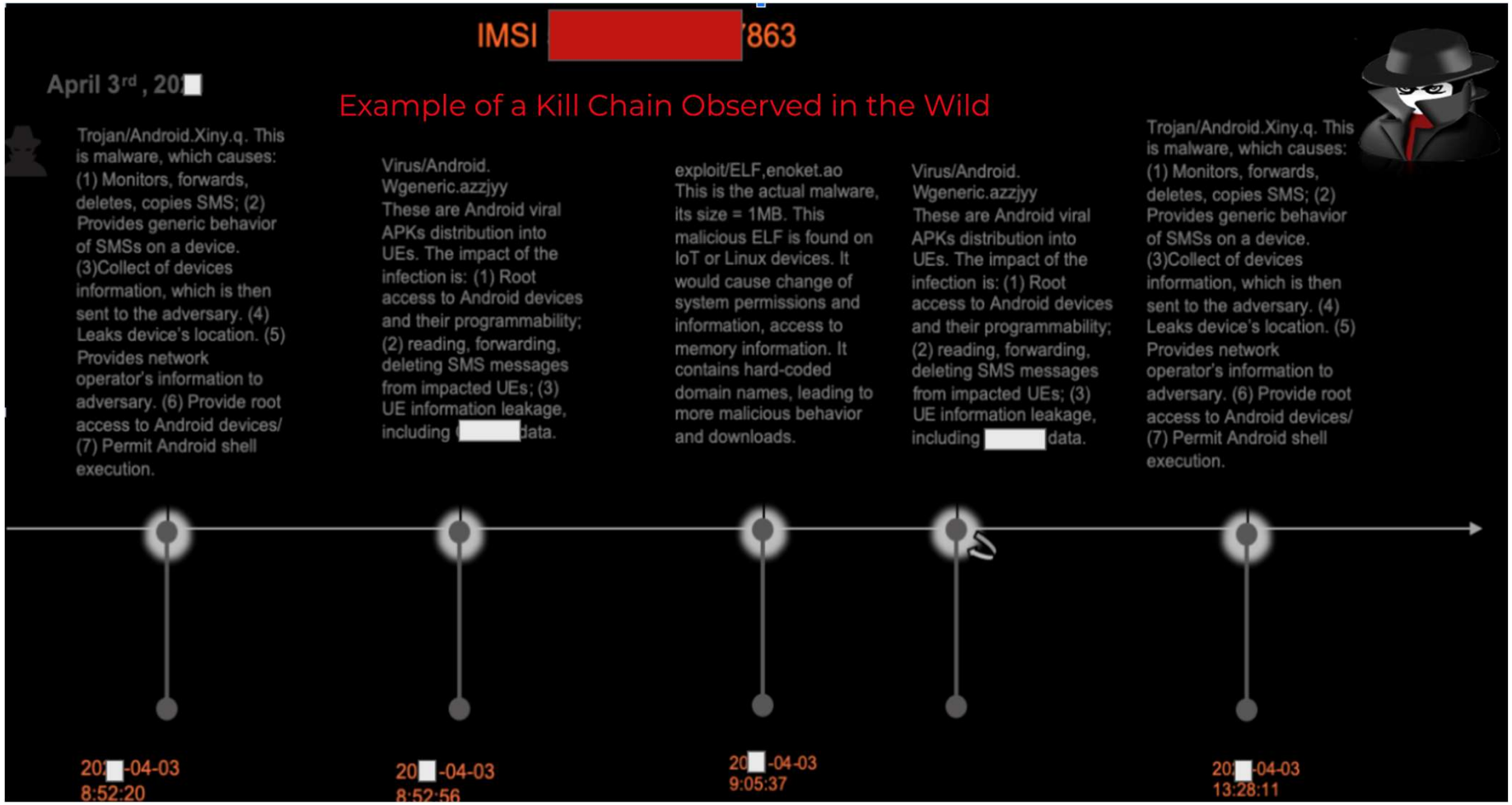
Sources: RYUK ransomware Verkada security camera hack St. Jude cardiac devices are vulnerable

