ダッシュボード

グローバル脅威アラート（以前はCognitive Intelligence）機能は、すでに進行中しているか、お客様のネットワーク内でプレゼンスを確立しようとしている高度で密かな攻撃を迅速に検出して対応するのに役立ちます。この機能は、不審なWebベースのトラフィックや悪意のあるトラフィックを自動的に調査します。確認済みの脅威と潜在的な脅威の両方を特定することで、感染を迅速に修復し、攻撃の範囲と損害を軽減できます。これは、既知の脅威キャンペーンが複数の組織に拡散している場合でも、これまでに見たことのない固有の脅威である場合でも同様です。

クラウドベースのサービスであるグローバル脅威アラートは、ハードウェアやソフトウェアを追加せずに、既存のWebセキュリティソリューションによって生成された情報を分析します。セキュリティ制御をバイパスした悪意のあるアクティビティに焦点を定めます。

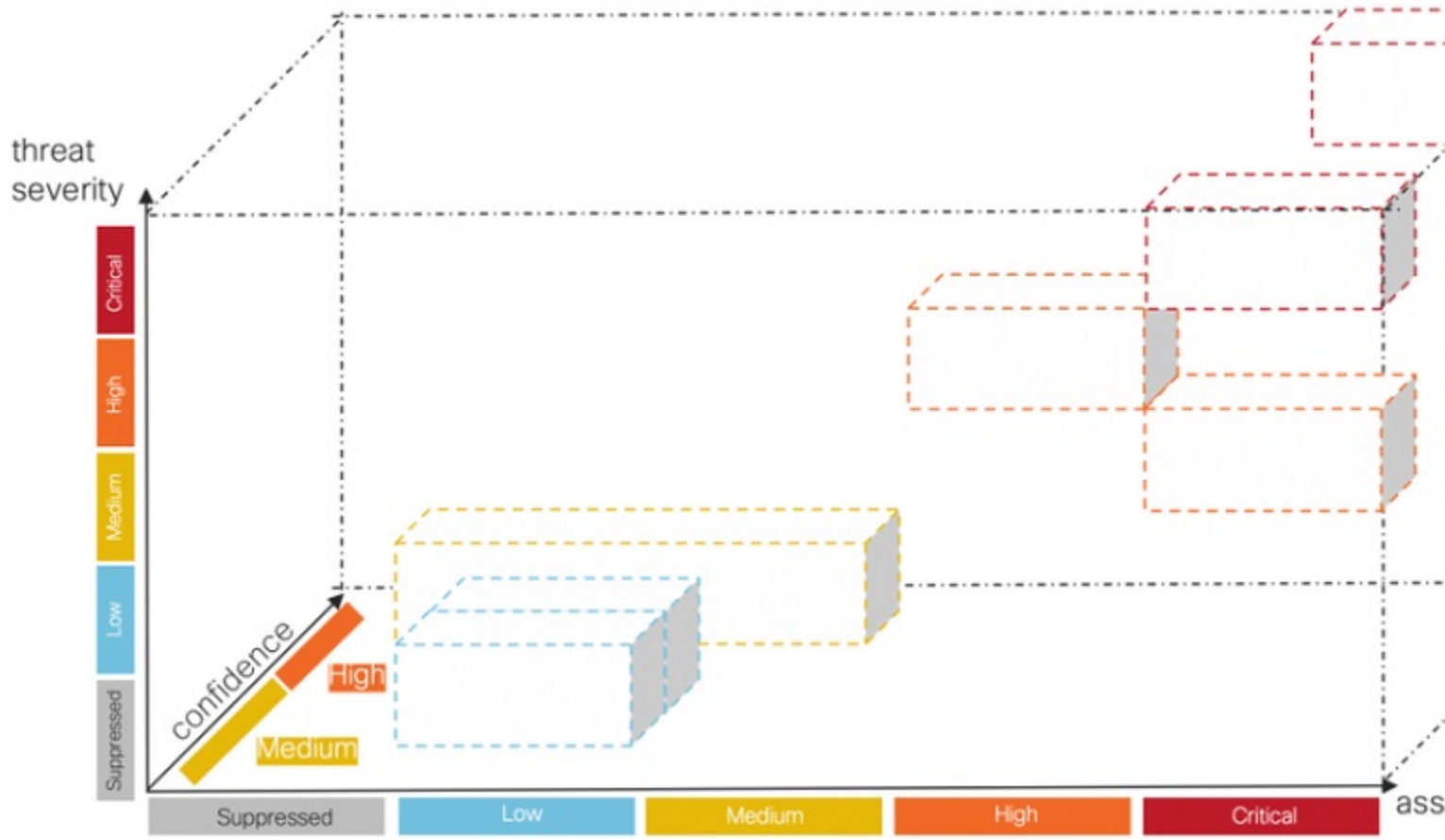
グローバル脅威アラートは、機械学習とネットワークの統計モデリングを使用して、通常のアクティビティのベースラインを作成し、ネットワーク内で発生する異常なトラフィックを特定します。デバイスのふるまいとWebトラフィックを分析して、コマンドアンドコントロール通信とデータ漏洩を特定します。

