Template - Identity Protection | Risky users | Risky sign-ins   
Risk detections

Link to alert

**Description**

Identity Protection identifies risks of many types, including Anonymous IP address use Atypical travel, Unfamiliar sign-in properties, etc. The risk signals can trigger remediation efforts such as requiring users to: perform Azure AD Multi-Factor Authentication, reset their password using self-service password reset, or blocking until an administrator takes action.

**Classification**: Incident

**How to investigate**

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection>

**Alert details**

User:

Date:

Application:

Location:

IP address:

Device ID:

Device Display Name:

Severity:

**Remediation**

Confirm with the user if the user is working from **Device Display Name** at **Location**.

If the user is not using **Device Display Name** at **Location,** then inform NSOC team member to **Confirm that the user is compromised** and rest the user’s password to a strong password.

***NB: PROVIDE A SCREESNHOT OF THE WORK DONE***