

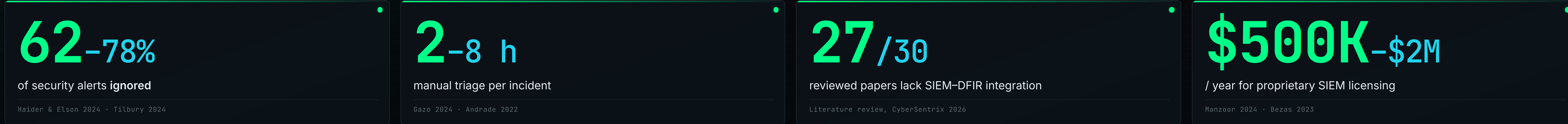
CyberSentrix

Integrating AI for Automated Forensic Investigation and Dynamic Incident Response in SIEM

TEAM · GROUP 9MY1		SUPERVISORY COMMITTEE			
Mustafa Ali Al-Jishi	2220002432	Mohammed Essam Al-Abdulhay	2220000530	Mr. Saad Abdulrahman Alharathi	Supervisor
Mohammed Abdulmuhsen Almutawah	2220005395	All Nasser Al-Hussain	2220006383	Prof. Nazar A. Saqib	Committee
Abdullah Musaad Bin Saeed	2220000092			Mr. Sghaier R. Chabani	Committee

01 THE PROBLEM

Modern Security Operations Centres drown in alerts while powerful DFIR tooling sits **one door away** — disconnected, manual, and slow.



02 SOLUTION · FOUR-LAYER ECOSYSTEM

L1 DATA ACQUISITION
Wazuh agents on Windows / Linux endpoints stream EventLogs · Sysmon · Auditd over AES-256 / TCP 1514. Wazuh Agent Sysmon Auditd

L2 DETECTION & ANALYTICS
Wazuh Manager correlates **3 000+** rules mapped to MITRE ATT&CK. OpenSearch indexes events for **sub-millisecond** queries. Wazuh Manager OpenSearch MITRE ATT&CK

L3 FORENSIC RESPONSE
Python bridge polls alerts every 30 s and triggers Velociraptor VQL hunts for memory, registry, network & filesystem artefacts. Velociraptor VQL Python 3.11

L4 INTELLIGENCE & ORCHESTRATION
AI Copilot (LLM + RAG) contextualises alerts, recommends VQL, and summarises incidents in natural language — all under analyst oversight. Mistral 7B Qdrant BAAI/bge-Large FastAPI

HITL APPROVAL GATE

03 AI COPILOT CAPABILITIES

Alert Contextualization
Plain-English alert summary + MITRE ATT&CK tactic / technique mapping on demand.
`> contextualize alert 4847291`
T1059.B01 PowerShell · attacker enumerating AD via Get-DomainUser → likely reconnaissance stage.

Forensic Action Recommendation
Context-aware VQL queries suggested for memory, registry, persistence, network capture.
`> recommend VQL for persistence check`
Artifact.Windows.Persistence.ScheduledTasks → pulls autoruns, scheduled tasks, registry Run keys.

Incident Summarization
Fuses detection + forensic evidence into a cohesive incident narrative ready for analyst review.
`> summarize incident INC-0142`
4-stage intrusion: phishing → PS beacon → lateral via PsExec → credential dump on DC01.

04 METHODOLOGY

RAG Knowledge Pipeline

- Ingest**
MITRE ATT&CK · NIST CSF 2.0 · SOAR playbooks · IR guides
- Embed**
BAAI/bge-large-en-v1.5 · Matryoshka multi-dim
- Index**
Qdrant · cosine similarity · 3 collections (3 061 chunks)
- Retrieve + Generate**
top-k 50 · top-p 0.9 · temp 0.1 · max 4 096 tok

Attack Simulation Suite

TA0011	C2 Communication	Sliver / Cobalt Strike
TA0006	Credential Access	Mimikatz-style
TA0008	Lateral Movement	Pass-the-Hash · PsExec
TA0003	Persistence	Scheduled Tasks · Run keys

Validation Framework

Design Paired: manual baseline vs. CyberSentrix
Primary MTR (alert → forensic evidence)
Secondary FP rate · cognitive load · end-to-end latency
Stats Paired t-test / Wilcoxon · Cohen's d · $\alpha = 0.05$

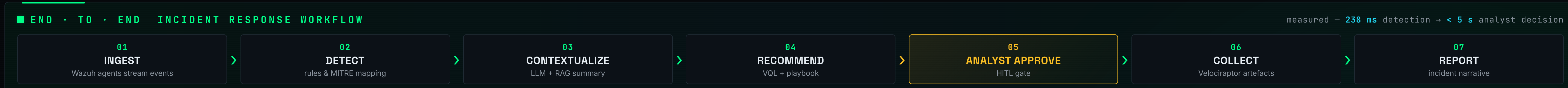
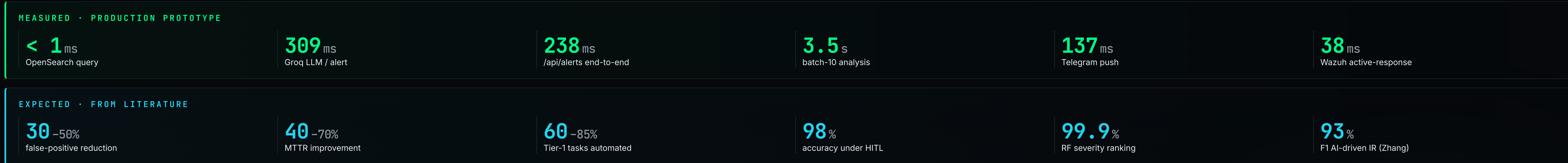
05 RESULTS · SYSTEM IN ACTION

SCREENSHOT · UNIFIED SOC DASHBOARD
cyber.shari.digital / dashboard

SCREENSHOT · AI ALERT TRANSLATION
plain-English severity judgement

SCREENSHOT · MITRE ATT&CK HEATMAP
tactic / technique coverage

SCREENSHOT · HITL ACTION QUEUE
approve · reject · execute



06 IMPACT & CONCLUSION

CyberSentrix closes the **SIEM-DFIR integration gap** flagged in 27 of 30 reviewed papers, delivering sub-second AI contextualisation under **mandatory analyst approval** — entirely on open-source infrastructure, at **zero licensing cost**.

- HITL** by design — every forensic action is analyst-approved
- OPEN** fully open-source stack, reproducible on commodity hardware
- FAST** sub-second detection and AI reasoning in production
- AUDIT** immutable AI/HITL audit log, 365-day retention



SCAN FOR LIVE DEMO
cyber.shari.digital

KEY REFERENCES

- [1] Ban et al. *AI-assisted SIEM*. 2023. 99.0% recall, 97.8% alert reduction
- [2] Kim et al. *CyberAly: KG-RAG SOC Copilot*. 2025. 99.92% triage precision
- [3] Freitas et al. *Microsoft Copilot Guided Response*. 2025. 84.8% accuracy
- [4] Ismail et al. *SERC: RAG Copilot for Wazuh*. 2025. 84.8% accuracy
- [5] Eckhoff et al. *Graph-based Alert Contextualisation*. 2025.
- [6] Tilbury & Flowerday. *SOC Automation Matrix*. 2024.
- [7] Manzoor et al. *Wazuh: 14 000 EPS*. 2024. 93% F1, 58 ms latency

PROJECT CONTACT

Group 9MY1 · CyberSentrix
cybersentrix@iau.edu.sa
github.com/cybersentrix