Incident Response Plan

Major steps in an Incident Response Plan are :

1. Identification
2. Scoping
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned

1. Identification of Data Breach

Security alerts or Event notifications are crucial as they can be a hint towards a potential threat or occurrence of an actual security incident. These alerts are pivotal in triggering the incident.

Triaging these alerts helps in identifying the severity of the beach.

Steps to Identify a Data Breach:

1. **Monitor and Detect:**
    - SIEM : Implement continuous monitoring systems (e.g., SIEM) to detect unusual activity.
    - EDR / AV : Review the information provided with events that triggered the alert such as EDR (Endpoint Detection and Response) systems or Anti-Virus alerts.
    - IDS / IPS : Use intrusion detection/prevention systems (IDS/IPS) to identify potential breaches.
    - Network Tap Alert : Review the information of alerts for anomalous network activity.
    - Auditing : Conduct regular audits and vulnerability assessments.
2. **Initial Investigation:**
    - Analyze alerts and logs from security systems.
    - Confirm the breach by identifying unauthorized access or Data Encryption suspicious traffic moving out of the network or any other suspicious activity.
3. **Notification:**
    - Notify the incident response team (IRT) immediately upon confirming the breach.
    - Document the incident, including the time of detection and initial findings.

Tools to be Used :

- Endpoint Detection and Response (EDR)
    - Aurora EDR
    - Wazuh

- Intrusion Detection and Prevention Systems (IDPS)
    - Snort
    - Suricata
- Security Information and Event Management (SIEM)
    - Splunk
    - IBM Security QRadar
- Network Traffic Analysis
    - Wireshark
    - Zeek
- Log Analysis
    - LogRhythm
    - ELK Stack

2. Scoping

Scoping includes determining the impact of security incident which includes identifying theh affected systems and the type of data at risk. It also includes the potential impact of incident on organization.

The Asset Inventory

It is a crucial tool for incident response. It lists all the assets of an organization which helps in identifying the scope of an incident. It helps in assessment of affected systems during a breach.

The Spreadsheet of Doom (SoD)

It is an organized source of information about known threats serving as a single reference point. Each row in this spreadsheet contains information about a unique threat identifier or an Indicator of compromise (IoC).
It includes IP Addresses, domain names, URLs, file hashes etc. related to malicious actvities It also provides information about source of each IoC and type of threat linked to it.

Steps for Scoping the Data Breach:

1. **Scope and Impact Assessment:**
    - Determine the extent of the breach, including affected systems and data.
    - Identify the type of data compromised (e.g., personal, financial, intellectual property).
2. **Root Cause Analysis:**
    - Investigate the source of the breach (e.g., malware, phishing, insider threat).
    - Review logs, network traffic, and system configurations to trace the breach's origin.

3. **Risk Assessment:**
    - Evaluate the potential impact on the organization and stakeholders.
    - Prioritize affected systems and data based on their criticality.

3. Containment

Containment aims to minimize the damage caused by an incident and further prevent the damage. Containment is crucial for collecting evidence for forensic analysis. Normal operations can only be continued after an incident has been successfully contained.

Pre Containment

Gather as much information as possible about the incident and the adversary. This includes collecting evidence from infrastructure such as IDS and SIEM and this evidence will form an Indicators of Compromise (IoCs).

Containment Strategies

Isolation

Entire Isolation is an aggressive but very effective strategy. Threat can be contained by completely isolating the infected systems from the rest of the network and it will stop the threat from spreading. This can be done in two ways : Network Segmentation and Physical Segmentation.

This strategy is noticeable by adversaries so it is possible that they may rush on their “action on objectives”. They may start deleting the data, damaging systems or compromising unnoticeable systems. So think about following :

- How aggressive the isolation should be ?
- How likely the adversary will rush for their “action on objectives” ? (Threat Intelligence)
- Do we understand the adversary enough yet ?
-

Controlled Isolation

Controlled Isolation is a less aggressive strategy but not completely risk free.
You need to observe the actions of the adversary very carefully so that you can keep the systems accessible to them to not tip off the adversary. This plays a vital role in gathering intelligence about adversaries.

Although, they are not allowed to roam freely like if they are about to perform a destructive task just stop them by revoking their access and covering that up by a regular maintenance to not tip off the adversary.

Consider the following before going for this strategy :

- What is the risk of allowing the adversary to continue ?
- Do we know about the adversary already ?
- If so, perhaps full on isolation would be best.
- Do we have the appropriate means to stop an adversary before they do something destructive ?

