redi madrid

instituto imdea

FORTINET

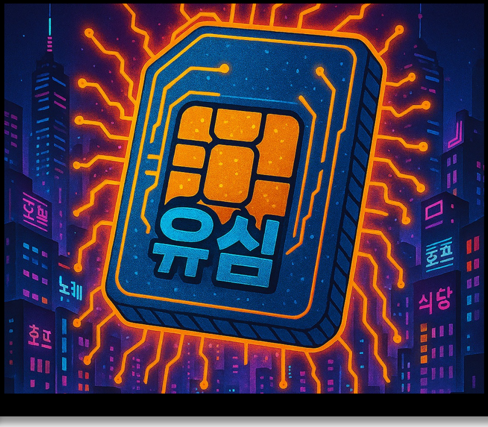
Cómo protegerse de ataques avanzados en las redes de telecomunicaciones

Pablo Molinero, Ph.D.
Sr.Dir., Product Management, Telco Vertical

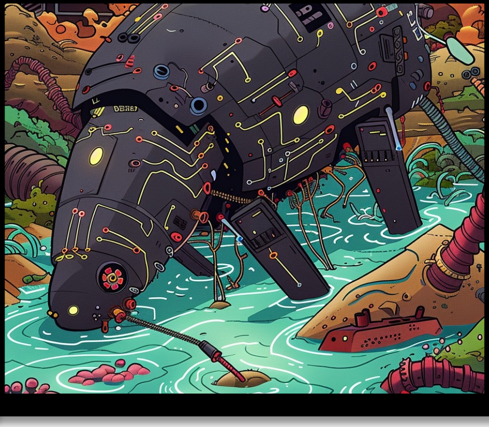
Some APT Groups Focused on Telco

Salt Typhoon

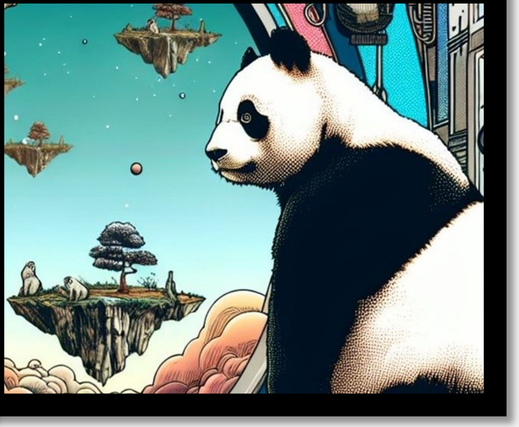
SKT Threat Actor



Muddy Water



Liminal Panda



sophisticated opponents

deep knowledge of
telecom networks and equipment

well-funded

difficult to detect

interested in information exfiltration & control, not damage

deep understanding of weak points

want to maintain long-term persistency

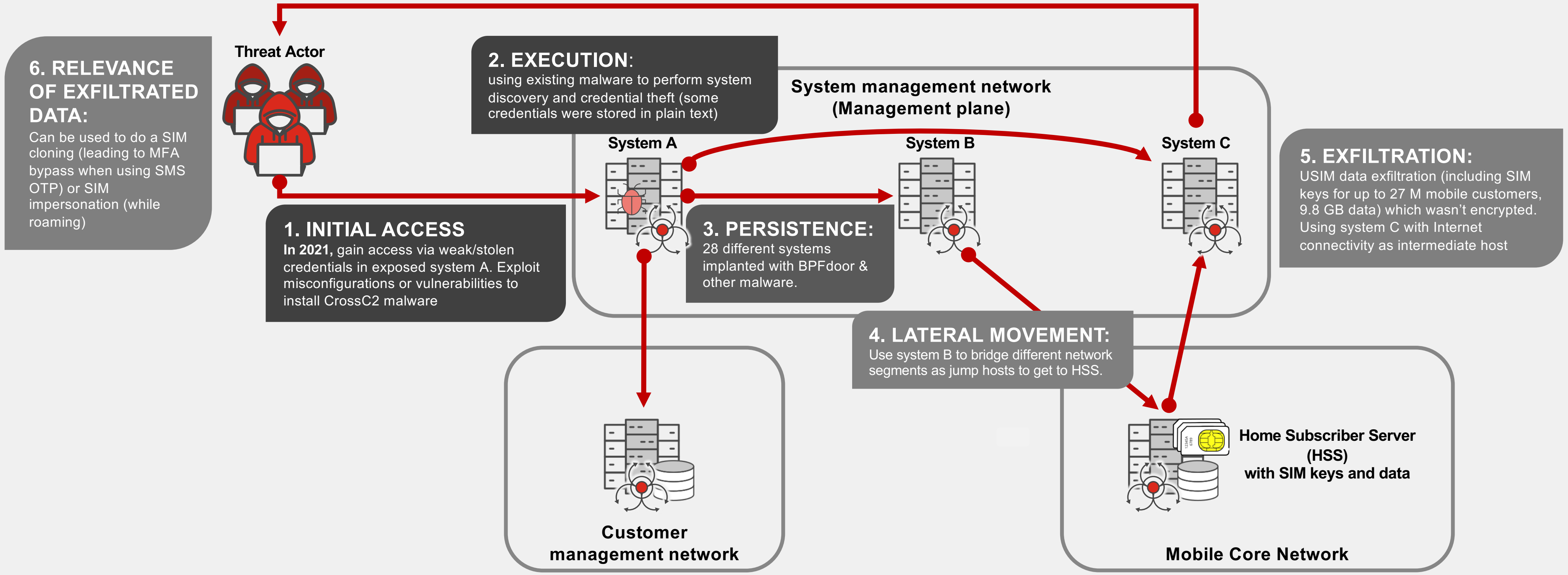
Financial

Espionage

Sabotage

Control

SK Telecom Attack – Simplified Overview



1. INITIAL ACCESS

In 2021, gain access via weak/stolen credentials in exposed system A. Exploit misconfigurations or vulnerabilities to install CrossC2 malware

2. EXECUTION:

using existing malware to perform system discovery and credential theft (some credentials were stored in plain text)

3. PERSISTENCE:

28 different systems implanted with BPFdoor & other malware.

4. LATERAL MOVEMENT:

Use system B to bridge different network segments as jump hosts to get to HSS.

