SOC Report - README

This document provides an overview of the SOC (Security Operations Center) report structure, purpose, and usage guidelines.

Purpose

The SOC report summarizes security events, incidents, detections, and response activities within a defined timeframe. It helps stakeholders understand threats, risk levels, and mitigation actions.

Contents

1. **Executive Summary**
2. High level overview of main findings
3. Critical incidents
4. Overall security posture
5. **Environment Overview**
6. Networks
7. Assets monitored
8. Tools and platforms used
9. **Incident Summary**
10. List of incidents
11. Severity levels
12. Detection source
13. Timeline of events
14. **Detailed Incident Analysis**
15. Incident description
16. Indicators of compromise
17. Attack vectors
18. Evidence collected
19. Containment steps
20. Eradication and recovery
21. Lessons learned
22. **Threat Intelligence**
23. New threats relevant to the environment
24. Correlation with active incidents

25. **SIEM Alerts Overview**

26. Alert volumes
27. Noise vs real threats

28. Tuning recommendations

29. **Vulnerability Review**

30. Critical vulnerabilities found
31. Patching status

32. Recommendations

33. **Recommendations**

34. Improvement actions
35. Policy changes
36. Hardening suggestions

How to Use This Report

- Share with security leadership and technical teams.
- Track progress on action items.
- Update incident knowledge bases.

Versioning

- Maintain version numbers for each update.
- Log changes in a change log section.

Contact

For questions or clarifications, contact the SOC team lead.