Threat Intelligence for Containment

Tactics Techniques Procedures (TTPs)

These 3 things are extremely important in understanding how the threat actors operate.

Tactics : This is high-level objectives that the threat actor aims to achieve

Techniques : This refers to specific tools or methods the threat actors employ to achieve their tactics.

Procedures : This refers to the attack chain used by the adversary.

Gather information from these 3 things about adversary and then start the containment of the incident.

4. Eradication

Eradication Techniques:

Automated Eradication

Some malwares can be automatically quarantined, cleaned up, and removed by tools such as Anti-Viruses (AVs) and EDRs. This is most effective in case of less sophisticated threats that use well-known malicious tooling.
Don’t depend on this technique if the threat is unique or very sophisticated because they are developed on the concept of FUD (Fully UnDetectable) that are meant to bypass these automated tools.

Complete System Rebuild

This is the most straightforward way to eradicate an attacker from a specific endpoint. Although it is an absolute technique which will wipe the entire system including all the important softwares and configurations.
So just use this technique only in the case where you have no other option left for eradication or if the system does not contain critical data.
Downtime is the major factor to take note of in this technique as this may cause losses of millions of dollars to the organizations.

Targeted System Cleanup

This technique should only be used when you know that repercussions for failure are very high and they can’t wait for the attackers to know that they have been detected and awaiting cleanup.

This kind of case is very sensitive and systems need to be cleaned with high precision and speed with the help of intelligence insights.

Steps for Eradicating the Threat:

1. **Remove Malicious Artifacts:**
    - Identify and remove malware, rootkits, or other malicious code from affected systems.
    - Patch vulnerabilities exploited during the breach.
2. **System Restoration:**
    - Rebuild or restore compromised systems from clean backups.
    - Reinstall or update software to ensure no remnants of the threat remain.
3. **Validation:**
    - Conduct thorough scans and tests to verify that all threats have been eradicated.
    - Monitor systems for any signs of persistent threats.

Remediation

Remediation is an important step without which eradication would not be effective for a longer period of time.

Remediation Techniques :

Network Segmentation

It ensures that only necessary communication should occur between specific computers and subnets greatly reduces the attack surface for adversaries.

Identity and Access Management (IAM) Review

Restrict Access to Compromised Accounts

The compromised accounts should be reviewed and their mode of compromise (plaintext passwords, vulnerable applications etc.) should be identified and eradicated.

Restrict Access to Highly Privileged Accounts

Access to highly privileged accounts should be controlled and audited carefully as if attackers gain access to these accounts can disturb the entire environment causing damage.

Patch Management

After cleaning we need to identify the root cause of the breach and patch the vulnerability that was exploited by the adversary to prevent future threats.

5. Recovery

The goal of the recovery phase is to be able to continue normal business operations as they were in the pre-incident state.

Steps for Recovering from the Incident:

1. Restoration of Services
    - Restore necessary systems, processes and services starting with most critical ones first.
    - Ensure that these restores systems are fully functional and secure
2. Data restoration
    - Use backups to restore and validate lost data
    - Implement data integrity checks for ensuring accuracy of data.
3. Testing Systems
    - Test the systems that were repaired, replaced or reinforced to ensure their proper working
    - This can be ensured by network pentesting, vulnerability assessments, simulated attacks and tabletop exercises.
4. Monitoring Systems
    - Restored and repaired systems need active monitoring to see if still there is any trace of an adversary.

6. Lessons Learned

This post-incident phase is about learning from the incident by recognizing the areas of improvement in the organization’s security posture and incident response plan and this should be documented to build upon their existing knowledge base.

Communication Guidelines

Communication with Stakeholders:

1. **Internal Stakeholders:**
    - Provide regular updates to senior management and affected departments.
    - Maintain transparency about the breach's status and actions taken.
2. **External Stakeholders:**
    - Inform customers, clients, and partners about the breach if their data is affected and what data is affected.
    - Offer guidance on mitigating potential impacts (e.g., changing passwords).

Communication with Regulatory Bodies:

1. **Compliance:**
    - Report the breach to relevant regulatory bodies (CERT, CSIRT) within required timeframes.
    - Provide detailed incident reports as required by laws and regulations (e.g., GDPR, HIPAA).
2. **Coordination:**
    - Cooperate with regulatory investigations and audits.
    - Implement any recommended corrective actions from regulatory authorities.