SecureSync Corp - Incident Response & Forensics

Date: May 3, 2025

This report consolidates the Project 6 submission: a NIST-aligned Incident Response plan and a Digital Forensics workflow for SecureSync Corp.

Part 1: Incident Response (NIST-aligned)

Roles and Responsibilities

- Incident Response Manager: Coordinates the response process, approvals, and service recovery.
- Security Analysts: Monitor alerts, investigate logs, scope attacks, and analyze events using SOPs and tools.
- Lead Investigator: Collects and analyzes evidence, determines root cause, directs analysts, and drives recovery.
- Communications Lead: Manages internal and external communications with stakeholders, partners, customers, and media.

Monitoring Checklist (Unusual Activity)

- Monitor for unauthorized access attempts and anomalous authentication events.
- Review system and application logs for spikes, errors, or suspicious patterns via SIEM.
- Assess IDS/IPS and EDR alerts, triage high severity signals.
- Check for unusual outbound traffic patterns or data exfiltration indicators.

Documenting Detected Incidents

- Time of detection: date and time when the incident was first observed.
- Severity of impact: business impact and affected stakeholders.
- Description: what occurred, suspected TTPs, and initial indicators of compromise.
- Initial containment actions: steps taken immediately to contain the incident.

Containment Strategies

- Isolate affected systems and network segments to prevent lateral movement.
- Disable or restrict compromised user and service accounts to reduce attacker capability.

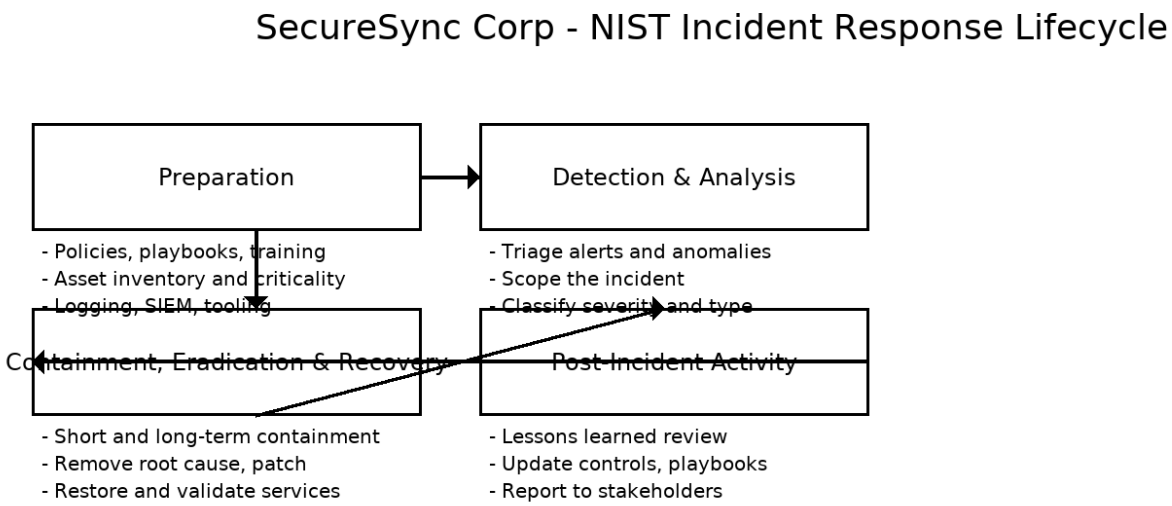
Post-Incident Review Framework

- Gather artifacts, logs, timelines, and stakeholder input.
- Conduct interviews and reconstruct the event sequence.
- Analyze response effectiveness and identify gaps.
- Document lessons learned and actionable improvements.

Plan Update Checklist

- Analyze findings and categorize by detection, containment, recovery, and governance.
- Identify gaps and improvements aligned to NIST guidance and organizational risk.
- Revise procedures, communicate changes, and validate through exercises.

