Toward a SOC Maturity Model for Artificial Intelligence

Dr. George Antoniou - Lynn University | Fulbright Scholar Residency

Agenda

Motivation & Aim

Scope & Research Questions

AI in Defense-in-Depth

Conceptual Benchmarking

Opportunities & Challenges

Proposed SOC AI Maturity Model

Recommendations, Metrics, Future Work

Motivation

Emerging environments often lack structured SOC processes.

Adopting AI without readiness introduces inefficiency and integration risks.

A maturity model creates a phased path.

Only 38% of organizations in emerging regions report having a formal SOC (ENISA, 2024)

AI without readiness = inefficiency and risk

Scope & Method

SYSTEMATIC LITERATURE REVIEW USING PRISMA METHODOLOGY.

EXTRACTED ATTRIBUTES FROM AI-DRIVEN IDS/DDOS STUDIES.

MAPPED TO SECURITY LAYERS, VALIDATED WITH INDICATORS OF COMPROMISE.

Research Questions

RQ1: What IOCs are most relevant for AI-based detection?

RQ2: How can AI techniques be mapped to defense-in-depth layers?

RQ3: How do AI-enhanced approaches benchmark against global incidents?

AI in Defense-in-Depth

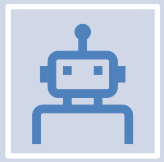
Mapped AI techniques to layers: perimeter, network, endpoint, application, IAM, data, and cloud.

Examples include LSTM for anomaly detection at the network layer and XAI for enhancing interpretability at the endpoint layer.

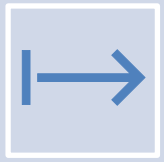
- LSTM = Long Short-Term Memory network, a type of recurrent neural network for sequential data.
- XAI = Explainable Artificial Intelligence.

AI strengthens, not replaces, defense-in-depth

Benchmarking Insights



AI approaches reduce false positives, improve detection latency, and strengthen SOC efficiency.



Trade-offs include integration complexity and computational overhead.

Reported benefits remain context-dependent.

Values drawn from reviewed studies (n≈40)

AI improves detection but increases computational demand

Opportunities & Challenges

Opportunities: forecasting attacks, federated learning, explainability.

Federated learning → collaboration without data sharing

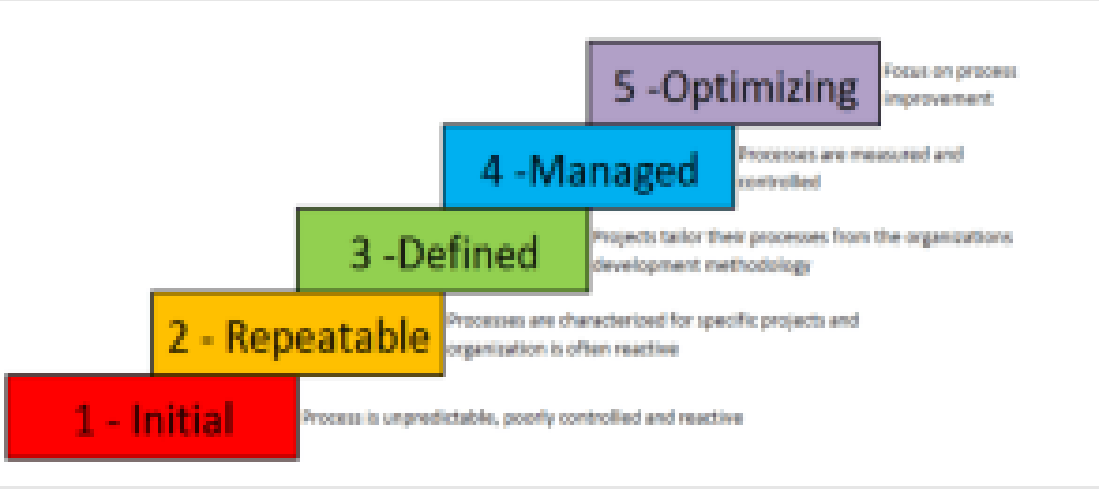
Challenges: integration with SIEM, adversarial robustness, lack of large-scale trials.

