Good Practices for Running Incidents

Running an incident smoothly **requires clear roles, effective delegation, communication, and timing**. Here's a breakdown of best practices, with insights into handling roles, communication, and management expectations throughout an incident.

1. Delegation Best Practices

- Assign Roles and Responsibilities Early: Use a **predefined incident response team (IRT)** structure. Common roles include:
  - **Incident Commander**: Leads the incident response, makes final decisions, coordinates efforts.
  - **Triage Lead**: Assesses and prioritizes alerts, determines severity.
  - **Forensics/Analysis Team**: Investigates the root cause, examines logs, and assesses attacker actions.
  - **Communications Lead**: Manages external/internal communication, including updates to legal, compliance, and users.
  - **Legal and Compliance**: Advises on regulatory requirements, reporting, and risk.
- **Use Playbooks**: Ensure team members **have access to playbooks for specific incidents** (e.g., phishing, malware). **Playbooks provide step-by-step guidance, improving response efficiency**.

2. Communication Management

- Channels:
  - Secure Chat Platforms (e.g., Slack or Teams): For real-time coordination. Create private channels for each incident.
  - Incident Management Platform (e.g., PagerDuty, ServiceNow): To track progress, document actions, and keep all information centralized.
- Frequency:
  - Initial Notification: Alert relevant teams immediately upon incident detection.
  - Regular Updates: Provide updates at predetermined intervals (e.g., every hour) for significant incidents.
- Stakeholder Updates:
  - Internal Team: Regular updates on status, containment efforts, and ongoing investigations.
  - Upper Management: Notify upper management **when impact becomes clear, and set realistic timelines**.

3. When to Stop an Attack

- Contain vs. Stop: Sometimes, monitoring attacker actions without immediate intervention can yield critical intelligence.
- Balance the Risk:
  - Stop if the attack's harm exceeds the value of continued observation, especially if sensitive data is actively being exfiltrated.
  - Delay if monitoring can uncover attacker techniques, tools, or broader compromise without significant damage.

4. Risks of Alerting the Attacker

- Considerations:
    - Premature Blocking: May prompt attackers to intensify, diversify, or attempt lateral movements in a system.
    - Data Exfiltration: Attackers may execute final data exfiltration if they detect containment efforts.
- Best Practices:
    - Plan carefully for containment and eviction, ensuring all affected entry points are addressed to prevent re-entry.
    - Coordinate timing so all containment actions occur simultaneously, reducing the chance of alerting the attacker prematurely.

5. Attacker Cleanup/Hiding Techniques

- Methods:
    - Log Deletion/Modification: Attackers may delete or alter logs to remove traces.
    - Backdoor Installation: Attackers install hidden access points for future entry.
    - File Timestamp Manipulation: Alter timestamps on compromised files to avoid detection.
- Detection: Regular, thorough log monitoring and use of forensic tools can help spot these activities.

6. Management Communication and Expectation Setting

- When to Inform:
    - For significant incidents, **inform upper management as soon as the potential impact is understood**.
- Setting Expectations:
    - **Share a high-level incident summary, anticipated timelines, and potential business impacts**.
    - Regularly update management on milestones (containment, eradication, recovery) to keep them informed without overwhelming them.

7. Prioritizing Incidents

- **Priority Metrics**:
    - **Data Sensitivity**: High-priority if sensitive information (PII, financial data) is affected.
    - **Business Impact**: Higher priority if core business functions are disrupted.
    - **Scope**: Broad scope incidents affecting multiple systems or users take precedence.
    - **Compliance Risk**: Higher priority if compliance or legal reporting requirements are triggered.
- **Escalate Priority** if an incident's severity or impact increases, such as new data exposures or expanding attacker access.

8. Using Playbooks for Efficient Responses

- Purpose: **Playbooks** offer structured **steps for specific incidents**, helping teams work **quickly and consistently**.
- Updating Playbooks: **Regularly update** playbooks based on recent incident reviews and lessons learned.
- **Customization**: Adapt playbooks to address organizational nuances, such as unique system architecture or compliance requirements.

Summary

These practices establish a disciplined, structured incident response process, ensuring that every team member knows their role, communication is clear, and management stays informed, all while minimizing risks and ensuring a swift resolution.