グローバル脅威アラートは、認識している情報から学習することで、継続的な侵害の特定を可能にし、繰り返し攻撃や継続的な感染のリスクを軽減します。複数のシスコセキュリティ製品と統合された直感的なWebベースのポータルを通じて情報を表示します。これにより、侵入の重大度と範囲を評価し、脅威のミッションとその仕組みを理解し、即座にアクションを実行できます。

概要

シスコの分析エンジンは、入力データストリームに機械学習を適用し、検出結果を3次元空間に投影します。

図 *1*:



- **脅威の重大度の次元。**脅威がどのぐらい深刻であるか。確認された脅威とその重大度。個々の脅威タイプに対する組織のリスクプロファイルとの整合性を高めるために、個々の脅威の事前定義された重大度を調整するオプションがあります。
- **アセット価値の次元。**アセットがどのぐらい貴重であるか。ネットワークに接続されているすべてのデバイスの重要度が等しくない場合は、個々のアセットグループのビジネス上の価値を調整して、より重要なデバイスの検出を優先させるオプションがあります。
- **信頼度の次元。**判定はどのぐらい信頼できるか。お客様の環境で観察された個々の脅威について、シスコのアルゴリズムが下している判定の信頼度。判定がほぼ確実となる十分な侵入兆候を観察できる場合もあります。その他の場合には、同様の症状にもかかわらず、実際の証拠が不完全なこともあります。そのため、許容誤差が大きくなります。

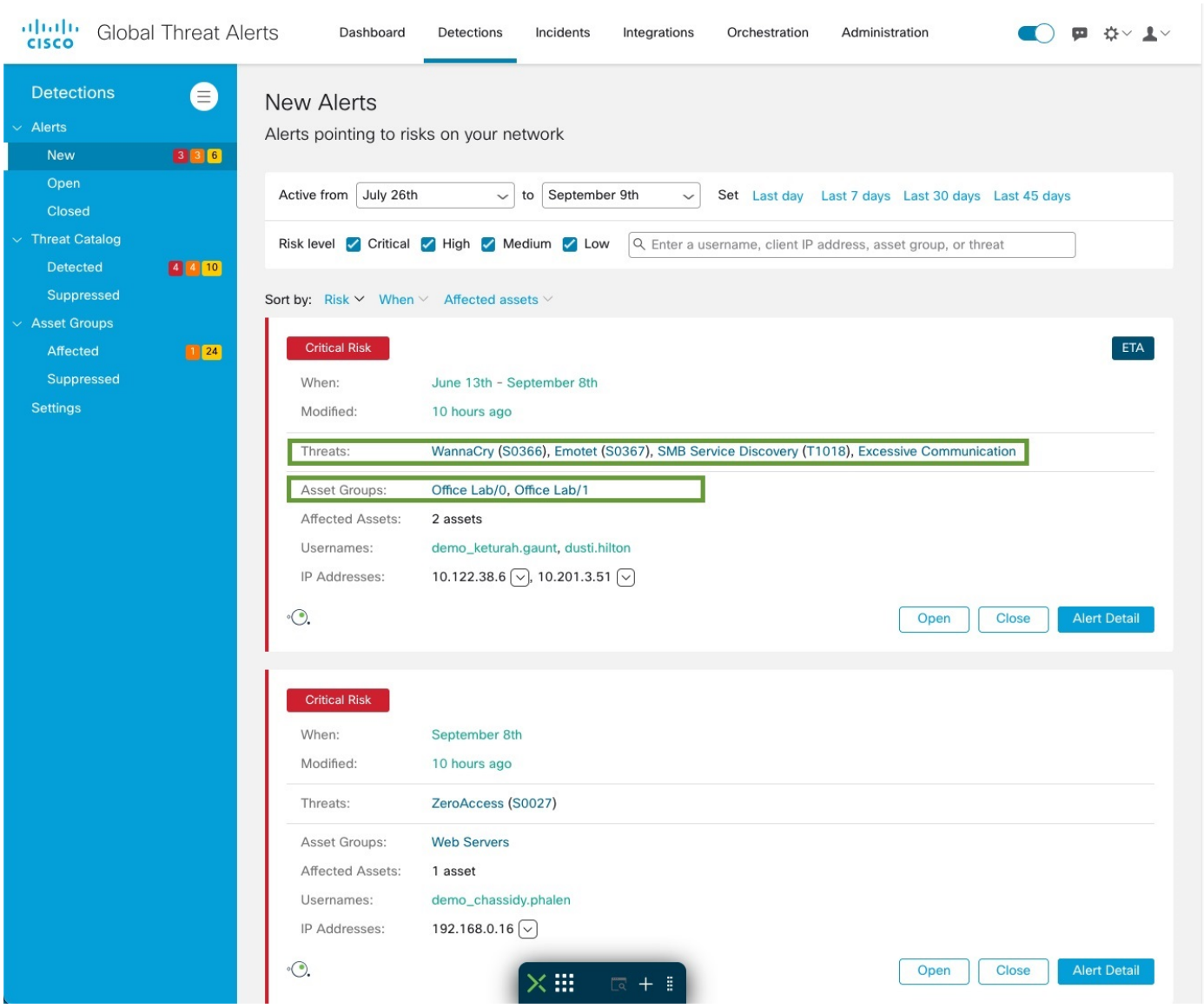
シスコのフュージョンアルゴリズムは、これらの検出結果を使用して同様の脅威とプロジェクションのクラスタを特定し、リスクレベルを計算します。シスコの Web ポータルでは、リスクレベルによって優先順位付けされたリストで、これらをセキュリティアラートとして表示します。各アラートは、ネットワーク上の脅威を指し、調査とその後の修復のための通常の作業単位を表します。

