

ASIP Cybersecurity Services





- 1.100 Cybersecurity Experts
- 2. Presence in Europe, Latin

  America and Middle East
- 3. Global Cybersecurity for Multinational & Government
- 4.+500 GLOBAL Customers
- 5.+30% Annual Growth
- 6. International Recognized Certifications by Gartner
- 7. Global Operations Facilities in 5 countries



1 AIUKEN CORPORATE INTRO VIDEO



Aiuken's mission is to continue developing its innovation, technologies, services and Security infrastructures to achieve the best level of security and secure access to the cloud, Internet and Systems

Worldwide



Aiuken, is an international Cybersecurity Leader company focused on Information, Communications and Internet Security, specialized in Cloud Security services with high added value for Governments and Big Enterprises.

#### Our vision

Managed Cloud Security and Protection services for large companies, SMEs and Public Administration, and securing the digital transformation of our clients.

We provide the technologies, services and infrastructures that facilitates security and secure access to the CLOUD, Internet and Telecommunications Systems.

#### Objective

Best Security levels, Quality, Security as a Service



O1 Cybersecurity Today



New Digital Era. Everybody Welcome







## New Digital Era. Everybody Welcome



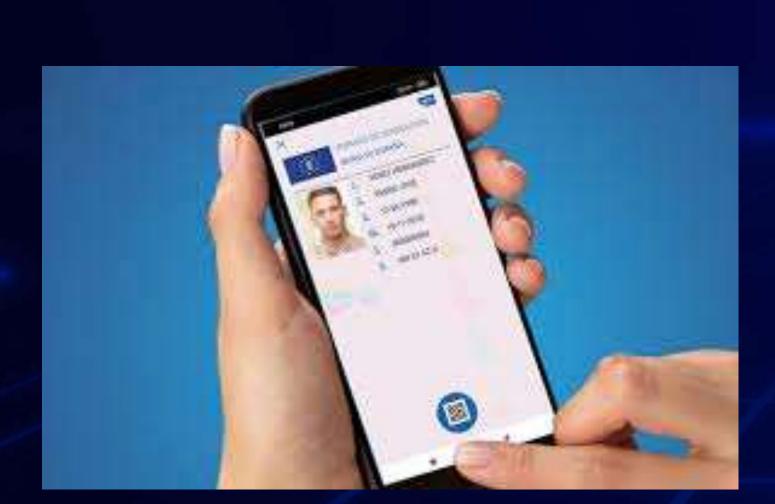




# New Digital Era. Everybody Welcome









Third-party music services

New visual status in Home app

for cameras

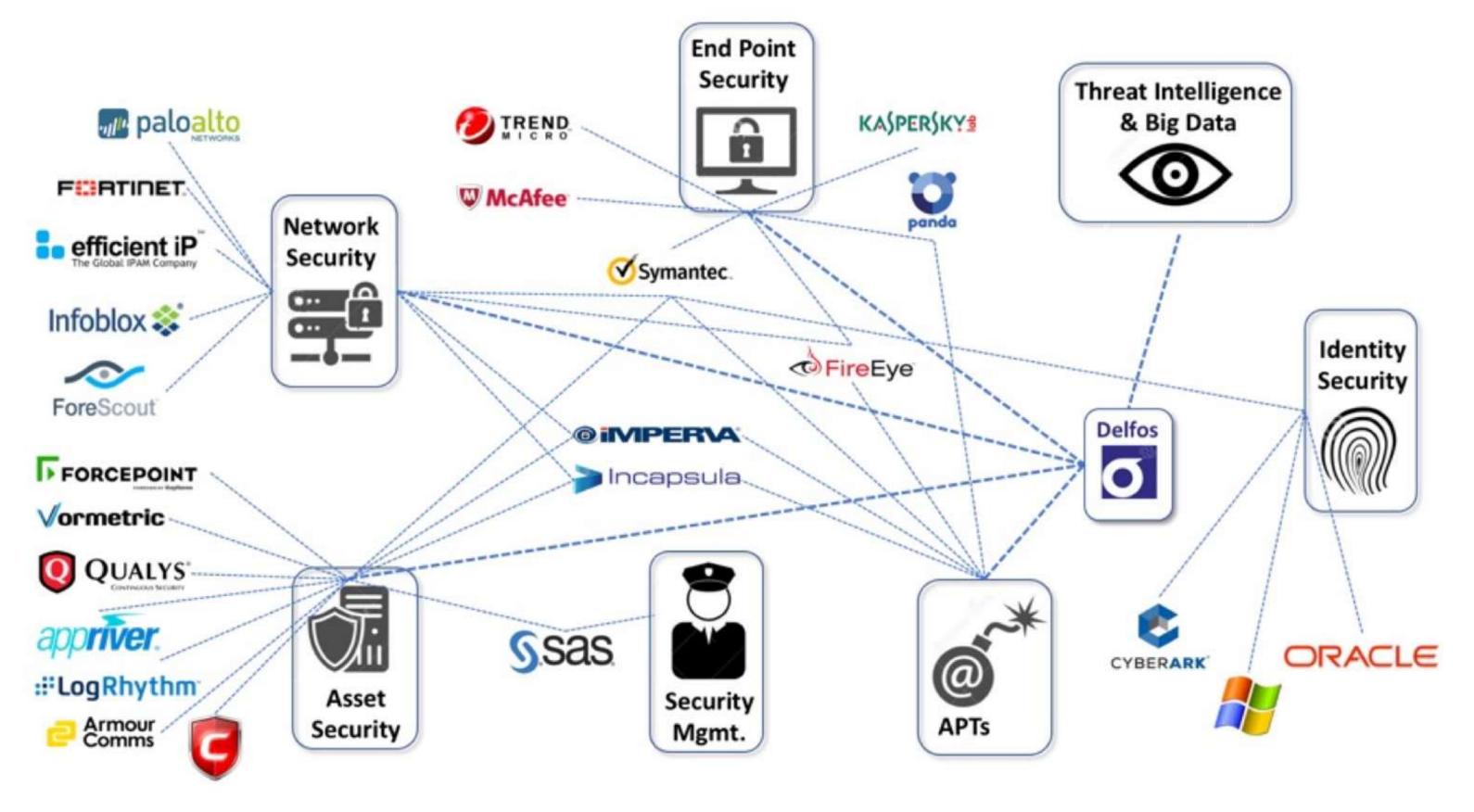




Imposible control humano

# O1 | Cybersecurity Now and Future Issues Complex scenarios. Not scalable operations.





Lot of technologies

Multiple dashboards

Multiple alerts consoles

Multiple ticketing systems

Multiple reporting systems

More expensive resources

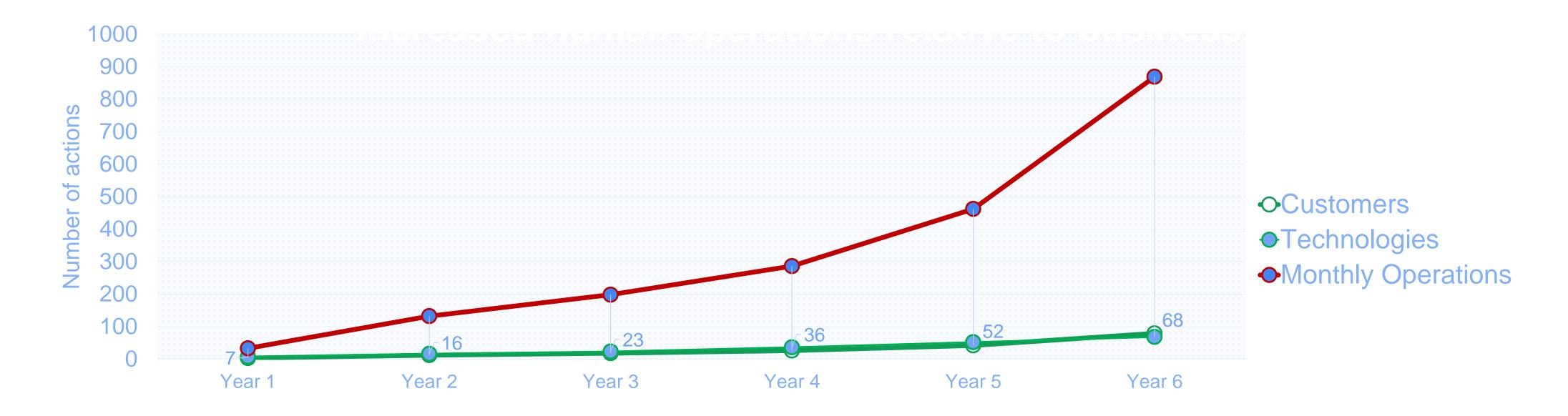
More specific vendor specialists

Information disaggregation

Inefficient reporting management



### Increased human operations relative to business growth



### **Human Operations**

- Alerts management
- Incidents management
- Tickets scalation
- Reports elaboration

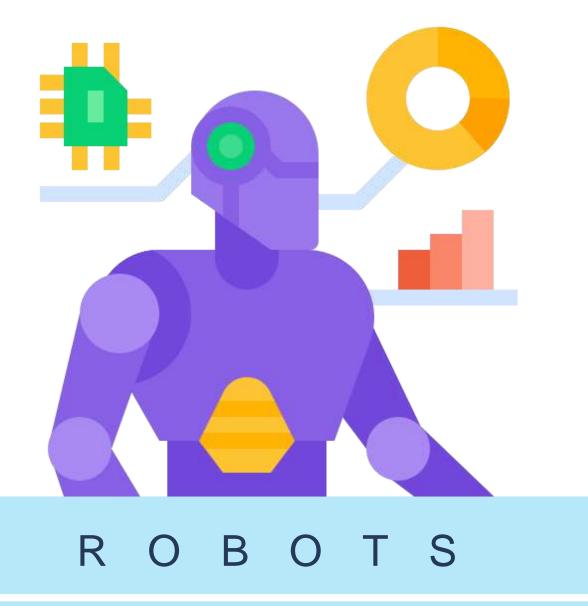
- Investigations
- Devices integrations
- Use cases implementation
- Dashboards elaboration





### H U M A N S

- Slow on alerts triage
- Slow on scoring calculation
- A single task at same time
- Work at 8 hours shifts
- Failures under pressure
- Limited and expensive
- Need to sleep and eat