SOC AI Maturity Model

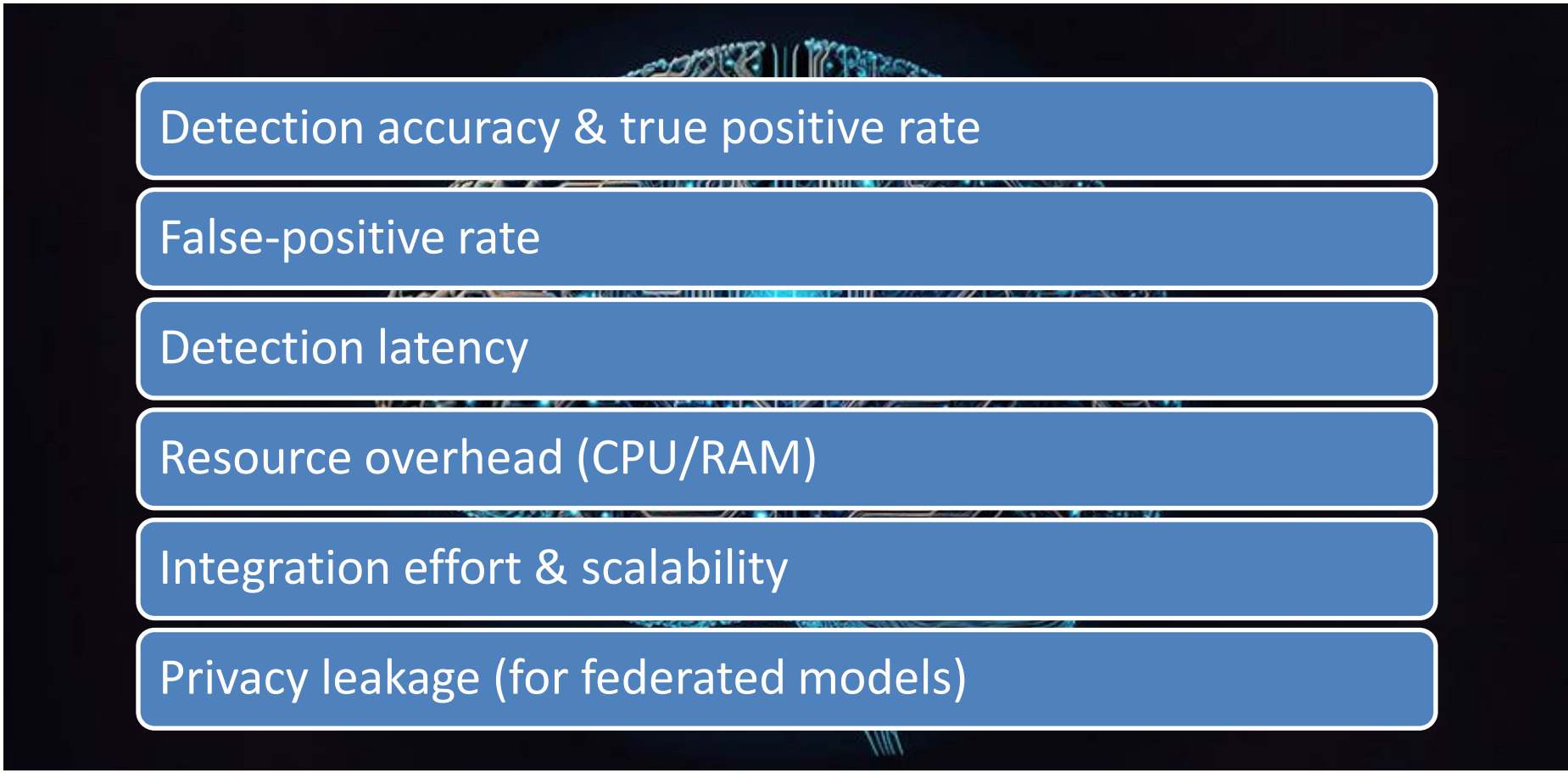
- Tier 1: Pilot Proof-of-Concept - Initial AI trials with ensembles, baseline metrics.
- Tier 2: Integrate Layered Deployment - XAI integrated into playbooks, metrics tracked.
- Tier 3: Collaborate Federated & Transfer - Federated learning, privacy-preserving.
- Tie 4: Autonomous Adversarial & Automation - Reinforcement learning, adversarial robustness, orchestration.

- Aligned with CMM and guidance from ENISA and NIST.

