PostecH

Tunich

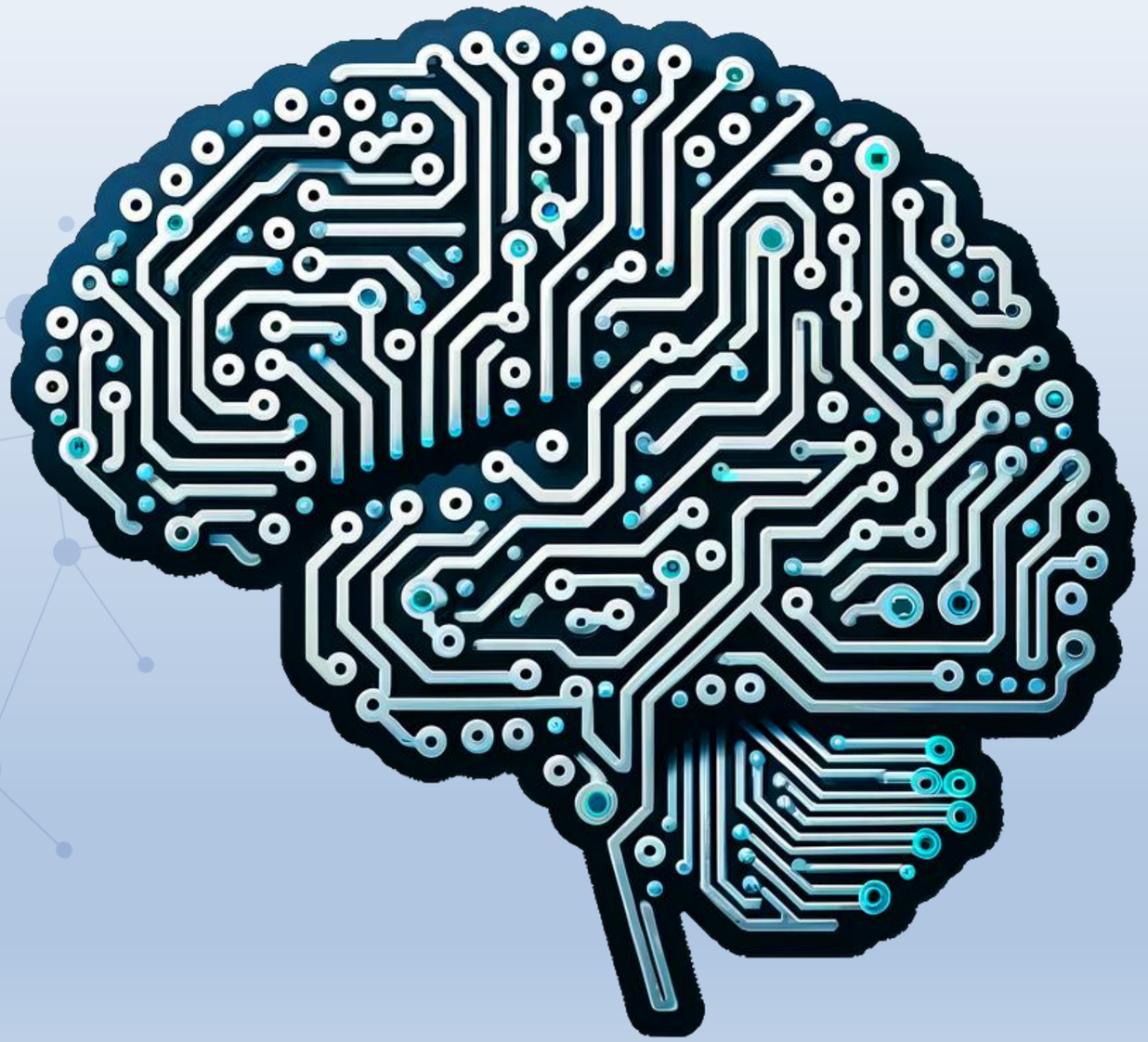
Brochure

postech.us

Tunich

Intelligent Automation for Triage and Enrichment of Cybersecurity Tickets.

Empower your Security Operations Center (SOC) team with a private AI engine that transforms alerts into actionable analytics, aligned with global frameworks in record time.



The Challenge: Alert Overload and Operational Friction

IT and security directors face a critical paradox: more tools generate more alerts, but human teams aren't scaling up. This results in:

ALERT FATIGUE
Analysts overwhelmed reviewing false positives.

SLOW RESPONSE TIME
Manual triage and initial investigation consume more than 50% of critical time.

FRAGMENTED KNOWLEDGE
Difficulty consistently aligning incidents with frameworks such as MITRE ATT&CK, NIST or ISO 27001.

RISK OF ESCAPE
Staff turnover brings with it valuable tacit knowledge.

Our Solution: An AI Copilot for your SOC

SOC Assistant AI is an on -premise software platform that securely deploys a specialized Language Model (LLM) within your infrastructure. It acts as an automated junior analyst, working 24/7, performing the initial analysis of each ticket.

