Template – Sign-ins from Anonymous IP address

Link to alert

**Description**

This risk event type indicates sign-ins from an anonymous IP address (e.g. Tor browser, anonymizer VPNs). Such IP addresses are commonly used by actors who want to hide their login telemetry (IP address, location, device, etc.) for potentially malicious intent.

**Classification**: Incident

**How to investigate**

<https://docs.microsoft.com/en-us/cloud-app-security/investigate-anomaly-alerts>

User details

User:

Country or region:

Office:

**Alert details**

Activity:

Date:

Application:

Device:

IP address:

Location:

Authentication detail:

* Authentication method:
* Authentication method detail:
* Succeeded:
* Result detail:

ISP:

Severity:

**Remediation**

Confirm if the user has a VPN or Tor browser in use which would explain the alert.

Otherwise, reset the password to a strong password and ensure that MFA is enabled with two MFA methods.

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