5. EXFILTRATION:

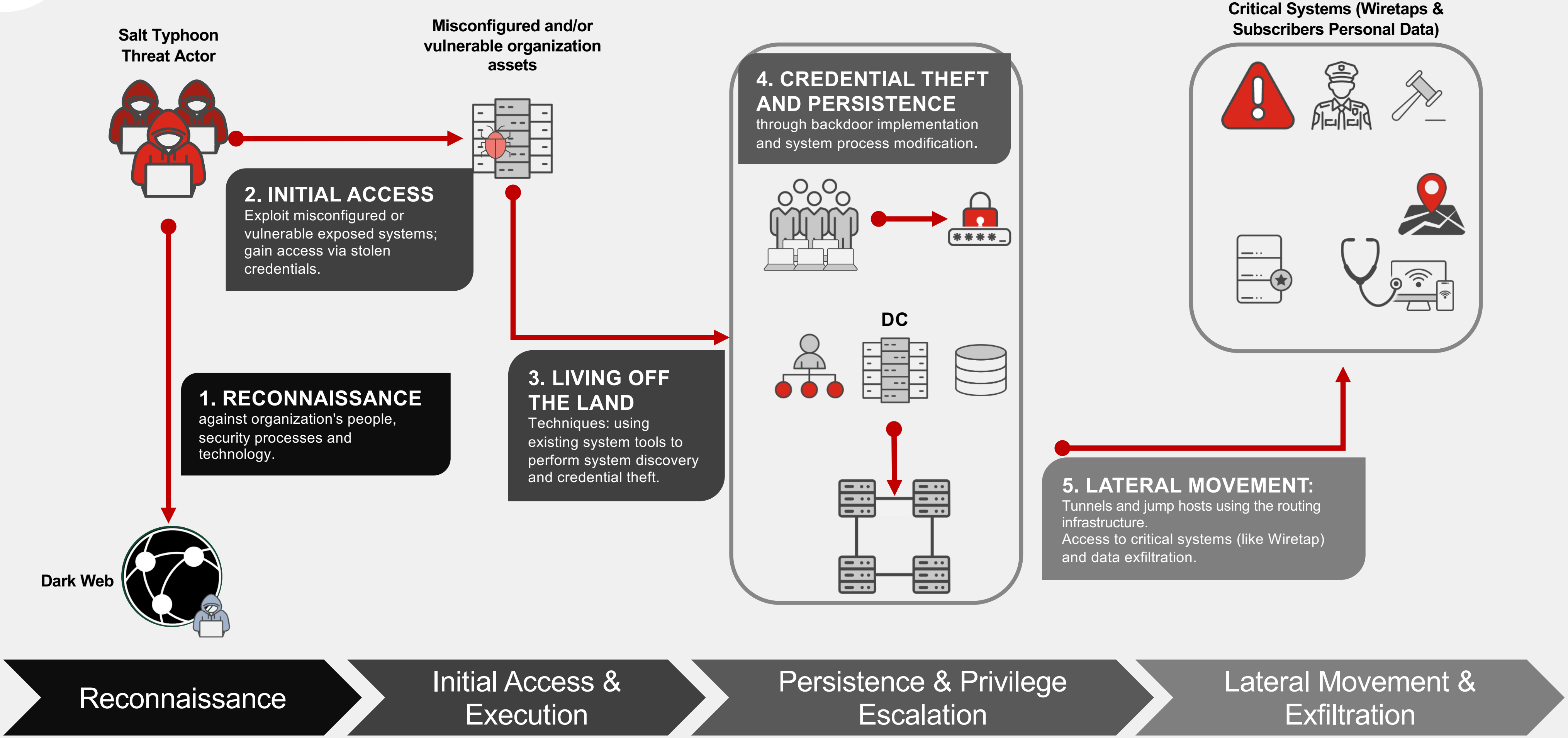
USIM data exfiltration (including SIM keys for up to 27 M mobile customers, 9.8 GB data) which wasn't encrypted. Using system C with Internet connectivity as intermediate host

6. RELEVANCE OF EXFILTRATED DATA:

Can be used to do a SIM cloning (leading to MFA bypass when using SMS OTP) or SIM impersonation (while roaming)

Reconnaissance → Initial Access & Execution → Persistence & Privilege Escalation → Lateral Movement & Exfiltration

SALT Typhoon Attack – Simplified Overview



Salt Typhoon Threat Actor

Misconfigured and/or vulnerable organization assets

2. INITIAL ACCESS
Exploit misconfigured or vulnerable exposed systems; gain access via stolen credentials.

1. RECONNAISSANCE
against organization's people, security processes and technology.

Dark Web

3. LIVING OFF THE LAND
Techniques: using existing system tools to perform system discovery and credential theft.

4. CREDENTIAL THEFT AND PERSISTENCE
through backdoor implementation and system process modification.

DC

Critical Systems (Wiretaps & Subscribers Personal Data)

5. LATERAL MOVEMENT:
Tunnels and jump hosts using the routing infrastructure.
Access to critical systems (like Wiretap) and data exfiltration.

