Template - Traffic detected from IP addresses recommended for blocking

Link to alert

**Description**

Azure Security Center detected inbound traffic from IP addresses that are recommended to be blocked. This typically occurs when this IP address doesn't communicate regularly with this resource. Alternatively, the IP address has been flagged as malicious by Security Center's threat intelligence sources.

**Classification**: Request

**How to investigate**

<https://docs.microsoft.com/en-us/azure/security-center/alerts-reference>

**Alert details**

Date:

Destination Port:

Protocol:

Source IP(s) [Number of attempts]:

Resource Type:

Compromised Entity:

**Remediation**

Confirm if the IP address is blacklisted on an 3rd party website.

Review the IP addresses and determine if they should be communicating with the virtual machine.

Enforce the hardening rule recommended by Security Center which will allow access only to recommended IP addresses. You can edit the rule's properties and change the IP addresses to be allowed, or alternatively edit the Network Security Group's rules directly.

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