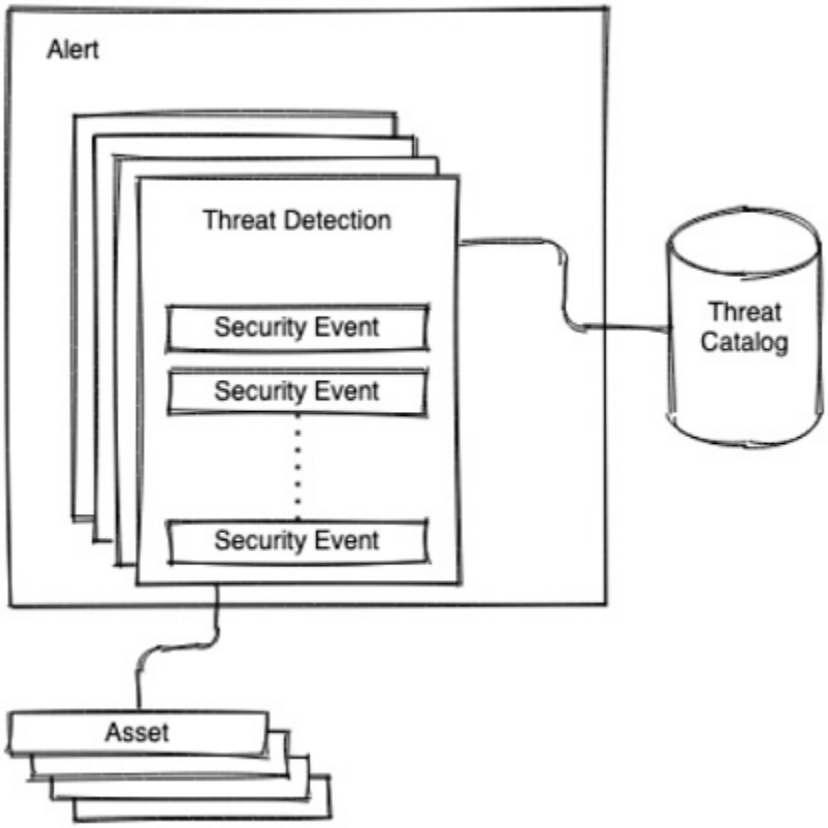
用語集

アラート

アラートとは、脅威の検出を調査するようにユーザに促す通知です。

グローバル脅威アラートでは、アラートは1つ以上の脅威の検出に焦点を当てます。これらの脅威の検出は、1 つ以上のアセットで発生します。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。

図 *1:*



セキュリティ イベント

セキュリティイベントとは、悪意のある動作または疑わしい動作を示す可能性がある重要なセキュリティイベントです。脅威検出エンジンがセキュリティイベントを処理します。疑わしい動作や悪意のある動作の検出に大きな影響を与えるセキュリティイベントは、有害と呼ばれます。脅威の検出時に影響を受けるアセットで観察されるセキュリティイベントは、コンテキストと呼ばれます。各セキュリティイベントには、その重要性を示す説明が含まれています。この説明はセキュリティアノテーションと呼ばれます。

脅威カタログ

脅威カタログは、検出された脅威の可能性を整理し、マルウェア、ツール、攻撃パターンの 3 つの基本カテゴリに分類します。これには MITRE へのマッピング（存在する場合）も含まれます。

脅威の検出

脅威の検出とは、アセットに影響を与える疑わしい動作や悪意のある動作を検出することです。グローバル脅威アラートの脅威カタログでは、複数のタイプの脅威の検出を認識します。

脅威検出エンジンは、セキュリティイベントなどのさまざまなソースと連携します。これらを関連付けて、特定の信頼レベルで脅威の存在を明らかにする、または分析によって脅威の存在が確認される、異常なパターンや傾向を明らかにします。

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。