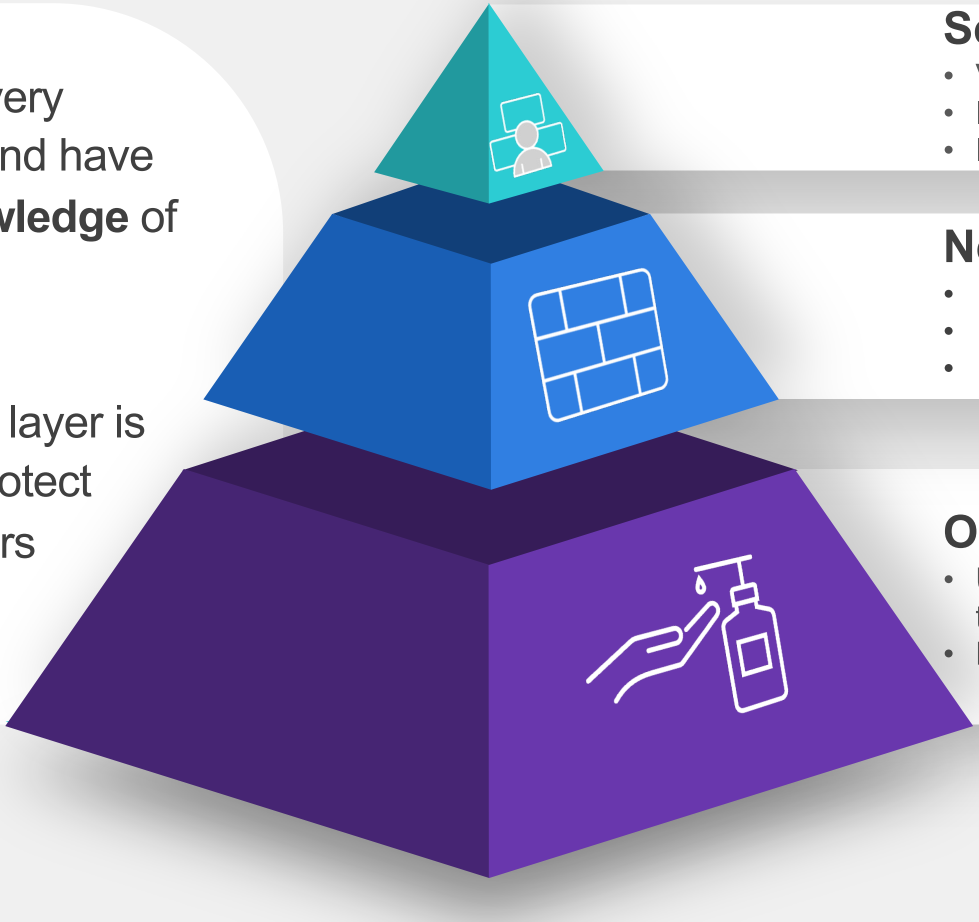
Reconnaissance → Initial Access & Execution → Persistence & Privilege Escalation → Lateral Movement & Exfiltration

How to Prevent APT Attacks (e.g. Salt Typhoon)

Layered approach

Opponents are very **sophisticated** and have **very good knowledge** of the network and equipment

A single security layer is not enough to protect the network, users and subscribers



Security Operations (SecOps)

- Visibility/detection (beyond NW & user protection)
- Incident response/mitigation & reporting
- Integration: One platform

Network, data & user protection

- Eliminate unnecessary attack vectors
- Detect threats
- Stop threats

Operator's security hygiene

- Users, teams, roles, credentials, vendor selection, trust zones, hardening, patching, procedures, …
- Hygiene is the basis for all other security layers

Operator’s Security Hygiene

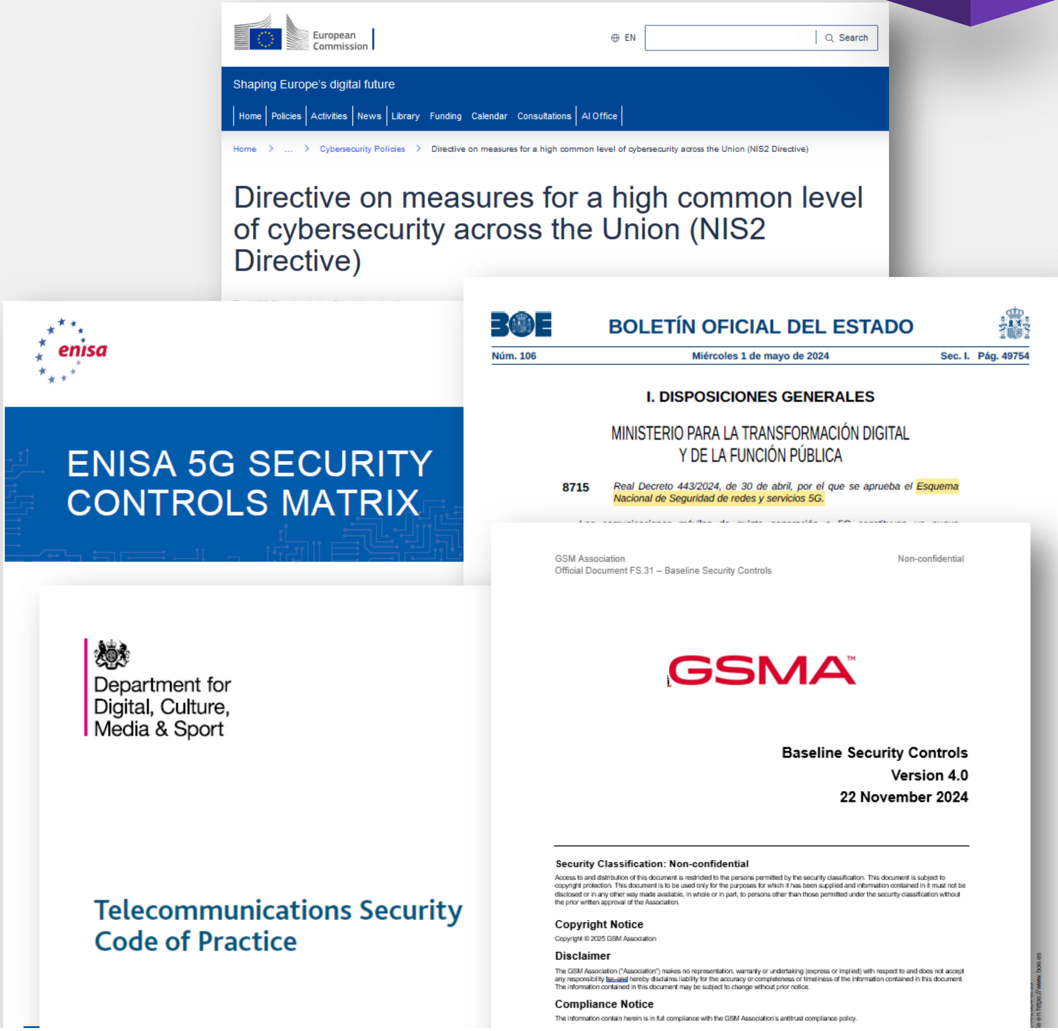
Regulation places this responsibility under the operator

Hygiene is key

- Without hygiene, nothing that is done in the other points works

Some obvious recommendations

- **Physical security**
- Select **reliable vendors** (who take security seriously)
- **Patch & harden** nodes (ASAP)
- Good **network design** (separate trust zones, avoid unnecessary exposure, …)
- Good **password management** (strong passwords, no password reuse, no default passwords, …)
- **Security procedures** (define roles and privileges, revoke credentials when employees leave, ...)



