Cybersecurity Capstone Project: Ransomware Attack Incident Response Playbook

Outline

1. Aim and Objective

The aim of this project is to create a comprehensive Incident Response (IR) playbook specifically for ransomware attacks. The objective is to provide the organization with a clear, actionable, and time-sensitive framework to detect, contain, eradicate, and recover from ransomware incidents swiftly, minimizing operational disruption and data loss while safeguarding critical assets.

2. Methodology

Concept of Project

Ransomware attacks pose a significant threat by encrypting critical data and demanding payment for its release. This project focuses on designing a detailed playbook that guides the cybersecurity team through a structured response to ransomware incidents. It emphasizes early detection using advanced monitoring tools, immediate containment to prevent lateral spread, eradication of malware, and secure recovery procedures. Clear roles, communication strategies, and measurable metrics are integrated to improve response effectiveness and organizational resilience.

Tools Used

Endpoint Detection and Response (EDR): CrowdStrike Falcon, SentinelOne, or Microsoft Defender for Endpoint for real-time ransomware detection and isolation

Backup and Recovery Solutions: Veeam Backup & Replication, Acronis Cyber Backup for restoring encrypted data securely

SIEM: Splunk, IBM QRadar, or Microsoft Sentinel for correlating ransomware indicators and alerting

Network Security Tools: Cisco Firepower, Palo Alto Networks Next-Gen Firewall for network segmentation and blocking malicious traffic

Incident Management Platforms: ServiceNow Security Operations or PagerDuty for coordination and tracking

Communication Tools: Slack, Microsoft Teams for internal coordination; secure email channels for external communication

3. Incident Playbooks

Ransomware Attack Incident Response Playbook

Incident Identification: Triggers and Indicators

1. Alerts from EDR tools detecting suspicious file encryption behavior or ransomware signatures

2. SIEM correlation of anomalous network traffic, mass file modifications, or communication with known ransomware command-and-control servers

3. User reports of encrypted files or ransom notes appearing on systems

4. Sudden unavailability of critical systems or network shares

5. Spike in failed login attempts indicating possible lateral movement

Incident Response Phases

Detection:

1. Continuous monitoring via EDR and SIEM dashboards for ransomware indicators

2. Expected detection time: within 10 minutes of initial malicious activity or user report

Containment:

3. Immediate isolation of affected endpoints via EDR to stop ransomware spread within 15 minutes post-detection

4. Segmentation of network segments and blocking of malicious IP addresses at firewalls within 30 minutes

5. Disable affected user accounts to prevent further lateral movement within 1 hour

Eradication:

1. Use EDR tools to remove ransomware payloads and related malware artifacts within 6 hours after containment

2. Verify backups and initiate restoration of affected systems using Veeam or Acronis within 12 hours

3. Deploy patches and hardening measures to close exploited vulnerabilities during eradication phase

Recovery:

1. Restore encrypted data from clean backups, with priority systems restored within 24 hours post-eradication

2. Resume normal business operations with continuous monitoring for residual threats for at least 14 days

3. Conduct post-incident user awareness and phishing simulation training within 2 weeks of recovery

Roles and Responsibilities

Incident Commander: Leads the incident management, escalation, and coordination of all phases; ensures timelines are met

Technical Lead: Directs containment, eradication, and recovery activities; oversees EDR and backup restoration processes

Network Security Analyst: Manages firewall rules, network segmentation, and blocks malicious traffic

Helpdesk/Support: Facilitates user communication, account management, and support ticket resolution

Communications Officer: Handles internal updates, external notifications, and liaises with legal and PR teams

Communication Strategy

Internal:

1. Immediate alert to security and IT leadership teams via Slack or MS Teams within 5 minutes of detection

2. Regular status updates every 2 hours until incident containment

3. User guidance communications dispatched within 30 minutes of containment, including steps to avoid spreading ransomware

External:

1. Regulatory notification within 72 hours if sensitive data compromise is suspected (e.g., GDPR, HIPAA)

2. Customer or partner communication coordinated through legal and PR as needed

3. Maintain clear and transparent messaging while avoiding unnecessary alarm

Metrics

Metric Target	Time/Value	Tool for Measurement
Time to Detect	≤ 10 minutes	EDR (CrowdStrike, SentinelOne) alert logs
Time to Contain	≤ 15 minutes post-detection	EDR isolation logs, firewall configuration timestamps
Time to Eradicate	≤ 6 hours after containment	EDR reports, backup system logs
Time to Recovery	≤ 24 hours post-eradication	Backup solution logs (Veeam/Acronis), Incident management system

Number of Systems Affected: Minimum possible; tracked via logs EDR and SIEM event reports

User Downtime: Minimized to ≤ 24 hours for critical systems IT operations tracking

4. Presentation/Report

Design Choices Explanation

The ransomware playbook prioritizes ultra-rapid detection and containment due to ransomware's ability to spread quickly and encrypt critical data. The 10-minute detection and 15-minute containment goals are achievable with cutting-edge EDR

solutions like CrowdStrike or SentinelOne. Network segmentation and account disabling further prevent lateral spread. Recovery plans rely heavily on tested backup solutions like Veeam to avoid ransom payments. Communication is streamlined for urgency internally, while external communications follow legal and reputational considerations. The metrics are aligned with practical operational capabilities and compliance requirements.

Expected Benefits

1. Rapid containment limits ransomware spread and data encryption

2. Clear roles and timeline accountability streamline incident management

3. Use of reliable backup solutions mitigates data loss without paying ransom

4. Defined communication pathways reduce confusion and maintain stakeholder trust

5. Post-incident metrics enable continuous improvement of ransomware defenses

5. Post-Incident Review Template

Section: Details to Capture

Incident Description Summary of ransomware incident timeline, affected systems, ransom note details
Detection: Detection time, tools involved (EDR/SIEM), user reports
Response Actions: Detailed timeline of containment, eradication, and recovery steps with tool usage
Roles & Communication: Effectiveness of role execution and communication strategy, including any delays or miscommunications
Challenges Faced: Technical difficulties (e.g., backup restoration failures), process gaps
Metrics Results: Actual timeframes for detection, containment, eradication, recovery vs. targets; affected systems count
Lessons Learned: Insights on vulnerabilities exploited, response improvements, and user behavior
Recommendations: Updates to playbook, patching schedules, backup testing, and user training enhancements
Follow-up Actions: Assigned owners, deadlines for implementing improvements and follow-up audits

6. Conclusion

This Ransomware Attack Incident Response Playbook, supported by stringent detection and response timelines and leading security tools, enables the organization to swiftly isolate and eradicate ransomware threats, minimizing operational impact and data loss. Clear roles, detailed communication plans, and measurable metrics provide a strong framework for efficient incident handling and continuous security posture enhancement.

7. Reference

NIST SP 800-61 Revision 2: Computer Security Incident Handling Guide

SANS Institute Incident Handler's Handbook

Verizon Data Breach Investigations Report (DBIR)

CrowdStrike Falcon product documentation

SentinelOne Endpoint Protection resources

Veeam Backup & Replication user manuals

ServiceNow Security Operations documentation

Cisco Firepower Next-Gen Firewall guides