- Alerts triage at machine speed
- Scoring calculation at machine speed
- Thousands of tasks at same time
- Work 24 x 7 x 365
- Always just as accurate
- Unlimited and cheap
- Don't sleep and don't eat

We need to exclude humans from Cybersecurity

Operations

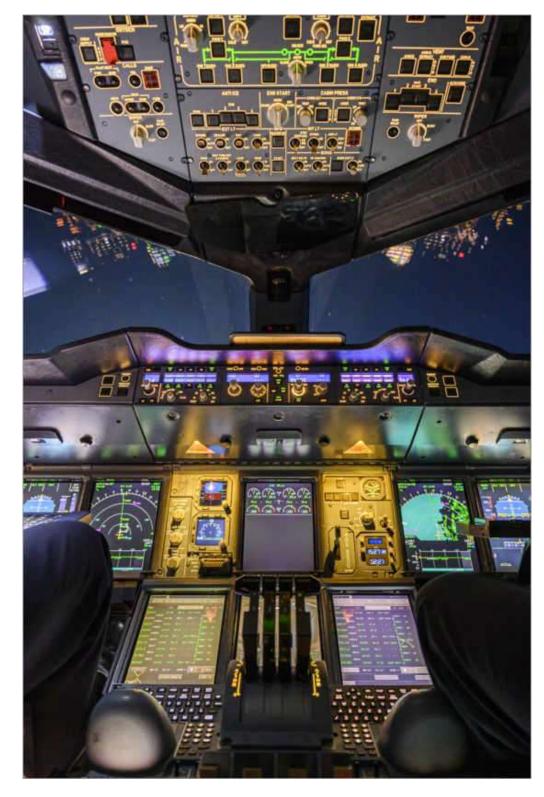






