PROJECT_03 – Future Improvement Scope

Security Monitoring & Incident Response

Overview

This document outlines potential future improvements that could enhance the effectiveness, efficiency, and scalability of the Security Monitoring & Incident Response process demonstrated in this project. The recommendations are based on observations from the phishing simulation exercise and reflect common best practices used in mature SOC environments.

---

1. Automation and SOAR Integration

One of the most impactful improvements would be the integration of Security Orchestration, Automation, and Response (SOAR) capabilities.

Potential Enhancements:

- Automatic blocking of confirmed malicious domains and URLs
- Automated user notification emails for phishing incidents
- Automatic ticket creation and assignment for Tier 2 analysts
- Automated password reset workflows when credential compromise is suspected

Automation would significantly reduce analyst workload and response time, allowing SOC teams to focus on higher-level investigations.

---

2. Improved Alert Correlation Across Data Sources

While alert correlation was performed manually during the simulation, future improvements could include automated correlation between email, proxy, firewall, and endpoint logs.

Benefits:

- Faster identification of complete attack chains
- Reduced alert fatigue
- Improved accuracy in severity classification

Correlating alerts across multiple log sources helps detect advanced phishing campaigns that generate multiple related events.

---

3. Enhanced Threat Intelligence Integration

Expanding the use of threat intelligence feeds can improve detection accuracy and early threat identification.

Potential Improvements:

- Integration of multiple external threat intelligence sources
- Automatic enrichment of alerts with reputation data
- Continuous updating of blacklist and indicator feeds

Threat intelligence enrichment enables analysts to make faster and more informed decisions during triage.

---

4. Reduction of False Positives

Although false positives were successfully identified during the simulation, further improvements could help minimize unnecessary alerts.

Suggested Actions:

- Fine-tuning detection rules based on historical alert data
- Maintaining and updating trusted domain whitelists
- Applying behavioral scoring instead of single-indicator detection

Reducing false positives improves SOC efficiency and prevents analyst fatigue.

---

5. Endpoint Visibility and Monitoring

Greater visibility into endpoint activity would strengthen incident response capabilities.

Improvements Could Include:

- Integration with Endpoint Detection and Response (EDR) solutions
- Automated endpoint scans after phishing link interaction
- Centralized visibility into browser activity and downloads

Improved endpoint monitoring ensures faster detection of post-click or post-compromise activity.

---

6. User Awareness and Phishing Training

Human behavior remains a critical factor in phishing incidents. Strengthening user awareness can significantly reduce successful attacks.

Future Enhancements:

- Regular phishing simulation campaigns
- Security awareness training for employees
- Simplified reporting mechanisms for suspicious emails

Educated users act as an additional layer of defense within the organization.

Conclusion

Implementing these future improvements would enhance the maturity of the Security Monitoring & Incident Response process. By combining automation, improved correlation, enriched threat intelligence, and user awareness, the organization can reduce response times, minimize risk, and build stronger resilience against phishing attacks.

Prepared by: Lala Alili
Date: February 25, 2026