CYNQ

AI-Driven Security Operations: Lessons from the Frontline

Chathura Abeydeera

*Director – **CYNQ***

About me

- Offensive Cyber and Intelligence
- I run **CYNQ**
- PhD Candidate
- GAICD, MBA, MSc
- CCSAM, CCT, OSCP, CISSP, CISM, CRISC
- Fellow of AISA, CREST

Every SOC Has the Same Challenge

The question isn't **"Should we use AI?".** It's **where does AI actually help?**

Alert Overload

Thousands of alerts daily, with no meaningful prioritisation

Attacker Speed

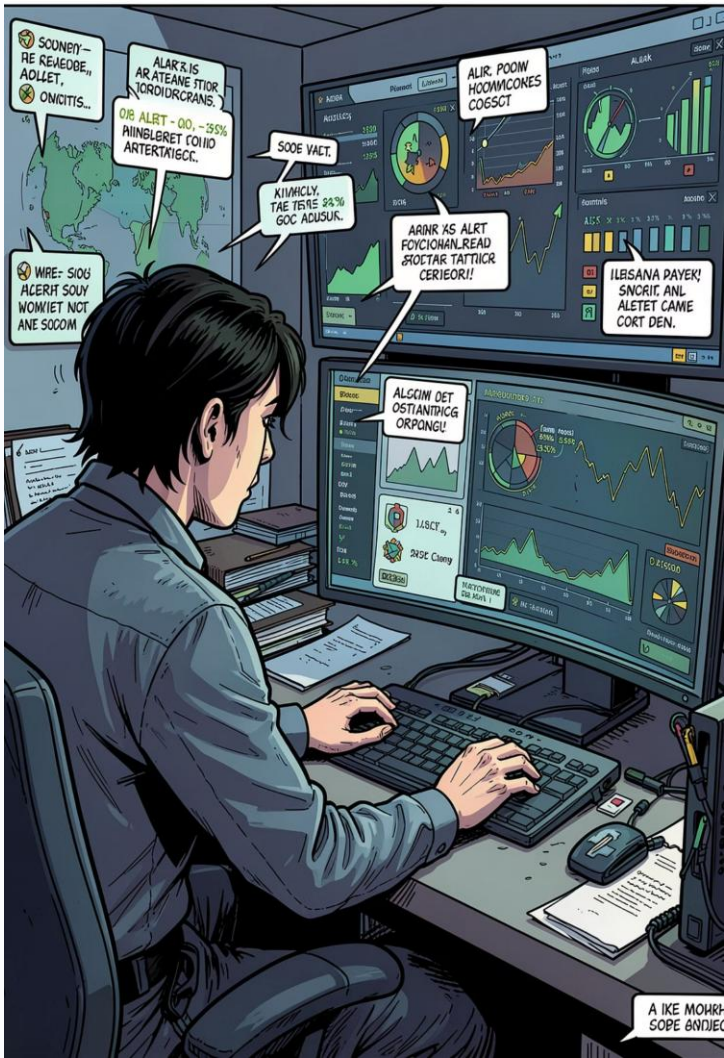
Adversaries move faster than manual investigation keeps up

Analyst Shortages

Investigation fatigue and a persistent skills gap

Pressure to Improve

Demands to reduce MTTD and MTTR across a growing attack surface



CYNQ

AI Isn't One Thing

Capability	Typical Use
Chatbots	Answer questions
Copilots	Assist analysts
AI Agents	Perform investigations
Autonomous AI	Execute actions independently

In Australia currently,

Most organisations sit between Copilot and Agents.

Full autonomy is still rare in production SOCs.

CYNQ

GenAI vs Agentic AI

GenAI - Assistant

- Answers questions
- Summarises logs
- Drafts reports
- Reactive, waits for prompts
- No tool integration
- Single-turn interaction

Agentic AI - Investigator

- Investigates incidents
- Correlates evidence
- Builds attack timelines
- Goal-driven pursues objectives
- Uses tools - SIEM, EDR, Cloud, CMDB
- Multi-step reasoning

GenAI explains. Agentic AI investigates.

