Incident Response Strategy for Complex Multi-Vector Attacks: A MITRE-Based Approach

Author: Gili Levy
Affiliation: CISO-as-a-Service Consultant
Email: gililevy1993@gmail.com
Date: August 2025

This paper presents a structured incident response strategy for complex multi-vector cyberattacks, leveraging the MITRE ATT&CK framework.
I will detail the challenges in detecting and responding to multi-vector threats and illustrate the methodology through a simulated Azure account compromise scenario, complete with full Azure sign-in logs.
The proposed playbook addresses each stage of incident response, from detection to post-incident review.

Introduction

> Multi-vector cyberattacks, where adversaries employ multiple attack vectors simultaneously, pose significant challenges to detection and mitigation.
> These types of attacks may involve phishing, credential stuffing, and ransomware deployment; consequently, it is essential to implement a robust, structured, and flexible incident response strategy.

The MITRE ATT&CK framework is a globally recognized knowledge base of adversary tactics and techniques based on real-world observations. It categorizes attacks into distinct phases, enabling security teams to map adversary behaviors and respond accordingly. Previous studies and incident reports (e.g., APT29, SolarWinds, and NotPetya) highlight the effectiveness of mapping adversary behavior to MITRE for improved detection and response. I have a strong preference for working with the MITRE framework, and every incident response playbook I design is fully aligned with it.

Methodology: MITRE-Based Incident Response Strategy

This methodology aligns each phase of incident response with the corresponding MITRE ATT&CK tactics. The main stages include:

1. Initial Access
2. Execution
3. Persistence & Privilege Escalation
4. Defense Evasion
5. Command & Control
6. Actions on Objectives.
   This approach helps ensure that detection, containment, and eradication efforts are mapped to the adversary's methods.

Case Study: Simulated Azure Account Compromise

The simulated attack scenario involves a coordinated campaign targeting Azure accounts with multiple attack vectors. Indicators include MFA reset attempts, sign-ins from multiple geographies, account lockouts ransomware deployment and data exfiltration.

Timeline of events (Sunday, 4 August 2025):

Time (UTC)	Event Description	Log Source / System	MITRE ATT&CK Technique
02:57	Multiple employees received unexpected multi-factor authentication (MFA) reset prompts overnight, suggesting a possible credential targeting attempt.	Azure AD Audit Logs	**T1078** – Valid Accounts / **T1098** – Account Manipulation
03:04	Several users, including neo@zionmatrix.org, were unable to access their corporate email accounts, indicating potential account lockouts.	Microsoft 365 Exchange Online Logs	**T1531** – Account Access Removal
04:12–04:39	Azure AD sign-in logs recorded successful password authentications followed by denied MFA challenges originating from Vietnam, Russia, and the USA.	Azure AD Sign-in Logs	**T1110** – Brute Force / **T1078** – Valid Accounts
04:40	Conditional Access policies blocked these login attempts, and Entra ID classified one account as **confirmedCompromised**.	Azure AD Sign-in Logs / Entra ID	**T1078** – Valid Accounts
04:51	An Endpoint Detection and Response (EDR) alert on a related workstation flagged the creation of a ransomware ransom note.	Endpoint Detection & Response (EDR)	**T1486** – Data Encrypted for Impact
04:58	The SOC detected anomalous outbound data transfer over TLS from the user's device to an unrecognized external IP address, indicating possible data exfiltration.	SOC / Network Monitoring	**T1041** – Exfiltration Over C2 Channel / **T1048** – Exfiltration Over Alternative Protocol

Accordingly, these sign-in logs should be regarded as a single element within the context of a comprehensive multi-vector attack timeline. The corresponding excerpts from the Azure AD sign-in logs are provided below.

timespomp 2025-08-04T04:12:23 Z
user principal name neo@zionmatrix.org
IP address 192.203.179.11
location Hanoi, Vietnam
device detail Windows 10
authentication requirement multiFactorAuthentication
result (Authenticatethod Success
result (Text message to +972•••1234) ene])
risk level aggregated high
risk state confirmedCompromised
App Display name failure

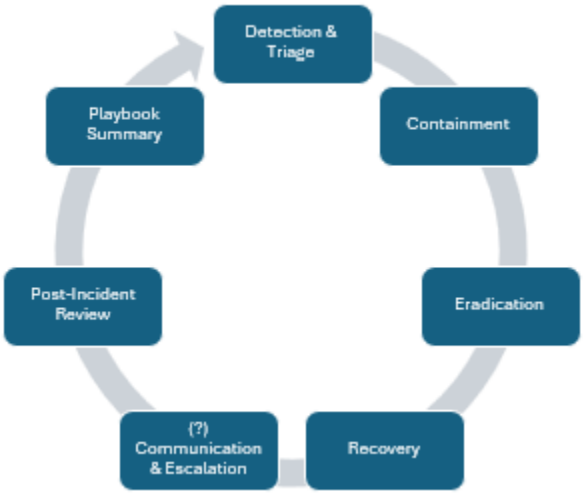
timespomp 2025-08-04T04:25:09Z
user principal name neo@zionmatrix.org
IP address 45.146.23.88
location St. Petersburg, Russia
device detail Windows 10
authentication requirement multiFactorAuthentication
result (Authenticator app Success
result denied atRisk
risk level aggregated atRisk
risk state Microsoft Graph
App Display name failure

timespomp 2025-08-04T04:39:14 Z
user principal name neo@zionmatrix.org
IP address 209.141.54.67
location Newark, United States
authentictail Edge 126.0
authentication requirement multiFactorAuthentication
result (Authenticator Success

Incident Response Playbook

The incident response playbook covers these stages:

1) **Detection & Triage**: Identify anomalous activity via SIEM and monitoring tools.
2) **Containment**: Isolate affected accounts and endpoints to prevent spread.
3) **Eradication**: Remove malicious artifacts and revoke compromised credentials.
4) **Recovery**: Restore systems from backups and monitor for re-infection.
5) **Communication & Escalation**: Notify stakeholders and escalate internally as needed.
6) **Post-Incident Review**: Analyze the root cause, update policies and improve defenses.



Conclusion

The MITRE-based approach was used to structure the response, aligning each step with documented adversary behaviors. This method reduced time-to-containment and facilitated coordination among SOC, IT, and management teams.

This paper demonstrates the value of a MITRE-aligned incident response strategy for complex multi-vector attacks. Future work should focus on automation of detection-to-containment workflows, integration with SOAR platforms, and expansion to cover emerging attack techniques.