

Release Plan

Product Name: Local Intrusion Detection System (LIDS)

Team Name: SlugShield

Release Name: MVP Release – Local IDS Prototype

Release Date: 10/21/25

Revision #: 1.0 **Revision Date:** 120/1/25

High-Level Goals

Deliver a privacy-preserving, locally running Intrusion Detection System (IDS) that captures, analyzes, and visualizes network activity in real time.

Across four sprints, the release will:

1. Build the local IDS core that detects suspicious activity.
2. Provide an interactive dashboard for real-time alerts and statistics.
3. Enable configurable alert frequency and explanatory severity levels.
4. Optimize performance, accuracy, and user experience for stability.

User Stories Defining the Scope of the Release

Each user story includes a story-point estimate and is assigned to one sprint in the release cycle.

Sprint 1 – Core Local System and Logging

Priority	User Story ID	Description	Story Points
High	US1	As a user, I want the system to run locally on my computer so my data stays private and never leaves my device.	8

High	US2	As a user, I want the IDS to monitor network traffic in real time so it can detect suspicious activities as the system is running.	13
Medium	US3	As a user, I want to see the IDS printing to the console log or writing to a log output when suspicious activity is detected so I know the IDS is working.	3

Total Sprint 1 Effort: ≈ 24 story points

Sprint 2 – Dashboard and Real-Time Alerts

Priority	User Story ID	Description	Story Points
High	US4	As a user, I want to access the dashboard through my browser locally so there isn't a need for third party softwares	8
High	US5	As a user, I want a main overview that shows overall systems health so I can get status at a glance.	5
Medium	US6	As a user, I want to view alerts on a simple dashboard so	8

		I understand my system is safe.	
Medium	US7	As a user, I want to see real time alerts that were detected along with simple charts comparing the real time alerts that were detected to normal behavior traffic so I understand what is happening and how severe it is.	8

Total Sprint 2 Effort: ≈ 29 story points

Sprint 3 – Customization and Alert Explanations

Priority	User Story ID	Description	Story Points
High	US8	As a user, I want clear explanations for each alert so I can understand what triggered it and what it means.	8
High	US9	As a user, I want to adjust the threshold for how frequently I receive suspicious alerts so I can	5

		manage notification frequency.	
Medium	US10	As a user, I want to pause and resume monitoring from the dashboard so I can control when analysis runs..	6
High	US11	As a user, I want to receive email notifications whenever an alert is detected so I can be notified when I am not near the computer	8

Total Sprint 3 Effort: ≈ 27 story points

Sprint 4 – Optimization and Final Refinement

Priority	User Story ID	Description	Story Points
High	US12	As a user, I want a more aesthetic webpage so that it will be easy to follow.	5
High	US13	As a user, I would like to see accurate metrics being reported so I understand the graphs.	5
Medium	US14	As a user, I want to receive email	4

		notifications whenever an alert is detected so I can be notified when I am not near the computer.	
--	--	---	--

Total Sprint 4 Effort: \approx 14 story points

Sanity Check

- **Total Story Points:** \approx 94
- **Capacity:** \approx 23.5 points per sprint (4-person team) \rightarrow feasible with minor buffer each cycle.
- **Balance:** Workload distributed evenly; each sprint adds a layer of functionality and stability.
- **Risk Coverage:** Early spikes and infrastructure allow technical exploration before UI and optimization phases.

Product Backlog

Deferred for future releases (Version 2.0 and beyond):

- Machine-learning traffic classification.
- Cloud synchronization (optional).
- Multi-device monitoring and alert sharing.
- CI/CD automation and deployment pipeline.

These items can be reprioritized once the MVP is stable and functional.

Last Modified: October 18, 2025 **Adapted from CMPS/CSE 115a Release Plan Template**