AI SecOps: Noise Into Insight

Samson Adewale

November 2025

Who dis??

- BSides ATL newbie presenter 🎤
- Threat Response Engineer @ Klaviyo 🛡️

Problem

Too Many Alerts. Too Little Time

- Thousands of daily signals
- Repetitive manual triage
- Context switching & fatigue

Opportunity

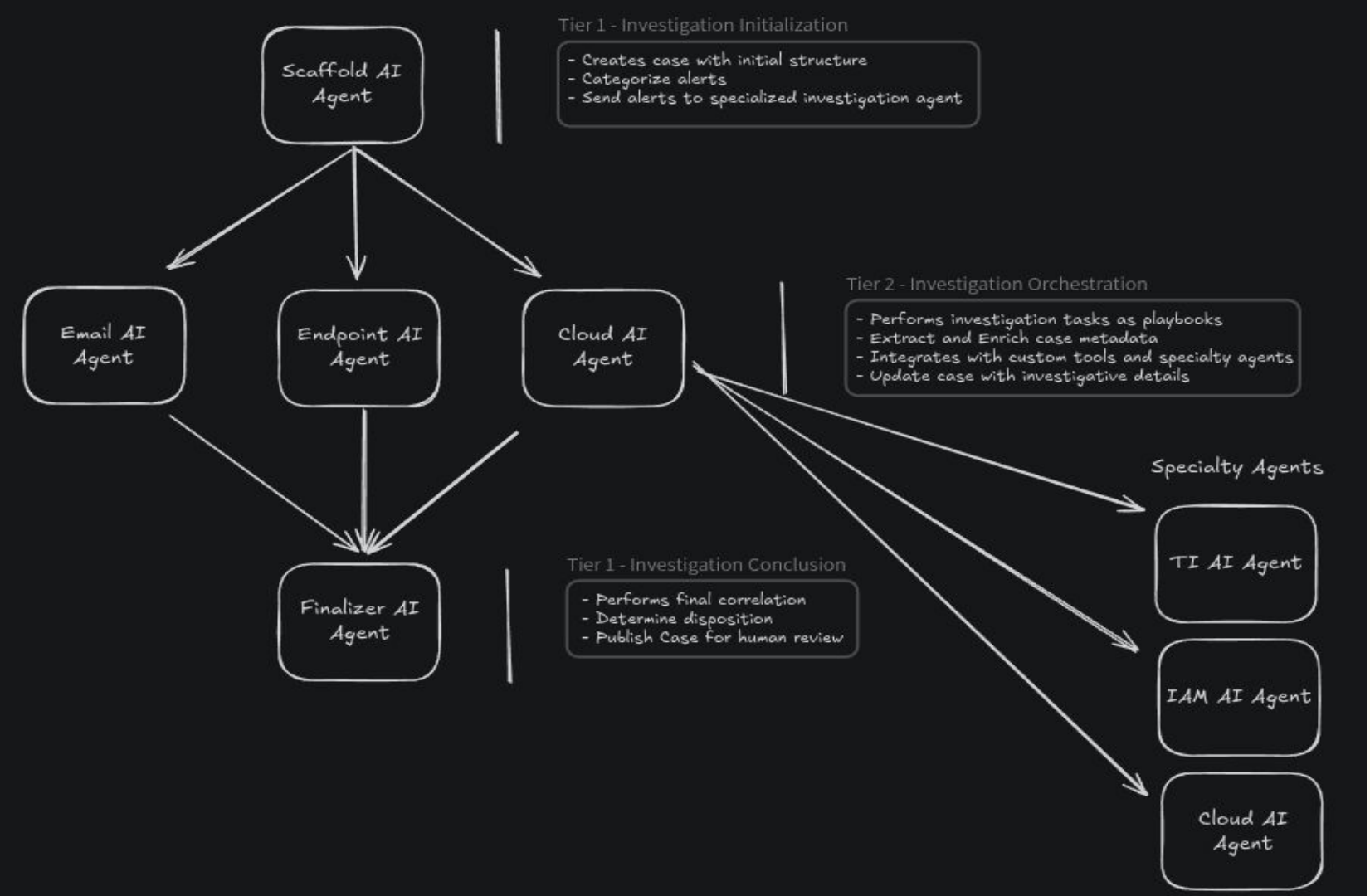
Cognitive Augmentation for Defenders.

🧠 *Assist, not replace.*

- Alert triage / analysis
- Incident summarization
- Context enrichment
- Response actions (HITL)

Designing the System

- Agent Frameworks 🧩
- Model Selection 🤖
- Prompt & Context Design ✍️
- Token & Cost Management 💰
- Workflow Orchestration ⚙️


Tier 1 - Investigation Initialization
- Creates case with initial structure
- Categorize alerts
- Send alerts to specialized investigation agent
Scaffold AI Agent
Email AI Agent
Endpoint AI Agent
Cloud AI Agent
Tier 2 - Investigation Orchestration
- Performs investigation tasks as playbooks
- Extract and Enrich case metadata
- Integrates with custom tools and specialty agents
- Update case with investigative details
Specialty Agents
TI AI Agent
IAM AI Agent
Cloud AI Agent
Finalizer AI Agent
Tier 1 - Investigation Conclusion
- Performs final correlation
- Determine disposition
- Publish Case for human review

Excalidraw

Demo

Key takeaways

1. Start small - pilot AI on low-risk, repetitive tasks
2. Keep humans in the loop - AI assists, not replaces
3. Track Metrics - Reduction in time and complexity
4. Share learnings - community-driven defense wins

Getting in touch

- Slides on samsonadewale.com
- Email via samwale008@gmail.com

Thank you

This content is for general informational purposes only and should not be considered a substitute for professional advice. Please credit Samson Adewale when using this content.

samsonadewale.com