# Incident Response Planning

Liam Dodd

April 8, 2024

# Introduction

## Purpose

This document outlines the procedures to follow in the event of a ransomware attack or data leak incident. The goal is to contain the incident, minimize damage, restore systems and data, communicate effectively, and document the incident.

## Scope

This plan applies to all systems, networks, data, and personnel. It covers incidents resulting from malware, unauthorized access, insider threats, and accidental data exposure.

## Goals

- Detect incidents early and contain them quickly
- Minimize loss or theft of data or disruption of services
- Recover damaged systems and data to restore normal operations
- Learn from incidents and improve defenses and response capabilities

# Incident Response Team

- CIO
- CISO
- IT Manager
- Security Engineer
- Legal Counsel

# Detection and Analysis

- Monitor antivirus, firewall, and intrusion detection logs for signs of malware or unauthorized access
- Watch for abnormal activity like encryption of files, access denied errors, or unusual outbound network traffic
- Interview personnel who spotted suspicious behavior and review activity on systems they used
- Determine scope and root cause of incident

# Communication Plan

1. Contact CIO and CISO immediately via call/text
2. CISO will alert incident response team members
3. CISO will provide instructions for containment and mitigation
4. IT Manager will communicate status to affected departments

## Containment

- Isolate infected systems by disconnecting from network
- Block suspicious IP addresses at firewalls and other security devices
- Disable user accounts that may have been compromised
- Prevent encryption of additional files if ransomware

## Eradication and Recovery

- Wipe and reimage infected systems using trusted media
- Restore data from backups if needed
- Change passwords and credentials that may have been compromised
- Scan restored systems and data to ensure threat is eliminated

## Post-Incident Activity

- Document details of incident for future reference
- Review circumstances that led to incident and see where security controls failed
- Implement additional monitoring or controls to prevent re-occurrence
- Provide updated training to personnel on threats and response procedures

# Security tooling

The following security tools and technologies are utilized to support incident detection, response, and recovery:

## Network Monitoring

- Firewalls - Detect anomalous traffic patterns and block malicious IP addresses.
- IDS/IPS - Malicious traffic patterns and known attack signatures are detected by intrusion detection and prevention systems.
- SIEM - Security information and event management aggregates and correlates logs from security devices.

## Host Monitoring

- Endpoint Detection & Response - Agents monitor endpoints for suspicious activities, policy violations, and security events.
- Antivirus - Malware execution is blocked and suspicious files are analyzed.

## Access Controls

- Proxy Servers - Control and inspect web traffic.
- Remote Access VPN - Secure VPN concentrators enforce MFA and access controls for remote users.

## Incident Response

- Ticketing system - to track incident response activities and document actions taken.
- Threat intelligence feeds - sources feed into security tools to block known bad actors.
- Forensics tools - used to analyze infected systems and capture evidence.

## Backups

- Immutable backups - Backups are maintained for quick recovery of compromised data and systems.
- Offline backups - Critical system backups are kept offline and physically secured for recovery from ransomware.

# Conclusion

An incident response plan is critical for protecting an organization's data, systems, and business functions. This incident response plan outlines procedures for quickly detecting, containing, eradicating, and recovering from security incidents like malware, data breaches, and ransomware attacks.

Key takeaways include:

- Having defined roles and responsibilities for the incident response team ensures accountability and coordination.

- Implementing monitoring tools and technologies provides visibility into threats and enables early incident detection.

- Containing incidents quickly is essential to minimize damage and loss of data. Strategies like isolating infected systems must be predefined.

- Restoring compromised systems from trusted backups and scanning them before reconnecting to the network allows recovery without reinfection.

- Documenting details during and after an incident aids in improving defenses and response plans.

- Conducting post-incident reviews and implementing learnings allows the organization to enhance detections, response capabilities, and overall resilience.

With the procedures and technologies outlined in this plan, the organization can rapidly respond to and recover from incidents while keeping business functions available. The plan is a living document and will be updated as the threat landscape evolves.