新しいASパスのエッジ（New AS Path Edge）

新しいASパスのエッジ（New AS Path Edge）

このアラームは、以前に確認されていない新しい AS ピアリングを検出します。

中間者（MITM）攻撃では、攻撃者が自身の AS をプレフィックスの AS パスに挿入し、AS を介してプレフィックスのトラフィックを誘導します。攻撃の検出を回避するために、MITM 攻撃は通常短命で、少数のプレフィックスをターゲットとします。

一時的な AS ピアリングの別の原因として、すぐに修正されるオペレータエラーが考えられます。

（注） AS ピアリング関係は、多くのピアによってアドバタイズされた多数のプレフィックスの AS パスに存在するか、または長期間存続しますが、正当なネットワーク設定の変更である可能性が高く、Crosswork Cloud Network Insights ではこれらのアラートは表示されません。

考えられる検出される問題

このアラームは、潜在的な MITM 攻撃またはオペレータエラーの特定に役立ちます。

例

[新しいASパスのエッジ（New AS Path Edge）] アラームルールを使用してプレフィックスポリシーを作成し、プレフィックス 8.8.0.0/24 にリンクします。アラームは、Crosswork Cloud Network Insights が、疑わしい AS ピアリング（すべてのプレフィックスのすべてのパスで以前に確認されていないピアリング、または新しいピアリング）を含む AS パスでプレフィックス 8.8.0.0/24 がアドバタイズされたことを検出したときにトリガーされます。一定の時間が経過すると、Crosswork Cloud Network Insights は、これらの AS ピアリング関係が長期間存続していると判断します。ピアリング関係が長期間存続していると判断されると、アラームはクリアされます。

新しいASパスのエッジ（New AS Path Edge）

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。