European Commission

EN Search

Shaping Europe's digital future

Home | Policies | Activities | News | Library Funding Calendar Consultations | AI Office

Home > ... > Cybersecurity Policies > Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)

Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)

enisa

ENISA 5G SECURITY CONTROLS MATRIX

BOE BOLETÍN OFICIAL DEL ESTADO

Núm. 106 Miércoles 1 de mayo de 2024 Sec. I. Pág. 49754

I. DISPOSICIONES GENERALES

MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL
Y DE LA FUNCIÓN PÚBLICA

8715 *Real Decreto 443/2024, de 30 de abril, por el que se aprueba el Esquema Nacional de Seguridad de redes y servicios 5G.*

Department for
Digital, Culture,
Media & Sport

Telecommunications Security
Code of Practice

GSM Association
Official Document FS.31 – Baseline Security Controls

Non-confidential

GSMA™

Baseline Security Controls
Version 4.0
22 November 2024

Security Classification: Non-confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Copyright © 2025 GSM Association

Disclaimer

The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Compliance Notice

The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

Secure Administrative Users

Management Plane Protection

1 Isolate the management plane

- Network infrastructure as **segmented** into security zones

2 Secure access to the management plane

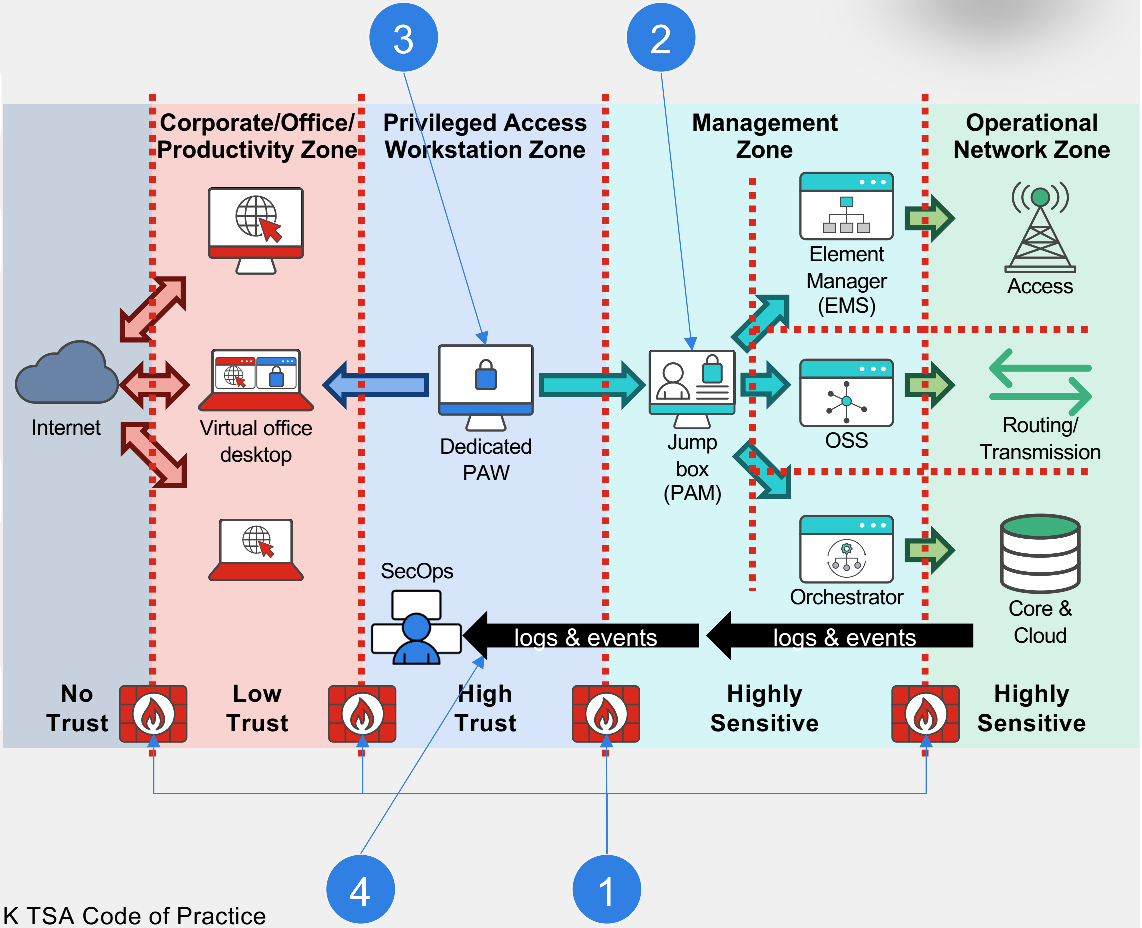
- Jump host or Privilege Access Management (**PAM**) to access management zone with **ZTNA**
- Strong credentials policies, Multi-factor authentication (**MFA**), Role-Based Access Control (**RBAC**)

3 Dedicated, secure workstation

- A Privileged Access Workstation (**PAW**) that can make changes to security critical functions
- Remote Browser Isolation (**RBI**) to secure the PAW