FDA recalls: https://www.alpinesecurity.com/blog/most-dangerous-hacked-medical-devices/

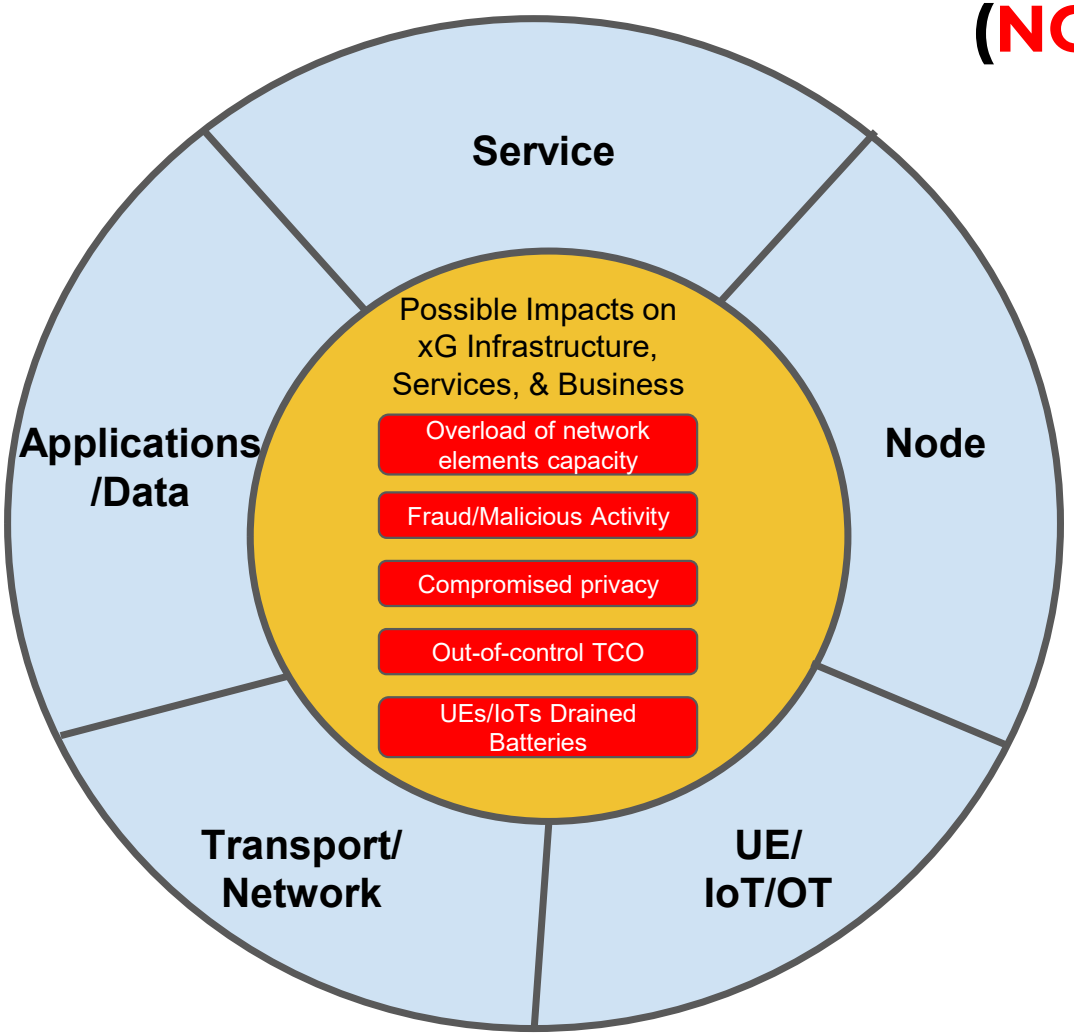
82% of Healthcare Organizations have experienced an IoT Cyber Attack | 82% of IoT Devices of HC providers targeted

