

Accelerate alert triage, incident analysis and response planning
with contextual AI support that keeps analysts in control.



AI-POWERED SOC AUGMENTATION FOR FASTER, MORE ACCURATE INCIDENT RESPONSE

Fast

Reliable Always available
Accelerated evidence
gathering and incident
prioritization.

Reliable

Explainable, auditable
decision support with
human-in-the-loop control

Always available

24/7 AI-assisted analysis
without operational gaps.

PRODUCT OVERVIEW

PULZARIS AI SOC Analyst is an AI-driven SOC augmentation layer that sits above SIEM environments. Designed to enhance and accelerate SOC operations across security environments. It automates alert triage, incident analysis, and response support while keeping analysts in control. It helps security teams reduce noise, prioritize real threats, and strengthen investigation workflows. SOC AI Analyst is the first component of PULZARIS — a growing ecosystem of interoperable AI agents.

SOC challenges

- Too many unhandled alerts and incidents
- Not enough human resources
- Lack of analysts with deep technical knowledge
- Slow alert and incident analysis time
- 24/7 worktime

CORE CAPABILITIES



Secure by Design

Privacy-preserving AI analysis
Data obfuscation before AI processing
Deployment-ready for enterprise environments



Built for SOC Reality

Deep telemetry analysis across alerts, logs, packets, endpoint and UEBA data
Entity correlation across data sources
24/7 continuous investigation



Explainable by Design

Explainable scoring with confidence levels
Analyst-in-the-loop validation
Repeatable, auditable workflows



Operational Impact

Risk-based prioritization using asset criticality
Automated enrichment and scoping
Exportable reporting with MITRE and VERIS context

Ready to learn more? Visit our website

www.pulzaris.ai

TECHNICAL OVERVIEW

AI Engine: Google Gemini Large Language Model.

Integration: NetWitness Respond, Concentrator, ESA rule database.

API Support: Google (required), VirusTotal (optional), AbuseIPDB (optional).

Deployment: Runs on a NetWitness host.

KEY BENEFITS

Modern SOCs face an overwhelming volume of alerts, a shortage of skilled analysts, and rising pressure to respond faster to evolving threats. The PULZARIS AI Module addresses these challenges by combining automation with contextual intelligence – ensuring real threats are prioritized, investigations are accelerated, and analyst workloads are reduced. With explainable AI and seamless integration into the NetWitness Platform, it strengthens defenses while keeping humans in control.

AI Analysis Results

Automatically generated reports:

- AI Engine: Google AI
- Executive Summary
- Confidence Score (T/F positive)
- To-Do list with recommended actions
- Malicious Activity Timeline
- Technical Details including IOCs and sources
- VERIS/MITRE framework



Rapid and flexible integration
with the existing SIEM environment



Transparent, explainable, auditable
result



Supports analysts
by taking over repetitive tasks



Focuses on validated threats
by filtering false positive



Speeds up response
with AI-driven investigation accuracy



24/7 Non-stop Operation
beyond human limits

PULZARIS AI

combines proven security operations expertise with scalable AI-optimized design to support multiple SOC use cases in one coherent framework

ABOUT US

20+ Years of Cybersecurity Expertise
– proven experience in protecting businesses.

Trusted Technology Partnerships
– strong collaborations with top security vendors.

Scalable AI-Optimized Solutions
– designed to grow with your organization.

Comprehensive AI-Powered Ecosystem
– one framework to solve multiple SOC challenges.