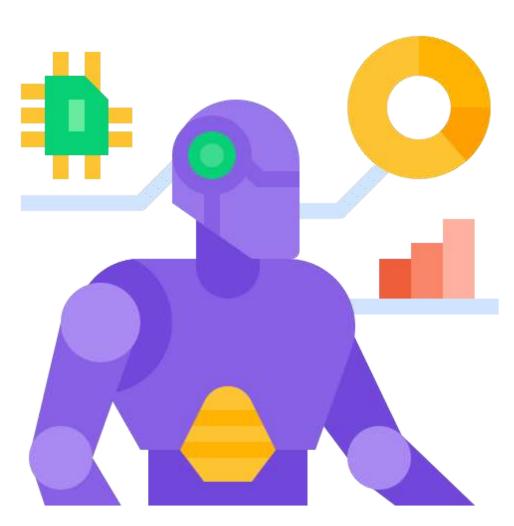
H U M A N S







R O B O T S







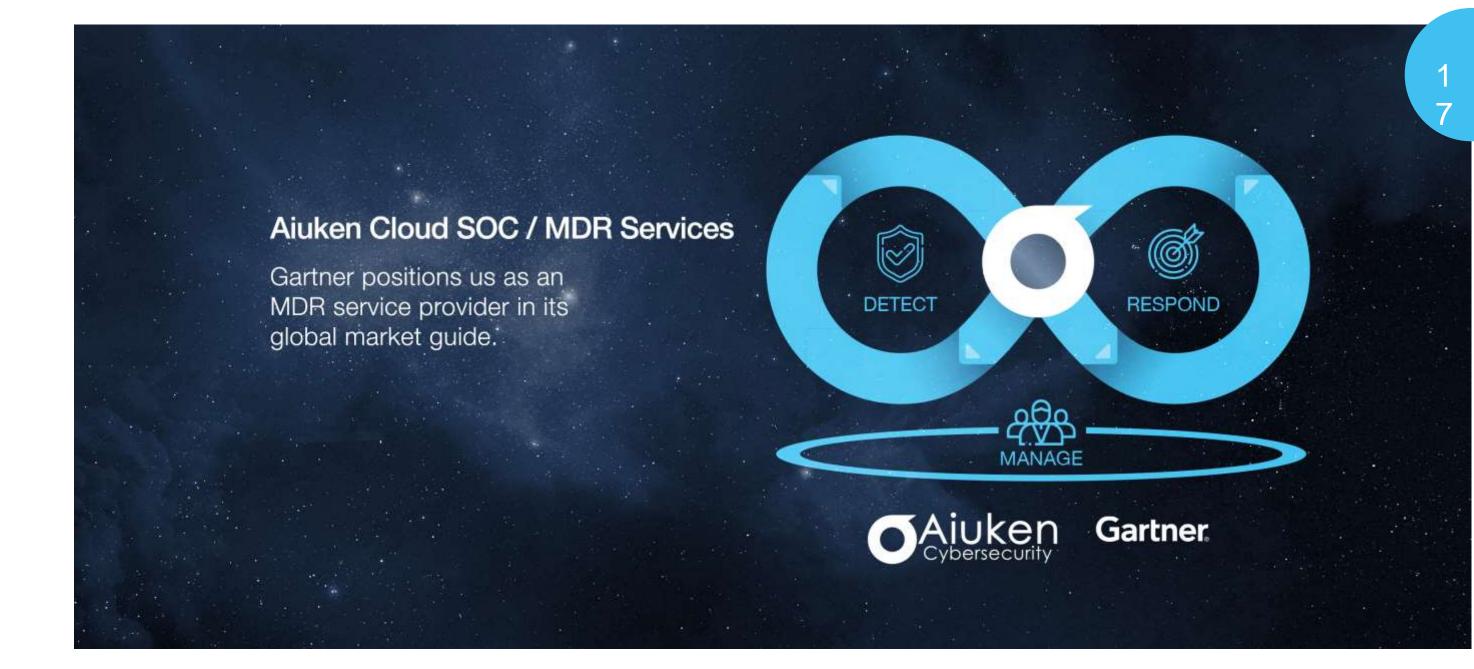
O3 Inteligencia
Artificial
El Futuro



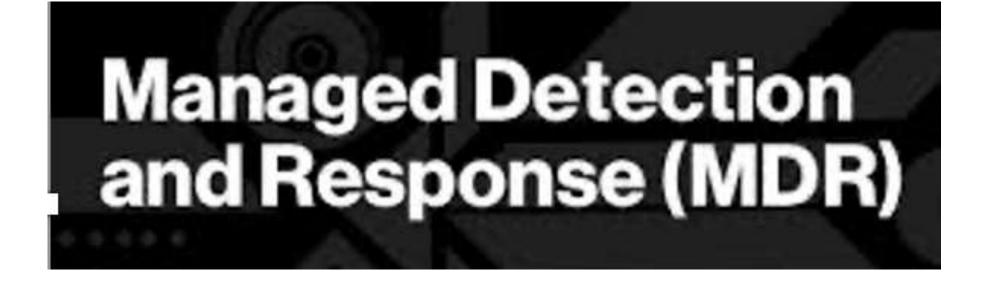


# Gartner



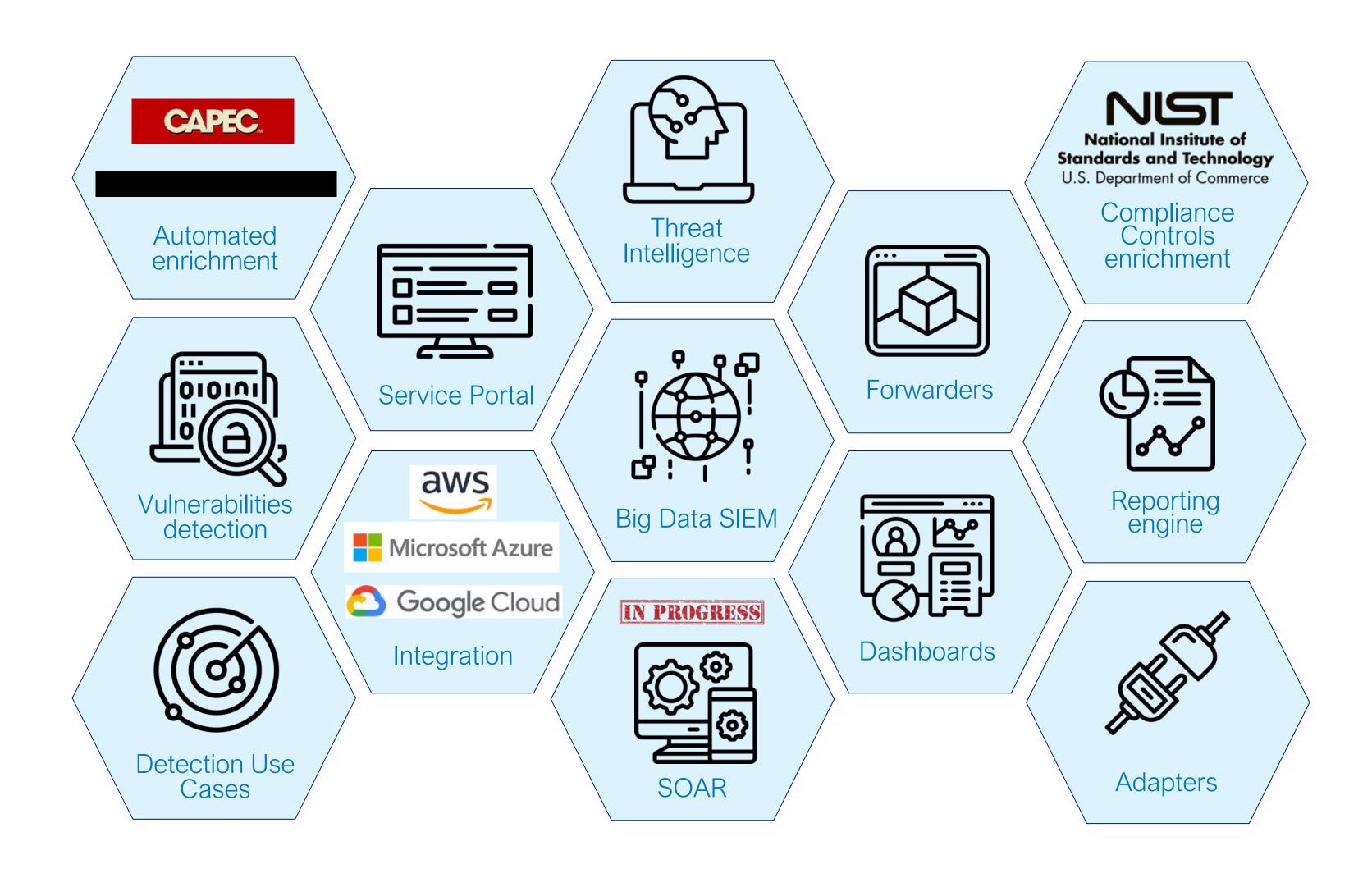