アラートの調査

ステップ 1 左側のナビゲーションメニューで [アラート（Alerts）] と [新規（New）] をクリックして、ネットワーク上のすべての新しいアラートを表示します。各アラートは、専用のカードに表示されます。

a) 各アラートカードには、同様のビジネス上の価値を持つネットワーク上の一連のアセットに同時に影響を与える 1 つ以上の脅威が集約されています。

図 *2*:



- **脅威**。同時に発生するさまざまな脅威。

- **アセットグループ**。これらの脅威は、同様のビジネス上の価値を持つアセットグループに属するエンドポイントで発生しています。

b) リスクレベルは、脅威の重大度レベルとアセットグループのビジネス上の価値に基づいています。リスクレベルが高いほど、脅威がネットワーク上の貴重なアセットに深刻な影響を与えるリスクがより高いことを示しています。

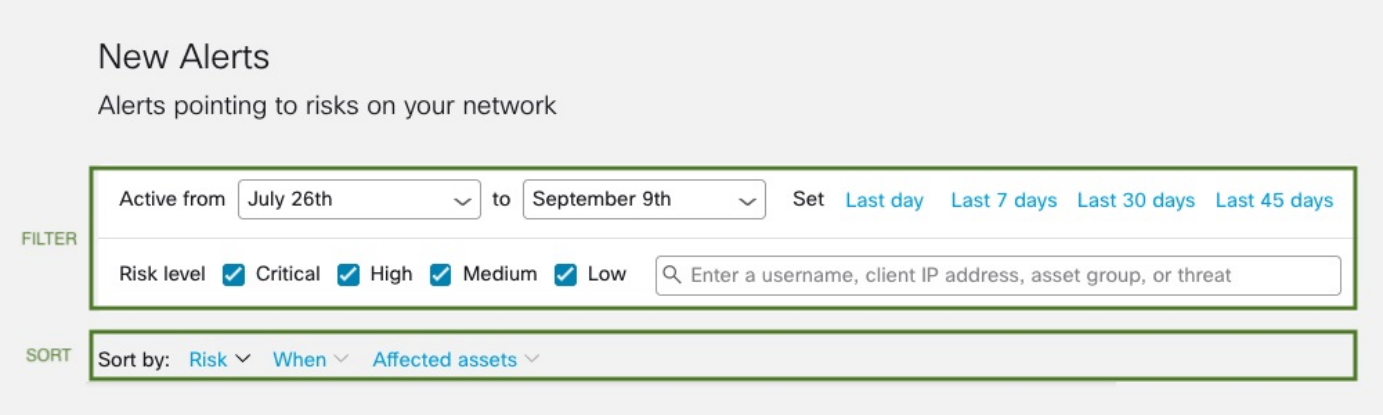
ステップ 2 アラートは、リスクの高い順に、リストの先頭から並べられます。リスクレベルに基づいてアラートに応答し、リスクの高いアラートを最初に調査することで、分析を優先順位付けします。

- 重大
- 高い
- 中規模
- 低い

（注） アラートカードは、新しい脅威がグループに追加されたときや、アセットグループのビジネス上の価値や脅威の重大度が変化したときなどに、動的に変更されます。

ステップ 3 経過時間、リスクレベル、ユーザー名、IPアドレス、アセットグループ、および/または脅威を選択して、表示するアラートをフィルタ処理するオプションがあります。また、リスクレベル、経過時間、または影響を受けるアセットの数でソートするオプションもあります。

