インシデント調査

概要

信頼度とリスクレベルに基づいて次のようにインシデントに対応します。

- **高いリスクと高い信頼度。**エンドポイントは、署名やルールベースのエンドポイントセキュリティを回避した高度な脅威により危険にさらされています。エンドポイントのクリーニングツールで脅威を削除できる見込みはありません。ユーザのプロファイルを完全にバックアップせずに、ドキュメントのみをバックアップして、エンドポイントを再イメージ化または再構築します。Cognitive Intelligence がアクティブなマルウェア感染を検出すると、通常は SOC とデスクトップチームからの手動操作が必要です。
- **中程度の信頼度または中程度のリスク。**エンドポイントには、エンドポイントのクリーニングツールで除去できるマルウェアが含まれています。選択したエンドポイントスキャンおよびアンチウイルスのクリーニングツールを実行します。発見した感染を除去し、エンドポイントを監視します。問題があれば、ユーザのプロファイルを完全にバックアップせずに、ドキュメントのみをバックアップして、エンドポイントの再イメージ化および再構築を実行します。
- **その他のすべて（低い信頼性および低いリスク）。**エンドポイントが感染しているかどうかは不明です。アラートは、スパムやフィッシング URL に従いユーザをリンクさせる可能性があります。通常のスキャンを実行し、発見された感染を除去します。何も見つからない場合、マルウェアの進行を防ぐために、すべてのエスカレーションのエンドポイントを監視します。

信頼度レベル：

- 高い（100 % ー 95 %）
- 中程度（94 % ー 85 %）
- 低い（84 % ー 0 %）

リスクレベル：

- 重大（10）
- 高い（9、8）
- 中程度（7、6）
- 低い（5、4、3、2、1）

詳細

ステップ 1 [Dashboard] タブをクリックします。

a) ヘルスステータス。ネットワークで検出された脅威の全体的な概要をリスクレベル別に表示します。未解決のユーザは、リスクカテゴリ別にグループ化されます。多数の低リスクの脅威は、時間の経過とともにより深刻な脅威につながる可能性があることに注意してください。

b) 相対的な脅威の危険性。同じセクター内の他の企業、同規模の企業、および世界中のすべての企業と比較した、インシデントの数とリスクレベルに基づく脅威の危険性。

c) 特定の動作。ネットワークで検出された脅威と未解決の動作の高レベルの内訳。

d) 最高リスク。現在ネットワークに最も高いリスクをもたらし、早急な対応が必要な未解決のインシデント。

e) 上位のリスクエスカレーション。最近リスクが増加している未解決のインシデント。

ステップ 2 [Confirmed] タブをクリックします。

a) このセクションでは、ネットワーク上で確認された脅威および侵害（100% の信頼レベルのインシデント）とその関連情報について示します。

b) 相関動作とともに検出されたインシデントは、脅威キャンペーンにグループ化され、各脅威キャンペーンは一意のハッシュタググループ名によってラベル付けされます。

c) 脅威キャンペーンは、ページの右側にある垂直のパネルに表示されます。状態ボックスをチェックして、どの脅威キャンペーンをパネルに表示するのかフィルタすることができます。

d) リスクの数字が大きければ、ネットワークに影響を与えるリスクが高い脅威であることを示します。クラスタ化されたインシデントを含む、より高いリスクの脅威を調査することで、分析の優先順位付けをします。

e) 調査に多くの時間を必要としないインシデントについては、迅速な対処が必要です。Cognitive Intelligence の結果に対してワークフローを調整するため、リカバリプロセスを設定します。

f) 脅威に固有の説明を確認し、対象をより明確にした修復のために推奨されるアクションを確認します。

ステップ 3 [Detected] タブをクリックします。

a) このセクションでは、相関性のない Cognitive Intelligence インシデントおよび AMP のレトロスペクティブ インシデントを含む、検出されたインシデントの概要を示します。また、[Confirmed] セクションの脅威にグループ化された、相関性のある Cognitive Intelligence インシデントを表示することもできます。

b) AMPやCognitive Intelligenceを選択し、日付選択、検索フィールド、環境設定、および状態を調整することで、どのインシデントが示されるかをフィルタすることができます。
c) [Email Notifications] ページを使用して電子メールアドレスを入力し、24 時間おきに新しい更新されたインシデントのサマリーが送信されるようにします。

ステップ 4 インシデントの調査を開始するには、そのインシデントをクリックして、その詳細を見直します。リスクと信頼性の高いものを優先してインシデントを調査します。インシデントは通常、複数のアクティビティや疑わしい動作のタイプで構成されます。

