IPv6 2030 : Les conditions d’un futur de l’internet en IPv6
(ARCEP – IDATE - IPv6 Forum)

Cybelia
Augmented Cybersecurity

IA et Cybersécurité

Protéger les infrastructures à l’ère des réseaux intelligents

Reda YAICH
(Head of Cybersecurity and Networks)

Mardi 27 janvier 2026

AIRBUS Rte SystemX INSTITUT DE RECHERCHE TECHNOLOGIQUE

Augmented Cybersecurity, for French Industry

Associated partners

CAMPUS CYBER · PROGRAMME DE transfert AU campus cyber · PEPR CYB3RSECURITE

Cybersecurity Operations

Evolve based on what happened
(Knowledge -> Capitalization)

Understand what's happening
(Information -> Observability)

React to what's happening
(Decision -> Steerability)

Cybersecurity Operations

Evolve based on what happened
(Knowledge -> Capitalization)

Understand what's happening
(Information -> Observability)

React to what's happening
(Decision -> Steerability)

The bitter reality!

Too much time spent on «understanding» meaning slow « reacting »

- Too many alerts, not enough context
  - Incidents start with a suspicious connection from IP X
  - Firs SOC activities, identify asset, owner, impact, etc.
- Too many tools, not enough integration
- Most expensive time for SOC operators is **attribution** and **triage**!

SOC Operation: a never-ending mission!

Why most organizations already struggle to run effective SOC operations.

- Volume → Fatigue
  Overwhelming data sources: logs, alerts, Cyber Threat Information, etc. Dual-stack and partial adoption increase telemetry and edge cases (two stacks, more failure modes).
- Velocity → Fear
  Necessity of rapid decision-making increases stress
- Variety → Friction
  Diverse technologies (Operational/Cyber) and data sources (Internal/External)
- Variability → Fluctuation
  Constant evolution of threat and supervised systems
- Veracity → False positives
  Lake of precision in detection and prioritization of alerts
- Visualisation → Fragmentation
  Poor UI/UX and limited interaction capabilities
- Value → Frustration
  Limited enrichment capabilities reduces insights

IPv6 doesn’t create new problems difficulties!

But it amplifies the existing ones. How?

- Dual-stack doubles network reality (two address families, more flows)
  - **Volume**
- Faster lateral movement in segments you don’t monitor well (IPv6 paths bypassing IPv4-only controls)
  - **Velocity**
- Some tools speak IPv6 well, others badly (firewalls OK, legacy apps/collectors/SIEM parsers not)
  - **Variety**
- Temporary addresses rotate while cloud workloads churn.
  - **Variability**
- « unknown host» explosions when attribution fails
  - **Veracity**
- UIs that don’t render IPv6 well, queries that fail, dashboards built for IPv4 assumptions
  - **Visualisation**
- Weaker attribution turns IPv6 logs into « more noise »
  - **Value**

Motivations

This project is not about **why** AI could be used in SOC Operations

But rather about

where, **when** and **how** AI can augment SOC operators

to enhance the cyber-resilience of Critical Networks and Systems

What SOC Operators are supposed to do?

Evolve based on what happened
(Knowledge -> Capitalization)

Understand what's happening
(Information -> Observability)

React to what's happening
(Decision -> Steerability)