Diagram: NIST Incident Response Lifecycle



Part 2: Digital Forensics

Evidence Sources

- Computer systems: file systems, memory, system logs.
- Mobile devices: call logs, messages, emails, location, app artifacts.
- Network traffic: PCAP and flow data to identify unauthorized access and C2.
- Cloud services: storage, email, collaboration logs and artifacts.

Integrity and Verification Steps

- Acquire data using forensically sound imaging and preserve originals.
- Verify authenticity with cryptographic hashes and preserve chain of custody.
- Analyze data with forensic tools; document methodology and findings.

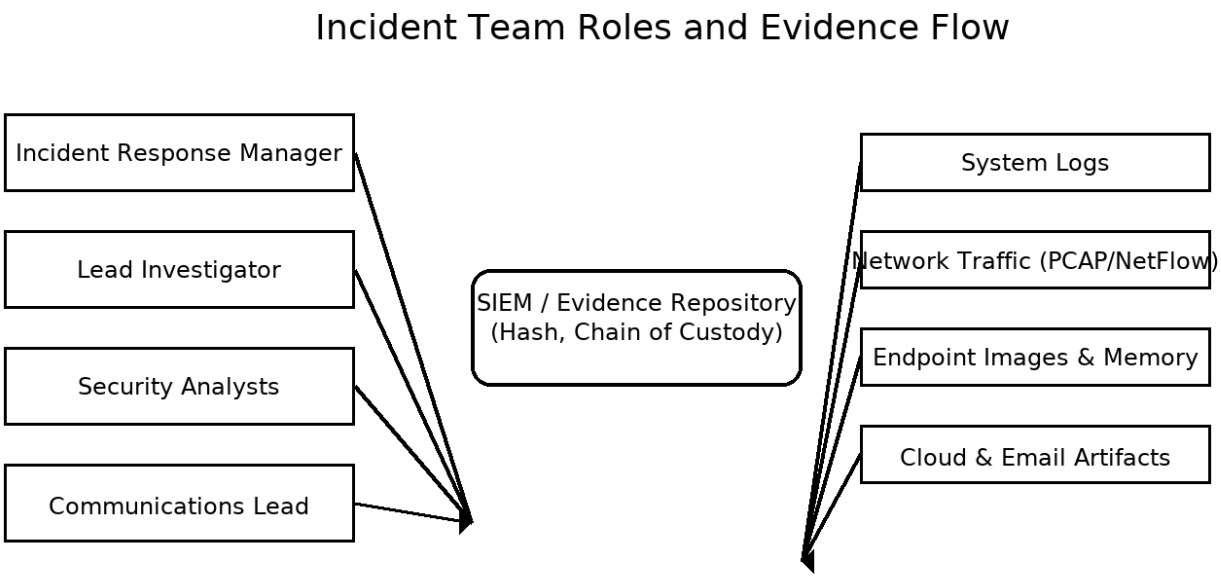
Evidence Types and Purpose

- System logs: show who did what and when; support timeline and scope.
- Network traffic: reveal communications, exfiltration, and attacker infrastructure.
- Endpoint images and memory: identify malware, artifacts, and file timeline evidence.

Reporting Components

- Methodology: tools used, acquisition methods, hash values, and custody trail.
- Evidence presentation: structured tables and identifiers for clarity.
- Analysis and timeline: findings, correlations, and sequence of events.
- Conclusions and recommendations: remediation and prevention actions.

Diagram: Incident Roles and Evidence Flow



- All evidence hashed (SHA-256) and tracked via chain of custody.
- Roles collaborate via tickets and war-room channels.
- Only authorized personnel can access the repository.

References

References
- NIST SP 800-61 Rev. 2: Computer Security Incident Handling Guide
- NIST SP 800-86: Guide to Integrating Forensic Techniques into Incident Response
- MITRE ATT&CK knowledge base for adversary behaviors
- SANS Incident Handlers Handbook (overview concepts)