Harnessing AI for Next-Gen Threat Detection & Response

Securing Telecom Networks & Digital Infrastructure in the era of 5G

Zeina Zakhour
VP, Global CTO Cybersecurity
@ZeinaZakhour

ENISA Telecom & Digital Infrastructure Security Forum
20th of March 2025

Atos

Navigating the Cyber Risk landscape in Telecom

Application Transformation, Data & BSS

- *Telco Operational Excellence powered by automation*
- *BSS Transformation*
- *Customer Engagement Platform*
- *Enable Digital Marketplace and Data Monetization*
- Gen AI Product & Service Offerings

Telco B2B Solutions and Services

- *B2B Cloud*
- Edge Computing - Video Analytics
- Mobile Private Networks
- Gen AI Product & Service Offerings

OSS-MANO and Next Generation Networks

- *OSS MANO*
- *5G Networks*
- *Network on the Cloud*
- Gen AI Product & Service Offerings

Cybersecurity Risks

- Regulatory Pressure & Compliance Overload
- Complexity (5G, IoT, Omnichannel, etc.) & disconnected security stack
- Supply Chain is the new attack surface (digital sovereignty)
- Identity (machine, consumers) is the new perimeter
- API is the new Single Point Of Failure
- The constantly changing business model introduces new cyber risks
- Ever changing Cyber threat Landscape

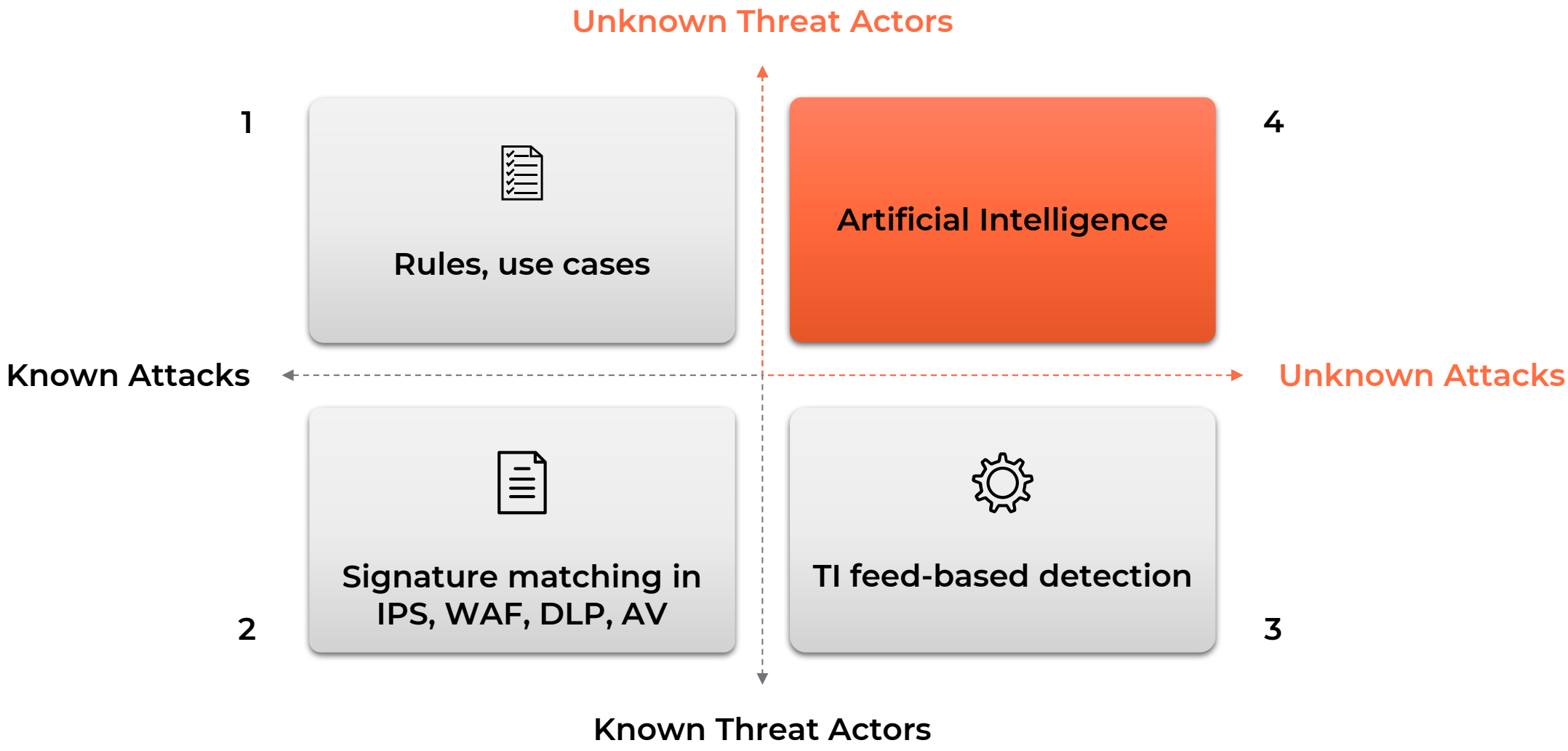
300%

increase in cyber attacks against satellite infrastructure over last five years

Third

Most targeted industry by cybercriminals in the Telecommunication & Media Industry

AI is for Precision & Adaptability – not the Panacea



 © Atos - for external use

“

84% of MITRE ATT&CK techniques are not covered by traditional rules & signatures

”