図 *3:*

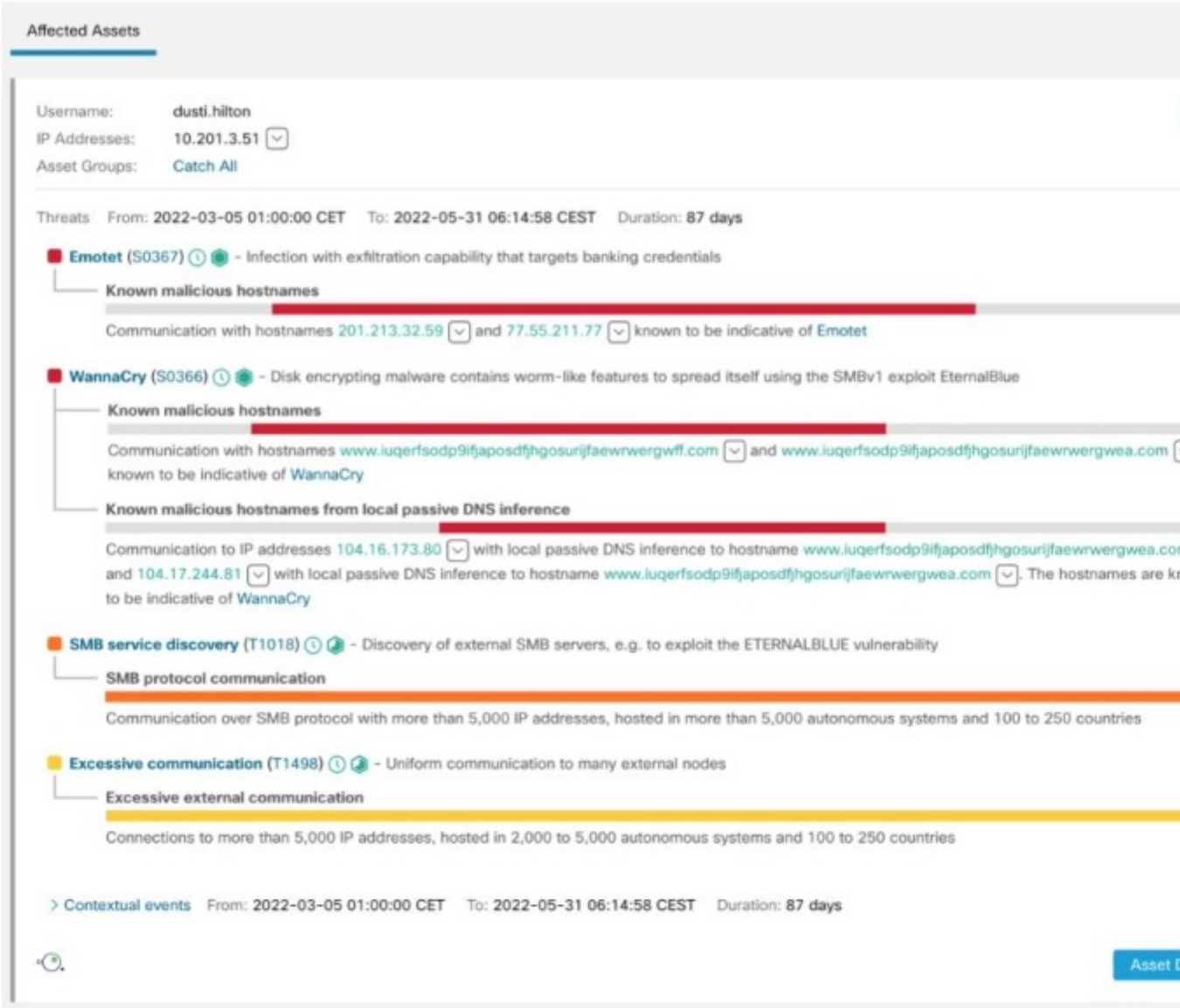


ステップ 4 アラートの状態を [オープン（Open）] に変更して、アラートの調査を開始します。

（注） 状態が [新規（New）] でなくなると、アラートカードは変更されず安定するため、調査が容易になります。

ステップ 5 [アラートの詳細（Alert Detail）] をクリックすると、検出された各脅威と影響を受けるアセットに関する追加のコンテンツが表示されます。影響を受けるアセットにはそれぞれそのアセットで行われたすべての脅威検出をリストする [脅威（Threats）] セクションがあり、すべての有害となるセキュリティイベントが含まれています。

図 *4*:



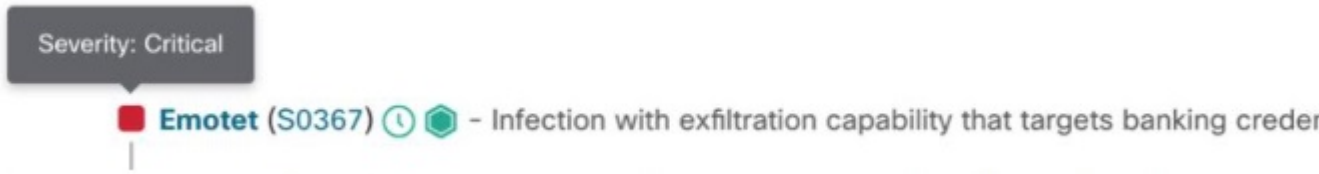
[脅威（Threats）] セクションの上部には、検出されたすべての脅威の合計観測期間と、特定のアセットでのそれらの有害となるセキュリティイベントが表示されます。

図 *5*:

それぞれの脅威検出には、その名前、MITRE リンク、説明、および以下のものが表示されます。

- 重大度

図 *6*:

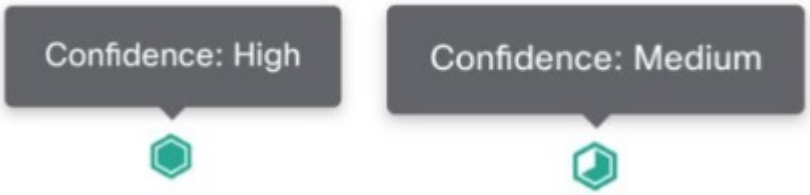


- 観測期間

図 *7*:

- 信頼度

図 *8*:



それぞれの脅威検出は、下にあるセキュリティイベントによって裏付けられています。イベントの多くには、イベントの作成につながった証拠を提供する豊富なセキュリティアノテーションが含まれています。

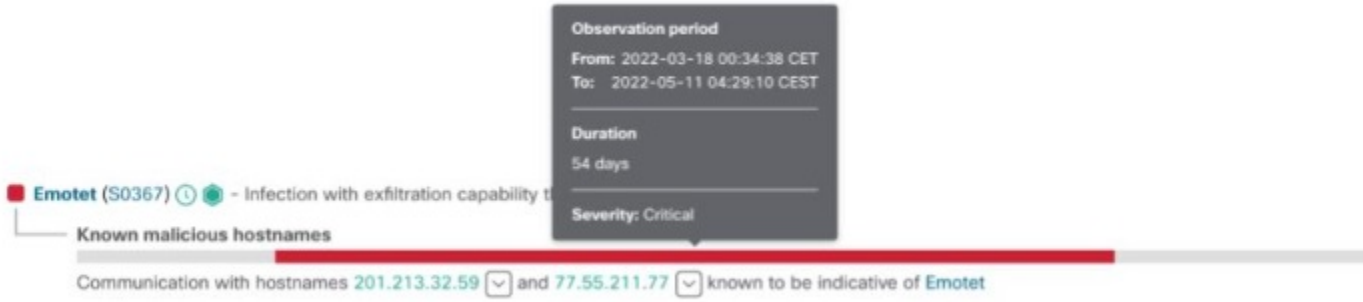
図 *9*：

イベントアノテーションには、他のシスコのセキュリティ製品にピボットして、監視対象に関する追加情報とインテリジェンスを取り込めるドロップダウンメニューが含まれている場合もあります。

図 *10*：

それぞれのセキュリティイベントには、[脅威（Threats）] の合計観測期間のコンテキスト内での動作のタイミングと発生を示すタイムラインが含まれています。

図 *11* :

