Google Cloud

H2S

AI for Impact

APAC Hackathon 2024

A social-first initiative

Registration Deadline: Sun 17 November 2024

Team Details:

Team name: DEBUG AI

Team leader name: VIRAJ VILAS SAWANT

Problem Statement: Leveraging GEN AI to automate defensive cybersecurity processes to enhance security of civic engagement platforms, ensuring safety and resilient digital spaces for public participation.

Brief about the idea

Generative AI can be effectively used in cybersecurity to automate the tasks, enhancing the security and resilience of civic digital engagement platform. This majorly include:

1. Automated monitoring and anomaly detection to identify potential threats or malicious activity.
2. Providing AI-powered tailored responses and mitigation strategies based on issues detected by the model.
3. Continuous assessment and optimization of security through AI powered vulnerability analysis and penetration testing.
4. Creating automated documentation of the incident and recovery strategies for future references.

Opportunities

How different is it from any of the other existing ideas?

1. Most of the current cybersecurity solutions rely on manual approach for threat detection and mitigation which can be time-consuming.
2. By leveraging the speed and analytical capability of AI, the solution can provide a more comprehensive security monitoring system.

How will it be able to solve the problem?

1. The solution uses AI to automate the monitoring task for detecting anomalies and threat detection.
2. It continuously undertakes the task of security assessment and optimization through AI-powered vulnerability analysis and penetration testing for identifying the evolving threats.

USP of the proposed solution

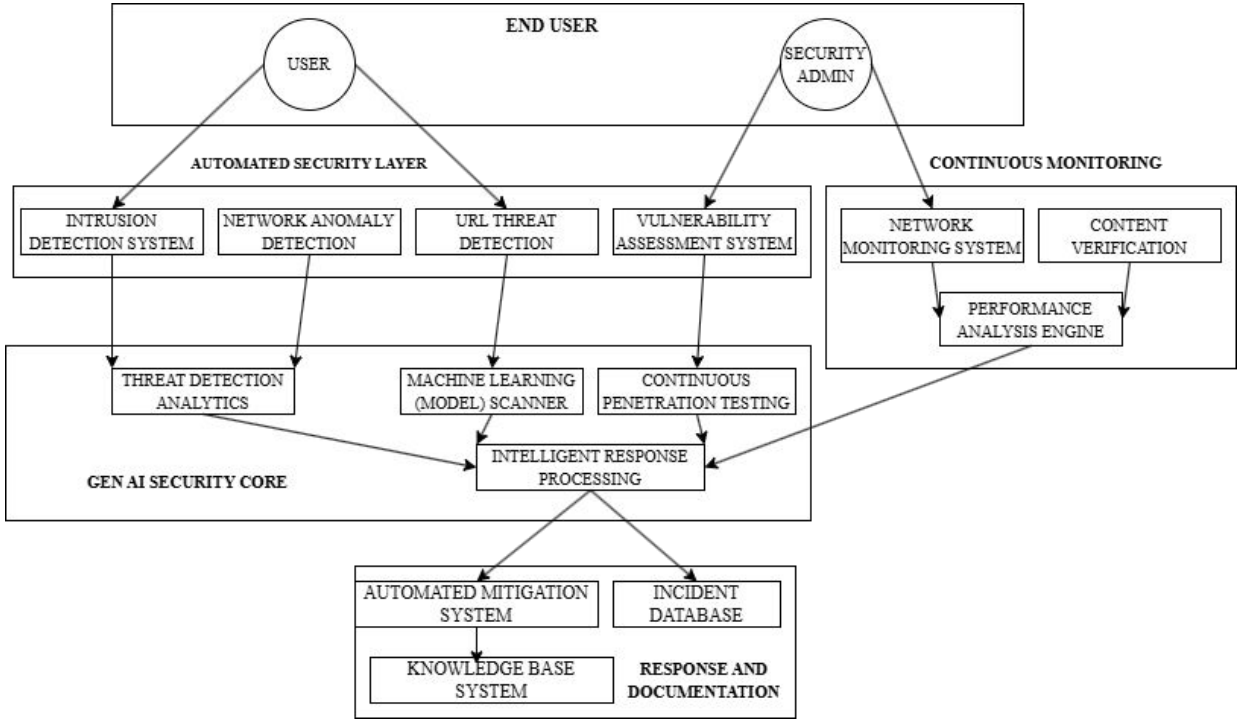
1. Proactive, AI powered solution for civic engagement platforms for enhancing security of digital public places.
2. Reduced Dependency on large cybersecurity teams, hence decreasing operational cost.