4 Read-only access

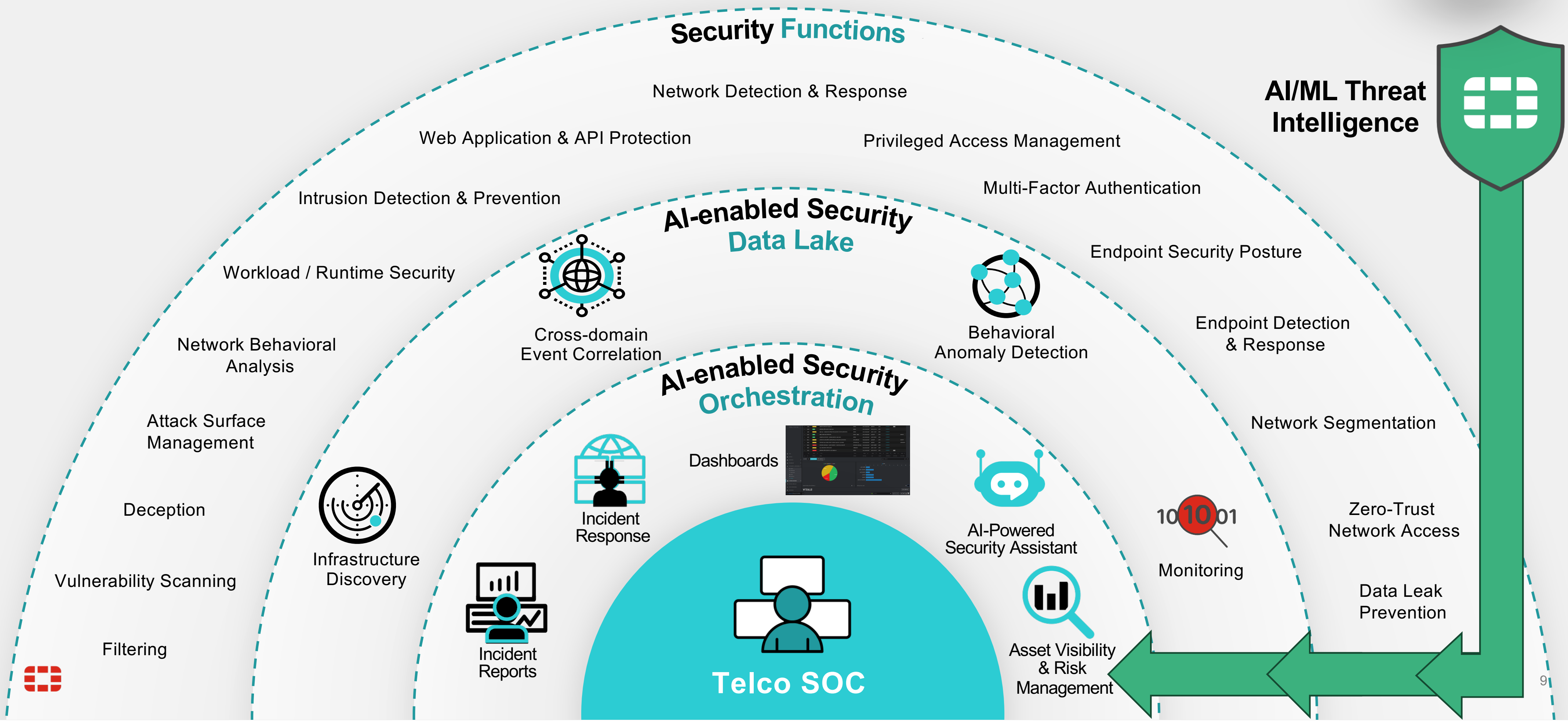
- Push logs and security events from network equipment to the lower trust zones. Process them in a **SecOps platform**



Based on UK TSA Code of Practice

Fortinet Telco SecOps Platform

Functional View



Security Functions

Network Detection & Response

Web Application & API Protection

Privileged Access Management

Intrusion Detection & Prevention

Multi-Factor Authentication

Workload / Runtime Security

Endpoint Security Posture

Network Behavioral Analysis

Endpoint Detection & Response

Attack Surface Management

Network Segmentation

Deception

Zero-Trust Network Access

Vulnerability Scanning

Data Leak Prevention

Filtering

AI-enabled Security Data Lake

Cross-domain Event Correlation

Behavioral Anomaly Detection

Infrastructure Discovery

Monitoring

AI-enabled Security Orchestration

Dashboards

Incident Response

AI-Powered Security Assistant

Incident Reports

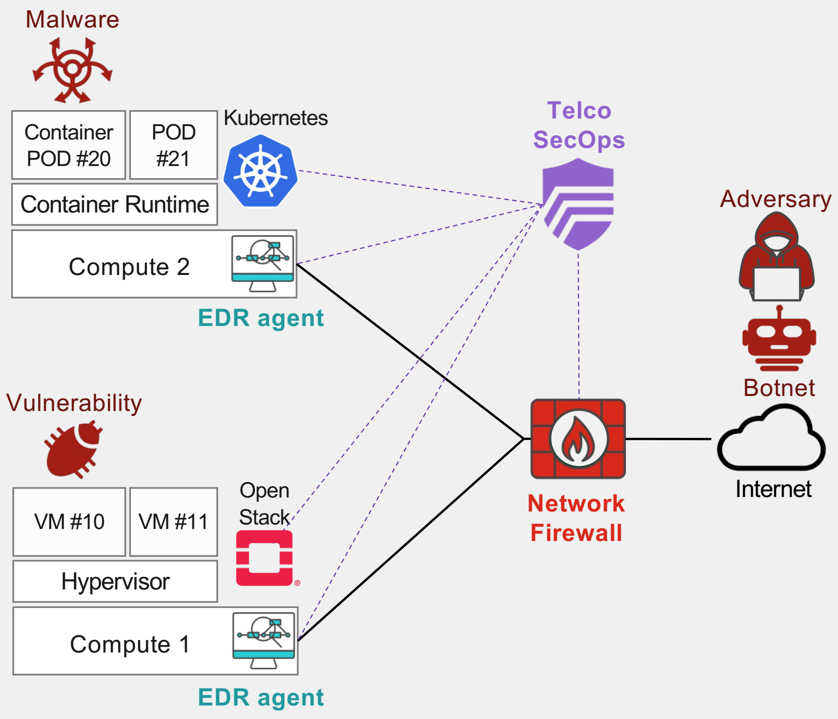
Asset Visibility & Risk Management

Telco SOC

AI/ML Threat Intelligence

Firewall + EDR + SecOps

Multi-Layer Telco Security



Network Firewall (NW Security)

- Sees in-flight packets
- Complete visibility of the network traffic
- Can detect and block external attacks, C&C channel, DDoS attacks, …

EDR Agents (Host Security)

- Sees files, memory, network sockets, … in the compute node where it is installed
- Can detect and block ransomware file encryption, execution of malware, …

Telco Security Operations

- Sees events from all network (logs, traces, …)
- Correlates the events between domains
- Performs behavioral analysis
- Acts upon detected threats