## 03 | AIUKEN AI + SOAR PLATFORM = ASIP









### Autonomous Security Operations Center

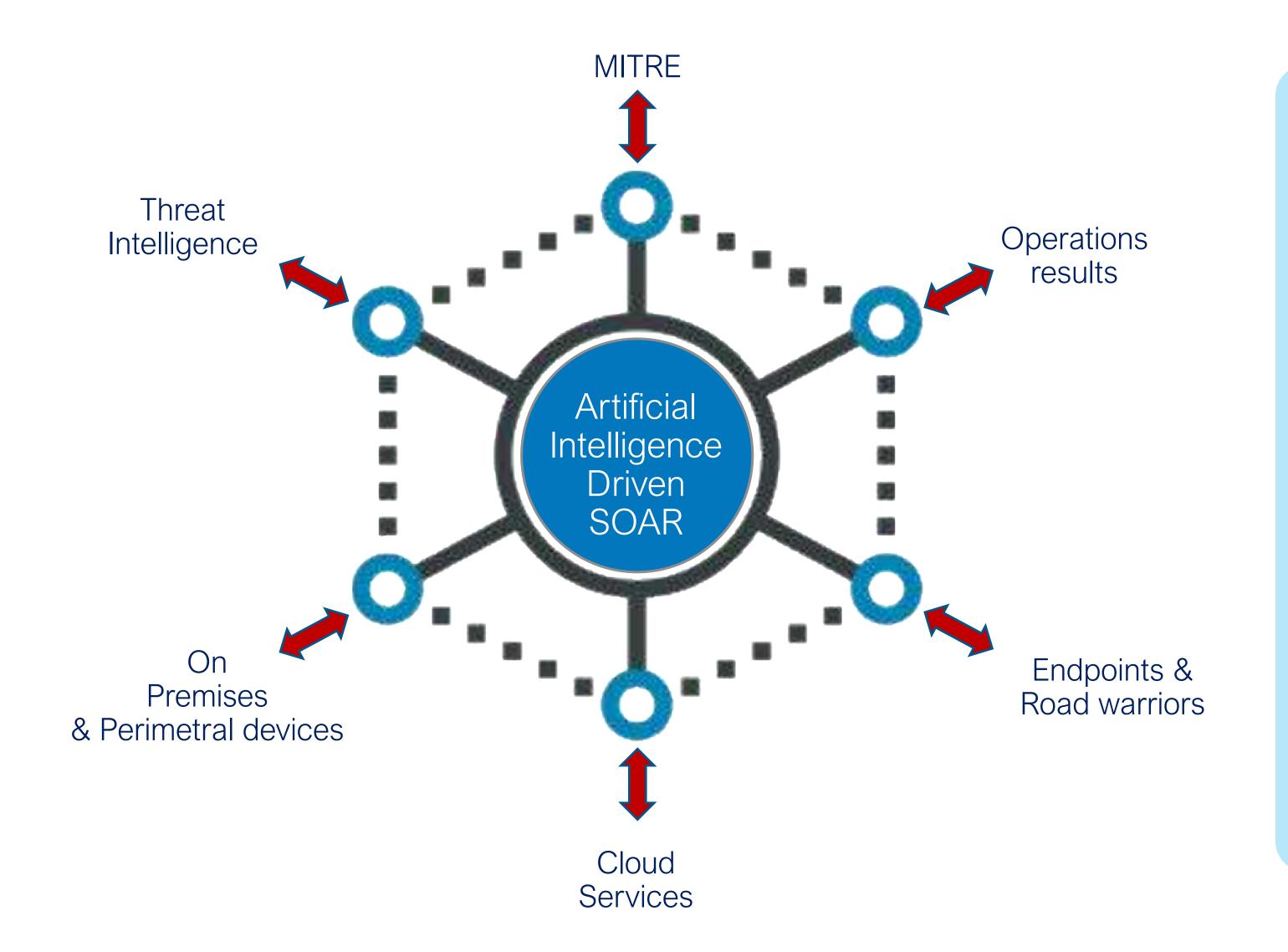
Automatic Detection
Automatic Triage
Automatic Mitigation

Automatic provision Automatic operations Scalable business

No human intervention required Fully automatic, Artificial Intelligence Driven, from The Cloud