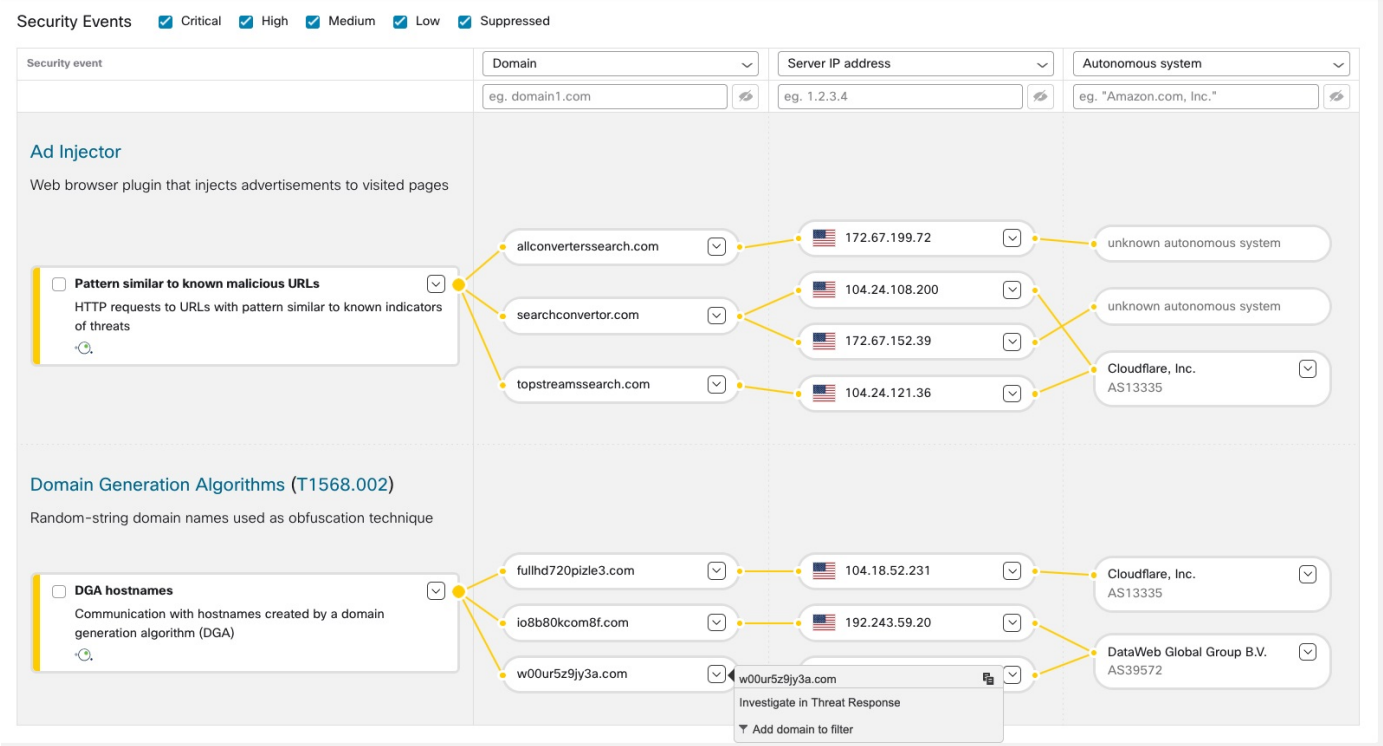


[コンテキストイベント（Contextual events）] セクションを展開して、アセット上で起こったことに関する追加のコンテキストを提供できる、より多くのイベントを表示することができます。

図 *12* :

ステップ 6 1 人のユーザーの特定のイベントの 1 つを選択すると、[セキュリティイベント（Security Events）] ビューに移動し、悪意のある検出をトリガーした特定のイベントの詳細なコンテキストを確認できます。

