Problem Statement: API Security Shield

Context:

APIs are vital to modern software systems, enabling integration and communication across applications. Ensuring API security is crucial due to the increasing reliance on these interfaces. This project challenges you to develop a comprehensive API security solution tailored for a modern enterprise.

Objective:

Develop a scalable, comprehensive, and user-friendly API security solution that seamlessly integrates into an enterprise's Software Development Life Cycle (SDLC), providing robust protection against common API security threats and offering a centralised platform for managing API security efforts.

Key Pointers:

1. **API Inventory Management:**
    - ○ Create a system that discovers and inventories all APIs within an organization. This system should integrate seamlessly into the SDLC and provide continuous updates.
    - ○ Ensure real-time monitoring to alert the security team of any new APIs added to the SDLC.
2. **OWASP Top 10 API Attacks Coverage:**
    - ○ Implement protections against the OWASP Top 10 API security risks, including continuous and on-demand scanning options.
    - ○ Automate regression suites with security objectives.
3. **Dashboard Management View:**
    - ○ Design a centralized dashboard to manage and resolve API security issues, offering clear insights into the status and history of each API.
    - ○ Include detailed reporting features and support for efficiently closing resolved issues.
    - ○ Build the solution on a scalable technology stack as a web application, allowing users to login and manage API security remotely.
    - ○ Ensure the solution can handle an increasing number of APIs and security checks as the organization grows.

Deliverables:

1. A fully functional web application demonstrating the above features.
2. A simulated SDLC environment showcasing the integration and effectiveness of your API inventory management system, with an emphasis on discovery.

3. Documentation outlining the architecture, design decisions, and user instructions.
4. A presentation detailing your approach, implementation, and key findings.

Evaluation Criteria:

- Effectiveness of the API inventory management system.
- Real-time monitoring capabilities.
- Coverage and effectiveness of OWASP Top 10 API security scans.
- Usability and functionality of the dashboard.
- Scalability and robustness of the web application.
- Quality and clarity of documentation and presentation.