Govern d'Andorra

ANDORRA DIGITAL

ANC AD

2ª Jornada CISO

Protecció de la cadena de subministrament i risc digital

Joan Ruiz

1 de Març de 2024

Agenda

1. Organitzacions Cibercriminals i actors “state-sponsored”
2. Atacs a la cadena de suministrament
3. Noves regulacions i ciberseguretat en la cadena de suministrament
4. Estratègies i casos d’ús per la protecció de la cadena de suministrament i la gestió del risc digital

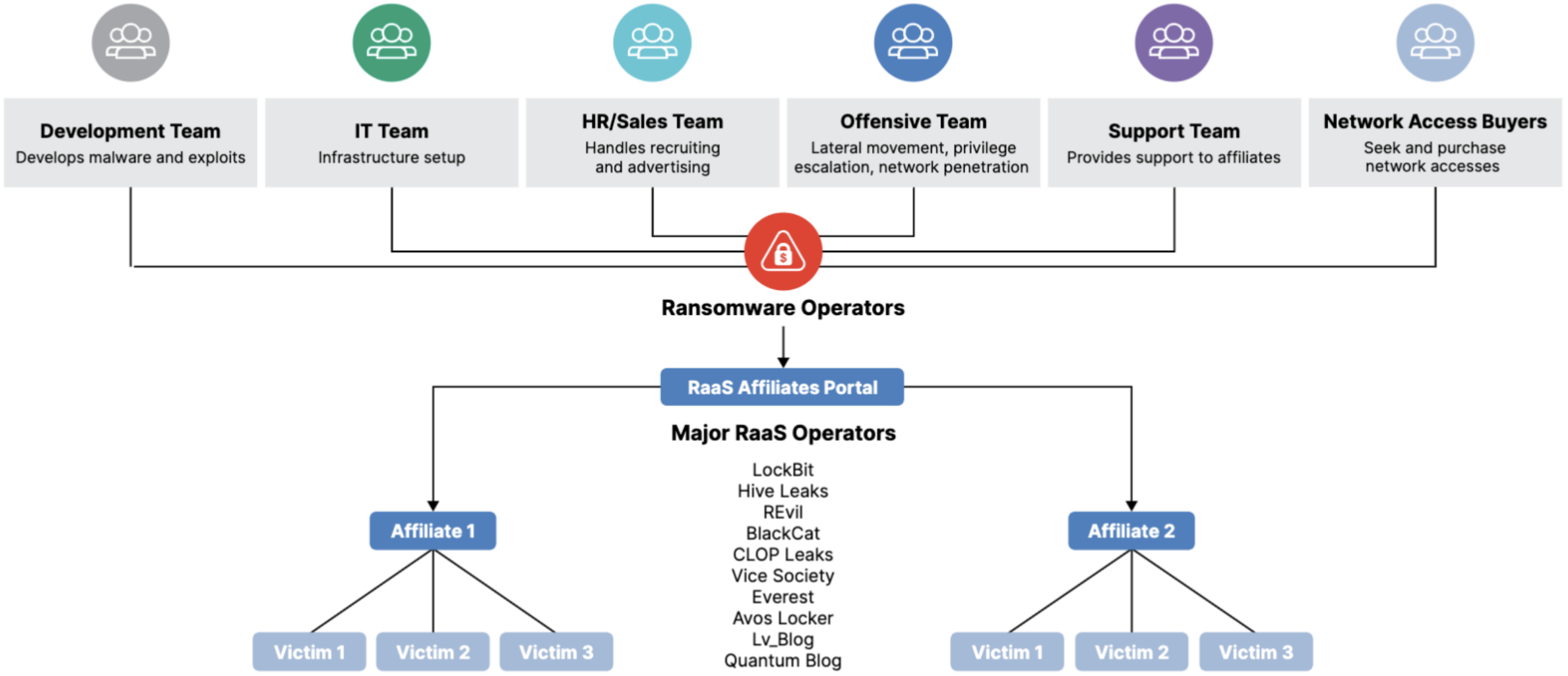
Organitzacions Cibercriminals i actors “State-sponsored”


LAZARUS
HACKER GROUPS
THE EQUATION GROUP
CYBER SECURITY TRAINING
& CONSULTING LLC
THE SHADOW BROKERS
72
Hf
Hafnium
178.490
LOCKBIT 3.0
CLOP
Volt Typhoon
CONTI

Directory: Conti/

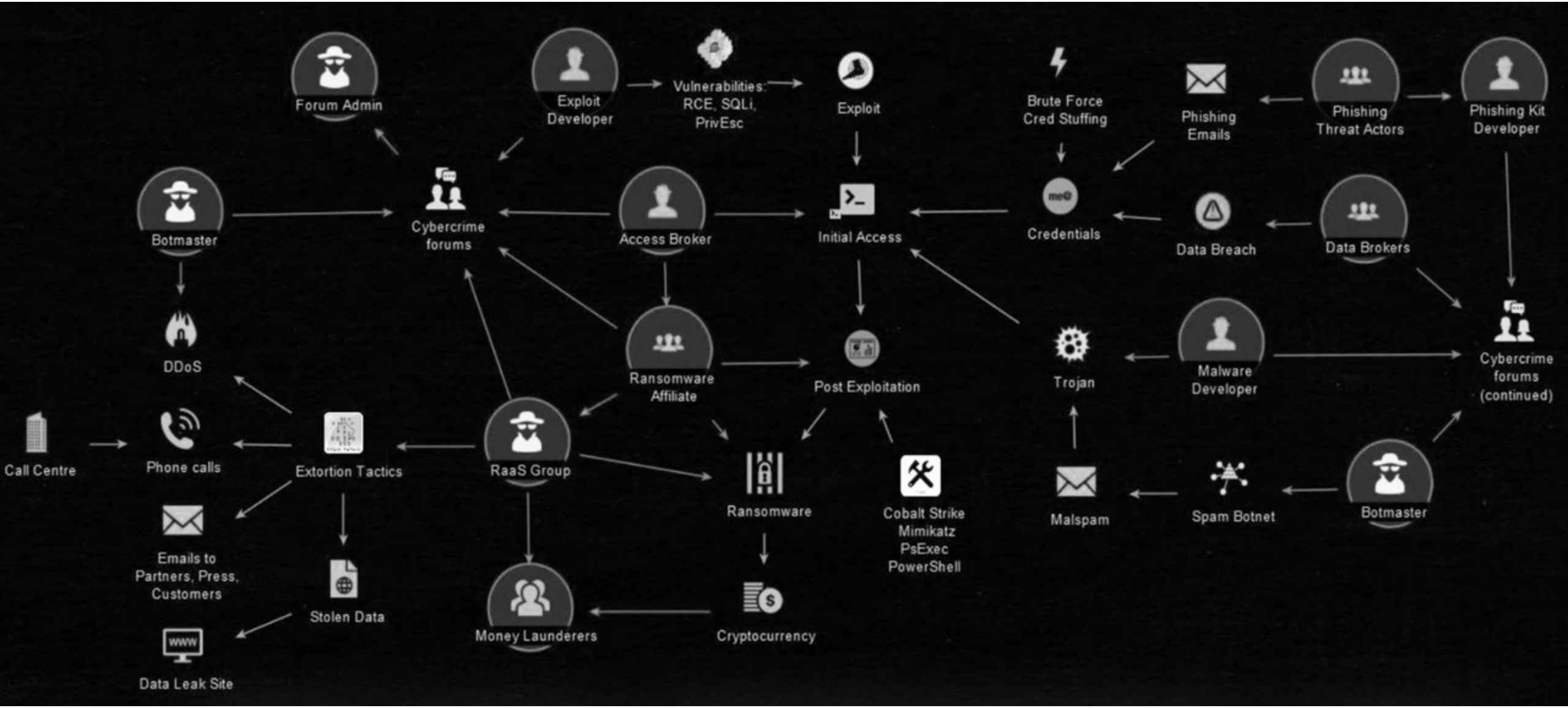
File Name ↓	File Size ↓	Date ↓
Parent directory/	-	-
Conti Chat Logs 2020.7z	2417273	2022-03-01 02:46:14
Conti Documentation Leak.7z	234714	2022-03-01 05:29:38
Conti Internal Software Leak.7z	3911885	2022-03-01 02:57:08
Conti Jabber Chat Logs 2021 - 2022.7z	1160294	2022-03-02 13:10:39
Conti Locker Leak.7z	6852466	2022-03-05 04:29:03
Conti Pony Leak 2016.7z	62014991	2022-03-01 02:51:14
Conti Rocket Chat Leaks.7z	3370574	2022-03-01 02:47:40
Conti Screenshots December 2021.7z	452894	2022-03-01 02:46:06
Conti Source Code Version 3.7z	619761	2022-03-20 09:34:51
Conti Toolkit Leak.7z	94186791	2022-03-01 02:42:15
Conti Trickbot Forum Leak.7z	8542211	2022-03-01 02:50:56