# 03 | ASIP XDR Unattended Services

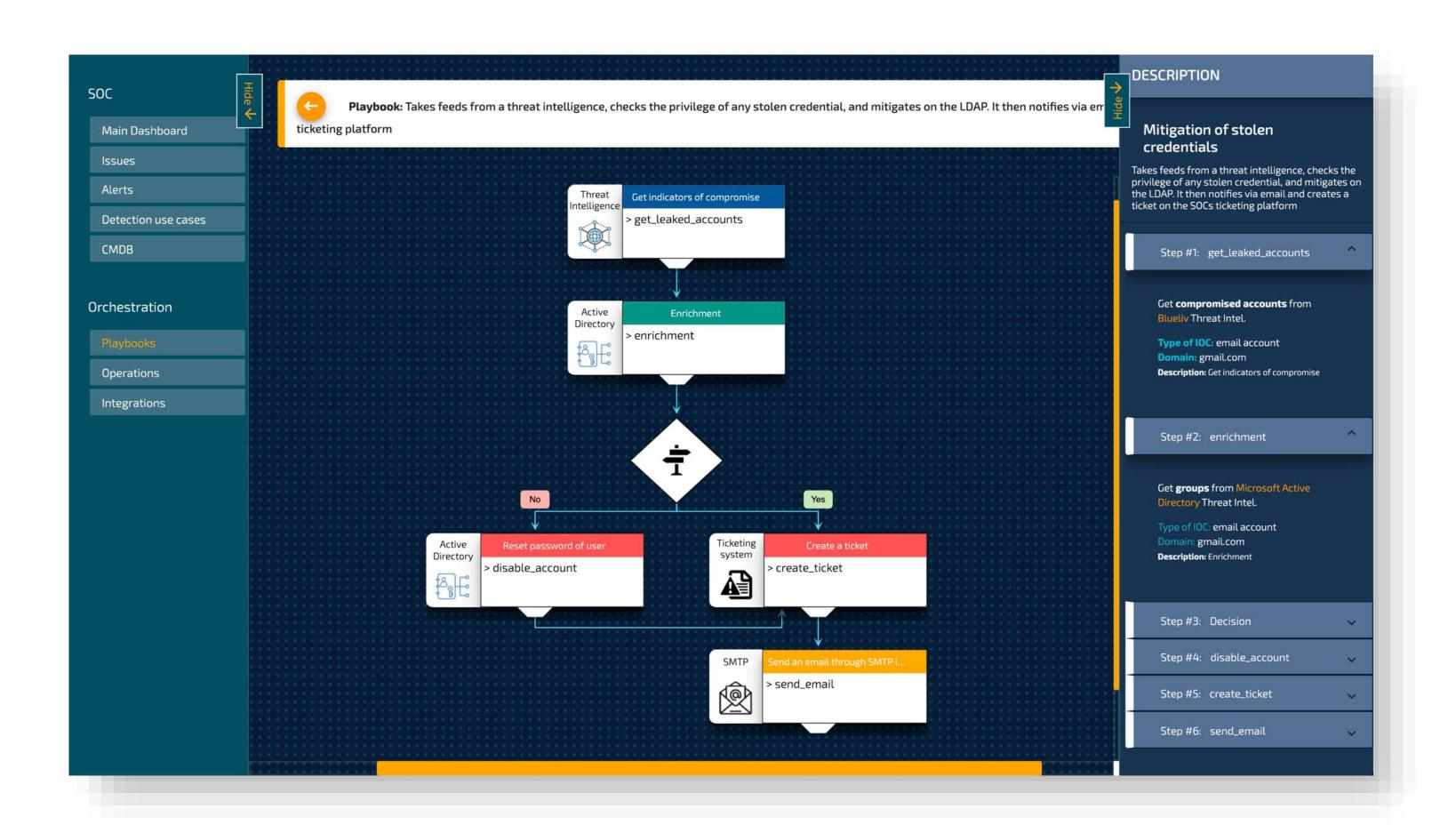




- Multi-Customer autonomous SOC
- Driven by Artificial Intelligence.
   Feed by cloud Data Lake currently in production
- Unattended Triage within MITRE framework
- Unattended Mitigation in endpoints and cloud services
- Unattended resolution & ticket scalation to customers

# 04 | SOAR (Auto-Mitigation)





- Multi-customer playbooks: pipelines abstracted from vendors and devices
- One single playbook per use case for all SOC customers
- Easy SOC playbook maintenance: scalable operations