When Telco Vendors Don’t Accept Agents

Cannot run an EDR on their server

1 If you cannot check inside, use deception

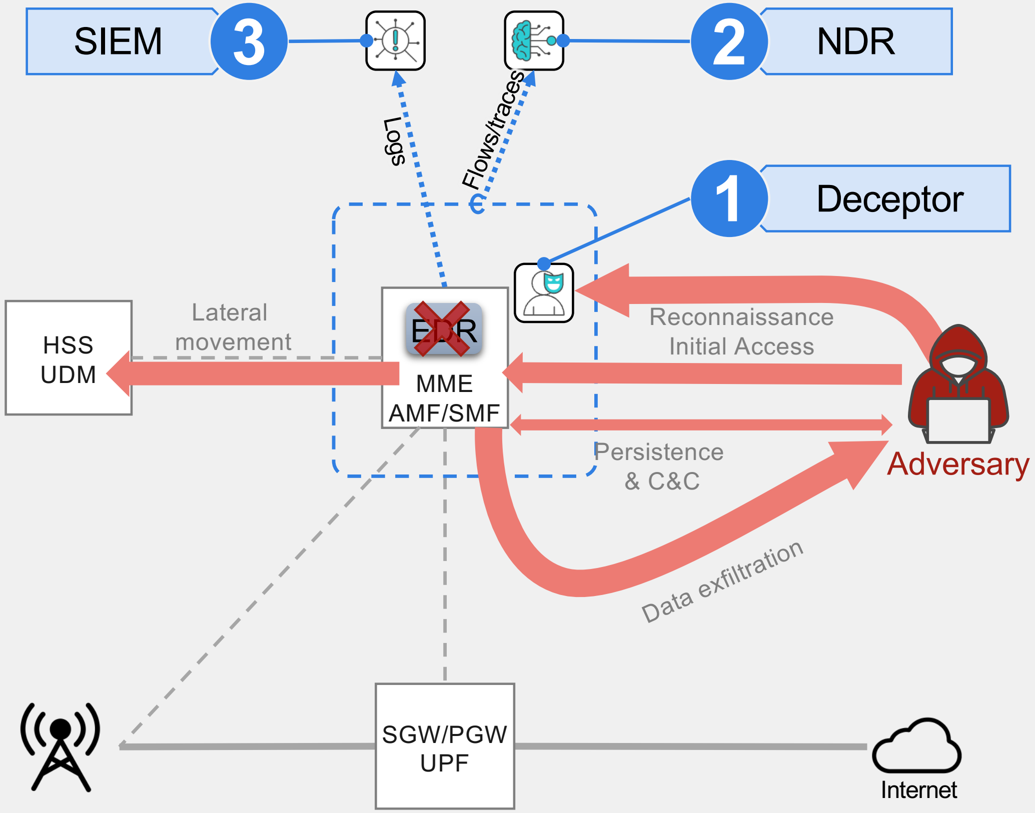
- Credible decoys in the network to deceive the attacker
  - Place lures and breadcrumbs to attract the attacker (e.g., announce it in the DNS or NRF as a test node)
  - Learn from the attack and the techniques used
- **FortiDeceptor**

2 If you cannot check inside, check its traffic

- Tap on the traffic that is coming in and out of the nodes (Specially the management plane)
  - Analyze traffic for unexpected protocols or parameters
  - Analyze the behavior for anomalies using AI/ML
- **FortiNDR**

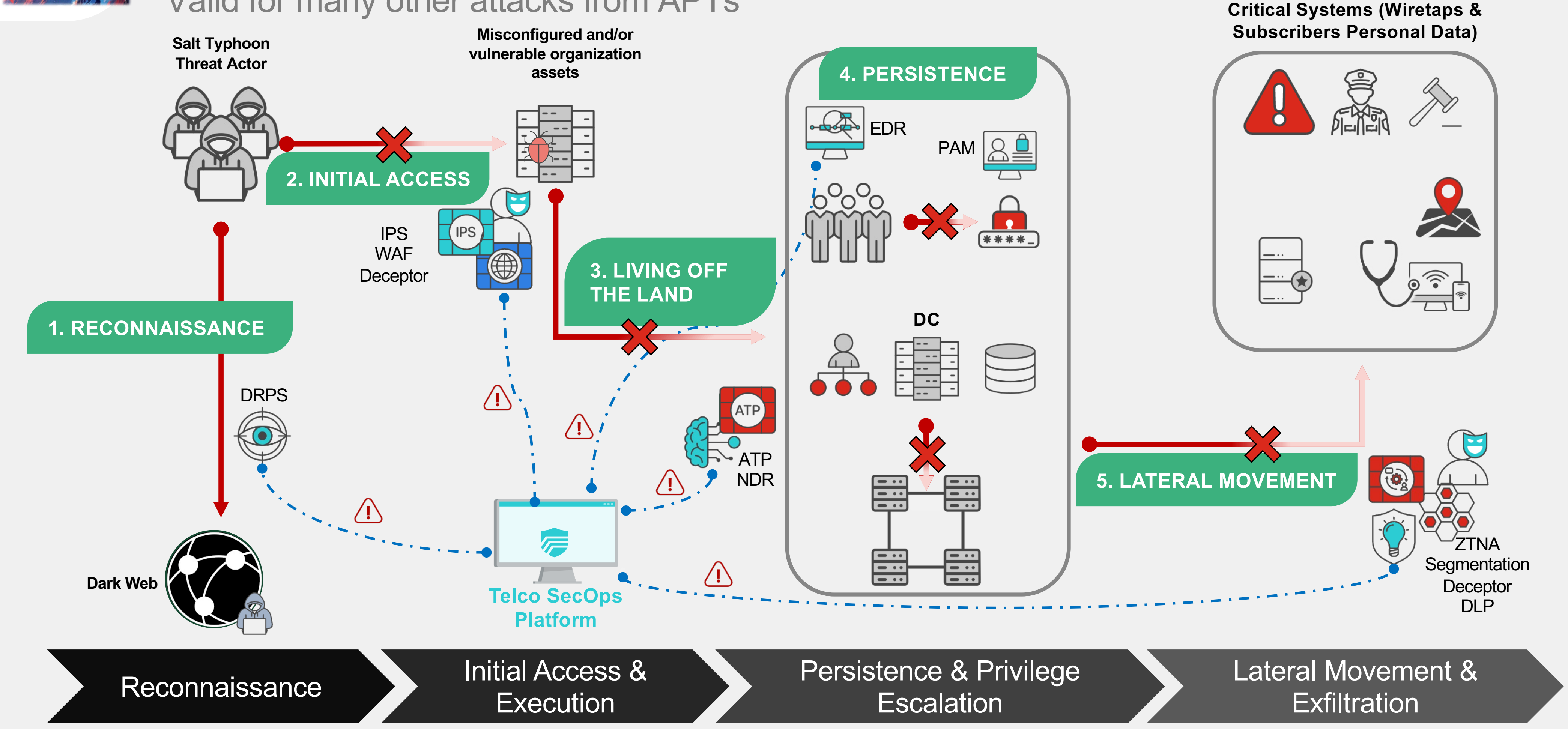
3 If you cannot check inside, check its logs