List of features offered by the solution

The solution combines the capabilities of an Intrusion Detection System(IDS) with advanced security mechanism integrated with GEN AI capabilities providing following features:

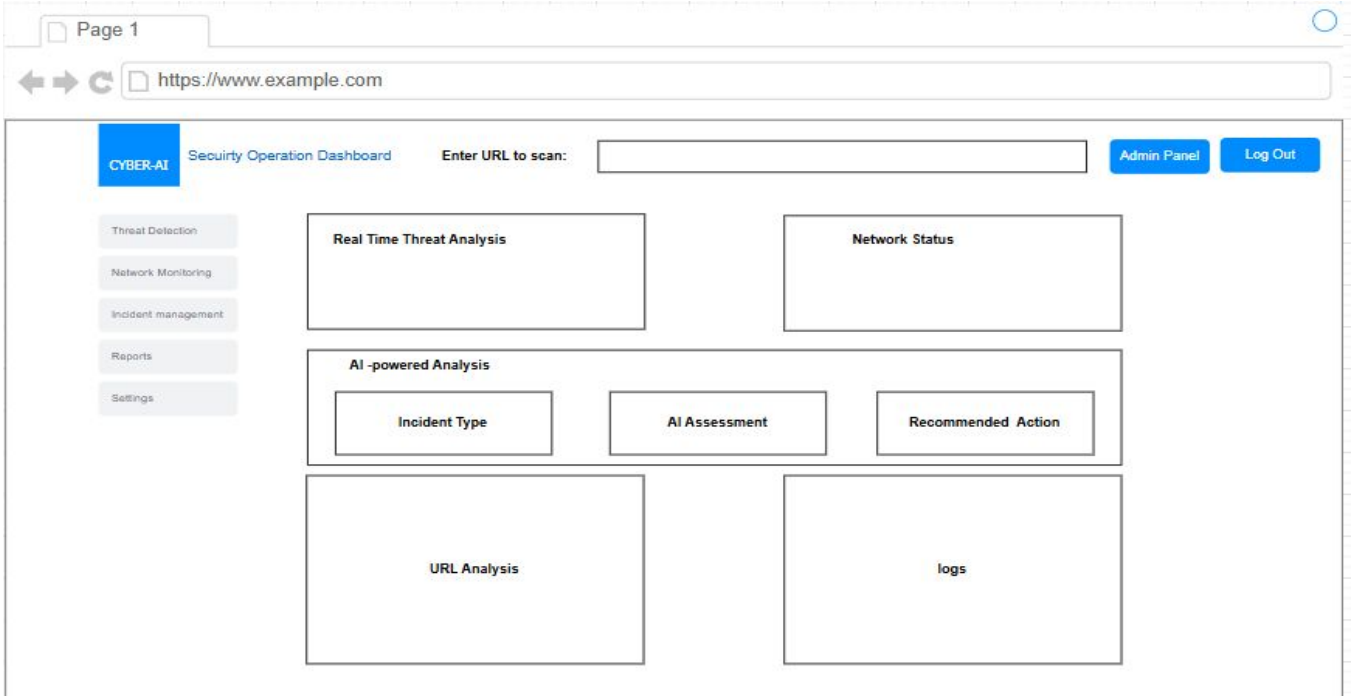
1. Automated threat detection and mitigation strategies.
2. Detecting whether the URL is malicious or not.
3. Continuous monitoring of network.
4. Identifying misleading content.