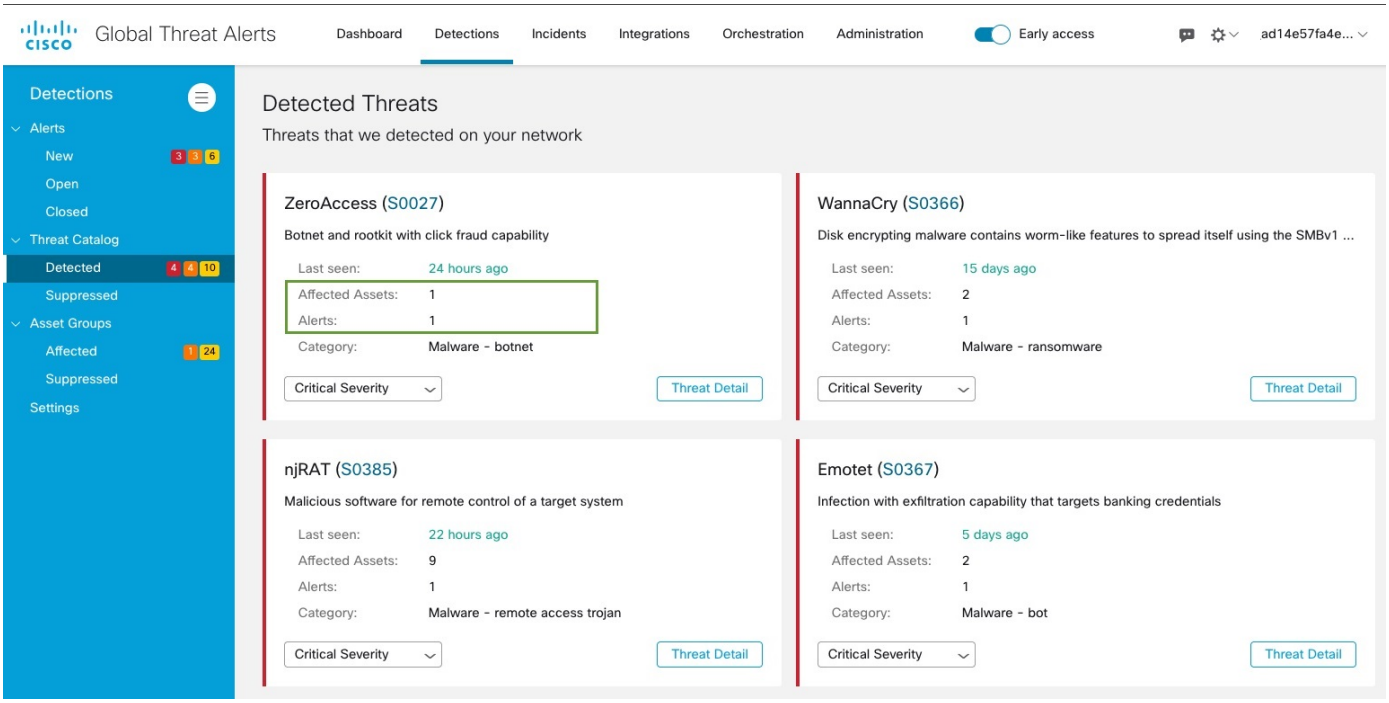
図 *13 :*



脅威の調査

ステップ 1 ネットワークで報告され、重大度で優先順位付けされた脅威のリストを表示するには、左側のナビゲーションメニューで[脅威カタログ（Threat Catalog）]および[検出（Detected）]をクリックします。各カードは、アラートにグループ化されるさまざまな脅威を表します。

図 *14 :*



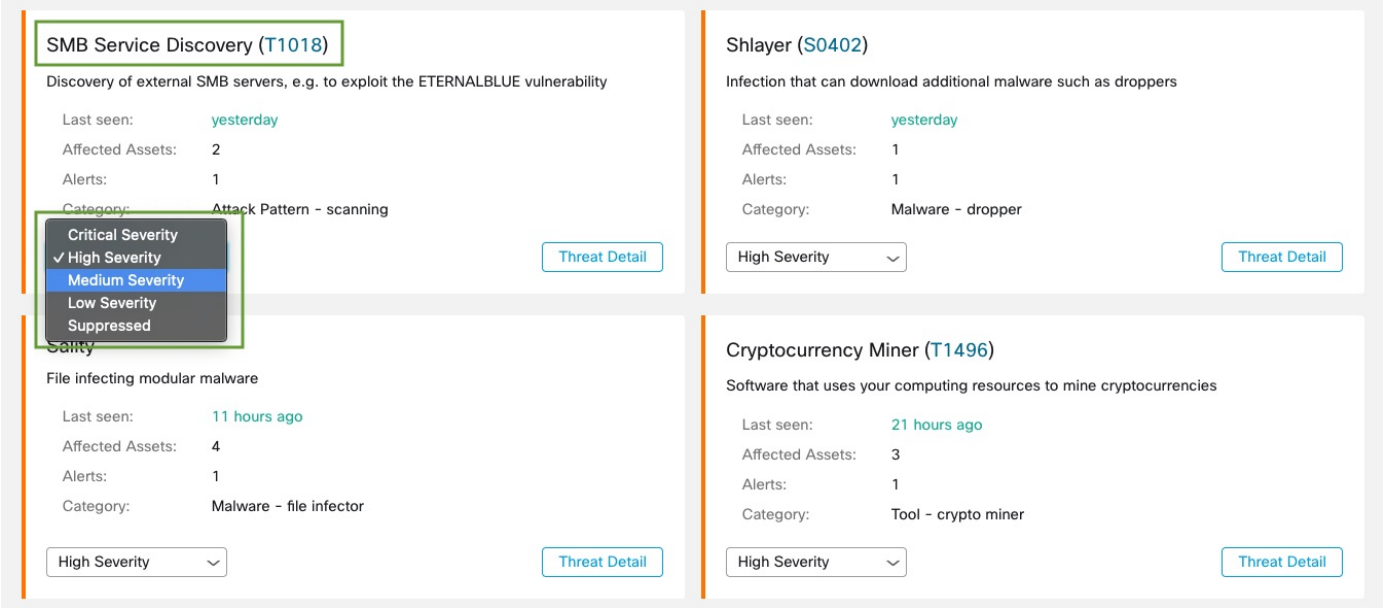
ステップ 2 特定のタイプの脅威が複数のアラートに関係している場合があります。この特定のタイプの脅威が関係するアラートの数と、この脅威の影響を受けるアセットの数を示すカウンタがカードにあります。

ステップ 3 グローバル脅威アラートの脅威インテリジェンスは、関連する ATT&CK の戦術、テクニック、およびソフトウェアエントリへの参照を提供します。

ステップ 4 ネットワーク固有の条件やビジネスニーズに応じて、脅威の重大度を調整するオプションがあります。

- その結果、このタイプの脅威を含むすべての [新規（New）] アラートのリスクレベルが再計算され、新しい重大度にアセットの価値と信頼度レベルが重み付けされます。
- その後、リスクレベルの変更は、 [新規（New）] アラートの相対的な順序に影響します。
- たとえば、脅威の重大度を下げると、関連付けられたアラートのリスクレベルが低下し、関連付けられたアラート カードが [アラート（Alerts）] タブのリストの下位に表示されます。
- ドロップダウンリストをクリックして、脅威の重大度を調整できます。

