New AS Path Edge

New AS Path Edge

This alarm detects a new AS peering that was not previously observed before.

Man-in-the-Middle (MITM) attacks involve an attacker injecting their own AS into the AS path of a prefix, thereby directing traffic for the prefix through their AS. To avoid detection of the attack, MITM attacks are usually short-lived and target a small set of prefixes.

Another source of a transient AS peering could be an operator error which is corrected quickly.

Note An AS peering relationship that appears in the AS path of a large number of prefixes advertised by many peers or is long-lived, is most likely a legitimate network configuration change and Crosswork Cloud Network Insights does not alert on those.

Possible Problem Detected

This alarm helps identify potential MITM attacks or an operator error.

Example

You create a Prefix policy with the **New AS Path Edge** alarm rule and is linked to prefix 8.8.0.0/24. The alarm triggers when Crosswork Cloud Network Insights detects that prefix 8.8.0.0/24 is advertised with an AS path that includes suspicious AS peerings (peerings that have not been previously seen across all paths for all prefixes or are new). After a certain amount of time, Crosswork Cloud Network Insights determines that these AS peering relationships are long-lived. After it determines that the peering relationships are long-lived and legitimate, the alarm is cleared.

New AS Path Edge