Incident Response Playbook: Unusual VPN Login / Impossible Travel

Team AnubisX

Version 1.0
September 17, 2025

Document Control

Attribute	Value
Version	1.0
Status	Final
Owner	AnubisX Security Team
Review Cycle	Every Quarter

Contents

1 Introduction

1.1 Purpose

The purpose of this playbook is to provide a structured incident response process for unusual VPN login and impossible travel scenarios, with the objective of detecting potential account compromise, minimizing unauthorized access, and maintaining secure remote connectivity.

1.2 Scope

This playbook applies to VPN infrastructure, authentication systems, identity providers (IdPs), and all employees using remote access solutions. It covers all stages of incident response, from preparation to post-incident lessons learned.

2 Overview of Unusual VPN Login / Impossible Travel

Unusual VPN login or impossible travel occurs when a user account is observed logging in from geographically distant locations within an unrealistic timeframe (e.g., logging in from New York and then London within 30 minutes). Such events may indicate credential theft, account compromise, or the use of anonymization/VPN services by attackers.

3 Incident Response Phases

This playbook follows the NIST Incident Response lifecycle framework.

3.1 Phase 1: Preparation

Goal: To ensure the team is equipped and ready to detect and respond to suspicious VPN login incidents.

- **Roles and Responsibilities:** Define roles (Incident Commander, Lead Analyst, Identity/AD Lead, Network Security Lead).
- **Tools & Resources:** Ensure availability of SIEM, VPN logs, MFA solutions, geolocation analysis tools, and identity monitoring.
- **Training:** Conduct awareness training for employees on phishing, credential theft, and MFA usage.
- **Hardening Controls:** Enforce MFA, geo-blocking, conditional access policies, and anomaly detection rules.
- **Contact Lists:** Maintain contacts for IdP admins, VPN service providers, executive management, and IR vendors.
- **Threat Intelligence:** Monitor reports of stolen credentials, brute-force campaigns, and APT targeting VPN solutions.

3.2 Phase 2: Identification & Analysis

Goal: To confirm unusual VPN login/impossible travel activity and determine its scope and severity.

1. **Initial Triage:** Collect VPN authentication logs, correlate with IdP/SIEM alerts, and activate secure communications.

2. **Initial Analysis and IOC Evaluation:** Analyze logs and alerts to identify Indicators of Compromise (IOCs). Common IOCs include:
   - **Authentication:** Logins from geographically impossible locations within short timeframes.
   - **Endpoint:** Login attempts from unrecognized devices or browsers.
   - **Network:** VPN connections from high-risk geolocations or anonymizing services.
   - **Account:** Disabled or bypassed MFA, password reset requests, or unusual privilege escalation.
3. **Severity Level Assessment:** Classify the incident to ensure appropriate allocation of resources. Severity is determined based on the operational impact, the sensitivity of the user account, and the scope of the potential compromise.

Level	Description	Example	MTTD	MTTR
Low	Single unusual VPN login, user verified activity as legitimate.	Employee traveling abroad without notice triggers an alert but confirms activity.	6-12 hours	24 hours
Medium	Unusual login from a suspicious location, MFA successful.	User account logs in from a new country but no additional suspicious activity is observed.	12-24 hours	2-3 days
High	Multiple impossible travel logins with failed MFA or unrecognized devices.	Account logs in from two continents within 30 minutes, MFA bypass suspected.	24-48 hours	4-7 days
Critical	Organization-wide suspicious VPN logins indicating potential attack campaign.	Dozens of accounts show impossible travel logins tied to the same attacker IP ranges.	48 hours	7-14 days

Table 1: Incident Severity Matrix

4. **Alert Validation (TP vs. FP):** Correlate suspicious login activity with other data points and user communication.
   - **If True Positive (TP):** The activity is confirmed malicious or account-compromised. **Action:** Immediately proceed to the **Containment** phase, escalate to the Incident Commander, and activate the VPN login playbook.
   - **If False Positive (FP):** The activity is confirmed benign. **Action:** Document findings, close the alert, and recommend tuning detection rules.
5. **Incident Declaration:** If confirmed, formally declare a VPN login incident and escalate to leadership, legal, and relevant IT teams.

3.3 Phase 3: Containment

Goal: To limit the attacker's access and prevent further damage.

- **Short-Term Containment (Immediate Actions):**
  - Temporarily disable affected user accounts.
  - Block suspicious IPs/geolocations at VPN gateways and firewalls.

  - Revoke all active sessions for the compromised account.

- **Evidence Preservation:** Acquire forensic images of authentication logs and VPN server logs **before** remediation.
- **Long-Term Containment Strategy:** Enforce stricter conditional access policies for high-risk logins.

3.4 Phase 4: Eradication

Goal: To remove attacker access and prevent re-entry.

- **Root Cause Analysis:** Identify how the credentials were compromised.
- **Credential Reset:** Reset and rotate compromised passwords and enforce MFA re-enrollment.
- **Persistence Removal:** Check for and remove any unauthorized devices or authentication tokens associated with the account.
- **Security Hardening:** Patch VPN infrastructure and identity systems; harden conditional access and anomaly detection rules.

3.5 Phase 5: Recovery

Goal: To safely restore user accounts and normal operations.

- **System Restoration:** Restore accounts with secure authentication methods.
- **Enhanced Monitoring:** Increase monitoring of the restored accounts and related network traffic.
- **Validation:** Ensure restored accounts and systems are clean before reconnecting to the production network.
- **Business Continuity:** Resume normal VPN operations with increased monitoring and user verification.

3.6 Phase 6: Post-Incident Activities (Lessons Learned)

Goal: To strengthen resilience and prevent recurrence.

- **Post-Incident Meeting:** Conduct a blameless post-mortem meeting with identity, VPN, and security teams.
- **Final Incident Report:** Create a detailed report covering attack vectors, timeline, and remediation steps.
- **Action Plan:** Create a tracked action plan to improve anomaly detection models, geolocation-based alerts, and educate employees on secure VPN usage.

4 MITRE ATT&CK Framework Mapping

Unusual VPN Login / Impossible Travel ATT&CK Mapping

- **Tactic: Initial Access**
  - *T1078 – Valid Accounts*
  - *T1133 – External Remote Services*
  - *T1110 – Brute Force*
- **Tactic: Persistence**
  - *T1078 – Valid Accounts*
  - *T1136 – Create Account*
- **Tactic: Privilege Escalation**
  - *T1078 – Valid Accounts*
- **Tactic: Defense Evasion**
  - *T1078 – Valid Accounts:* Using legitimate credentials to bypass defenses.
  - *T1562.007 – Disable or Modify Cloud Firewall*
- **Tactic: Credential Access**
  - *T1003 – OS Credential Dumping*
  - *T1621 – Multi-Factor Authentication Request Generation*
- **Tactic: Discovery**
  - *T1087 – Account Discovery*
  - *T1018 – Remote System Discovery*
- **Tactic: Lateral Movement**
  - *T1021 – Remote Services*
- **Tactic: Impact**
  - *T1531 – Account Access Removal*
  - *T1499 – Endpoint Denial of Service*