図 *15 :*



（注） [新規（New）] 状態ではなくなった他のすべてのアラートは、脅威の重大度の変更による影響を受けません。調査を容易にするために変更されず安定したままになります。

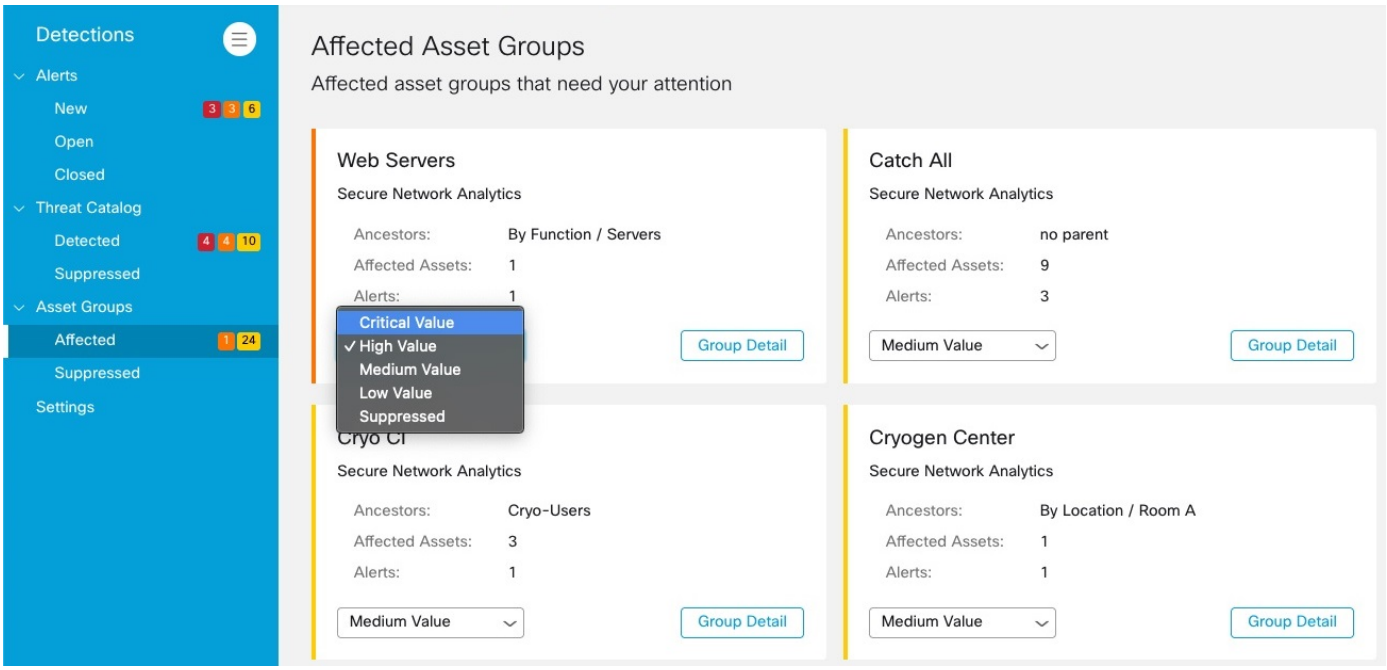
アセットグループ

ステップ 1 グローバル脅威アラートにトラフィックが送信されたすべてのアセットグループを表示するには、左側のナビゲーションメニューで [アセットグループ（Asset Groups）] および [アセット（Assets）] をクリックします。各カードは、グローバル脅威アラートが少なくとも 1 つのアラートを報告しているアセットグループを表します。

ステップ 2 アセットグループが組織にとってどのぐらい重要または価値があるかを判断します。アセットグループのビジネス上の価値を調整するオプションがあります。

- その結果、このアセットグループに影響するすべての [新規（New）] アラートのリスクレベルが再計算され、新しいアセットの価値に重大度と信頼度レベルが重み付けされます。
- その後、リスクレベルの変更は、 [新規（New）] アラートの相対的な順序に影響します。
- たとえば、アセットグループのビジネス上の価値を高めると、関連付けられたアラートのリスクレベルが高くなり、関連付けられたアラートカードが [アラート（Alerts）] タブのリストの上位に表示されます。
- ドロップダウンリストをクリックして、アセットグループのビジネス上の価値を調整します。

図 *16 :*



（注） [新規（New）] 状態ではなくなった他のすべてのアラートは、脅威の重大度の変更による影響を受けません。調査を容易にするために変更されず安定したままになります。

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。