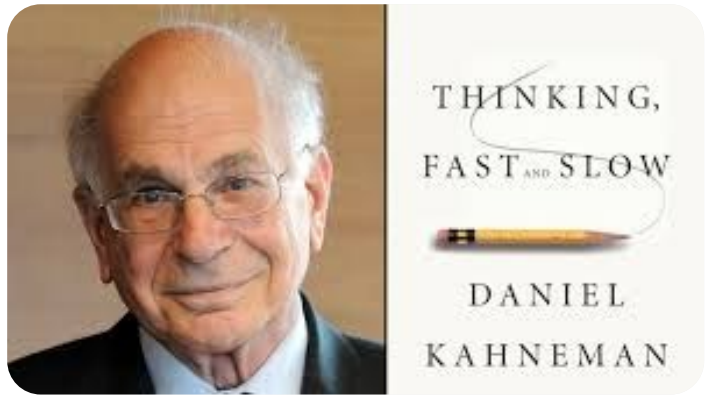
Human dimensions of SOC Operations

Cognitive Models

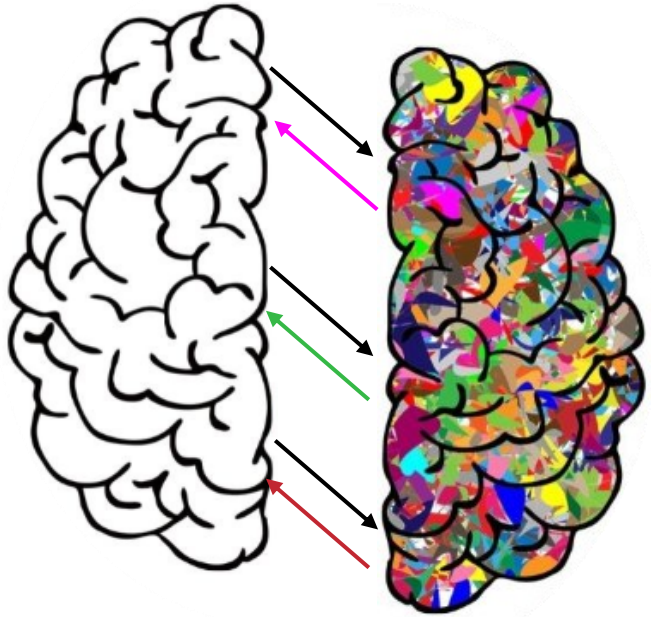
Attention Models

Collaboration Models

How SOC operators think?



