Report: Effective Cyber Incident Response Plan

Intern Name: Ammarah Taj

Date: 08-09-2025

Objective

Develop a structured response plan for handling cybersecurity incidents effectively.

Step 1: Preparation

This phase focuses on readiness, prevention, and resilience.

Key Actions

- **Incident Response Team (IRT)**: Define clear roles and responsibilities, Incident Commander, Forensic Analyst, Communications Officer, Legal Liaison.
- **Security Policies & Playbooks**: Maintain up-to-date security procedures for various incident types.
- **Zero Trust Implementation**: Enforce strict access controls — verify every user, device, and connection request.
- **Immutable & Offline Backups**: Maintain tamper-proof backups stored both offline and in secure cloud environments.
- **Simulations & Drills**: Conduct quarterly tabletop exercises and phishing simulations to test readiness.
- **Forensic Toolkit Readiness**: Pre-install and maintain forensic tools on dedicated incident response machines.

STEP 2: Threat Detection

Continuous monitoring by using tools such as:

- **24/7 SIEM and SOAR Integration**: Combine Security Information and Event Management (SIEM) with Security Orchestration, Automation, and Response (SOAR) for automatic detection and response to threats in real-time.
- **Threat Intelligence Correlation**: Integrate **MITRE ATT&CK** mapping to classify threats by tactics and techniques immediately upon detection.
- **Behavioral Analytics (UEBA)**: Monitor user and entity behavior to detect anomalies that traditional signature-based tools might miss.
- **Deception Technology**: Deploy honeypots and decoy files to trap attackers and gain intelligence on their methods.

These tools and technologies can help automatically detect anomalies like suspicious login attempts, unusual process activity, or abnormal file access patterns. By continuously collecting and analyzing data, the security team can identify potential threats early and take immediate action before they escalate.

STEP 3: Containment & Mitigation

Once a threat is confirmed, our priority should be to limit its spread and neutralize immediate damage. We can do this by either short-term containment or Long-term containment depending on the risk levels and impact of attack.

Short-Term Containment:

- Isolate compromised devices from the network automatically via SOAR integration.
- Disable affected user accounts and reset credentials.
- Apply dynamic firewall rules to block malicious IPs and domains.

Long-Term Containment:

- Segment the network into smaller zones to limit lateral movement.
- Patch exploited vulnerabilities.
- Deploy multi-factor authentication (MFA) organization-wide if not already in place.

4. Eradication & Recovery

Completely remove the threat and restore operations securely, ensuring no re-entry points remain.

Actions:

1. **Threat Removal** – Scan and clean all affected systems, removing malware, persistence mechanisms, and unauthorized accounts. Quarantine devices during cleaning.
2. **System Rebuild** – For heavily compromised systems, wipe and reinstall OS from trusted golden images, apply patches, and harden configurations.
3. **Backup Restoration** – Restore only from verified clean backups, using hash checks to confirm file integrity. Test applications and databases post-restore.
4. **Phased Reintroduction** – Bring systems online in priority order, testing functionality and monitoring closely before full integration.
5. **Extended Monitoring** – Monitor for 30+ days with SIEM and endpoint tools, watching for IOCs or reinfection attempts.
6. **Communication** – Provide progress updates and final documentation, including root cause and improvements made.

Post-Incident Review

After containment and recovery, it is a beneficial practice to analyze and document the Incidents which we can use later as a learning opportunity and avoid similar incidents from reoccurring.

Activities:

- Conduct a Lessons Learned Workshop with all involved departments.
- Document incident timeline, root cause, attack path, and mitigation steps.
- Update playbooks and policies based on findings.
- Share anonymized incident details with national CERTs, ISACs, or industry peers to improve collective defense.