- These nodes generate logs continuously
  - Analyze them for security events, anomalies, and abnormal behavior using AI/ML
- **FortiSIEM**



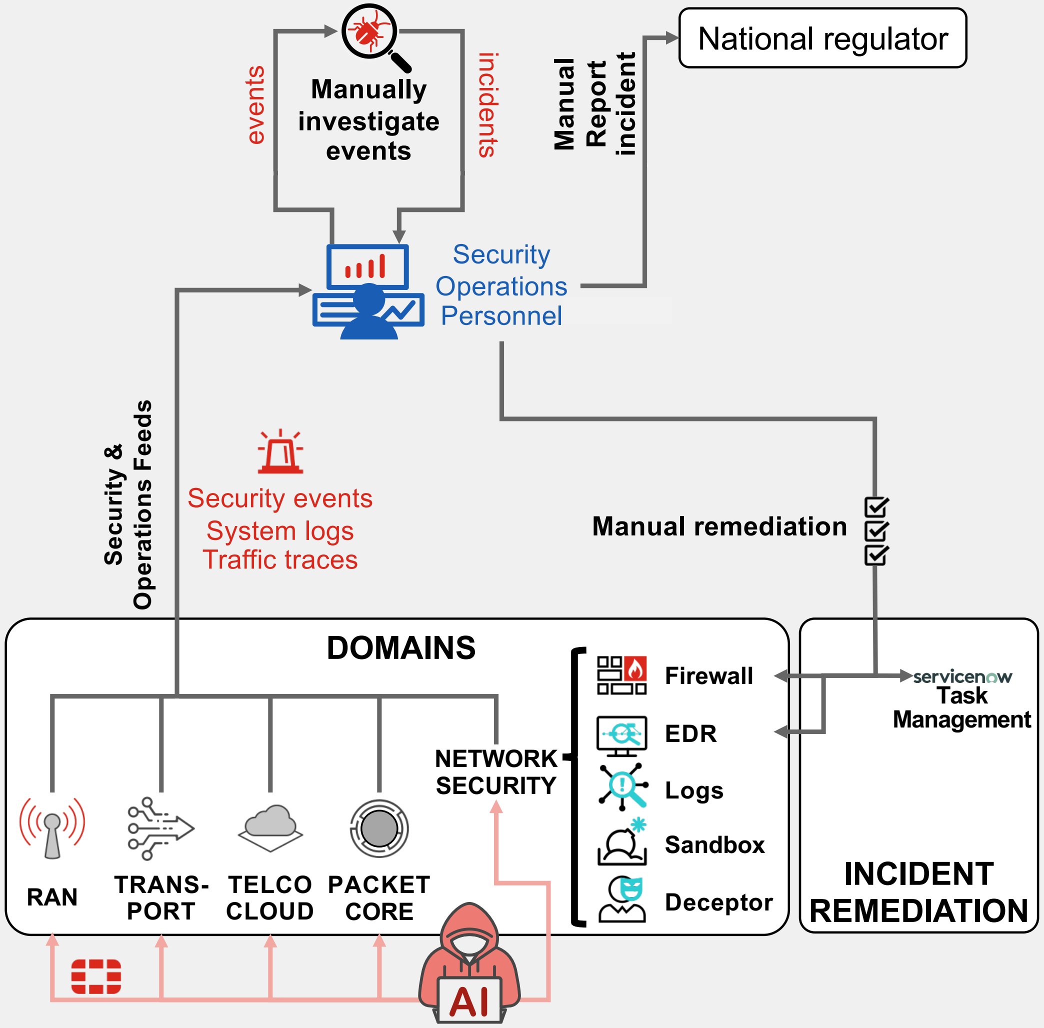
Salt Typhoon Attack with Telco SecOps Platform

Valid for many other attacks from APTs



Traditional Security Operations

A slow, manual process that does not meet the new regulatory timeframes



events

Manually investigate events

incidents

Manual Report incident

National regulator

Security Operations Personnel

Security & Operations Feeds

Security events
System logs
Traffic traces

Manual remediation

DOMAINS

RAN

TRANS-PORT

TELCO CLOUD

PACKET CORE

NETWORK SECURITY

Firewall

EDR

Logs

Sandbox

Deceptor

servicenow Task Management

INCIDENT REMEDIATION

Regulation

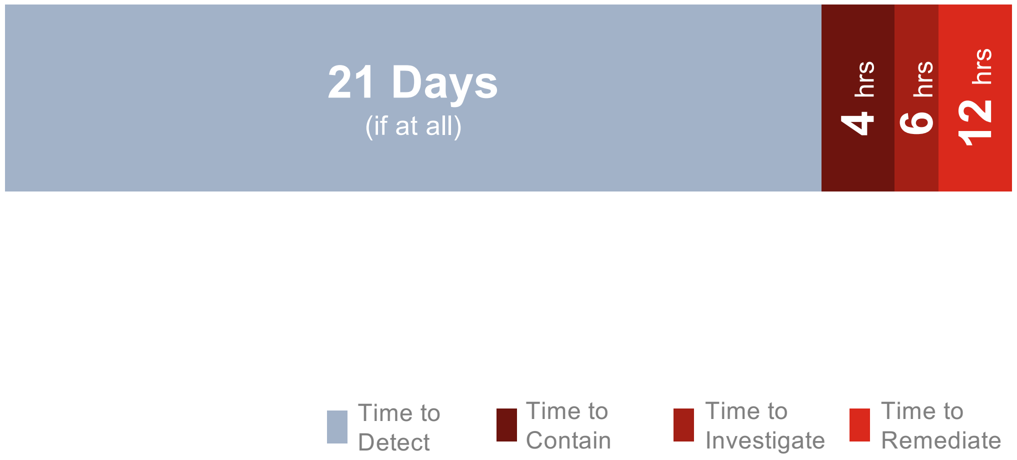
NIS2:
- Initial incident report to national CSIRT within 72h
- Final incident report to national CSIRT within 1 month

