Portfolio Project 1 – Alert Triage Walk-through “Impossible Travel”

Introduction

This is a simulated alert triage scenario designed to demonstrate how a SOC analyst investigates and responds to a suspicious login event.
The alert is based on a common “Impossible Travel” use case, which often indicates potential credential misuse or VPN activity.
This project shows my step-by-step thinking, investigation process, and final decision-making, as would be expected in a SOC analyst environment.

Alert:

```
**Alert Name:** Impossible Travel Detected
**Source:** Microsoft Sentinel
**Severity:** Medium
**Timestamp:** July 6, 2025 – 08:17 AM
**Description:**
SIEM has detected a login for user `j.smith@acmeinc.com` from **Bangkok,
Thailand** followed by another login from **Frankfurt, Germany** within 12
minutes.
This violates baseline travel speed thresholds and may indicate credential
compromise, VPN misuse, or session hijacking.
```

Triage Process:

1. Acknowledge and Assign Alert

- Alert assigned to Tier 1 analyst
- Initial review begins in SIEM interface
- Verify user identify (active account, old account)

2. Review Alert Metadata in SIEM

- Alert triggered by built-in “Impossible Travel” rule
- User: j.smith@acmeinc.com
- Logins detected from:
    - Bangkok, Thailand – 08:17 AM
    - Frankfurt, Germany – 08:26 AM
- Time between logins: 9 minutes

- Geo-velocity calculation: 9000 km in under 10 minutes

3. Investigate User Account Activity

- Check recent logins for this user
- Look for login frequency, device types, previous impossible travel flags
- Confirm this user's device is known and consistent with past use

4. Check Endpoint Detection and Response (EDR)

- Query device used in Thailand login
- Review process tree for suspicious activity
- Confirm if endpoint has active EDR coverage (e.g., Defender, CrowdStrike)

5. Review MFA and Authentication Logs

- Was MFA triggered and completed?
- Were there failed login attempts prior to this?
- Confirm authentication method used (e.g., password + push notification)

6. Perform IP Reputation Check

- Use tools like VirusTotal or AbuseIPDB
- Frankfurt IP: Identified as common VPN provider (NordVPN)
- Bangkok IP: Appears residential, normal Thai ISP
- No malicious indicators tied to either IP

7. User Verification (If Needed)

- Analyst emails user to confirm travel or VPN use
- User replies confirming use of NordVPN while travelling
- No other users reported similar issues

8. Correlate With Other Alerts

- No lateral movement or privilege escalation detected
- No associated malware or phishing activity
- Alert appears isolated and non-malicious

Findings Summary

- User j.smith@acmeinc.com was confirmed to be using NordVPN at the time of the alert
- MFA was successfully completed for both login events
- No malware, phishing, or lateral movement detected in the environment
- Endpoint logs show normal behaviour during login sessions
- Frankfurt IP identified as VPN exit node with clean reputation

Analyst Decision

Based on investigation, this alert is determined to be a false positive caused by legitimate VPN usage by the user while travelling. No signs of compromise or malicious activity were found.

Action Taken

- Alert marked as **False Positive**
- Closed in SIEM with full investigation notes
- User educated on how VPN usage can trigger travel-related alerts
- No further action required

Final Summary

This walk-through demonstrates my ability to investigate and document a realistic alert triage scenario based on an “Impossible Travel” login.

It reflects key Tier 1 SOC skills, including:

- Reviewing SIEM metadata and authentication logs
- Analysing IP reputation and endpoint behaviour

- Making confident, justified decisions
- Writing clear, structured findings for ticketing systems and team escalation

Tools referenced (e.g., Sentinel, Defender, VirusTotal) were simulated, but the investigative logic and documentation flow are modelled on real SOC workflows.