O4 The Roadmap to the future

# 04 | MITRE -> INDICATORS OF ATTACK



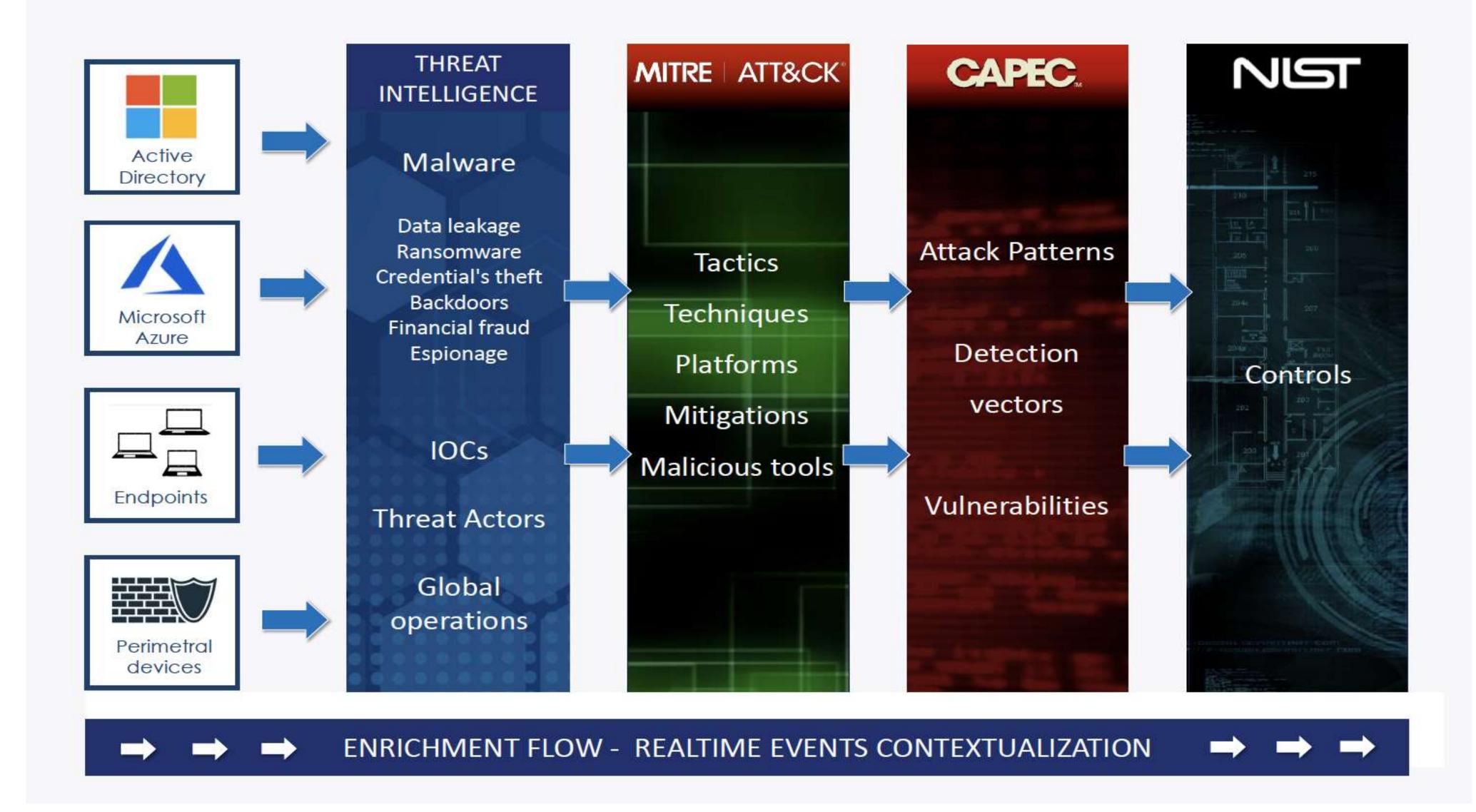
### Malicious next actions prediction: connecting the dots