RaaS Organization

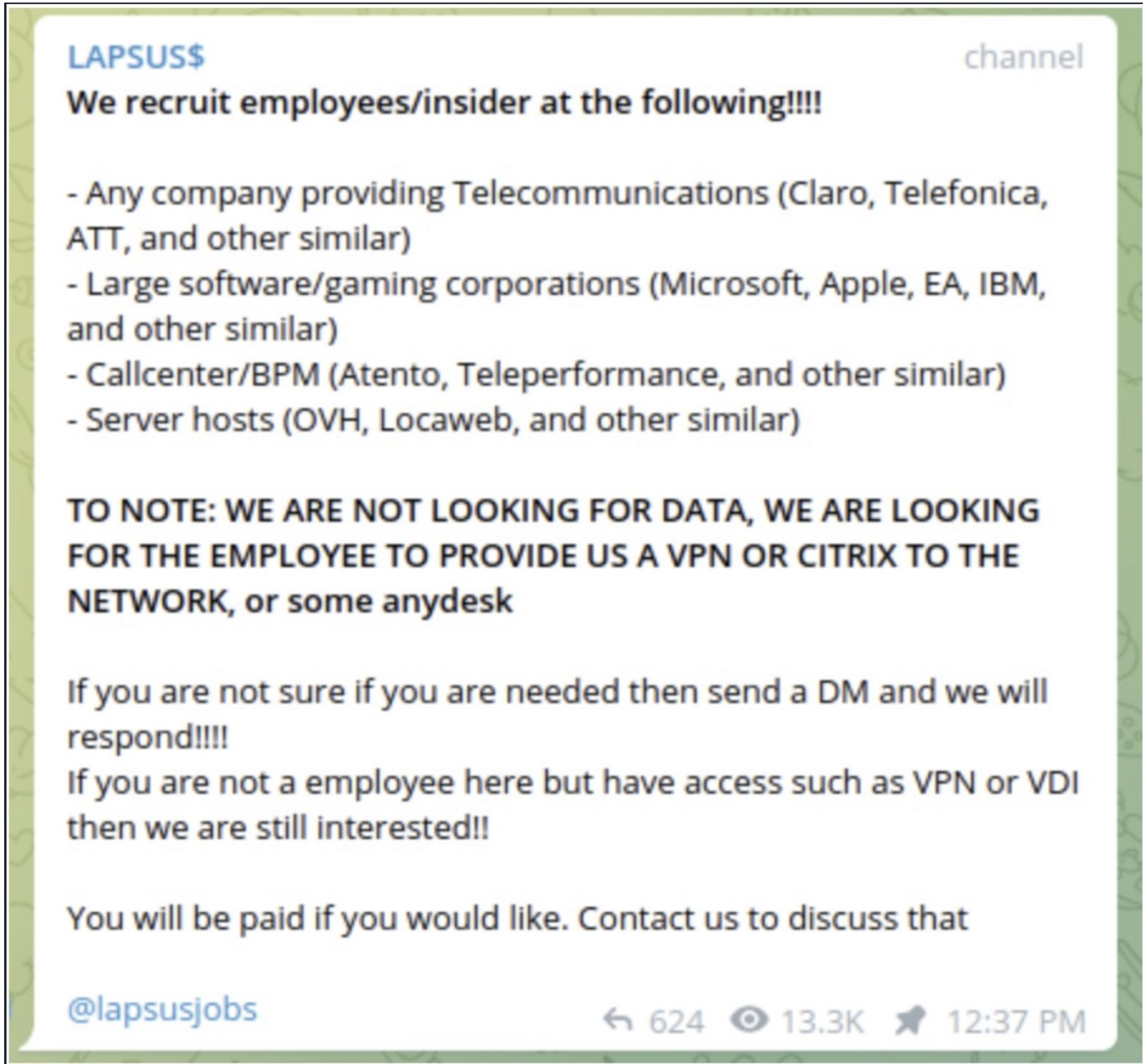


Anatomy Of The Ransomware Cybercrime Economy

Image credits: Will @BushidoToken



Lapsus jobs



LAPSUS$ channel

We recruit employees/insider at the following!!!!

- Any company providing Telecommunications (Claro, Telefonica, ATT, and other similar)
- Large software/gaming corporations (Microsoft, Apple, EA, IBM, and other similar)
- Callcenter/BPM (Atento, Teleperformance, and other similar)
- Server hosts (OVH, Locaweb, and other similar)

TO NOTE: WE ARE NOT LOOKING FOR DATA, WE ARE LOOKING FOR THE EMPLOYEE TO PROVIDE US A VPN OR CITRIX TO THE NETWORK, or some anydesk

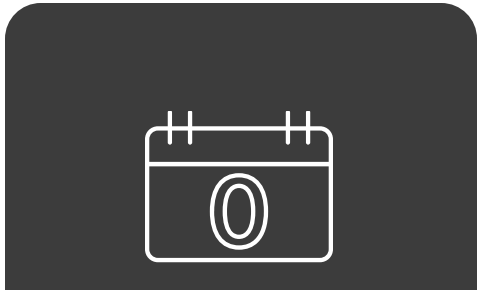
If you are not sure if you are needed then send a DM and we will respond!!!!
If you are not a employee here but have access such as VPN or VDI then we are still interested!!

You will be paid if you would like. Contact us to discuss that

@lapsusjobs 624 13.3K 12:37 PM

State-Nation Sponsored actors

Una visió actualitzada al panorama de ciberamenaces



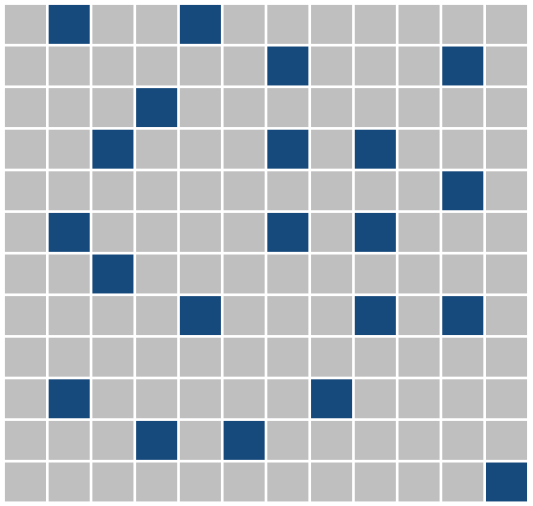
Advanced Persistent Threat Actors

More Nation State Attacks

- Intellectual Property
- Financial Gain
- Terrorism
- Political Espionage
- Hacktivism

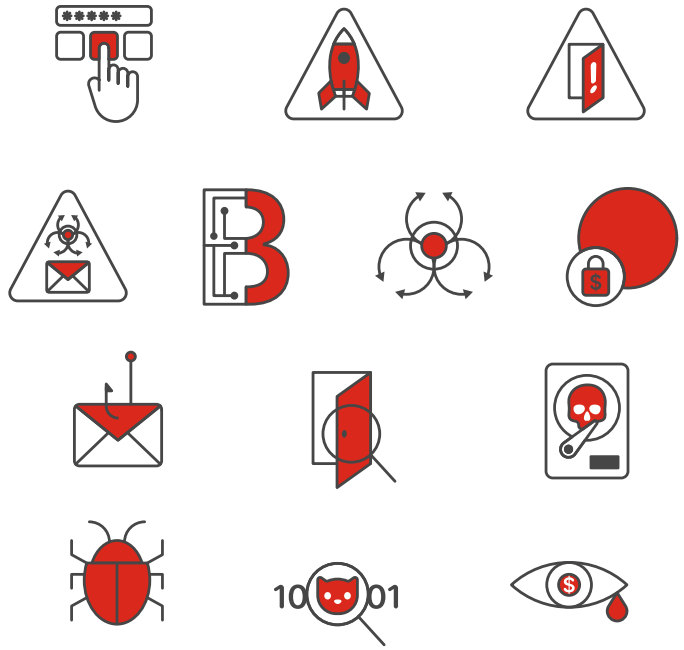
Nation states have different motives

More APT Groups Active



30% of APT groups were detected as active in just the 1H 2023

More Sophistication



Threat actors are expanding their playbooks

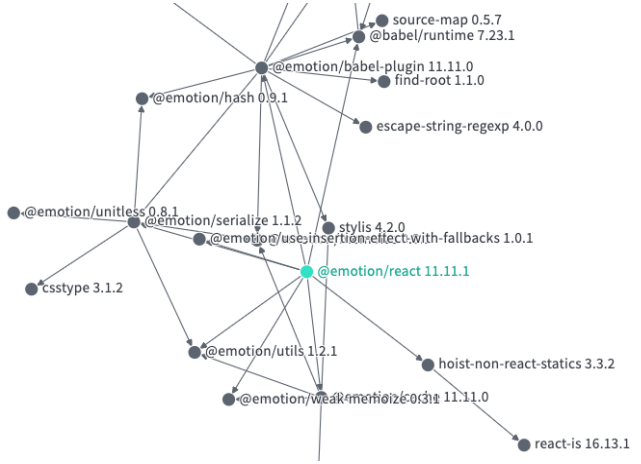
Supply Chain Attacks

Open Source Software is Leveraged Everywhere

The building blocks of modern enterprise applications

Most Apps Have Many Direct and Indirect Dependencies

They all come with the potential for vulnerabilities



Vulnerabilities in Widely Used Components Hit Hard and Fast

Multiple threat actors jump in with their own attacks

Addressing Cybersecurity Challenges in Open Source Software - Report.pdf (hubspotusercontent-na1.net)

Atacs a la cadena de suministrament

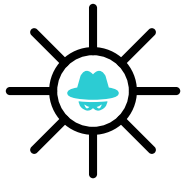
Supply Chain Attack Trend

- Supply Chain Cybersecurity Gap

Supply Chain Cybersecurity Gap

Nation state and supply chain attacks are happening with increased frequency and become more sophisticated.

