Title: Threat Hunt Scenario: Phishing Attack Compromise

Overview

This threat hunt scenario simulates a phishing attack leading to credential theft or compromised accounts. It outlines the steps to detect, investigate, remediate, and prevent such incidents using real-world tools and methods.

Objective

- Detect and mitigate phishing attempts targeting organizational email accounts.
- Investigate malicious activities, such as compromised account logins and unauthorized email forwarding.
- Apply preventive measures to enhance security against phishing threats.

---

1. Setup a Virtual Environment

Create a Virtual Machine (VM)

1. Use a cloud provider like **Microsoft Azure**, **AWS**, or a local hypervisor such as **VirtualBox** or **VMware**.
2. Install **Windows 10** or the primary operating system used by your organization.
3. Ensure the VM has access to your organization's mail platform (e.g., Office 365).

Simulate Phishing Activity

1. Set up a dummy email account for testing.
2. Use an email simulation platform like **Gophish** to send test phishing emails.
3. Include a link to a credential-harvesting page to simulate real phishing activity.

---

2. Detection

Query 1: Email Logs for Phishing Detection

KQL Query:

kql

Copy code

```
EmailEvents

| where ThreatTypes has "Phishing"

| project Timestamp, Sender, Recipient, Subject, Url
```

Example Output:

Timestamp	Sender	Recipient	Subject	Url
2024-12-20T10:15:34Z	phisher@example.com	victim@example.com	Action Required: Update Password	http://malicious-link.com/login

---

Query 2: Authentication Logs for Suspicious Logins

KQL Query:

kql

Copy code

```
SigninLogs

| where UserPrincipalName == "victim@example.com"

| where Location not in ("USA", "Known Locations")

| project Timestamp, UserPrincipalName, Location, IPAddress
```

Example Output:

Timestamp	UserPrincipalName	Location	IPAddress
2024-12-20T12:45:23Z	victim@example.com	Russia	203.0.113.45

Query 3: Detection of Email Forwarding Rules

KQL Query:

kql

Copy code

```
EmailSettings

| where Action == "ForwardingRuleCreated"

| project Timestamp, UserPrincipalName, ForwardingAddress
```

Example Output:

Timestamp	UserPrincipalName	ForwardingAddress
2024-12-20T13:12:45Z	victim@example.com	attacker@example.com

---

3. Response

Immediate Actions to Contain the Threat

1. **Quarantine Phishing Emails:**

    - Use your email security solution (e.g., Microsoft Defender for Office 365) to remove phishing emails from all user inboxes.

Query all recipients of the phishing email:
kql
Copy code

```
EmailEvents

| where Sender == "phisher@example.com"

| project Timestamp, Recipient
```

    -
    - Execute an email recall or quarantine action on the identified emails.
2. **Reset Compromised Accounts:**
    - Force a password reset for all accounts flagged in the incident, especially those with suspicious login activity.
    - Enable multifactor authentication (MFA) immediately for affected accounts.
3. **Revoke Forwarding Rules:**
    - Remove any malicious email forwarding rules:
        - Review rules in Microsoft Exchange Admin Center or similar tools.

Use PowerShell to remove rules:
powershell
Copy code

```
Remove-InboxRule -Mailbox "victim@example.com" -Identity "Forwarding
to attacker@example.com"
```

        -
4. **Monitor Active Sessions:**
    - Terminate any active sessions for compromised accounts.

Use PowerShell or admin dashboards to log off sessions:
powershell
Copy code

```
Get-SecurityToken | Revoke-SecurityToken -User "victim@example.com"
```

    -

Investigation

- **Phishing Source Analysis:**
    - Investigate the sender's IP address and domain using DNS lookups or services like VirusTotal.
    - Block the sender domain and IPs in email security filters.

- **Analyze Affected Systems:**
  - Review endpoint logs to ensure no malicious payloads were downloaded.
  - Use EDR solutions to scan affected devices for malware or unauthorized changes.
- **Assess Data Exposure:**
  - Check if sensitive files/emails were accessed or exfiltrated.

---

4. Prevention

Technical Measures

1. **Improve Email Security:**
   - Enable **Advanced Threat Protection (ATP)** to analyze email attachments and links.
   - Implement **Domain-based Message Authentication (DMARC)** to block spoofed emails.
   - Enable real-time URL scanning for all email links.
2. **Strengthen User Authentication:**
   - Require multifactor authentication (MFA) for all users.
   - Implement **Conditional Access Policies**:
     - Restrict login access based on geolocation or known IP ranges.
     - Block high-risk sign-ins automatically.
3. **Enhance Monitoring and Detection:**
   - Deploy continuous monitoring tools (e.g., Azure Sentinel) for real-time alerting.
   - Use threat intelligence feeds to update your SIEM with the latest indicators of compromise (IoCs).

---

5. User Awareness Training

1. **Phishing Simulations:**
   - Regularly test employees with phishing simulation campaigns using platforms like Gophish.
   - Provide targeted training to users who fail the tests.
2. **Security Awareness Programs:**
   - Teach employees how to identify and report phishing emails.
   - Promote the use of security buttons to report suspicious emails in email clients.

---

6. Summary

This guide provides a comprehensive approach to detecting, mitigating, and preventing phishing attacks. By implementing the remediation and prevention steps outlined above, organizations can strengthen their defenses against similar threats.