Process flow diagram or Use-case diagram

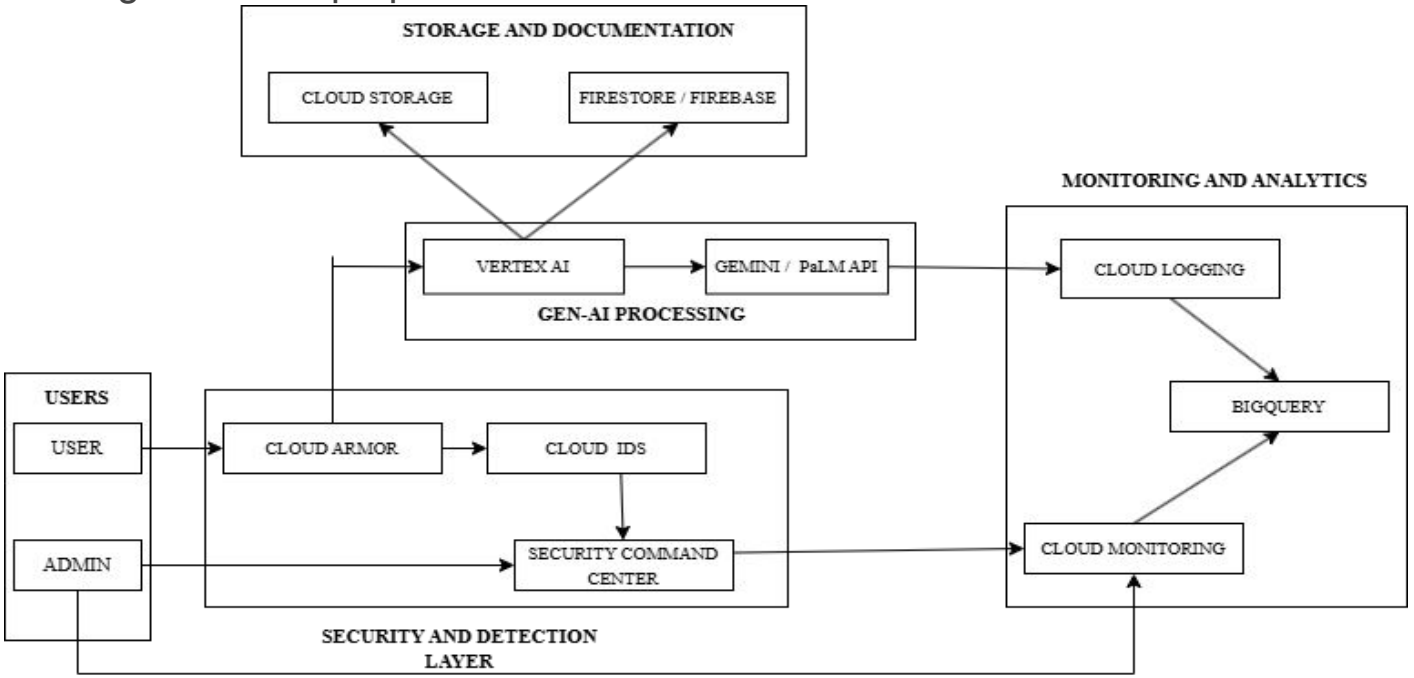


Use Case diagram for AI powered GEN AI cybersecurity system.

Wireframes/Mock diagrams of the proposed solution (optional)



Architecture diagram of the proposed solution



Architecture diagram for AI powered GEN AI cybersecurity system.

Technologies to be used in the solution

1. Vertex AI
2. Cloud Armor
3. ReactJS
4. Cloud Storage
5. Cloud Logging and Cloud Monitoring
6. BigQuery

Use case of Vertex AI/Gemma/Gemini or any of the Google Gen AI tools used

1. **Vertex AI and API key:** Vertex AI is used for URL analysis and classifying it into malicious or not, also it is used for anomaly detection, content verification and providing responses based on the Machine Learning model trained.
2. **Cloud Armor:** Cloud Armor is used for WAF and DDoS protection. Since it has the capability of URL filtering.
3. **Cloud Storage and Firestore/Firebase:** Cloud storage can be used for storing the data and firestore/firebase for documenting the incident in structured way.
4. **Cloud IDS:** Cloud IDS is used for network threat detection.
5. **Cloud Logging:** Cloud logging is used to keep logs of events happening and providing comprehensive log analysis.
6. **Cloud Monitoring:** Cloud monitoring is used for real-time system monitoring.
7. BigQuery: BigQuery can be used for long term storage and security event analysis.

Estimated implementation cost (optional)

- The estimated implementation cost for this solution is contingent upon the Google cloud resources utilized.

Google Cloud

H2S

AI for Impact

APAC Hackathon 2024

A social-first initiative

Registration Deadline: Sun 17 November 2024

Thank You