SolarWinds
(Dec 2020)



Sunburst, Teardrop, Raindrop Malware *Hack*

Attackers gained access to SolarWinds infrastructure by exploiting an Authentication Service vulnerability.

Colonial Pipeline
(May 6 2021)

DarkSide *Ransomware*

Operation Technology Attack. Covid 19 has accelerated the removal of the air gap for remote access

Microsoft Exchange
(Jan 6 2021)

HAFNIUM *Zero Day* DearCry *Ransomware*

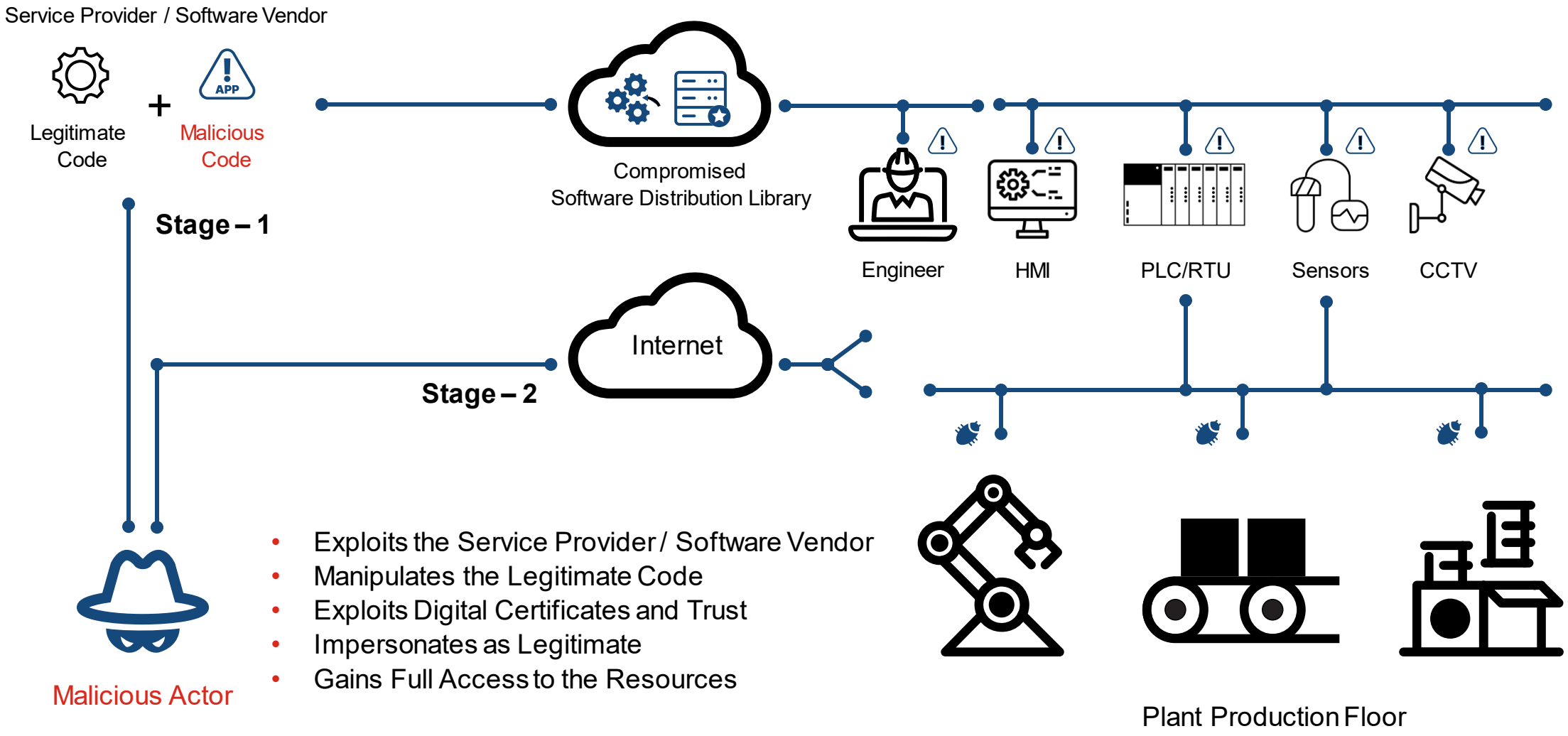
The original Zero Day was used by the HAFNIUM group for global Ransomware campaign

F5 Big IP
(March 10 2021)

F5 Vulnerability

F5 reported several new vulnerabilities under attack, urged immediate upgrades.

Anatomy of Supply Chain Attack



- Exploits the Service Provider / Software Vendor
- Manipulates the Legitimate Code
- Exploits Digital Certificates and Trust
- Impersonates as Legitimate
- Gains Full Access to the Resources

Solarwinds suppy attack lifecycle

- The SolarWinds cyber attack timeline stretched out over six months, during which time the hackers patiently and systematically executed their hack. Here are the most critical milestones in the attack:
- In September 2019, hackers were able to access the SolarWinds network.
- They started testing their code injection in Orion in October 2019.
- About four months later, they injected malicious code called Sunburst into Orion.
- On March 26, 2020, SolarWinds began distributing Orion updates that contained the hackers' malicious code.
- The malware spread as thousands of SolarWinds customers installed the malicious code in the hacked update. Once on a victim's system, the malware gave hackers access to customer IT systems. At this point, the attackers could install more malware, which enabled them to spy on additional organizations.

https://www.fortinet.com/resources/cyberglossary/solarwinds-cyber-attack#:~:text=The%20SolarWinds%20assault%20was%20a,third%2Dparty%20supplier%20was%20SolarWinds.

100+ Hospitals and Healthcare sites hit by ransomware in Romania

bd2c2cf0631d881ed382817afcce2b093f4e412ffb170a719e2762f250abfea4 **ProcessHacker.exe**

8bae7326cb8456ce4c9409045264ca965e30f6381ddcaa6c87ba3ac5e7683555 **pw-inspector.exe**

57c56f7b312dc1f759e6ad039aac3f36ce5130d259eb9faad77239083398308b **SbieSupport.dll**

5713d40dec146dbc819230daefe1b886fa6d6f6dbd619301bb8899562195cbab **ToolStatus.dll**

0c11cdc3765ffb53ba9707b6f99ec17ae4f7334578a935ba7bcbbc9c7bdeed2e **Updater.dll**

fc9d0d0482c63ab7f238bc157c3c0fed97951ccf2d2e45be45c06c426c72cb52 **UserNotes.dll**

282696487ea5dc781788d5d8477b977f72b7c70f201c2af0cfe7e1a9fd8d749a **WindowExplorer.dll**

e71cda5e7c018f18aefcdfbce171cfeee7b8d556e5036d8b8f0864efc5f2156b **BulletsPassView64.exe**

b19dfe440e515c39928b475a946656a12b1051e98e0df36c016586b34a766d5c **BulletsPassView.exe**

c4304f7bb6ef66c0676c6b94d25d3f15404883baa773e94f325d8126908e1677 **ChromePass.exe**

