SERA AI

AI-Driven Cybersecurity Intelligence Feature for aiSIEM

Overview

SERA AI is a GenAI-based feature designed to enhance our aiSIEM, by offering advanced, AI-driven insights. Leveraging Retrieval-Augmented Generation (RAG) and Anthropic Cloud Sonet 3.5 models from AWS, SERA AI personalizes responses using real-time data from aiSIEM, while ensuring privacy through PII masking

Key Features:

1. Deep Tracker: Complex Query Analysis:

- Allows for the analysis of complex cybersecurity queries using natural human language.
- Users can frame queries in plain English, and SERA AI translates these into actionable insights by searching through relevant security data.

2. Alert Analysis & Actionable Intelligence:

- SERA AI processes and analyzes alerts from aiSIEM, delivering concise, human-readable interpretations of the alerts.
- Provides actionable intelligence like MITRE attacker group, guiding security teams with practical steps for remediation.

Highlighting SERA AI: New Add-On for aiSIEM

GAIN TRUST WITH UNIFIED VISIBILITY AND THREAT INTELLIGENCE CAPABILITIES

Uncover a myriad of threat vectors lurking inside your existing logs,auto-discovered hosts, network, cloud, OT and loT infrastructure, Seceon aiSIEM combines this telemetry with 360° inference drawn from events, network traffic, packets, identities and behavioral patterns.

REDUCE MEAN TIME TO DETECT AND RESPOND

Considerably shorten Mean-Time-To Detect (MTTD) and Mean-Time-To Response (MTTR) with automated threat detection and remediation in real-time and score them by confidence level and criticality.

EFFORTLESS DEPLOYMENT AND INTEGRATIONS

With just one collector, you can start sending flows and logs and deploy Seceon aiSIEM. Then you can connect your existing technology stack with hundreds of integrations.

CONTINUOUS COMPLIANCE

Ensure compliance 24x7 with Seceon's audit and reporting capabilities for PCI-DSS, HIPAA, NIST, GDPR and more. Additionally monitor security postures, operations and investigations reporting.

3. **Data Privacy and Security:**

- All data retrieved from aiSIEM is masked before being sent to the GenAI model, ensuring no Personally Identifiable Information (PII) is exposed.
- Ensures privacy compliance while delivering contextual, personalized AI responses tailored to each tenant or user.

4. **Retrieval-Augmented Generation (RAG):**

- Employs RAG techniques for improved response generation by pulling relevant, context-specific data from aiSIEM.
- Enhances the accuracy and relevance of responses, making SERA AI highly adaptive to the latest security alerts and events.

Technical Specifications:

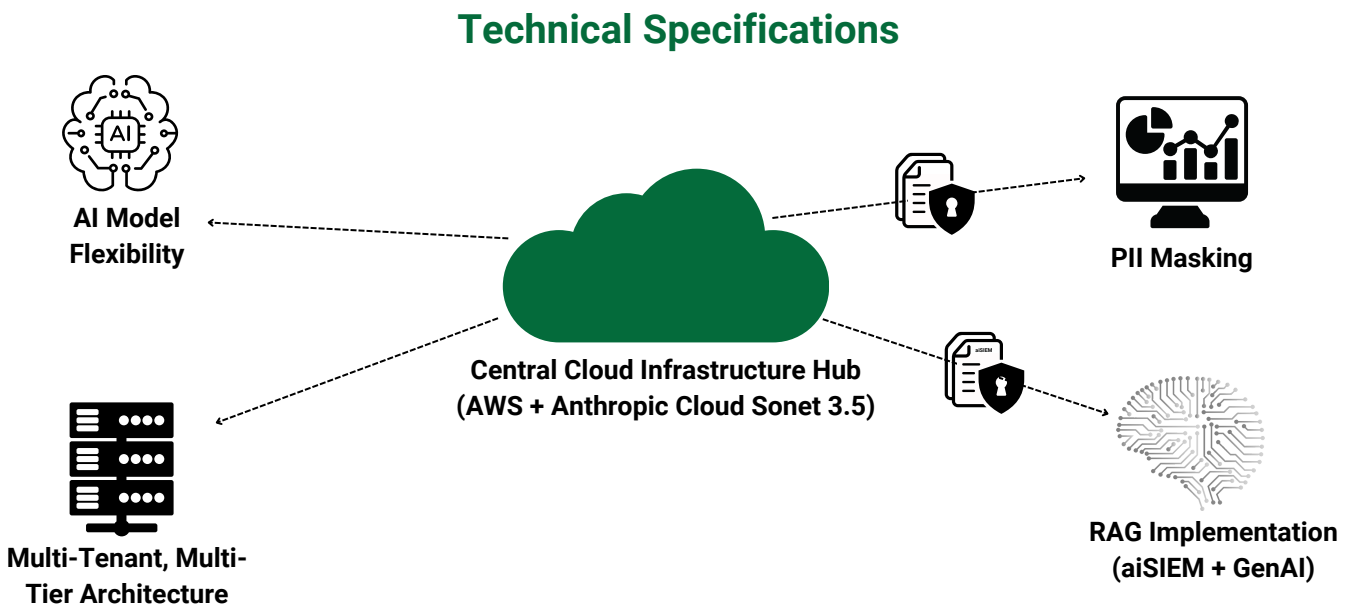
Cloud Infrastructure: AWS, utilizing Anthropic Cloud Sonet 3.5 for GenAI processing.