Artificial Intelligence in Cybersecurity

- Rapid synthesis of voluminous data
- Automated threat detection and response
- Early detection and proactive defense
- Coverage of unknown threats

Advanced Detection and Response powered by AIsaac Platform

Technologies

Multi-Vector

- Endpoints
- Identity
- Network
- Cloud Infra/SaaS
- Applications
- Database
- OT/IoT
- Issues

EVIDEN TECHNOLOGY

- SIEM
- SOAR
- Security Analytics
- UBA
- Threat Intel

PARTNER TECHNOLOGY

- EDR
- SIEM
- NTA
- Vulnerability Management
- Policy Management
- EASM

Threat Detection and Response

Attack Surface

External Attack Surface Management
Continuously scan external digital estate to identify issues

Policy Management
Continuously detect policy violations and enforce them

Vulnerability Management
Continuous vulnerability detection and mitigation

Deeper Detection

1000+ rules and signatures

200+ threat intel sources

100+ ML models

24 X 7 SOC monitoring for known threats powered by **industry specific** use cases

24 X 7 threat intelligence for known attackers enriched with risk scoring

24 X 7 Threat hunting for unknown threats/attackers powered **by industry specific** use cases

Full Response

Incident analysis
Enrichment with Attack Surface Management.

Threat containment
Immediately stop threats and contain the spread

AI Responder
AI Assistance for automated response

Recovery Management
Recover from cyber threats

Singular Risk Visualization with real-time risk scoring

Expert teams - governance and continuous improvement

Atos

Threat Hunting Using AI

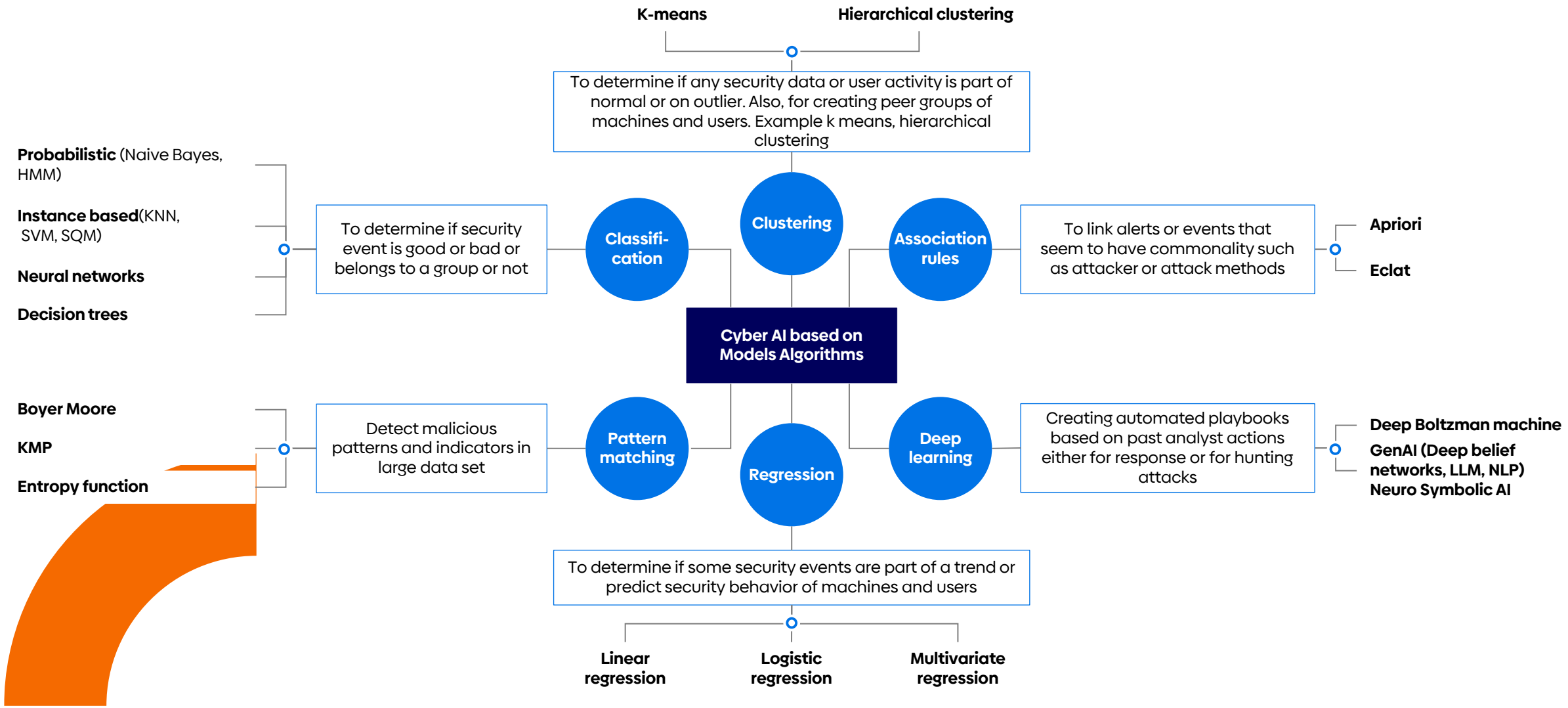
Anomaly Based

Learn normal
Login patterns,
Data transfer, Email transactions
Detect abnormal

Hypothesis based

Learn Malicious patterns
Detect similar

AI Algorithms for Advanced threat Detection



What the future holds?

AI-first Security

Security for AI (Now!)

AI-powered Autonomous & self-healting Cybersecurity

Quantum Computing Threats

Green Innovation