paloalto NETWORKS

Networks Obscured by Threats (NOTs) Lead to Networks' Dysfunctions



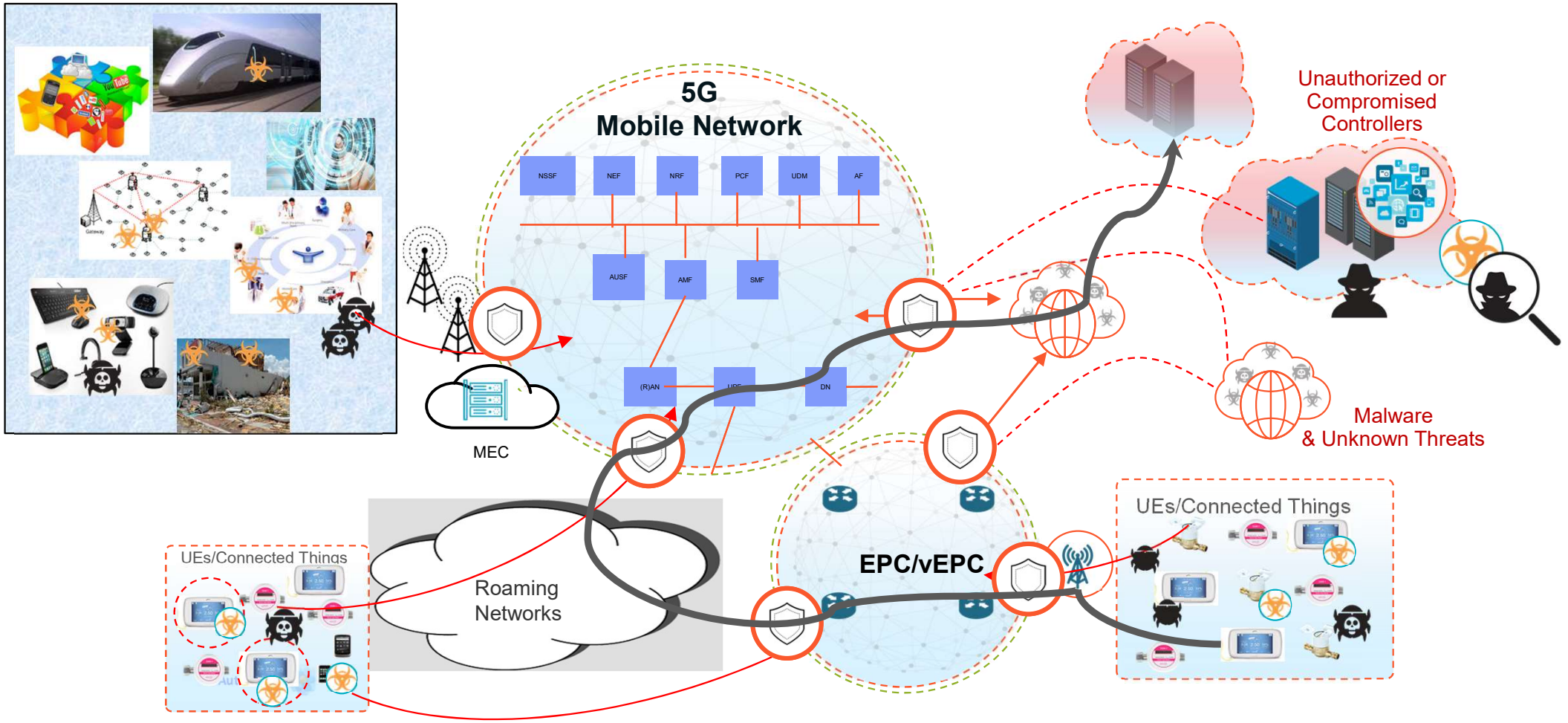
Lack of Zero Trust Leads to Networks Obscured by Threats (NOTs)



"We found that on average, an organization takes more than three weeks to investigate and remediate a critical exposure"

[source: https://start.paloaltonetworks.com/rs/531-OCS-018/images/Unit42_ASM_Threat_Report_2023.pdf]

Zero Trust ⇒ Achieve through E2E-Microsegmentation



Questions?

THANK YOU

Galina Pildush - gpildush@paloaltonetworks.com

https://ca.linkedin.com/in/dr-galina-diker-pildush-67baa71

paloalto NETWORKS