System 1 System 2

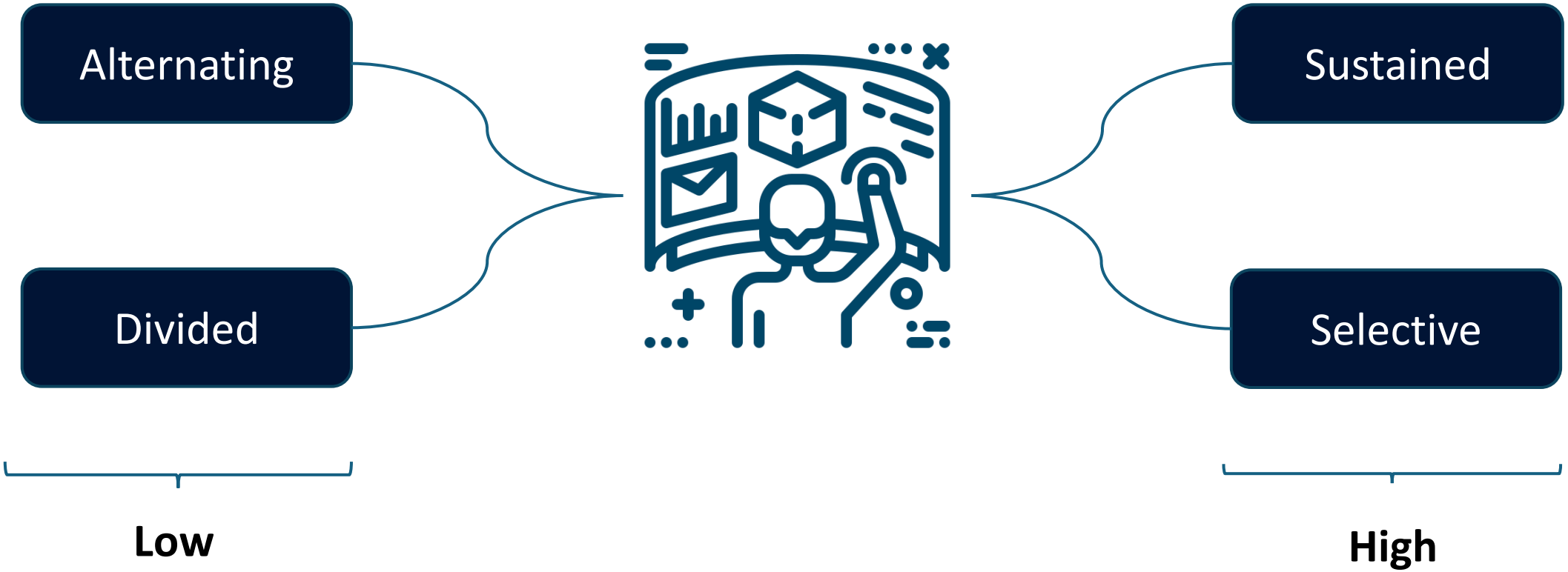


- Rapid
- Automatic
- Limited
- Emotionnal

- Slow
- Controllable
- Open
- Rational

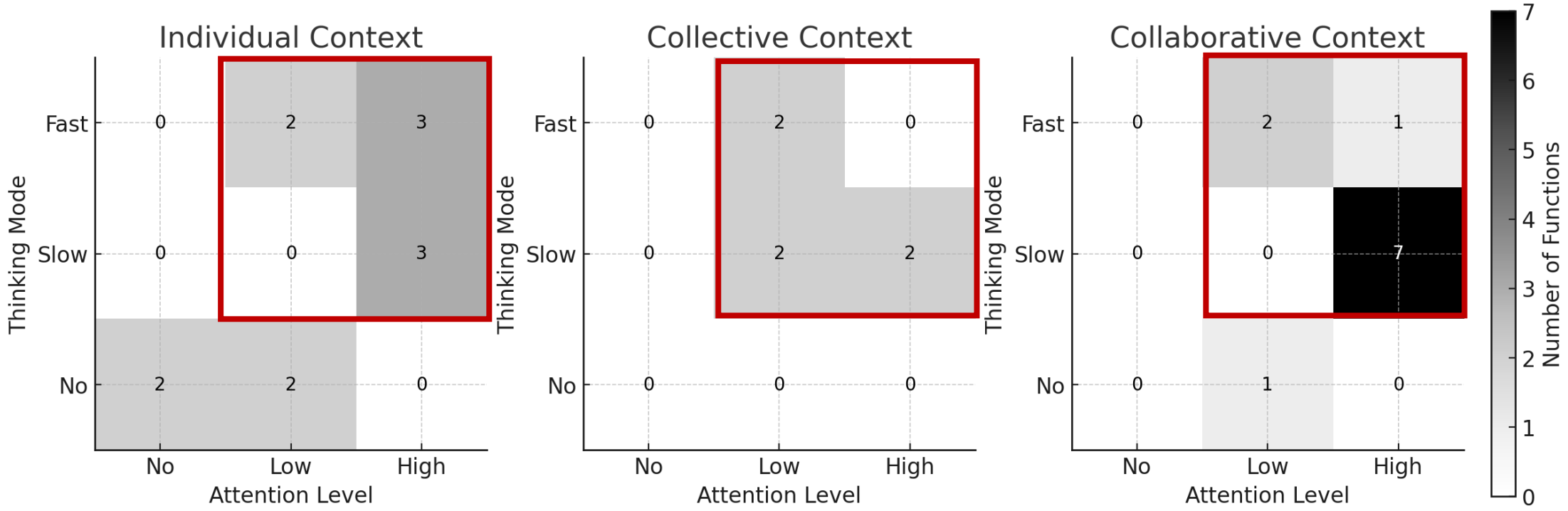
Understands situations → Identifies solutions

How to manage SOC operators Attention?



