2.1 Problem Statement

There is a lack of easily accessible and comprehensive cloud hosted applications that are legally allowed to be exploited for educational purposes. In addition to this, there are almost no environments that give users hands-on experience in cloud based threat analysis or incident response.

2.2 Requirements & Constraints

- **Functional Requirements**
    - Incorporates common AWS-specific vulnerabilities/misconfigurations
    - Vulnerabilities should be actively exploitable
    - Design custom API code to implement vulnerabilities
    - Logging and Monitoring to capture user and security events
    - Include an Incident Response Component that enables users to assess impact
- **Resource Constraints**
    - Utilize AWS CloudFormation for consolidated resource configuration
    - Utilize AWS Identity and Access Management for resource permissions
    - Include AWS CloudWatch alarms to be notified of resources failing intended functionality
    - Cloud resource usage should be minimal, if not all in the free tier
- **Qualitative Requirements**
    - Design a unique AWS Service that reflects existing AWS resources
    - Identity Management roles and policies should reflect professional roles and use cases)
    - Documentation on the intended exploits and incident response components must be available to users
    - Implements safeguards to prevent unintended damage to actual AWS resources

2.3 Engineering Standards

- OWASP - Globally recognized consensus of critical web-app security risks that we can implement in our AWS services
- IAM - IAM is a critical aspect of AWS Security. Our product will test IAM's standards with permissive policies, granting privileges, and the principle of least privilege.
- PCI - crucial to safeguard sensitive payment card data and maintain trust with customers by adhering to security standards and best practices.
- HIPAA - safeguard sensitive healthcare data and maintain regulatory standards in the digital landscape.
- ISO 12207 - Standard for software life cycle processes including developing and maintaining the software.
- ISO 27001 - Recognized as best-known standard for information security management systems (ISMS). Related to access controls and IAM.
- ISO 29119 - Series of five international standards for software testing. Part of the project will be testing the developed API like an intended user will use it

2.4 Intended Users and Uses

Intended Users:

- IT Administrators
  - Are responsible for Identity Access Management implementation which plays a key role in many vulnerabilities
- Software Architects
  - Will gain additional insight into available cloud resources and their intended functionality
- Cybersecurity Students
  - Will benefit from hands on experience with common exploits and incident response
- Risk Consultants
  - Will benefit from continuous learning/training to be prepared to investigate cloud infrastructure
- Application Developers
  - Deploy and test software instances

Additional Use cases include:

1) Performance Optimization: optimize resources for performance and cost reduction.
2) Testing and Development: Developers and QA teams will be enabled to create reliable testing environments.
3) Security: IT Administrators utilize the project to enforce robust security measures, including encryption, access controls, and threat monitoring. This ensures data integrity and safeguards against potential cyber threats, and meeting specific security requirements
4) Education: Potential new hires for positions related to our intended users can use this as grounds for experimentation and education