Project Design Documentation: Jordan Fields

# 1. Project Title & Version Control

Project Title: Mini SOC – Law Enforcement-Inspired Cybersecurity Analysis  
Version: Draft  
Date: 09/29/2025  
Change Log: Initial design created from proposal.

# 2. Project Summary

The Mini SOC project is designed to simulate a real-world Security Operations Center (SOC) workflow for training and demonstration purposes. It provides hands-on experience with log collection, SIEM dashboards, detection engineering, incident response playbooks, and case management reporting. This project matters because it bridges the gap between classroom knowledge and practical SOC analyst workflows, preparing students and professionals for entry-level SOC roles in corporate and law enforcement cybersecurity.

# 3. Problem Statement / Use Case

Many entry-level cybersecurity learners lack practical exposure to full-cycle SOC operations. Employers expect candidates to understand SIEM tools, detection rules, and evidence documentation, but most training environments don’t replicate real incident workflows.  
  
The Mini SOC solves this by building a small-scale, law enforcement–inspired SOC lab that:  
- Collects and visualizes logs from multiple sources.  
- Runs simulated attacks (phishing, brute force, malware).  
- Produces structured case reports, mirroring law enforcement evidence handling.  
  
Users: SOC analyst trainees, cybersecurity students, entry-level job seekers, and educators designing hands-on labs.

# 4. Goals and Objectives

- Build and configure a functional SIEM (ELK stack or Splunk).  
- Create dashboards and detection rules for key SOC scenarios.  
- Develop 4–6 incident response playbooks (SOP-style).  
- Document 10+ case reports with evidence screenshots and workflows.

# 5. Key Features / Functions

- SIEM Dashboards: Failed login tracking, network monitoring, process execution.  
- Detection Rules: Brute force, port scan, suspicious processes, malware activity.  
- Playbook Library: Standardized response steps for common incident types.  
- Case Management: Case files stored in Monday.com or similar system.  
- Evidence Reporting: Screenshots, logs, and workflow documentation.  
- Attack Simulations: Brute force attempts, phishing campaigns, malware execution.

# 6. Tech Stack and Tools

- Languages: Python, Bash scripting  
- Platforms: VirtualBox (VMs with Ubuntu, Parrot, and Windows)  
- SIEM: ELK Stack or Splunk Free Edition  
- Tools: Nmap, Hydra, Medusa, Syslog, Filebeat/Winlogbeat, Suricata  
- Collaboration: Monday.com (case tracking), GitHub (documentation)  
- Reporting: Markdown/PDF for playbooks and case files

# 7. Architecture / Workflow Diagram

Workflow Overview:  
1. Log Collection (Linux/Windows/Network) →  
2. SIEM Ingestion (ELK/Splunk) →  
3. Dashboards & Detection Rules →  
4. Alerts Triggered by Simulated Attacks →  
5. Analyst Investigation →  
6. Case Management Documentation →  
7. Final Reports & Portfolio  
  
A diagram can be inserted to show flow.

# 8. Timeline / Weekly Milestones

Phase 1 – Lab Setup (Weeks 1–2)  
- VM & SIEM installation, configure log forwarding, validate ingestion.  
  
Phase 2 – Dashboards & Detection (Weeks 3–5)  
- Create dashboards, write detection rules, run simulated brute force/port scans.  
  
Phase 3 – Incident Playbooks (Weeks 6–7)  
- Draft, refine, and export SOP playbooks.  
  
Phase 4 – Case Management (Weeks 8–9)  
- Build workflow board, document 4 core cases with evidence.  
  
Phase 5 – Wrap-Up (Weeks 10–11)  
- Add combined attack case, expand to 10+ total case reports, finalize portfolio.  
  
Final Week (Week 12)  
- Deliver final demo presentation (SIEM + playbook + case portfolio).

# 9. Risks and Risk Mitigation

- Complex SIEM Setup: Mitigate by using community guides and snapshots.  
- Tool Compatibility Issues: Mitigate by testing with multiple OS/log sources early.  
- Time Constraints: Follow phased timeline with sub-item checklists.

# 10. Evaluation Criteria

- SIEM dashboards fully functional with live log ingestion.  
- Detection rules correctly trigger on simulated attacks.  
- Playbook library complete with at least 4 polished SOPs.  
- Case portfolio includes at least 10 documented investigations with evidence.  
- Final presentation demonstrates end-to-end SOC workflow.

# 11. Future Considerations

- Integrate advanced detection tools (Zeek, Suricata IDS).  
- Expand case management into full ticketing system (TheHive, RTIR).  
- Add machine learning detection for anomaly analysis.  
- Include cloud log sources (AWS CloudTrail, Azure Sentinel).