PII Masking: Built-in masking mechanism to anonymize sensitive data before sending it to the AI model.

RAG Implementation: Utilizes aiSIEM data in conjunction with GenAI to produce contextually accurate and insightful responses.

Data Processing: Supports multi-tenant, multi-tier architecture, enabling robust, scalable processing of security alerts and events.

AI Model Flexibility: Supports integration with models like OpenAI GPT, LLaMA, BERT, and other advanced GenAI frameworks for enhanced capabilities.



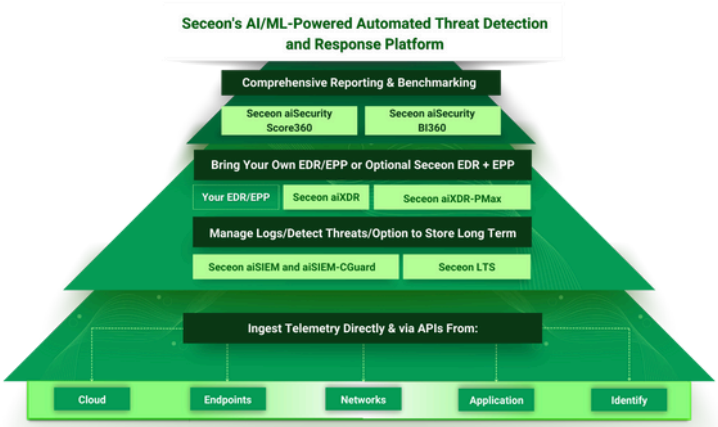
Use Cases:

- **Complex Query Resolution:** Security professionals can ask complex, multi-faceted questions in natural language, with SERA AI providing targeted, contextually relevant answers.
- **Alert Prioritization:** Automatically analyzes alerts, identifying the most critical incidents, and offering actionable recommendations to mitigate risks.
- **Security Intelligence Assistant:** Acts as an AI-driven assistant, helping with cybersecurity decision-making, reducing alert fatigue, and enhancing team productivity.

Advancements and Current Limitations:

- **Getting Better with Every Interaction:** With each user interaction, SERA AI continues to evolve, learning from feedback and refining its analysis capabilities. While the tool is a powerful assistant, human oversight is advised to ensure precision.
- **Occasional Errors:** SERA AI, while highly capable, may occasionally misinterpret complex queries or alerts. Users are encouraged to review the responses for accuracy and provide feedback to improve future interactions.

seceon



About Seceon

Seceon simplifies cybersecurity for MSPs, MSSPs, and IT teams by reducing risk and complexity. Our AI and ML-powered aiSIEM and aiXDR platform provides comprehensive threat detection and response. By integrating data from logs, identity management, networks, endpoints, clouds, and applications, we deliver real-time, accurate alerts and automated remediation. Trusted by over 620 partners, Seceon supports more than 8,200 clients with efficient, high-margin security services and continuous compliance.

Learn more about Seceon SERA AI and

Schedule a Demo www.seceon.com/contact/