

Sprint Planning Meeting Minutes

Attendees:

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

Start time: 6:00 PM

End time: 7:00 PM

After discussion, the velocity of the team was estimated to be **one story per member per sprint**. The product owner chose the following user stories to be done during the next sprint. They are ordered based on their priority.

Team Roles

- **Cloud Security Architect (Environment Design)**

Reynaldo Rodriguez

- **Red Team Operator (Adversary Simulation)**

Jonathan Nava-Arenas

- **Detection Engineer (Threat Logic & Signal Quality)**

Rickoy Cunningham

- **Cyber Threat Intelligence Analyst (Context & Attribution)**

Luisa Faria Novy E Silva

- **AI & Automation Lead (Synthesis & Communication)**

Anthony Whiteman

Selected User Stories

1. **Environment Design & Lab Setup**

- As a Cloud Security Architect, I want to design and deploy a realistic cloud-based environment so that Vulnerd reflects real-world small organization infrastructure, including visibility gaps and security risks.

2. **Adversary Simulation**

- As a Red Team Operator, I want to generate controlled and realistic malicious or suspicious activity within the environment so that detection logic can be evaluated against real threat behavior.

3. **Threat Logic & Signal Quality**

- As a Detection Engineer, I want to define and refine detection logic so that meaningful security events are surfaced while minimizing false positives and unnecessary noise.

4. Context & Attribution

- As a Cyber Threat Intelligence Analyst, I want to enrich detected activity with external threat intelligence so that alerts include relevant context and alignment with known threat patterns.

5. Synthesis & Reporting

- As an AI & Automation Lead, I want to translate technical findings into clear, structured summaries so that non-technical stakeholders can understand risks and recommended actions.

The team members indicated their willingness to work on the following user stories

- **Reynaldo Rodriguez**

- #1 (Cloud Security Architect)

- As a Cloud Security Architect, I want to design and deploy a realistic cloud-based environment so that Vulnerd reflects real-world small organization infrastructure, including visibility gaps and security risks.

- **Jonathan Nava-Arenas**

- #2 (Red Team Operator)

- As a Red Team Operator, I want to generate controlled and realistic malicious or suspicious activity within the environment so that detection logic can be evaluated against real threat behavior.

- **Rickoy Cunningham**

- #3 (Detection Engineer)

- As a Detection Engineer, I want to define and refine detection logic so that meaningful security events are surfaced while minimizing false positives and unnecessary noise.

- **Luisa Faria Novy E Silva**

- #4 (Cyber Threat Intelligence Analyst)

- As a Cyber Threat Intelligence Analyst, I want to enrich detected activity with external threat intelligence so that alerts include relevant context and alignment with known threat patterns.

- **Anthony Whiteman**

- #5 (AI & Automation Lead)

- As an AI & Automation Lead, I want to translate technical findings into clear, structured summaries so that non-technical stakeholders can understand risks and recommended actions.