598555a7e053c7456ee8a06a892309386e69d473c73284de9bbc0ba73b17e70a **Dialupass.exe**

dbe98193aced7285a01c18b7da8e4540fb4e5b0625debcfbabcab7ea90f5685d **iepv.exe**

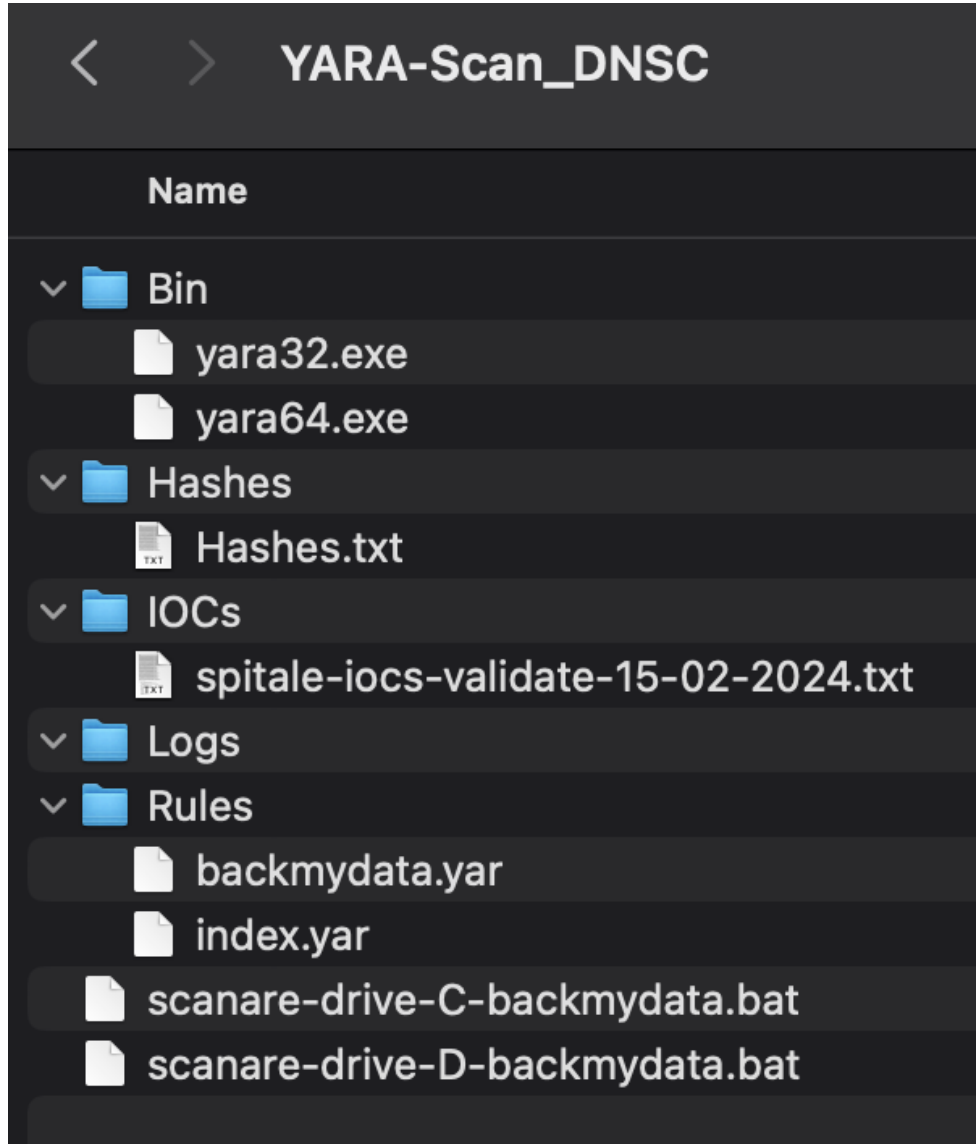
16c6af4ae2d8ca8e7a3f2051b913fa1cb7e1fbd0110b0736614a1e02bbbbceaf **mailpv.exe**

d032001eab6cad4fbef19aab418650ded00152143bd14507e17d62748297c23f **mimidrv_32.sys**

d43520128871c83b904f3136542ea46644ac81a62d51ae9d3c3a3f32405aad96 **mimidrv.sys**

66b4a0681cae02c302a9b6f1d611ac2df8c519d6024abdb506b4b166b93f636a **mimik_32.exe**

31eb1de7e840a342fd468e558e5ab627bcb4c542a8fe01aec4d5ba01d539a0fc **mimik.exe**



Noves regulacions i ciberseguretat en la cadena de suministrament


NIS2
DIRECTIVE

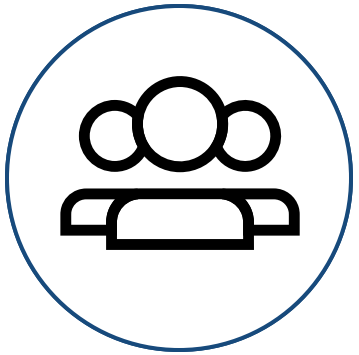
NIS2 – Accions clau

1. Disposar de Política de Seguretat de la iniformació I gestió proactiva del risc
2. Implantar estratègies de Prevenció, Detecció I Resposta d'incidents de ciberseguretat
3. Disposar de mecanismes de continuitat de negoci davant de ciberatacs
4. Obligació de notificar incidents a les autoritats en base a un calendari definit
5. Us d'encriptació a les comunicacions
6. Us d'autenticació forta i multiples factors d'autenticació
7. Seguretat dels proveidors i de la cadena de suministrament
8. Revelació de vulnerabilitats
9. Col·laboració amb les autoritats locals, nacionals i europees (EU-CyCLONe)
10. Multes per incumpliment

L'equip directiu pot ser considerat peresonalment responsable d'incomplir amb NIS2

Estratègies i casos d'ús per la protecció de la cadena de suministrament i la gestió del risc digital