- Increasing Capability and AI Governance



Metrics for Governance



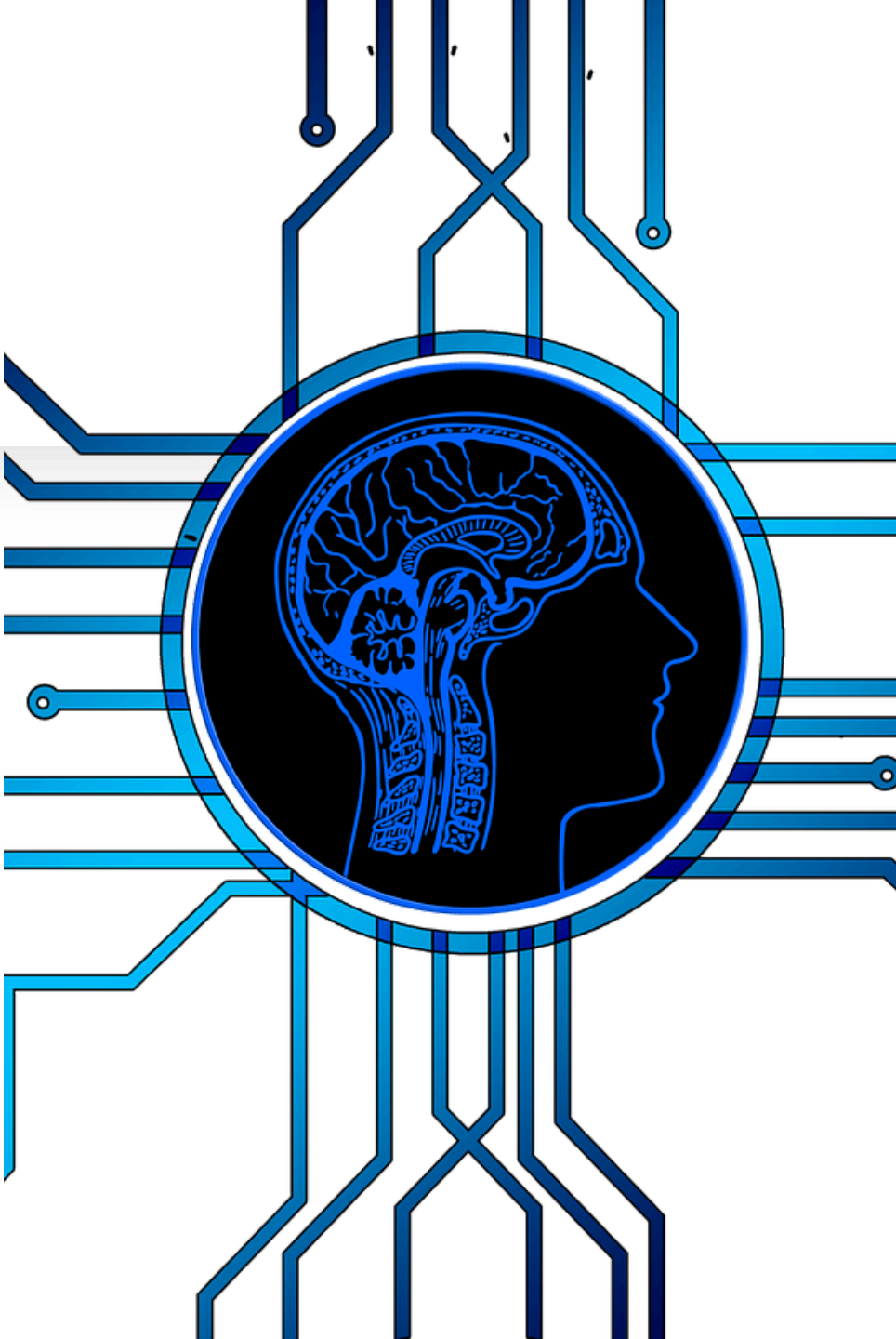
Metrics = checkpoints for maturity progression

Example target: reduce false positives by 25% before advancing to next tier.

Conclusion

- This roadmap and metrics framework provide a structured way for SOCs to assess readiness and guide AI adoption responsibly.
- AI should extend human expertise, not replace it

Q&A



Thank you.
Questions welcome.

Contact:
gantoniou@lynn.edu