Step 3 – Post-Incident Analysis (RCA)

Executive Summary

Successfully completed comprehensive Root Cause Analysis (RCA) of simulated phishing incident. Despite exceptional technical response time (9.1 minutes vs 280-minute industry average), analysis revealed critical security awareness gaps requiring immediate remediation.

Activities Completed

1. Mock Phishing Incident Execution – Successful credential capture within 2 minutes.
2. 5 Whys Root Cause Analysis – Root cause: Insufficient organizational commitment to security awareness programs.
3. Fishbone Diagram – Highlighted gaps in People, Process, Technology, and Environment.
4. Incident Response Metrics – MTTR of 9.1 minutes (96.8% better than industry average).

Risk Assessment Summary

High Risk: User behavior, technology gaps.
Medium Risk: Process improvements needed.
Positive Strengths: Technical response and evidence collection.
Overall Classification: Mixed – excellent technical capabilities, critical awareness gaps.

Lessons Learned

Phishing simulation revealed gaps in user awareness despite excellent technical response. Priority: Implement systematic security awareness training and regular phishing simulations.

Critical Findings & Recommendations

High Priority: Deploy Email Security, Mandatory Security Training, Regular Phishing Simulations.
Medium Priority: Enhance Log Retention, Document Detection Methods, Share SOC Best Practices.

Conclusion

The analysis identified strong technical response capabilities but urgent need for better user training. Balancing human-factor security with technical controls is key to comprehensive protection.