Project Design Phase-I
Solution Architecture

Date	27 October 2023
Team ID	PNT2022TMIDxxxxxx
Project Name	Project – 6 AI-driven incident Response Platform That Assists Cybersecurity Teams in Automating Incident Triage And Response Tasks.
Maximum Marks	4 Marks

Solution Architecture:

A comprehensive AI-driven incident response system is crucial for organizations to effectively detect, analyze, and mitigate security incidents. This solution architecture integrates advanced technologies and methodologies to ensure a proactive and efficient response to potential threats.

The project focuses on establishing a robust security infrastructure that leverages AI algorithms and machine learning to swiftly identify and categorize potential security incidents. Through the seamless integration of a Security Information and Event Management (SIEM) system, the solution captures and monitors security-related logs and events, providing a comprehensive view of the organization's security landscape.

- **Continuous Monitoring and Feedback Loop:** The system incorporates continuous monitoring and a feedback loop to evaluate the effectiveness of the incident response process. It collects data on the response actions taken and uses this information to refine and improve the overall incident response strategy and the performance of the AI algorithm.
- **SIEM (Security Information and Event Management):** The system initially captures and stores logs of all security-related events and incidents. It continuously monitors and analyzes these logs to detect any anomalies or potential threats.
- **Incident Tracking and Case Management:** The system tracks and manages all incidents through a centralized case management system, providing a comprehensive overview of the incident lifecycle, from detection to resolution. This aids in maintaining a systematic record of incidents for future reference and analysis.
- **AI Algorithm for Threat Detection:** If an incident is identified as new or unknown, it is passed through an AI algorithm specially designed for threat detection. This algorithm leverages machine learning and pattern recognition techniques to identify potential security threats or malicious activities.
- **Alert System and User Notification:** Upon confirming a threat, the system triggers an alert mechanism to notify the appropriate user or security personnel. The alert includes details about the nature of the threat, its severity, and any immediate actions required.
- **Classification and Reporting:** The incident is classified based on its severity and impact. A detailed report is generated, outlining the specifics of the incident, the affected systems, and the potential risks involved. This report is shared with the management and relevant stakeholders for further assessment and decision-making.
- **High-Risk Data Protection:** As soon as the alert is generated, the system activates protocols to protect high-risk and confidential information. This includes isolating sensitive data, restricting access to critical systems, and implementing additional security measures to prevent unauthorized access or data breaches.

Integrating these elements into the solution architecture will enable a streamlined and effective AI-driven incident response process, ensuring timely threat detection, notification, and protection of critical data assets.

Example - Solution Architecture Diagram:

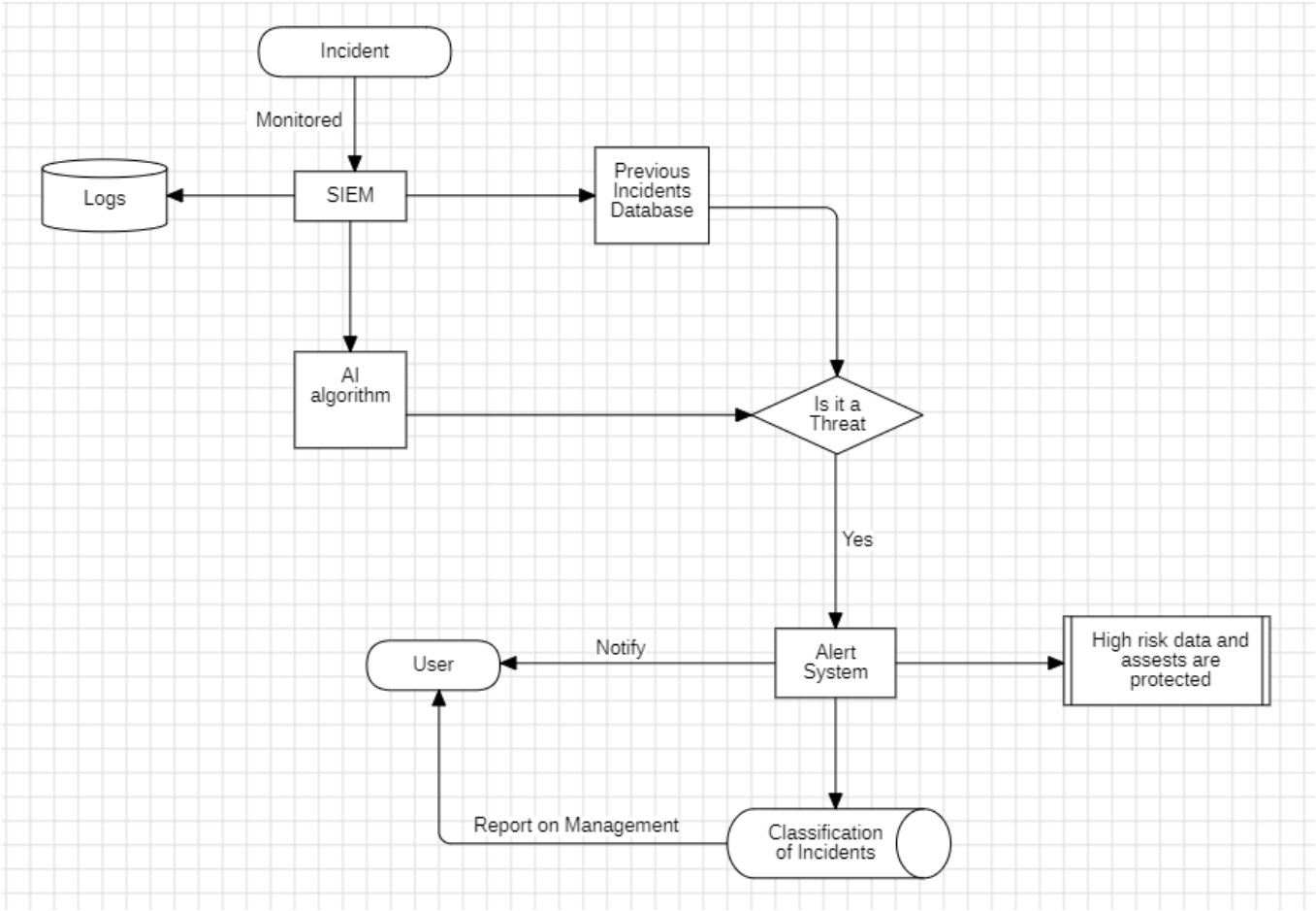

Figure 1: Architecture and data flow of the AI-Driven Incident Response Platform

Reference:

https://www.linkedin.com/pulse/leveraging-ai-enhanced-cyber-security-incident-novel-threat-drew/
https://medium.com/kmeanswhat/ai-automation-for-incident-management-c872ee10e833