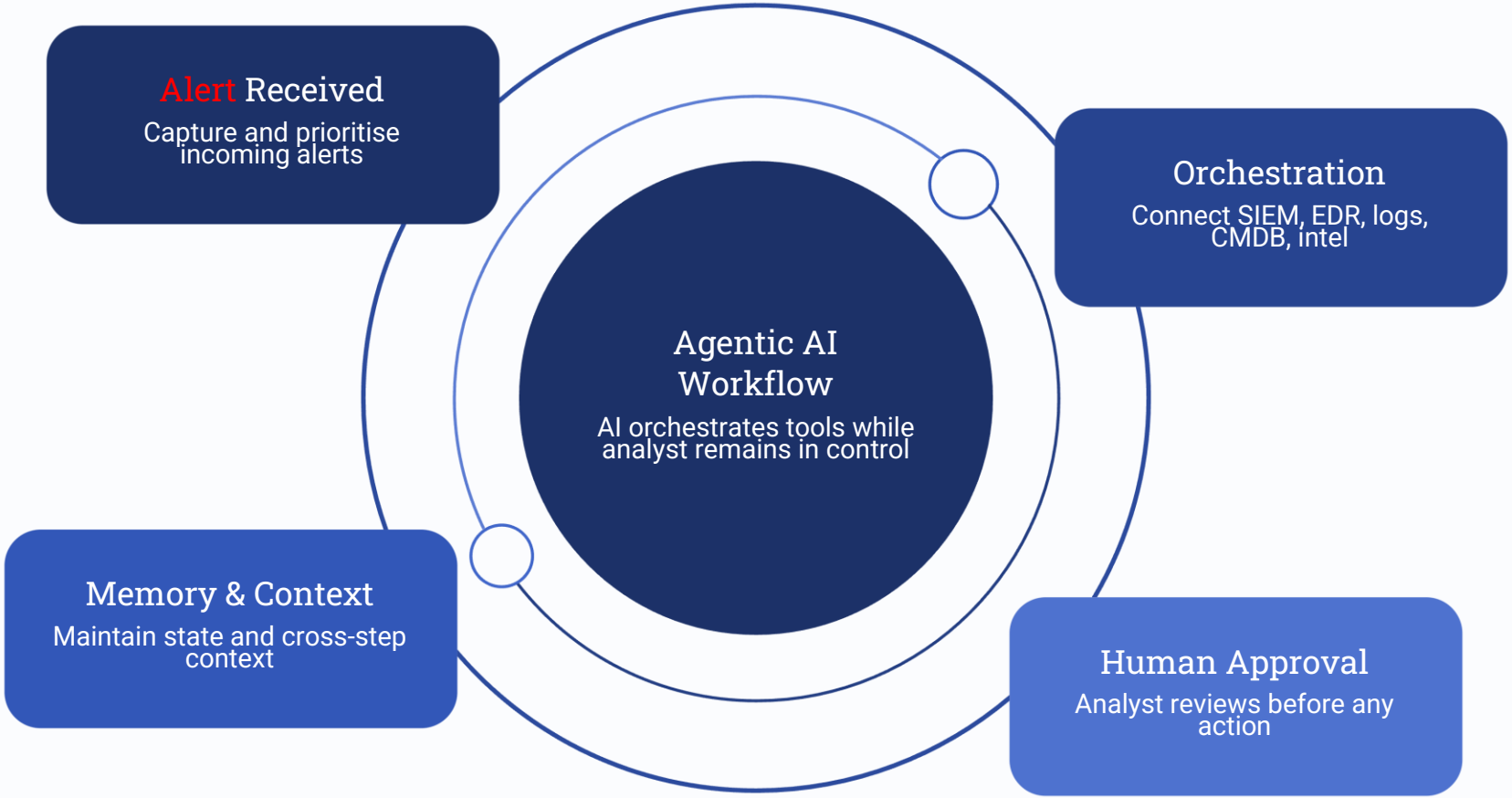
The Traditional SOC Investigation

Analysts spend most of their time moving between tools, not analysing. Each context switch adds time, risk, and fatigue.

This **tool hopping** is where AI adds the most value , not in replacing analyst judgement, but in eliminating the manual legwork between decisions.

Where Agentic AI Fits

AI doesn't replace your tools. It **orchestrates** them. The analyst stays in control; the AI handles the legwork.



CYNQ

Who Does What? - Human + AI: Redefining the Division of Labor

Clarity in role assignment eliminates friction and accelerates response.

AI Handles

- Correlation & IoC enrichment
- Timeline construction
- Documentation & report drafting
- Investigation support

Shared Actions

- Containment decisions
- Access revocation
- Escalation triggers

Humans Own

- Strategy & threat hunting
- Root cause analysis
- Risk acceptance & crisis leadership
- Executive communication

AI excels at repetitive investigative work. Humans own judgment.
Agentic AI is an operational capability, not a chatbot. Start small, measure outcomes, and build trust incrementally.

CYNQ

Vinaka!