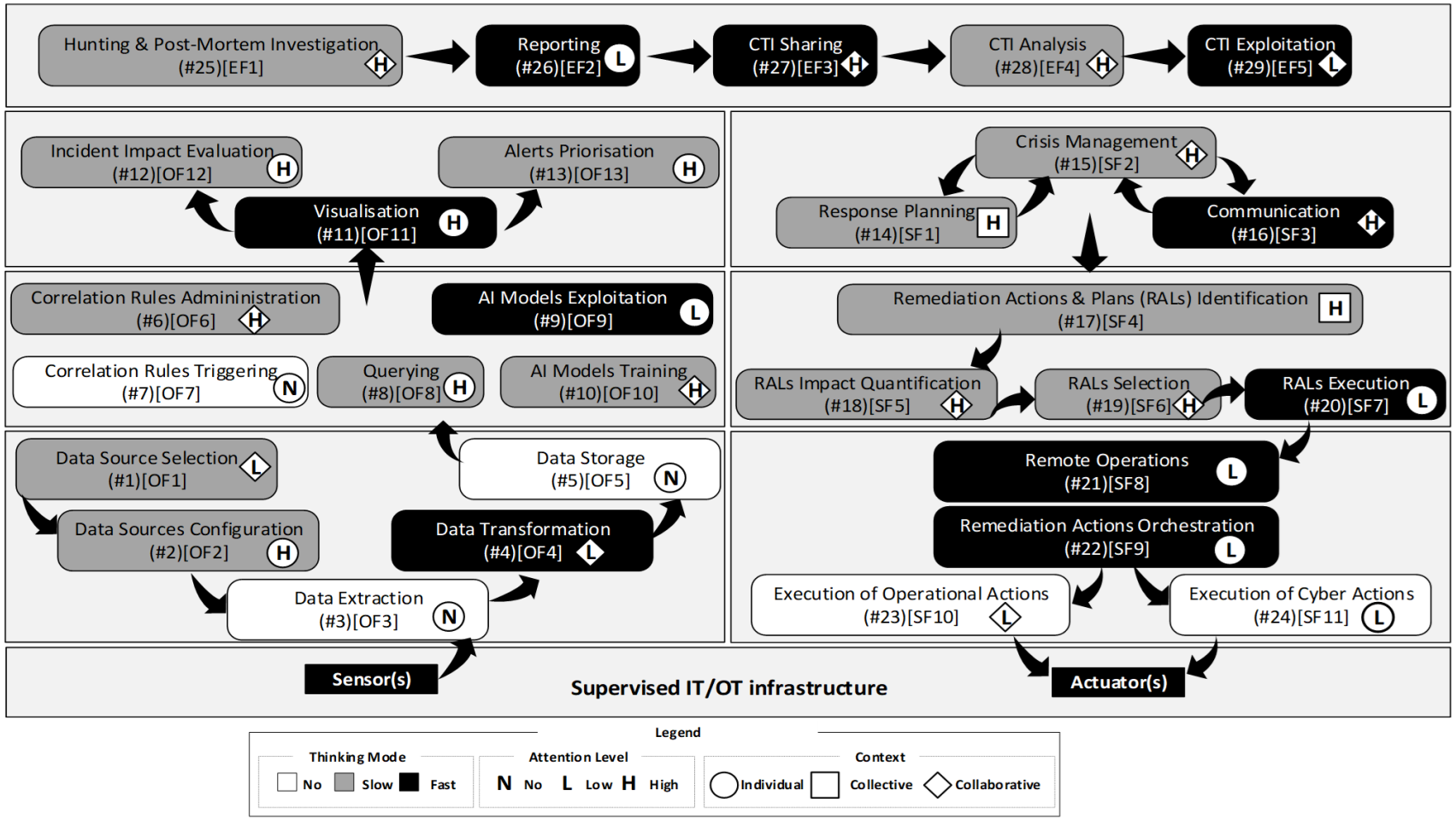
Based on Tremolada, M., Taverna, L., & Bonichini, S. (2019). Which Factors Influence Attentional Functions? *Behavioral Sciences*, *9*(1), 7.

Breaking the “black box” of SOC workflow

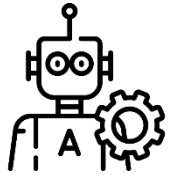


- 80% of SOC activities are cognitively demanding
  - More than 50% of SOC activities require High-Attention
  - Almost 50% of SOC activities are slow thinking (prevalence of System 2)

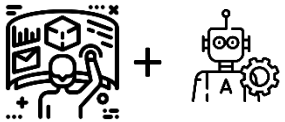
What SOC Operators are supposed to do? (Bis)



