

Project Vulnerd: Operational Overview

Project Purpose

Vulnerd is an automated cloud security monitoring and reporting system designed for small organizations that lack dedicated security personnel. The platform collects and correlates cloud security activity, enriches it with external threat intelligence, and generates clear, business-oriented incident summaries using generative AI. Its primary goal is to provide continuous visibility into security activity and surface meaningful threats in environments that would otherwise go unmonitored.

While Vulnerd provides automation and contextual analysis, it is not intended to replace human analysts. Human judgment, intuition, and decision-making remain essential. Vulnerd functions as a support system that enhances awareness and response until human expertise can be applied.

Team Roles and Responsibilities

Cloud Security Architect (Environment Design)

The Cloud Security Architect is responsible for designing a realistic cloud environment that represents a small business or under-resourced organization. Their role is to ensure the environment reflects real-world architecture decisions, risk exposure, and visibility challenges. They define how systems communicate, what data is generated, and where security blind spots may exist, creating a foundation that makes downstream detection meaningful.

Red Team Operator (Adversary Simulation)

The Red Team Operator is responsible for simulating malicious or suspicious behavior within the environment in a controlled and ethical manner. Their role is not focused on “breaking in,” but on producing realistic activity patterns that resemble common threats faced by small organizations. This role ensures the project evaluates real behaviors rather than hypothetical or sanitized scenarios.

Detection Engineer (Threat Logic & Signal Quality)

The Detection Engineer is responsible for defining what constitutes suspicious or malicious behavior within the system. Their role centers on translating abstract threats into practical detection logic, balancing sensitivity with accuracy. They ensure the system highlights meaningful security events while minimizing unnecessary noise, shaping how and when Vulnerd surfaces concerns.

Cyber Threat Intelligence Analyst (Context & Attribution)

The CTI Analyst provides external context to internal security events. Their role is to determine how observed activity aligns with known threat patterns, reputational data, or emerging trends. By adding external intelligence, this role helps transform isolated events into informed assessments that support decision-making.

AI & Automation Lead (Synthesis & Communication)

The AI & Automation Lead is responsible for translating technical security findings into clear, structured narratives suitable for non-technical stakeholders. Their focus is on how information is summarized, prioritized, and explained. This role ensures Vulnerd communicates findings in a way that supports understanding rather than overwhelming the user.

Role Collaboration & Team Workflow

Rather than strict team divisions, the project emphasizes collaboration between complementary roles:

- The Cloud Security Architect and Red Team Operator work closely to ensure the environment and simulated activity remain realistic and aligned with common threat scenarios.
- The Detection Engineer collaborates with both the Red Team Operator and CTI Analyst to refine detection logic based on observed behaviors and external threat context.
- The CTI Analyst and AI & Automation Lead work together to ensure intelligence enrichment is accurately reflected in user-facing summaries.
- The AI & Automation Lead interfaces with all roles, ensuring outputs remain aligned with system behavior and project goals.

This structure allows iterative feedback between environment design, threat generation, detection logic, and reporting.

Project Timeline & Milestones

(January 15, 2026 – April 20, 2026)

Phase 1: Foundation (Jan 15 – Feb 15)

- Define project scope and success criteria
- Design and deploy initial cloud environment
- Establish data flow for security events
- Identify relevant threat scenarios for simulation

Phase 2: Integration (Feb 16 – Mar 15)

- Begin controlled activity generation within the environment
- Develop and test initial detection logic
- Integrate external threat intelligence sources
- Establish AI-driven reporting pipeline

Phase 3: Refinement (Mar 16 – Apr 5)

- Improve detection accuracy and reduce noise
- Refine report clarity and prioritization
- Align system outputs with business-relevant language
- Design and finalize dashboard or notification format

Phase 4: Final Preparation (Apr 6 – Apr 20)

- Conduct end-to-end testing of the full pipeline
- Finalize documentation and system diagrams

- Record backup demonstration of the system
 - Prepare final presentation and written report
-

Potential Tools & Technologies (Subject to Change)

The following tools may be used to support development and testing. Specific selections will depend on feasibility and instructional guidance.

Cloud & Logging Platforms

- AWS EC2 for hosting simulated workloads
- AWS CloudWatch and VPC Flow Logs for activity visibility

Threat Simulation & Testing

- Custom scripts or controlled testing frameworks to generate suspicious behavior
- Open-source tools for simulating common attack patterns

Threat Intelligence Sources

- VirusTotal for file and indicator reputation
- AbuseIPDB for IP address reputation and reporting

Automation & Analysis

- Python for data ingestion, processing, and orchestration
 - Large Language Models for summarization and report generation
-

University Resource Coordination

The project will leverage university resources to support development and research. This includes requesting AWS Educate credits through the College of Engineering to support the cloud infrastructure required for a cloud-native capstone project.

Faculty and IT staff will be consulted for guidance and best practices related to cloud architecture, security monitoring, and responsible system design. Their role is advisory, helping ensure the project aligns with academic standards and institutional expectations.

Library research services will be used to access industry reports and academic publications, including sources such as Gartner and Forrester. These materials will provide data on cybersecurity risks and financial impacts for small businesses, supporting the project's justification and final analysis.