Holistic Approach to Cybersecurity—Security Program

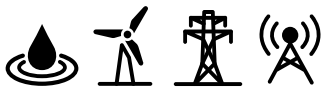


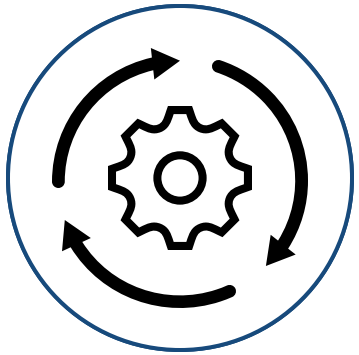
People

Security Governance

Security Awareness

Security Culture



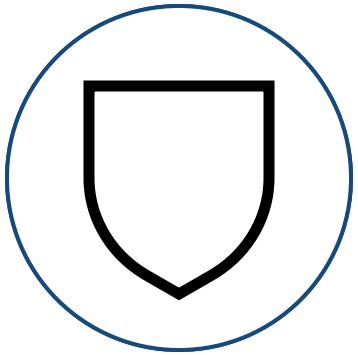


Process

Risk Assessment

Security Architecture

Compliance Audits



Technology

Visibility

Control

Actionable Intelligence

NIS2

CRA

MACHINERY ACT

ISO

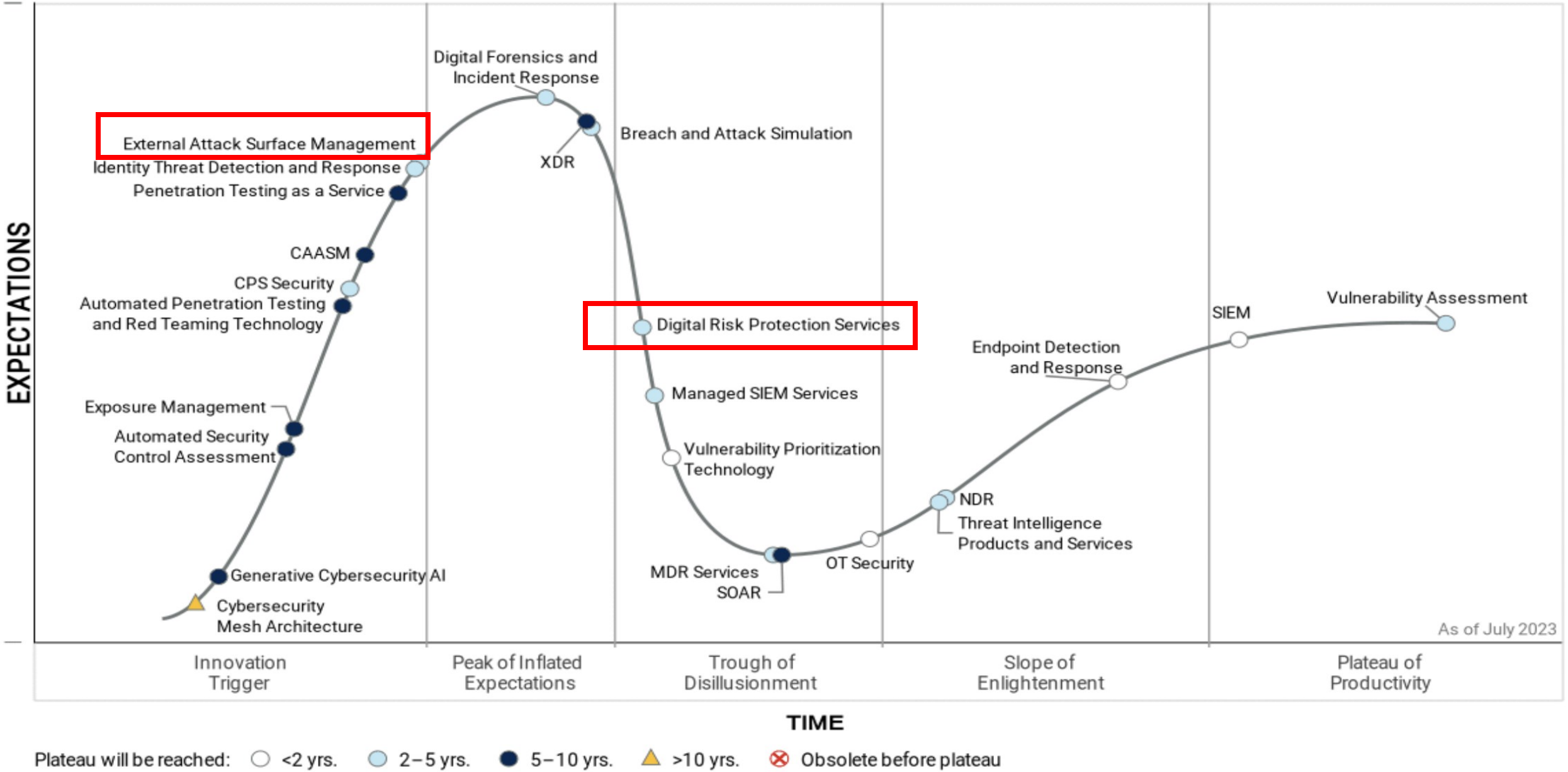
Manage Risk

Business Context

Automate Operations

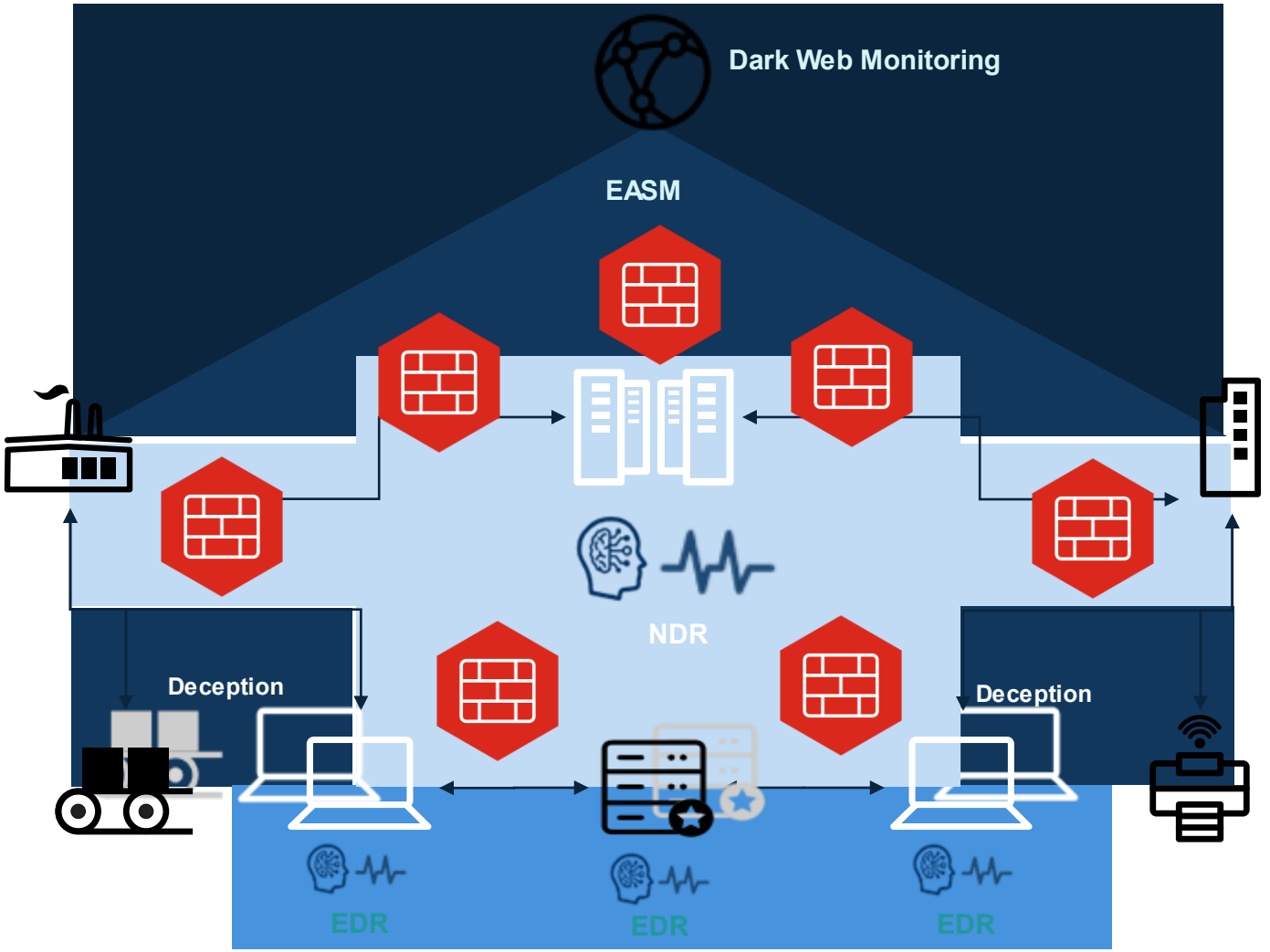
Technical Context

Hype Cycle for Security Operations, 2023



Gartner

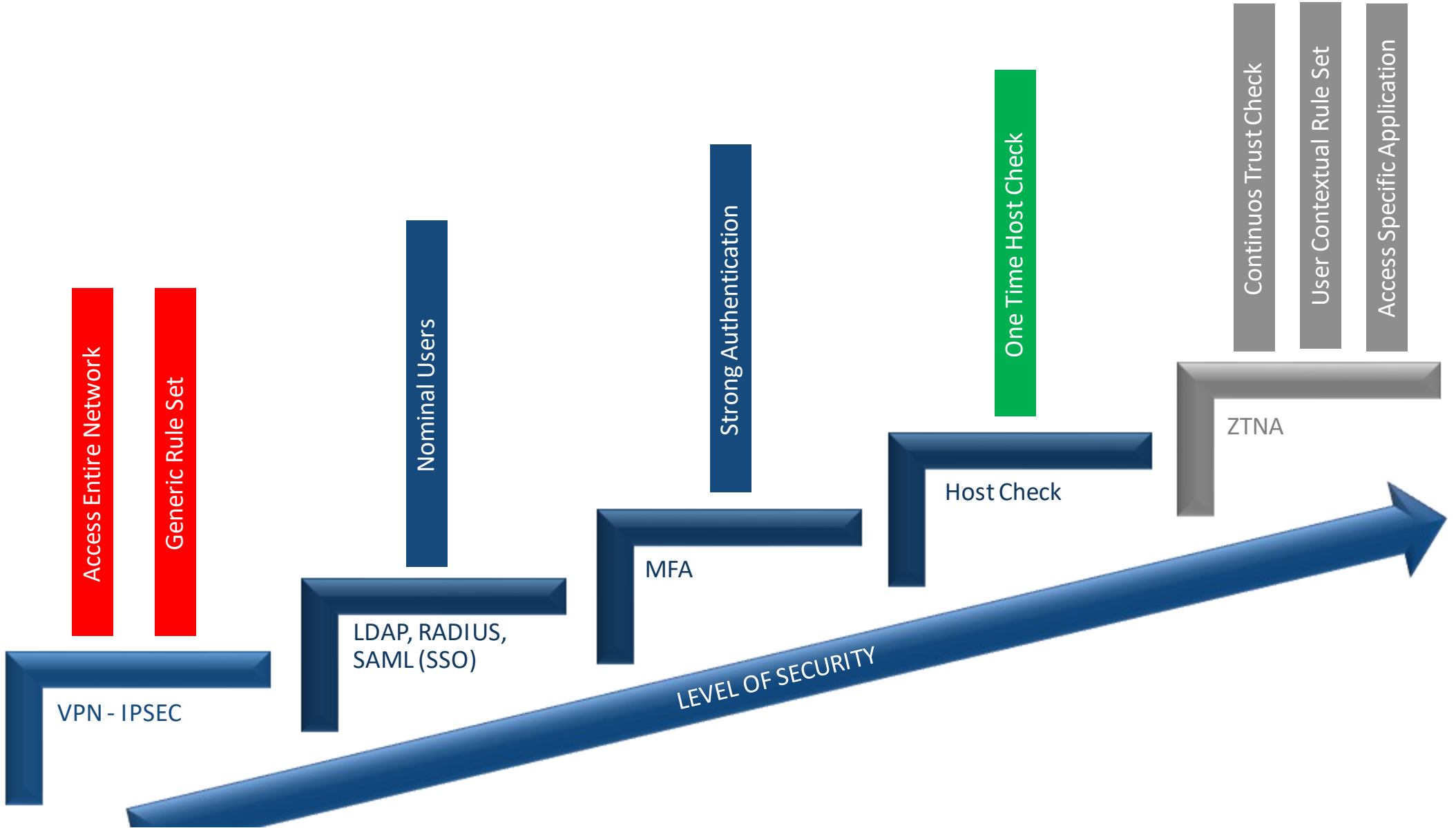
Detecció i protecció d'amenaces, estratègia general



Estratègies i casos d'ús per la protecció de la cadena de suministrament i la gestió del risc digital

Accés remot de proveïdors

Estratègia zero trust per accés remot de proveïdors



Estratègia Zero Trust

Zero trust is a **cybersecurity paradigm** focused on resource protection and the premise that trust is **never granted implicitly** but must be **continually evaluated**.

