Template - Malware linked IP address

Link to alert

**Description**

Sign-in from a malware linked IP address

**Classification**: Incident

**How to investigate**

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

**Alert detail**

User:

Date:

IP address:

IP address blacklisted (Yes/No):

ISP:

Location:

Malware name:

Severity:

**Remediation**

Scan the source of the IP address for malware (router - DC/DHCP)

Release the IP address from the user's device

Perform a full Scan on the user's device and remove any possible malware

Reset their passwords and enable MFA