Threat Intelligence Director

メリット

- オープンな業界標準のインターフェイスを使用した脅威インテリジェンスとの統合
- サードパーティのインテリジェンスでネットワークセンサーの有効性を活用
- 侵害の兆候をシスコのセキュリティ センサーにストリーミングし、疑わしいアクティビティを自動的にブロックまたはモニタ
- ネットワーク センサーからの監視結果を関連付けてインシデントのアラートを送信
- 高度なセキュリティ インテリジェンスに基づいてセキュリティ ポスチャを向上

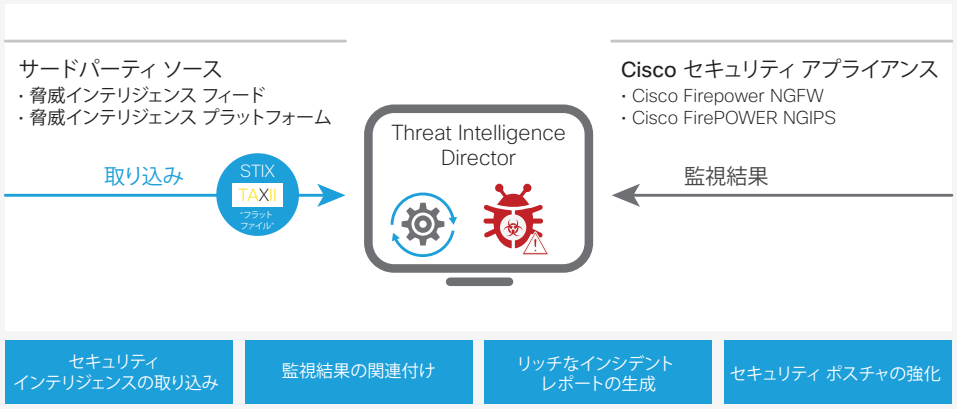
複数のソースからのインテリジェンスを運用可能

組織に対する脅威は、あらゆる場所から生じます。攻撃者は、従業員がマルウェアを意図せずダウンロードするように仕向けます。組織に不満を持つ従業員は、金銭的な利益を得るために会社の資産を密かに持ち出す可能性があります。ネットワークの異常をモニタするには、多くのリソースが必要になります。

疑わしい振る舞いの証拠を確認するのに役立ち、脅威を自動的に封じ込めるようなリソースを活用できるとしたらどうでしょうか。Threat Intelligence Director は、まさにこのような目的のために使用できます。サードパーティの脅威フィードや脅威インテリジェンス プラットフォームから脅威インテリジェンスを取り込むことで、Threat Intelligence Director はシスコのセキュリティ センサーから得られる豊富な監視結果を関連付けて、セキュリティ インシデントを検出しアラートを送信します。ユーザは潜在的に無害なアラートを手動で調査する作業から解放されます。代わりに、自動的にブロックまたはモニタされた実際のインシデントの確認に集中できるようになります。

ローカルの脅威インテリジェンスのみに依存するセキュリティ デバイスとは異なり、Threat Intelligence Director ではサードパーティの脅威フィードを使用して、セキュリティの有効性をさらに高めることができます。インテリジェンスを実用的な侵害の兆候に変換することで、ネットワークを防御するために、より多くの脅威をブロックまたはモニタできるようになり、確認が必要なアラートの数を減らすことができるため、全体的なセキュリティ ポスチャが向上します。脅威インテリジェンスの追加ソースを取り込んで配布できるようにすると、管理作業が簡素化され、誤ったアラートを確認して特定する必要もなくなります。

サードパーティ製セキュリティ インテリジェンスとの統合



インシデント対応の高速化と自動化

サードパーティのインテリジェンスを活用し、侵害の兆候を自動的に関連付けて対策を講じます。

シスコの技術アライアンス パートナーの一覧 [英語] にアクセスして、利用可能なサードパーティの脅威インテリジェンス ソースと脅威インテリジェンス プラットフォーム パートナーの最新の一覧を参照し、お客様のインテリジェンスの実用性を高めるために役立てることができます。

C45-738455-00 06/17