CYBER-AI-GO !
Complementarity in Human-AI Collaboration



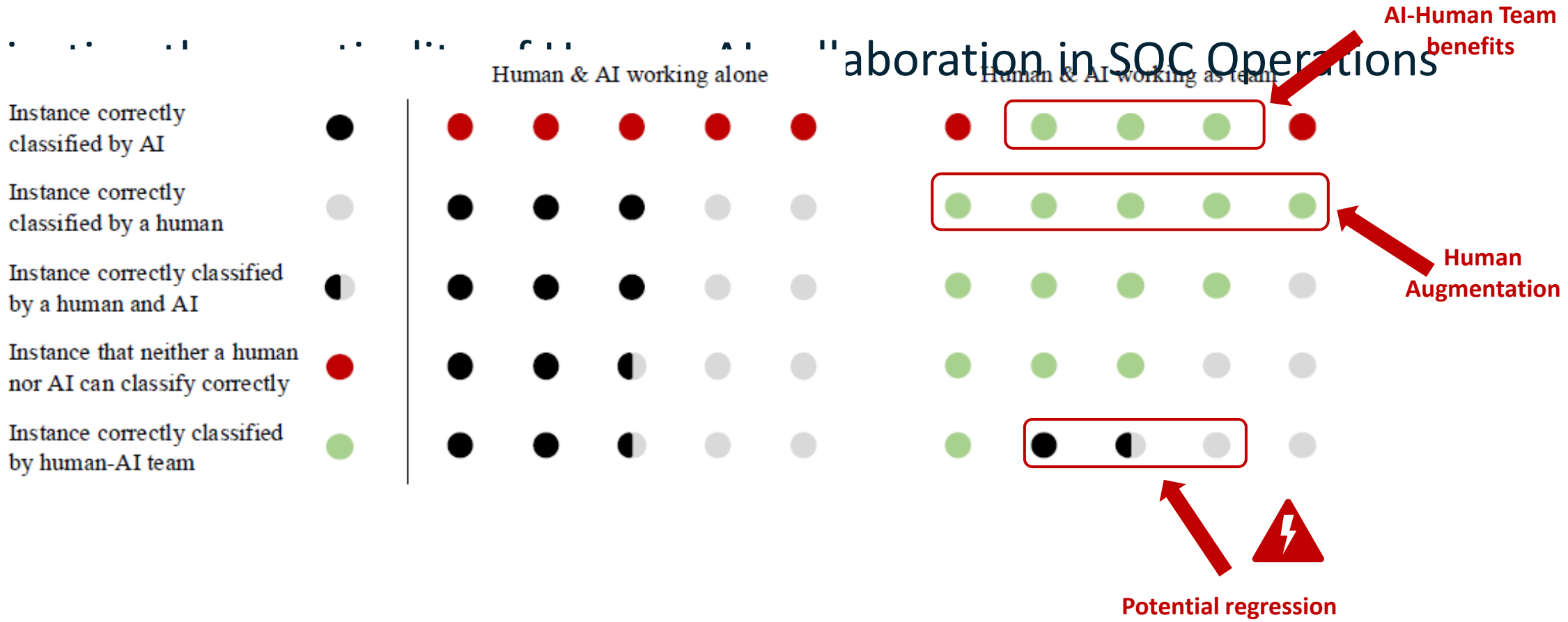
Inputs	**Information (Information / Knowledge)**	Asymmetry	**Information (Data)**
Processing	**Limited Reasoning (Time, pressure, stress, etc)**	Asymmetry	**Limited Contextualisation (Semantic Ambiguity)**
Outputs	**Actions**	Asymmetry	**Decisions**



Co-augmented Decision

Risk / Benefits of Human/AI Collaboration

Inves[illegible]aboration in SOC Operations



arXiv:2404.00029v2 [cs.HC] 25 Nov 2024

Objective: Shifting from "Human is the Loop" to "Human Over the Loop"

Cybelia
Augmented Cybersecurity

Human **is** the loop

Known

Unknown

Assistant

Human **in** the loop

Understand (✓)
Caracterize (✗)

Auto-Pilot

Human **out of** the loop

Understand (✓)
Caracterize (✓)

F30 Symbiotic Cybersecurity Operations

"Human Over the Loop"

Companion

Human **in** the loop

Understand (✗)
Caracterize (✓)

Operator

Human **out of** the loop

Understand (✗)
Caracterize (✗)

Thank you for your attention!

Cybelia

Cybersécurité augmentée
pour l'industrie

AIRBUS PROTECT

Rte

SystemX INSTITUT DE RECHERCHE TECHNOLOGIQUE

reda.yaich@irt-systemx.fr