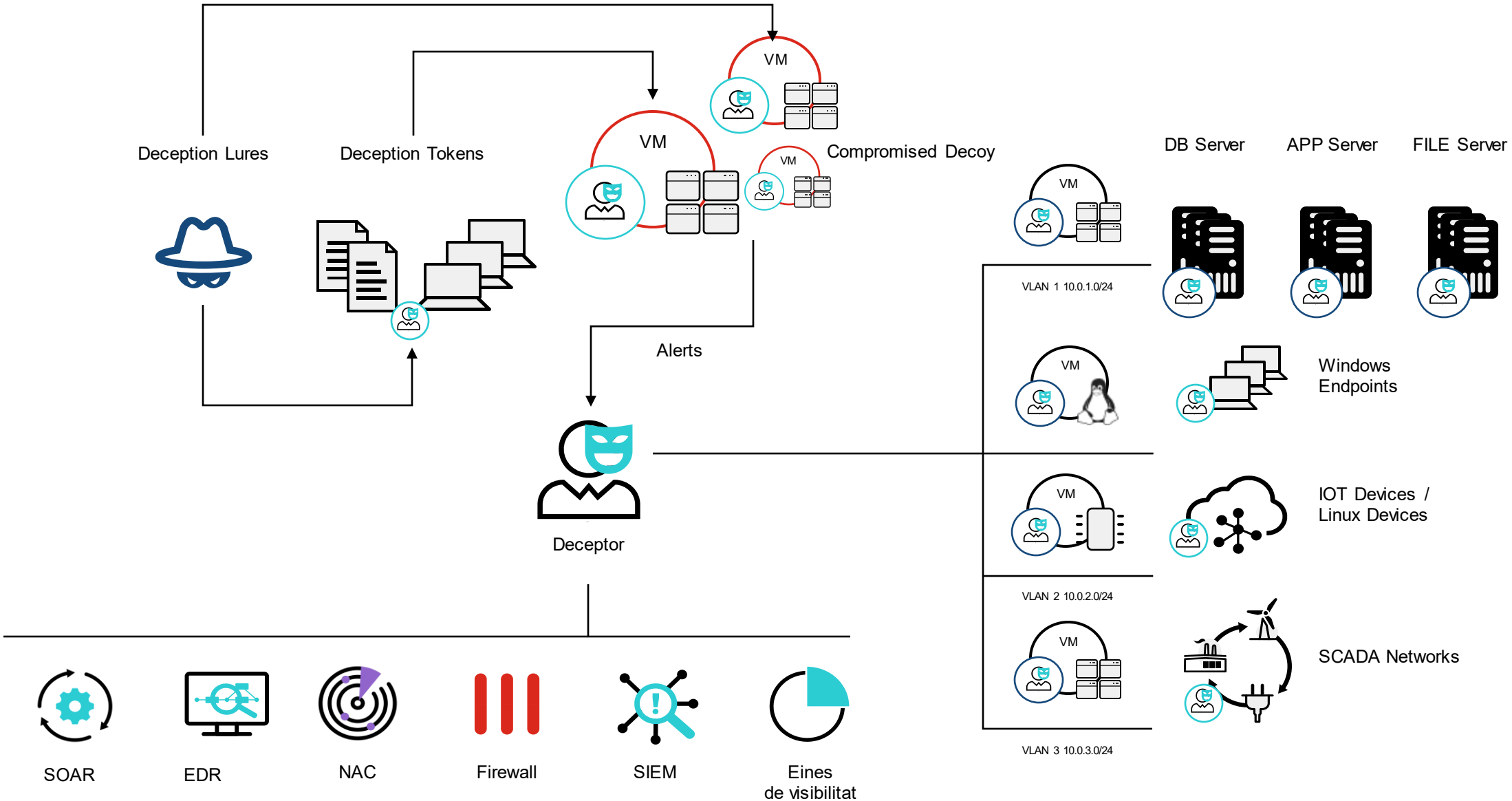
Zero Trust Concepts

Zero Trust	**Mindset**	A philosophy for only trusting a user or device after explicitly confirming their identity and status. It focuses on users, devices, and the specific resources being accessed, utilizing segmentation and zones of control.
Zero Trust Strategy	**Architecture**	Systematic Approach to replace implicit trust for network edges and remote users with consistent convergence of networking and security across the organization.
Zero Trust Initiatives	**Specific Projects**	• Zero Trust Network Access (ZTNA) • Network Segmentation • Micro-Segmentation • Identity/Authentication

Estratègies i casos d'ús per la protecció de la cadena de suministrament i la gestió del risc digital

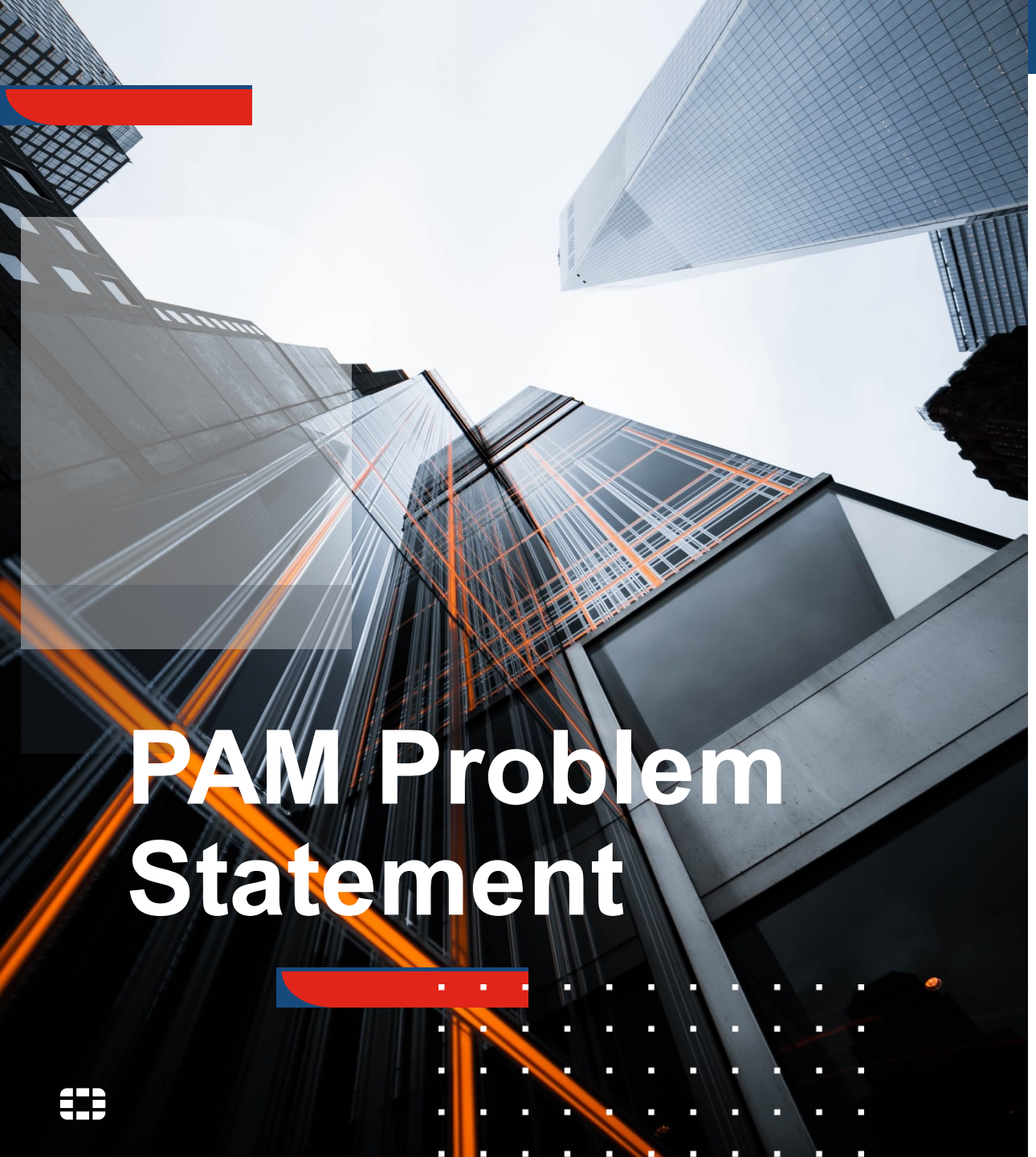
Estratègia de decepció o engany – Next Generation Honeypots

Estratègies de decepció – Next Generation Honeypots



Estratègies i casos d'ús per la protecció de la cadena de suministrament i la gestió del risc digital

Gestió d'usuaris privilegiats



PAM Problem Statement

ANDORRA DIGITAL

One shared Admin account means no auditing possible: actions can not be traced to a single person.

