Week 1 Summary Report

Executive Summary

The Week 1 assignment focused on SOC fundamentals, monitoring, log management, and incident response basics. Through theoretical study and practical exercises, analysts learned the essential workflows of a SOC environment.

This week provided a strong foundation in security operations, equipping participants with knowledge required to handle real-world threats.

Tools Used

SIEM platforms (conceptual), log management tools, and visualization dashboards were studied.

Students also explored the role of security documentation in operational workflows.

Key Learnings

Participants gained insights into SOC structure, event monitoring, and response workflows.

They understood the importance of documentation, dashboard visibility, and alert rule configuration in strengthening security operations.

Challenges & Future Improvements

The main challenge was differentiating false positives from genuine threats in monitoring scenarios.

Future improvements include practicing advanced detection use cases and integrating automation into SOC processes.