Reconnaissance 10 techniques	Resource Development 6 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 37 techniques	Credential Access 14 techniques	<b>Discovery</b> 25 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning	Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting	Account Manipulation (0/4)	Abuse Elevation Control	Abuse Elevation Control	Brute Force	Account Discovery (6/4)	Exploitation of Remote Services	Archive Collected	Application Layer	Automated Exfiltration (0/1)	Account Access Removal
Gather Victim Host Information (0/4)	Comp. mise Accounts (0)	Exploit Public- Facing Application	Interpreter (0/8) Exploitation for Q ent	BITS Jobs	Mechanism (0/4) Access Token	Mechanism (0/4) Access Token	Credent als from Password	Application Window Discovery	Internal Spearphishing	Data (0/3) Audio Capture	Protocol (C/4) Communication	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (0/3)	Compromise Infrastructure	External Remote Services	Execution Inter-Process	Boot or Logon Autostart xecution (0/12)	Manipulation (0/5) Boot or Logon	Manipulation (D)51 BITS Jobs	Stores (0/3) Exploitation for	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Through Removable Media	Exfiltration Over	Data Encrypted for Impact
Gather Victim Network Information (0/5)	Develop	Hardware	Communication (6/2)	Bot or Logon	Autostart Execution (0/12)	Deobfuscate/Decode	Credential Access	Cloud Infrastructure	Remote	Clipboard Data	Data Encoding (0/2)	Alternative Protocol (0/3)	Data Manipulation (0)
Gather Victim Org Information (0/4)	Capabilities (0/4) Establish	dditions  hishing (0/3)	Native AF	II Initialization Scrips (0/5)	Boot or Logon I Initialization	Files or Information  Direct Volume Access	Authentication	Discovery  Cloud Service	Service Session Hijacking (0/2)	Data from Cloud Storage Object	Data Obfuscation (0/3)	Exfiltration Over C2 Channel	II Defacement (0)
Phishing for Information (0/3)	10,0)	Replication Through Removable Media	Shared Modules	Compromis Client	10,4)	Execution Guardrails (0)1) Exploitation for Defense Evasion	Capture (0) Man-in-the- Middle (0/2)	Dashboard  Cloud Service Dovery	Remote Services (D/6) Replication Through	Data from Configuration	Dynamic Resolution (0/3) Encrypted Channel (0/2)	Exfiltration Over Other Network Medium (0/1)	II Disk Wipe (0/2) II Endpoint Denia
Search Closed Sources (0/2)			oftware Deployment Tools	Software Bin ry Create				Domain Tost Discovery		Repository (0/2)  Data from			of Service (0/4)
Search Open Technical		Comprimise (0)	System Services (0/2)	Account (0/3)  Create or Modify	Event Triggered Excution (0/15)	File and Directory Permissions	Modify Arthentication Process (0)/8	Fil and Directory Discovery	Removable Media	Information Repositories (0/2)	Fallback Channels	Exfiltration Over Physical Medium (0/1)	Corruption Inhibit System
Databases (0,5) Search Open		Relationship	User Execution (0/2)	III System	Exploitation for Privilege Escalation	Modification (0/2)	Network sniffing	Network Service Scanning	Software Deployment Tools	Data from Local System	Ingress Tool Transfer	Exfiltration Over Web	Recovery  Network Denial
Websites/Domains (0/2)		Accounts (0/4)	Windows Management	Event Triggered Execution (0/15)	Group Policy Modification	Modification	OS Credential Dumping (G/8)	Network Share Discovery	Taint Shared	Data from Network Shared Drive	Multi-Stage Channels	Service (0/2)	of Service (0/2)
earch Victim-Owned lebsites			Instrumentation	External Remote Services	Hijack Execution Flow (6/11)  Process Injection (6/11)  Scheduled Task/Job (6/8)  Valid Accounts (6/4)	II Hijack Execution Flow (0/11)  II Impair Defenses (0/7)  II Indicator Removal on Host (0/6)  Indirect Command Execution	Ace as Token  Steal or Forge  Kerberos Tickets	Network Sniffing		Data from Removable Media	Non-Application Layer Protocol	Scheduled Transfer Transfer Data to Cloud Account	Resource Hijackin Service Stop
				Hijack Execution Flow (0/11)				Password Policy Discovery		Data Staged (0/2)	Non-Standard Port		System Shutdown/Reboot
				Implant Container				Peripheral Device Discovery Permission Group Discovery (0/3)		Email Collection (0/3) I Input Capture (0/4)	Protocol Tunneling		
				Startup (0/6)					?		Proxy (C/4) Remote Access		
								Process Discovery		Man in the Browser	Traffic		
				Pre-OS Boot (0/5)		Modify Authentication Process (0/4)	Unsecured Credentials (0/6)	Query Registry Remote System		Man-in-the- Middle (0/2)	Signaling (O/T) Web		
				Task/Job (0/6) Server Software		Modify Cloud  Compute	(0/0)	Discovery Software		Screen Capture Video Capture	Service (0/3)		
				Component (0/3)		Infrastructure (0/4)		Discovery (0/1)					

What are the possible next malicious activities? What are the probabilities?

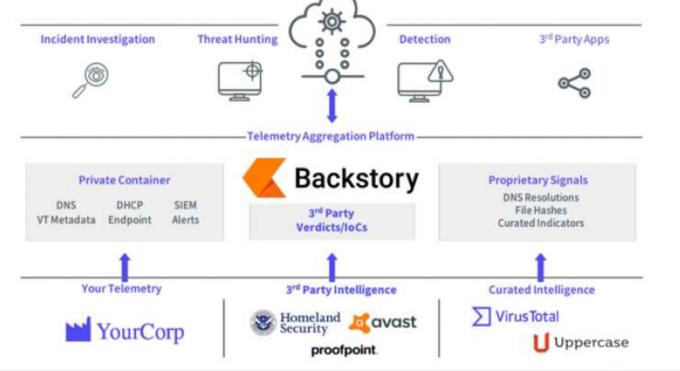
## PATRONES Y LOGS DINAMICOS

### Real-time events enrichment & context



### MULTI CLOUD SOC







Define user permissions and identities, infrastructure protection and data protection measures for a smooth and planned AWS adoption strategy.



#### Detect

Gain visibility into your organization's security posture with logging and monitoring services. Ingest this information into a scalable platform for event management, testing, and auditing.



#### Respond

Automated incident response and recovery to help shift the primary focus of security teams from response to analyzing root cause.



#### Remediate

Leverage event driven automation to quickly remediate and secure your AWS environment in near real-time.



Azure Sentinel – Cloud Native SIEM and SOAR (Preview)

Security Information and Event Management - 1 ---(SIEM)-----**Cloud App** Microsoft **Azure** Security

Office 365 **Advanced Threat Protection (ATP)** 

nalytics/Automation

**Azure** 



# Ese momento.... Que no podremos evitar







### Martine is teleworking during COVID-19

Malicious individuals can put you in a stressful or emergency situation and ask you to take unusual actions: large money transfers, extracts from HR databases, confidential client documents, etc.

You may feel more isolated to verify the legitimacy of this request, here are a few tips to help you get through this:



# CEO Fraud

In this scam, someone uses an authority report to ask you to perform an important and unusual action in the context of an emergency.







Often by phone call, but also by email



#### Targets

everyone is a potential target (especially administrative staff finance and HR dept.)



#### Unusual actions

abnormal / excessive situation for the target (e.g. large money transfer or list of confidential data)



### **Urgent timing**

crisis situation that cannot wait (out of usual processes)



### Calm things down and sweep doubts away

by validating the information before taking any action