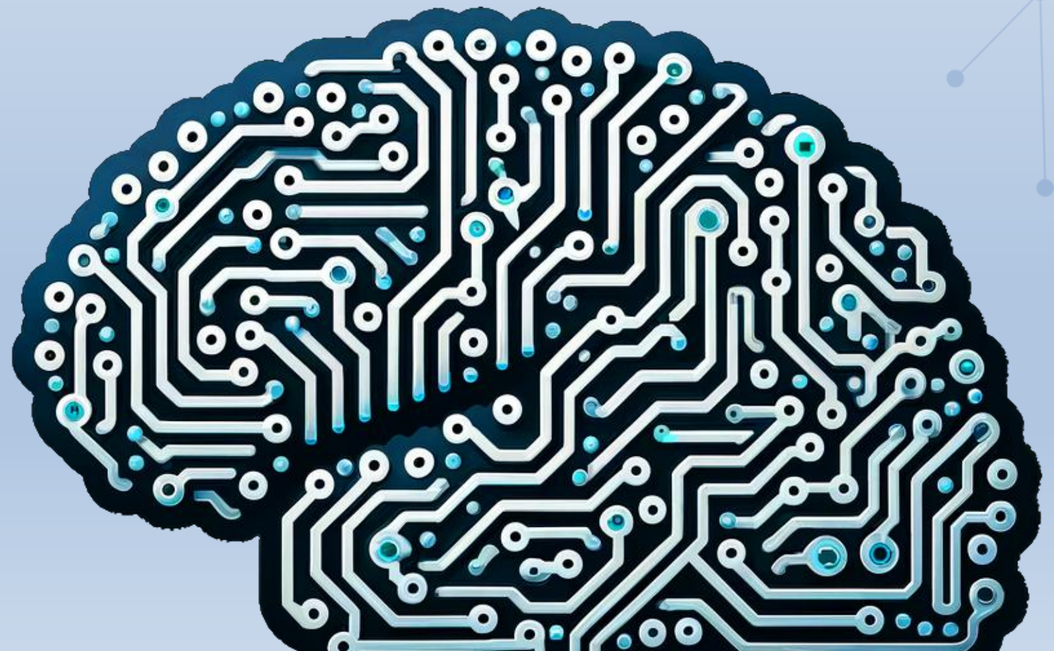
MITRE | ATT&CK®

NIST | NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

ISO 27002

How does he do it?

1. Automatic Ingestion: Connects with your ticket sources (email, API, SIEM).
2. Real-Time Analysis and Consultation: The LLM extracts key entities and automatically queries a unified knowledge base with the MITRE ATT&CK, NIST CSF and ISO 27001 frameworks.
3. Rich Ticket Generation: Produces a consolidated ticket with:
- Clear Classification and Context.
- Calibrated Risk Level (Based on context and frameworks).
- Mapping to Reference Frameworks: Tactics, techniques (MITRE), controls (NIST/ISO).
- Actionable Mitigation Recommendations.



Key Benefits for the IT Director/CISO

• Accelerate Response Time (MTTR): Reduce the triage and initial investigation phase by up to 80%, allowing your senior analysts to focus on complex threats.

• Standardize and Scale Knowledge: Ensure that every incident, regardless of who reviews it, is analyzed against industry-leading frameworks, raising the quality and consistency of your operations.

• Reduce Operational Risk: Decrease the probability of human error in initial classification and ensure that no ticket passes without the relevant compliance and mitigation references.

• Maximize your investment in personnel: Free your talented analysts from repetitive tasks, increasing their satisfaction and allowing them to develop threat-hunting skills and advanced response.

• Total Data Privacy and Sovereignty: Everything runs locally on your servers. Your sensitive incident data never leaves your network. Compliant with the strictest regulatory requirements (GDPR, LGPD, etc.).

• Frictionless Integration: Connects with your existing security stack via APIs . It's a strength multiplier for your existing tools (SIEM, SOAR, ticketing platform).

Why is our solution different?

Feature	Generic AI/ML Solutions	SOC Assistant AI
Privacy	Often in the public cloud (data risk).	100% On-Premise / Private Cloud.
Context	Generic alert analysis.	Specialized in Cybersecurity with integrated knowledge of MITRE, NIST, ISO.
Result	More data or scores.	Actionable and enriched ticket ready for SOC workflow.
Implementation	Complex black boxes.	Open and modular architecture, adaptable to your processes.

Reliable and Scalable Architecture

- Backend in FastAPI (Robust and fast).
- AI engine (LLM Open- Source) selected for balance between performance and accuracy.
- Vector Database (ChromaDB / Weaviate) for semantic search in knowledge frameworks.
- Optional Frontend (React) or full API integration with your ticketing system (ServiceNow , Jira, etc.).

Imagine a SOC where:

✓ Alerts are categorized and enriched in seconds, not minutes.

✓ Compliance reports (NIST, ISO) are automatically generated from tickets.

✓ Their team focuses on hunting threats, not cleaning data.
Tunich SOC Assistant AI is not just another tool; it is the natural evolution of your operations center.

Tunich SOC Assistant AI is not just another tool; it is the natural evolution of your operations center.

PostecH

THANK YOU

sales@postech.us

postech.us