

## **Sprint Backlog Grooming Meeting Minutes #2:**

Attendees: Jonathan Nava-Arenas, Reynaldo Rodriguez, Luisa Faria Novy E Silva, Anthony Whiteman, Rickoy Cunningham

Start time: 6:00PM

End time: 7:00PM

### **The following user stories were created/discussed/refined/prioritized:**

- **User Story #2:**

As a Red Team Operator, I want to simulate controlled malicious or suspicious activity within the environment so that Vulnerd can observe realistic threat behaviors without impacting production systems.

- Simulated activity is ethical and controlled
- Activity generates observable security signals
- Actions are documented for repeatability

- **User Story #3:**

As a Detection Engineer, I want to define and refine detection logic that identifies meaningful suspicious behavior so that the system surfaces real threats while minimizing noise.

- Detection logic is documented and tested
- False positives are reviewed and reduced
- Meaningful alerts are consistently generated

- **User Story #4:**

As a Cyber Threat Intelligence Analyst, I want to enrich detected events with external threat intelligence so that security findings are contextualized using known threat patterns and reputational data.

- External intelligence sources are identified
- Events are enriched with context or attribution
- Intelligence improves clarity of risk assessment

- **User Story #5:**

As the AI & Automation Lead, I want to automate the synthesis of technical findings into clear, business-oriented incident summaries so that non-technical stakeholders can understand risks and priorities.

- Reports are automatically generated
- Language is non-technical and structured
- Findings are prioritized by impact and risk

- **User Story #6:**

As a project team, we want to compile findings, risk analysis, and system outputs into a professional report and presentation so that Vulnerd's value, design, and results are clearly communicated.

- Final report is completed and reviewed
- Presentation aligns with project objectives
- Deliverables meet capstone requirements

The user stories below are completed:

- **User Story #1:**

As a Cloud Security Architect, I want to design and deploy a realistic cloud environment with logging and visibility enabled so that security activity can be collected and monitored in a way that reflects real-world small business infrastructure.

- Cloud environment is deployed and documented
- Logging sources are enabled and producing data
- Architecture reflects realistic small-business exposure