Incident Handler's Journal – Sample Entries

Incident 1 – Phishing Email

Type: Social engineering / phishing

Summary: An employee reported a suspicious email claiming to be from IT support asking them to reset their password using a link.

Indicators:

- Sender address did not match internal domain

- Generic greeting and urgent language

- Link pointed to an unknown external domain

Actions Taken:

- Instructed user not to click the link

- Collected the email headers and full message

- Reported and blocked the sender domain on the email gateway

- Searched mail logs for other recipients and removed the email from their inboxes

Lessons Learned:

- Reinforce phishing awareness training

- Encourage employees to report suspicious emails immediately

Incident 2 – Malware Detected on Workstation

Type: Malware / endpoint compromise

Summary: Antivirus software alerted on a malicious file downloaded from a free software website.

Indicators:

- AV alert with malware signature

- User reported system running slower

Actions Taken:

- Isolated the workstation from the network

- Ran full antivirus scan and removed detected malware

- Collected logs and noted time of infection

- Verified no lateral movement using network and authentication logs

- Reimaged the system as a precaution and restored user data from backup

Lessons Learned:

- Remind users not to download unapproved software

- Review application whitelisting and web filtering policies

Incident 3 – Unauthorized Login Attempt

Type: Account / authentication issue

Summary: Multiple failed login attempts were detected for an admin account from an unusual IP address.

Indicators:

- Login logs showing repeated failures

- IP address geolocation outside normal business region

Actions Taken:

- Locked the affected account temporarily

- Reset the account password and enforced MFA on admin accounts

- Blocked the suspicious IP at the firewall

- Reviewed other accounts for similar activity

Lessons Learned:

- Ensure MFA is enforced on all privileged accounts

- Regularly monitor login logs for anomalies

- Implement alerts for repeated failed logins and logins from unusual locations

Summary:

These incident journal entries demonstrate identifying indicators, taking containment and remediation actions, and documenting lessons learned for phishing, malware, and unauthorized access scenarios.