Exported from Obsidian. Formatting retained for Obsidian Compatibility.

\*\*1. Preparation & Ownership\*\*

- \*\*Assign Responsibility:\*\* Identify the lead analyst and relevant team members (Security Operations, IT, HR, Legal).

- \*\*Verify Tools & Access:\*\* Confirm access to SIEM systems, user audit logs, ticketing systems, and threat intelligence platforms.

- \*\*Document Initial Alert:\*\* Record who reported the issue, the time, and initial indicators (e.g., atypical travel events).

\*\*2. Incident Documentation & Communication\*\*

- \*\*Define Incident Scope:\*\* Document the affected user, observed anomalies, and any initial evidence.

- \*\*Establish Communication:\*\* Use backup channels (SMS, secure messaging) if primary systems are impacted.

- \*\*Notify Stakeholders:\*\* Inform management, HR, and Legal as necessary per the incident’s severity.

###Risky User Checklist###

\*\*1. Identification & Analysis\*\*

- \*\*Atypical Travel Events:\*\*

- Verify recent travel events versus normal behavior (check itineraries, geolocation data).

- Flag discrepancies in login locations compared to reported travel.

- \*\*Sign-In Logs:\*\*

- Analyze login timestamps, geolocations, and device fingerprints.

- Identify anomalous access patterns (e.g., multiple logins from disparate locations in a short time).

- \*\*User Account Audit Logs:\*\*

- Review recent account changes (password resets, permission modifications, MFA changes).

- Check for unusual account configuration modifications.

- \*\*Registered Devices & Connection Devices:\*\*

- Compare the list of registered devices with current login devices.

- Investigate any unrecognized or unauthorized device connections.

- \*\*Ticket History Review:\*\*

- Check past support tickets for recurring issues or previous security-related events involving the user.

- \*\*IP Address Analysis:\*\*

- Assess IP reputation using threat intelligence:

- Determine if the IPs are known for abuse or belong to the company’s approved ranges.

- Note any VPN or proxy usage that might mask true location.

- \*\*Additional Checks:\*\*

- Confirm MFA enforcement and any bypass attempts.

- Review recent system alerts related to the user account (e.g., unusual file access or network behavior).

\*\*2. Containment\*\*

- \*\*Immediate Measures:\*\*

- Temporarily restrict account access or force a password reset if suspicious activity is confirmed.

- Block or flag suspicious IP addresses and enforce geo-fencing if applicable.

- \*\*Escalate & Communicate:\*\*

- Notify impacted departments (IT, HR, Legal) about containment actions and potential risks.

\*\*3. Eradication & Remediation\*\*

- \*\*Clean-Up:\*\*

- Remove unauthorized changes in account settings.

- Revoke or reconfigure permissions that may have been escalated without proper authorization.

- \*\*Credential Renewal:\*\*

- Reset passwords and enforce MFA re-registration.

- Ensure all security tokens or recovery methods are updated.

\*\*4. Recovery & Monitoring\*\*

- \*\*Restore Normal Operations:\*\*

- Gradually restore account access after verifying no ongoing malicious activity.

- Continue enhanced monitoring of the account for any new anomalies.

- \*\*Enhanced Vigilance:\*\*

- Increase logging sensitivity and continue threat hunting around the account.