SEC:
- Per-incident report to SEC within 4 days

CISA:
- Remediate known exploited vulnerabilities within 14 days
- Remediate critical vulnerabilities within 15 days

Before

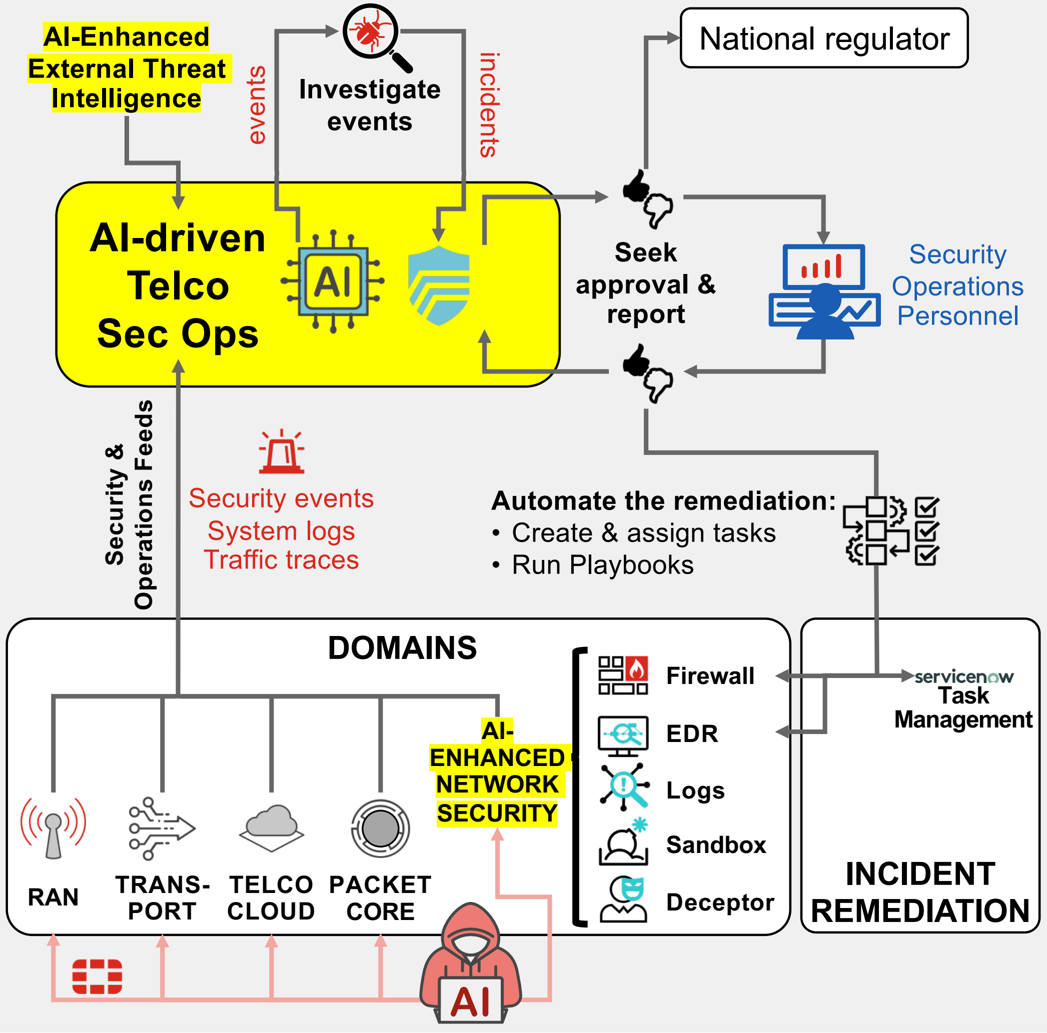
Manual incident response and reporting



Source: Enterprise Strategy Group, a division of Tech Target, Inc.

AI-Driven Security for Service Providers

Use AI to cope with complexity, sophistication and wealth of data



AI-Enhanced External Threat Intelligence

events

Investigate events

incidents

National regulator

AI-driven Telco Sec Ops

Seek approval & report

Security Operations Personnel

Security & Operations Feeds

Security events
System logs
Traffic traces

Automate the remediation:
- Create & assign tasks
- Run Playbooks

DOMAINS

RAN

TRANS-PORT

TELCO CLOUD

PACKET CORE

AI-ENHANCED NETWORK SECURITY

Firewall

EDR

Logs

Sandbox

Deceptor

servicenow Task Management

INCIDENT REMEDIATION

AI

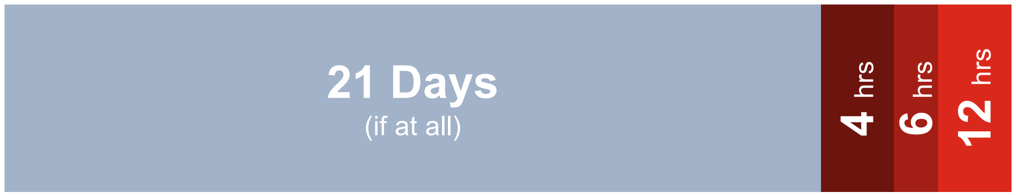
Regulation

NIS2:
- Initial incident report to national CSIRT within 72h
- Final incident report to national CSIRT within 1 month

SEC:
- Per-incident report to SEC within 4 days
- Annual report on cybersecurity risk management, strategy, and governance.

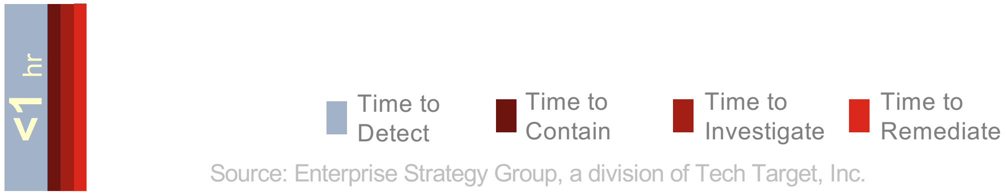
Before

Manual incident response and reporting



After

AI-driven Telco Sec Ops



Source: Enterprise Strategy Group, a division of Tech Target, Inc.

FORTINET