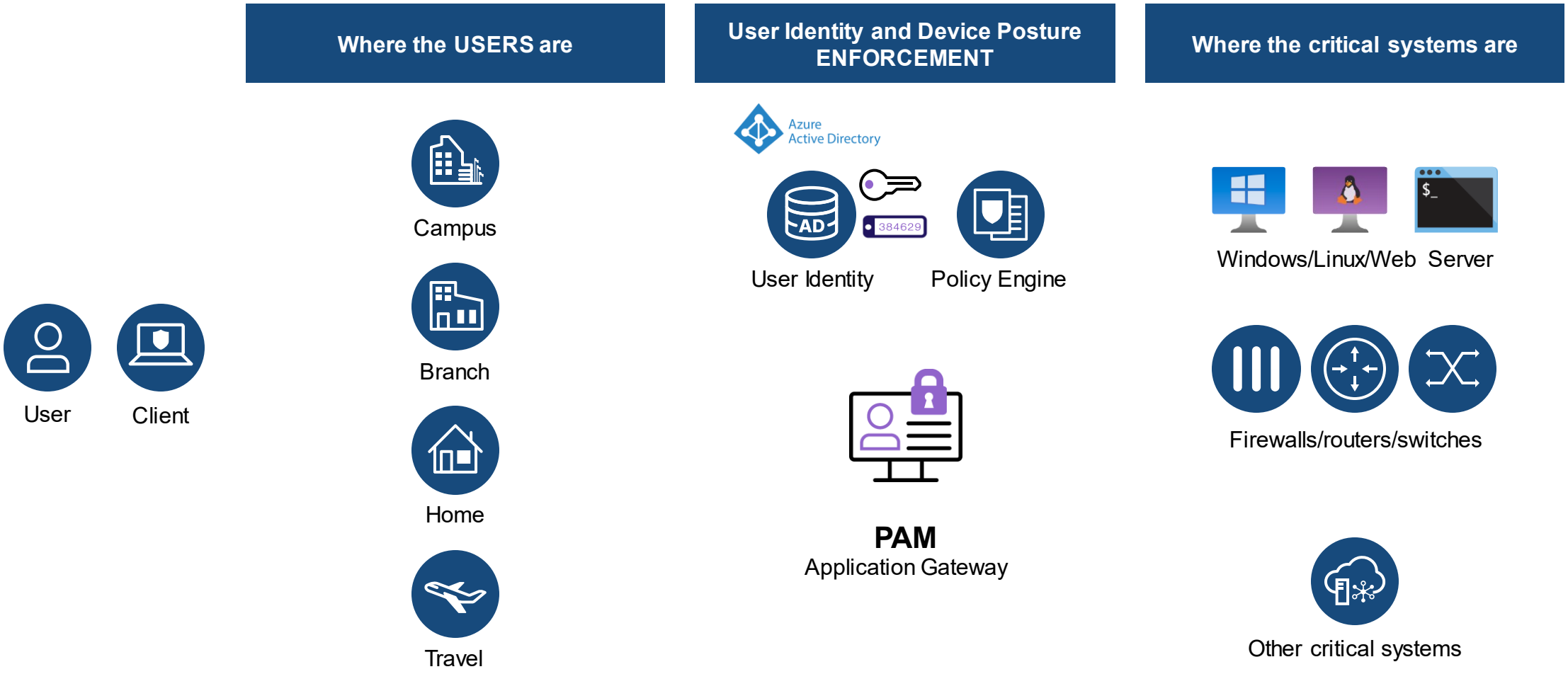
Solution is to have several admin accounts tied directly to individuals.

Separation of duties, Security best practices and standards dictate the use of two accounts per administrator. One user account, one admin account. In practice is very hard to enforce and leads to vulnerabilities especially in elevation of privilege attacks.

The PAM Solution, one set of accounts which can be used by several individuals and audits can trace back the actions and enforce accountability.

PAM as Application Gateway

Arquitectura genèrica de Gestió d'usuaris privilegiats (PAM)



Estratègies i casos d'ús per la protecció de la cadena de suministrament i la gestió del risc digital

Gestió del risc digital als proveidors

Vcigilància del risc digital de proveidors

- Valorar la maduresa de seguretat dels proveidors
- Monitoritzar nivell de risc dels proveidors
- Credencials robades
- Proveidors Compromesos
- Emprese de software
- Emprese de serveis gestionats

Solucions de DRPS

Gestió del risc digital

External Attack Surface Management (EASM)

