

## About SIEM AI

AI-Powered SIEM revolutionizes security operations by harnessing the power of artificial intelligence. This cutting-edge solution transforms the way you detect, prioritize, and respond to threats. Say goodbye to overwhelming alert fatigue and manual analysis. AI-Powered SIEM's intelligent algorithms automatically analyze alerts, identify critical threats, and provide actionable recommendations. With its automated mitigation steps, enhanced threat detection, and reduced false positives, AI-Powered SIEM empowers security teams to respond swiftly and effectively to protect your organization.

Whether you're a security professional, AI expert, or just starting out, AI-Powered SIEM offers unparalleled benefits. Experience the future of security today.

## Challenge

Traditional SIEM tools rely on rule-based analysis, which can be time-consuming to configure and maintain. Additionally, these tools often generate a high number of false positives, which can waste valuable analyst time investigating non-critical events. To address these issues and enhance the effectiveness of security operations, **AI-Powered SIEM** was introduced.

- **Overwhelming Number of Alerts:**
  - Alert fatigue due to a deluge of alerts.
  - Difficulty in distinguishing critical threats from noise.
- **Difficulty in Prioritizing Threats:**
  - Lack of context in alerts, hindering severity assessment.
  - Technical jargon that may confuse non-experts.
  - Complex root cause analysis requires specialized knowledge.

- **Inefficient Response Times:**
  - Delays in investigation due to insufficient information in alerts.
  - Learning curve challenges for new or less experienced engineers.
- **Time-Consuming Manual Alert Analysis:**
  - Manual review of each alert, leading to inefficiency and errors.
  - Increased risk of human error due to the volume of alerts.

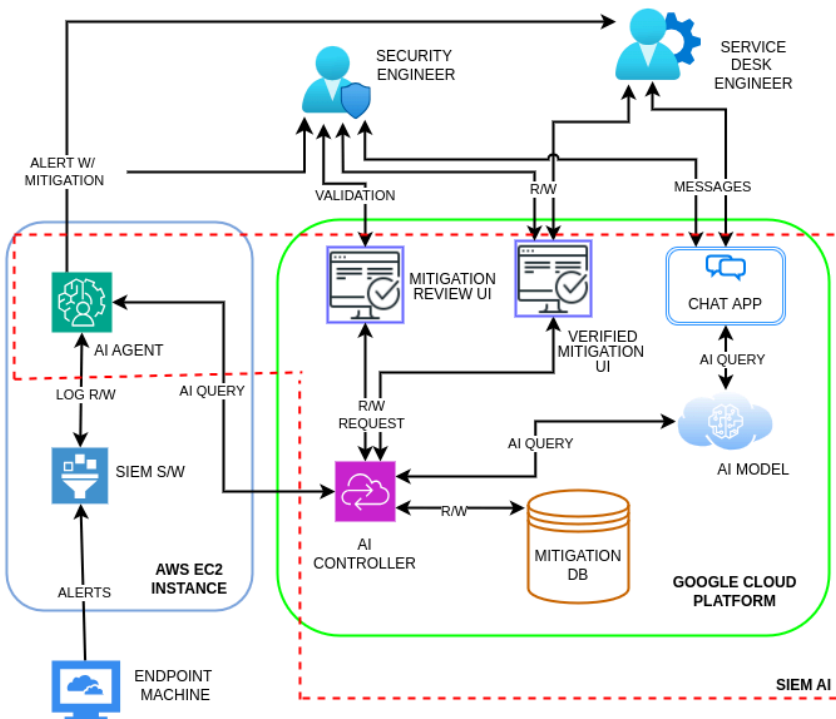
## Solution

**AI-Powered SIEM** is a comprehensive security solution designed to address the limitations of traditional security event management. By leveraging the power of artificial intelligence (AI), the product provides a more efficient and effective approach to threat detection, prioritization, and response.

## Architecture Overview

- **SIEM Software:**
  - Core security monitoring and alerting functionality.
  - Data collection and analysis for threat identification.
- **Watchdog (AI Agent):**
  - Monitors for new alerts and initiates processing.
- **AI Controller:**
  - Central hub for alert processing and data transfer.
  - API endpoint for external application interaction.
- **Mitigation review portal:**
  - User interface for reviewing and approving mitigation steps.
- **Mitigation DB:**
  - Data storage for mitigation steps and approval status.
- **Verified mitigation repo:** User interface for viewing/editing verified mitigation steps.
-

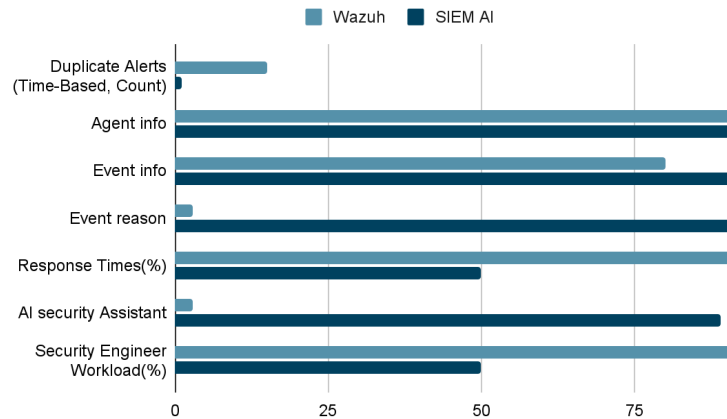
- **Vertex AI Model:**
  - AI engine for generating tailored mitigation steps.



- **Intelligent Threat Prioritization:** Focus on critical issues.
- **Accelerated Incident Response:** Faster resolution through automated responses, detailed alerts, and prioritization.
- **Automated Email Notifications:** Relevant information and reliable delivery.
- **Automated Mitigation Steps:** Reduced manual intervention, industry best practices, and contextual alert information.
- **Storage and Retrieval of Mitigations:** Efficient data storage and retrieval, reduced AI processing, and faster response time.
- **Time-Stamp Filtering for Alerts:** Identifying and suppressing redundant alerts.
- **Mitigation Step Approval Interface:** Interactive webpage for review, management, and informed decision-making.
- **AI-Chat Application:** Enhanced understanding, expert advice, and efficient problem-solving.
- **Secure AI-Powered SIEM Access:** Data protection, reduced unauthorized access risk, and compliance with industry regulations.

## Results

Points scored



**Duplicate Alerts (Time-Based, Count) :** Lower means better

**Agent info:** Higher means better

**Event info:** Higher means better

**Event reason:** Higher means better

**Response Times(%):** Lower means better

**AI security Assistant:** Higher means better

**Security Engineer Workload(%):** Lower means better

## How It Works:

- **Alert Detection:** The software collects and analyzes security data, identifying potential threats.
- **Alert Processing:** The watchdog script detects new alerts and sends them to the Flask server.
- **AI-Generated Mitigation:** The Vertex AI model analyzes the alert data and generates tailored mitigation steps.
- **Approval and Implementation:** Mitigation steps are presented to the security engineer for review and approval. Once approved, they are implemented automatically.
- **Continuous Learning:** AI-Powered SIEM continuously learns from new data and refines its mitigation strategies over time.

## Benefits

- **Enhanced Security and Efficiency**
- **Automated Mitigations:** AI-generated responses, email notifications, and detailed alerts for effective threat handling.