Cisco XDR と Cisco Meraki MX のネイティブなネットワーク統合

SNOC のパワー：セキュリティ運用とネットワーク運用の統合

Cisco XDR は、多様なセキュリティスタックに導入されているすべてのツールのデータとテレメトリを接続して関連付けることに優れています。そのため、防御担当者はより多くの情報を検出し、ためらうことなく行動し、生産性を上げることができます。これは、脅威の検出、調査、対応（TDIR）をセキュリティ態勢に統合し、すべてではないにせよ、セキュリティ運用（SecOps）のギャップをほぼ解消するための最も迅速で簡単な方法です。しかしこれでは、あらゆる規模の組織が依然として直面している課題、つまりセキュリティ運用とネットワーク運用の間に存在する盲点に対処することができていません。

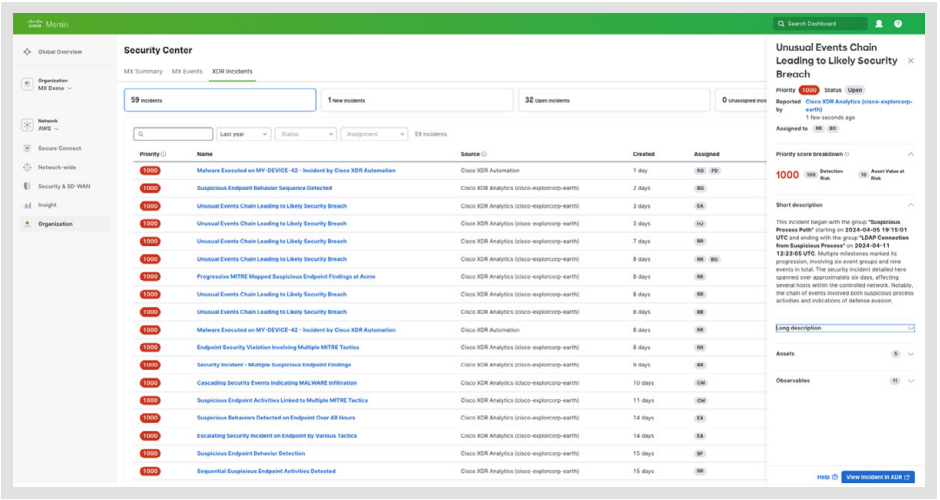
ですが、今後は違います。

Cisco Meraki MX ポートフォリオと Cisco XDR をネイティブに統合することで、シスコはセキュリティおよびネットワーク オペレーション センター（SNOC）を立ち上げました。この統合により、セキュリティ運用とネットワーク運用に双方向の利点が生まれます。セキュリティアナリストはネットワークから貴重な TDIR のインサイトを得られるので、課題であった盲点がなくなります。一方、ネットワーク管理者は環境内の新たな脅威をプロアクティブにモニターできるようになります。

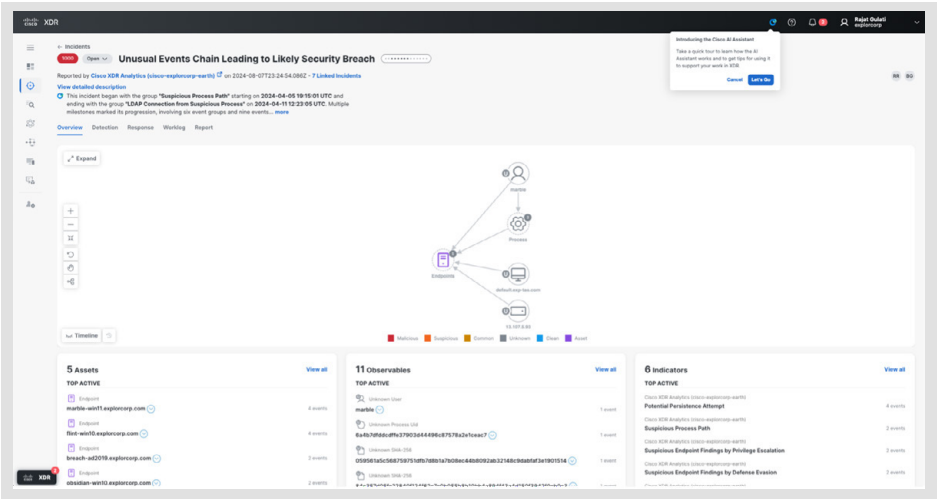
メリット

脅威検出の強化：
Cisco Meraki のログデータが Cisco XDR とシームレスに統合されるため、不審なアクティビティや脅威の早期検出が大幅に向上します。エンドポイントセキュリティの検出結果だけでは、影響を評価するのに十分な情報を得られない場合がありますが、検出結果とそれに対応するネットワークアラートを Cisco XDR でリンクさせることで、インシデントに高優先順位のマークが付けられ、この優先順位に応じた適切な管理が可能になります。

一元的な可視性、運用のシンプル化：
ネットワーク管理者はワンクリックで Cisco XDR を Cisco Meraki ダッシュボードに統合することができ、ダッシュボードに XDR インシデントが表示されるようになります。これにより、ネットワークの可用性と稼働時間に影響を与えかねない進行中の脅威についてネットワーク管理者が早期に警告を受けることができ、セキュリティ担当者へのインシデントの割り当てや、イベントのステータスの調整が可能になります。



管理者は、Cisco Meraki ダッシュボード内で Cisco XDR インシデントに直接アクセスできます。アクセスするには、Cisco Meraki ダッシュボードで [XDR でインシデントを表示（View incident in XDR）] ボタンをクリックします。



すると、Cisco XDR 内の [インシデント（Incident）] ビューに移動します。

鮮明なフォーカス、明確でタイムリーなアクション

現在利用可能な Extended Detection and Response（XDR）ソリューションのほとんどは、セキュリティに対して、エンドポイントにフォーカスしたアプローチを取っています。しかし、ほとんどの環境では、デバイスの半数以上がエンドポイントエージェントを実行できておらず、脅威の多くはエンドポイントでは発生しません。一部のツールは、電子メール、ファイアウォール、アイデンティティ製品からデータを収集するよう進化していますが、こうした異なるセキュリティ管理ポイントを結びつける接続の要、つまり「ネットワーク」についてはまだ考慮されていません。その結果、環境内で何が起こっているかがはっきりとせず、セキュリティ管理者もネットワーク管理者も状況を完全には把握できていません。

今回の Cisco Meraki デバイスとのネイティブ統合により、Cisco XDR でネットワーク接続データを独自に活用し、セキュリティイベント間の空白を埋めることができます。これによって強化されるラテラルムーブメントに対する可視性は、EDR ベースのソリューションが提供できる以上のものであり、セキュリティアナリストが攻撃の進行状況を追跡し、より多くの情報に基づいたタイムリーなアクションを実行するのに役立ちます。

ネットワーク管理者の場合は、Cisco Meraki ダッシュボード内でのワンクリック統合によって不審なインシデントの早期警告サインが明らかになるので、従来のようにセキュリティ担当者からの「緊急ニュース」を待つのではなく、詳細な調査のためにセキュリティアナリストにタスクを割り当てることができます。

SNOC のパワーを今すぐ活用

セキュリティチームとネットワークチームは、可視化されておらず、フォーカスが合っていない不完全な情報のせいで、セキュリティとネットワークの狭間にあるギャップを埋めるのに苦労していませんか？ Cisco XDR なら、Cisco Meraki MX ネットワークとのネイティブ統合によってこのギャップを埋めることができるので、両チームがセキュアなネットワーク運用のパワーを実感できます。詳細については、www.cisco.com/site/jp/ja/products/security/xdr をご覧ください。