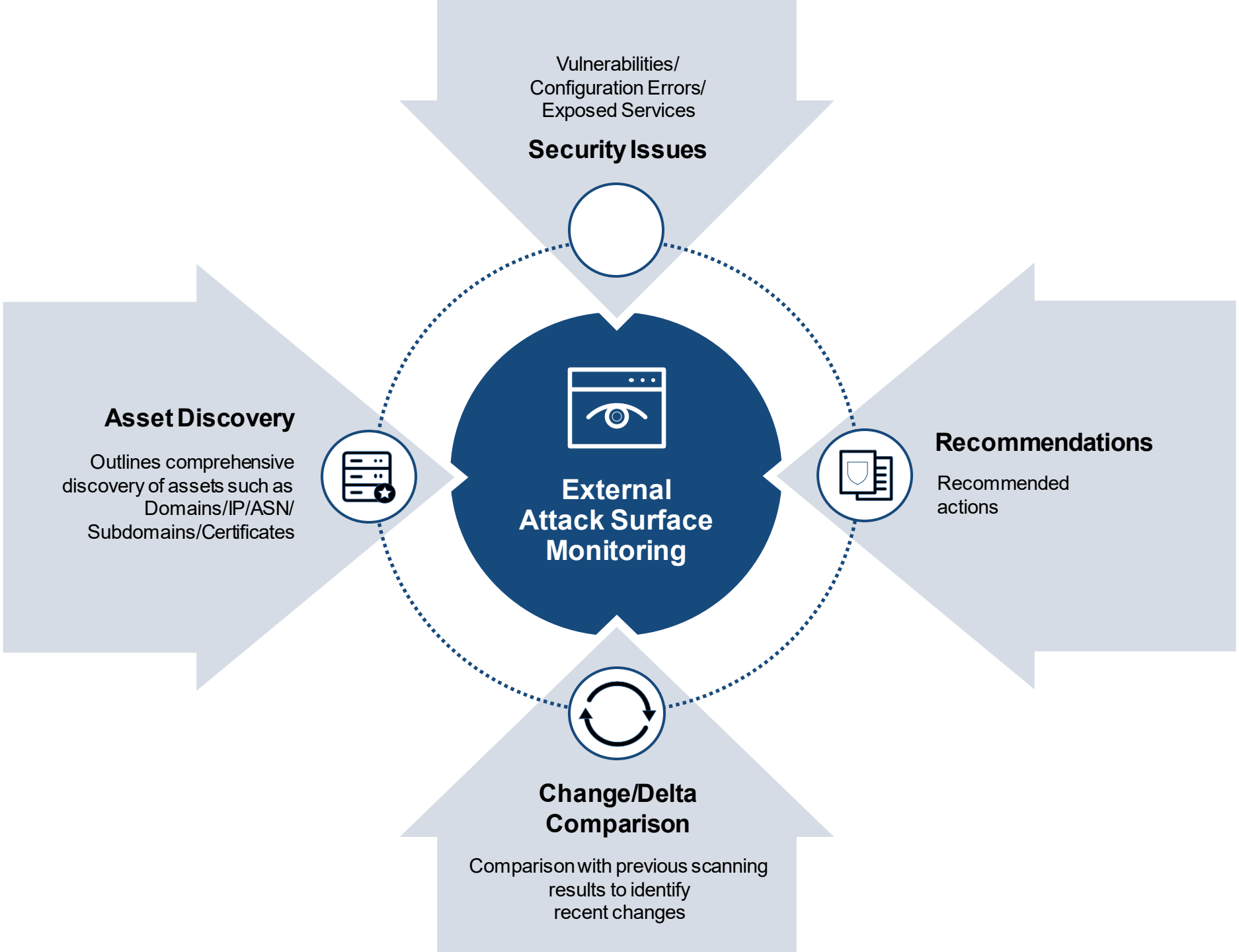
Brand Protection

Adversary Centric Intelligence

External Attack Surface Management

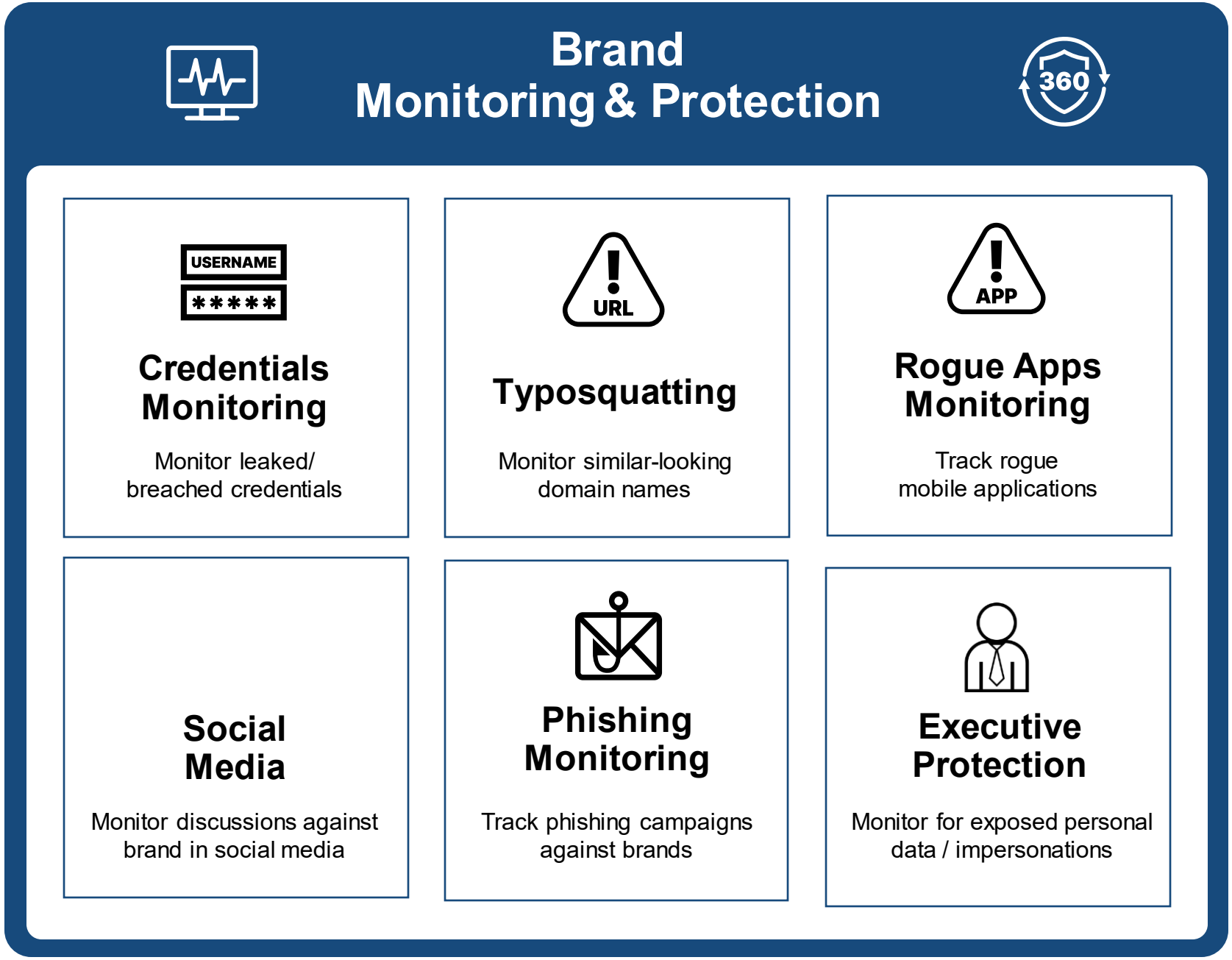
(EASM)

Zero-false positives, external risk prioritization and remediation



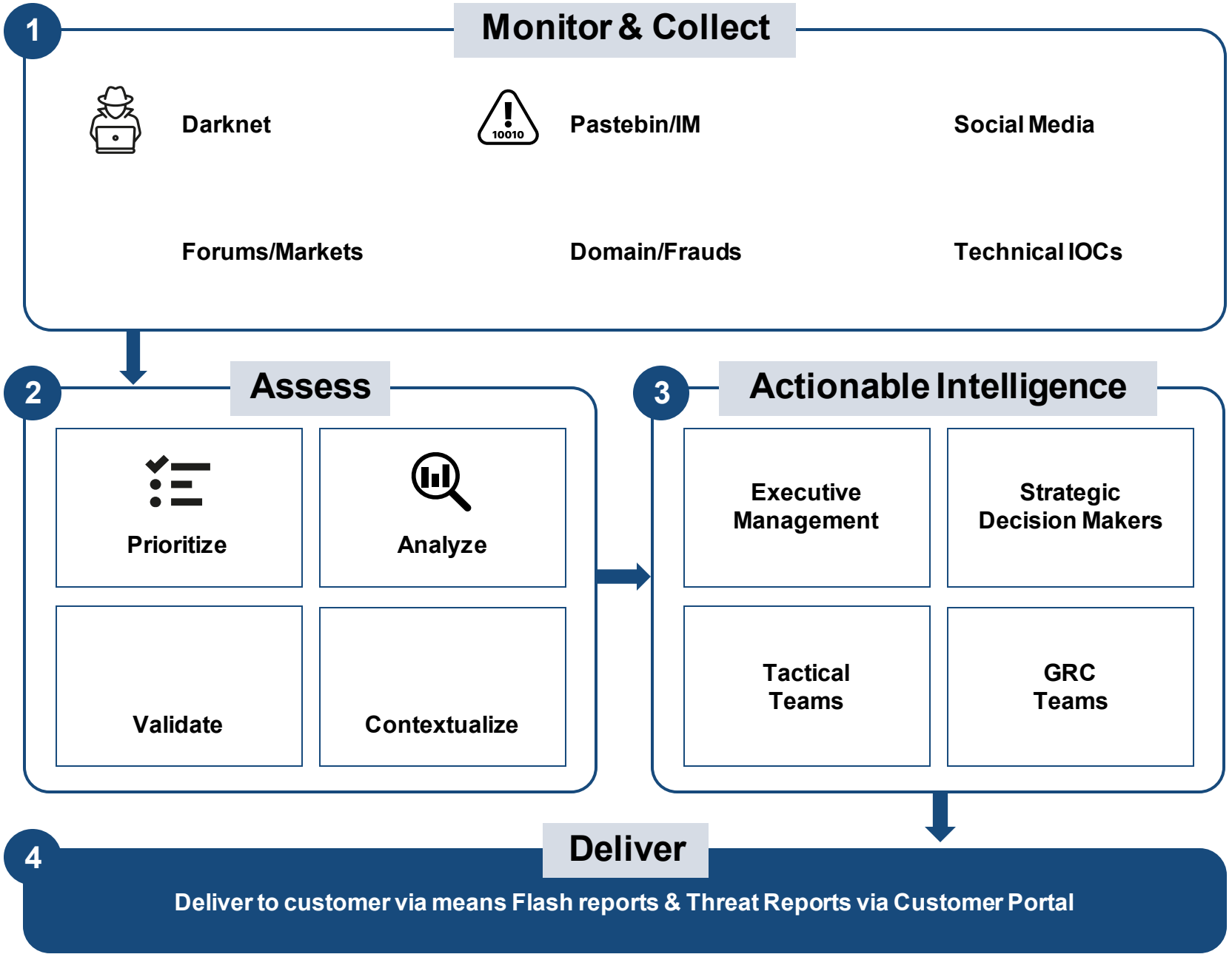
Brand Protection

Preserve customer trust and loyalty, and credibility with partners, suppliers, and investors



Adversary Centric Intelligence (ACI)

Curated, actionable intel tailored to your attack surface



MOLTES GRÀCIES

ANDORRA DIGITAL

ANC-AD

@anc_ad

@anc-ad

csirt.anc@govern.ad

ANC-AD