ステップ 5 影響を受けているデバイスまたはサーバを識別します。

ステップ 6 インシデント内の異常について情報を一覧できる並行座標グラフを調査します。相互接続情報を表示するには、折れ線グラフの各座標のノードにカーソルを合わせます。

a) リスク要因が最も高いものから開始し、低い方へと進みます。
b) [Time] 列の情報に注意します。マルウェアの活動がレポートされている時間の長さを確認します。高度なマルウェアの活動の特徴の 1 つは、通信が長期にわたって持続することです。インシデントが数日または数週間レポートされている場合は、高度なマルウェアによってインシデントが引き起こされている可能性が高まります。
c) 最近継続している活動を識別します。過去 48 時間の間に発生した異常に焦点を当てます。
d) 並行して発生する異常を探します。異常のシーケンスは、使用中のコマンドアンドコントロール通信チャネルを示唆する場合があります。
e) 接続された行を確認します。ドメインはまとまって成立していますか?それらが関連付けられていますか?IPアドレスが変わるのは、疑わしいドメインです。ドメインがデータを転送しているかどうかを判断するために、Web フローテーブルに関連付けます。
f) 多くの場合、より多くのマルウェアトラフィックが含まれているため、最も高いリスク要因に関連する異常を確認します。
g) 異常は、同じ AS、または異なる所有者および異なる場所の異なるシステムに結びついたものですか?ハッキングされ、攻撃元として使用されたシステムであることを示している可能性があります。

ステップ 7 Webフローをフィルタリングするには、グラフを使用できます。1つ以上のノードを選択してクリックし、関連する Web フローを表示します。

a) サーバの横のボックスに注意してください。赤のボックスは、そのサーバに対してマイナスの IP レピュテーションがあることを意味します。ドメイン名が含まれています。マイナスの IP レピュテーションは、攻撃者が運営するドメインからの疑わしい通信があったことを示すことがあります。
b) サーバから返される HTTP ステータスコードに注意してください。ステータスコードの横にある赤い [x] ボックスは、Webプロキシによってフローがブロックされたことを示します。ブロックされていないために、マルウェアの動作を許してしまっている、少なくとも 1 つのコマンドアンドコントロール（C&C）チャネルを持つインシデントに焦点を当てます。

ステップ 8 検出されたインシデントは、100%未満の信頼レベルです。実際のインシデントの詳細に基づいて、次の要因は、報告されたリスクを低減する、または増加する可能性があります。

リスクの低減	リスクの増加
レポートされた活動はプロキシですでにブロックされています。	レポートされた活動はプロキシでまだブロックされていません。

リスクの低減	リスクの増加
インシデントの特性（アクセスされた URL など）は、1 つのインシデントのみに固有です。	インシデントの特性（アクセスされた URL など）は、多くのユーザに繰り返されています。
インシデントの総量は、複数の要求を伴う 1 つの活動です。	インシデントの詳細は、長期にわたって、負荷が高く、永続的な動作を示します。
インシデントの詳細には、少量のデータ転送が表示されます。	インシデントの詳細には、大量のデータ転送、特にアップロードが表示されます。

次のタスク

収集した情報を分析して、このインシデントがネットワークに対して脅威であるかどうかを結論付けます。インシデントの詳細ページで、インシデントが脅威として解決されたか、誤検出として解決されたか、または無視として解決されたかをマークします。

脅威を緩和するため、組織の標準によるインシデント対応手順に従ってください。内部システムから脅威インテリジェンスより多くを収集することは、何らかのアクションを行う前の適切な慣行です。攻撃サイクルの侵害後のフェーズで運用をおこなっていることを、念頭に置いてください。これは、このフェーズ中に従来のセキュリティ対策が成功せず、脅威を完全に取り除くことができず、影響を受けたエンドポイントのイメージを再作成する必要性を意味します。

（注） 誤検出の数を減らすには、すべてのインシデントが事前にすぐにブロックされるわけではありません。異常は調査対象のインシデントとして検出およびレポートされます。分析、モニタリング、および時間追跡の後、脅威がブロックされたことを確認します。ただし、モーフィングマルウェアなどの脅威は検出を避けるために動作を変更できます。そのため、Cognitive Intelligence では時間経過とともに継続的にファイルを分析し、SenderBase に情報を送信し、Web-Based Reputation Score（WBRS）を更新しています。Cisco Security 製品は、次に脅威をブロックしますが、これが最終処理の包括的ソリューションであると見なすべきではありません。Cisco Security 製品が行うブロックは、通信の一部のみを対象としている場合があります。たとえば、Cisco Security 製品で保護されていない場所から接続した場合、マルウェアは、データを隠し、後からこっそり持ち出す可能性があります。完全なものにするには、感染したデバイスのイメージを作成し直します。