MicrosoftおよびVectra AI社がSOC可視化トライアドのビジョンを完成

前例のないサイバー攻撃によっても明らかなように、従来のセキュリティ対策は既にその効力を失っています。これらの脅威は目に見えることなく、暗号化されたトラフィックに潜んだり、トンネル内に身を隠して、長期間にわたり不正な活動を続けます。このように高度化した脅威にセキュリティチームが対抗するためには、システム環境全体で素早く脅威を可視化する必要があります。

2019年3月18日に公開された、ガートナーリサーチレポート（ID: G00373460）「Applying Network-Centric Approaches for Threat Detection and Response（ネットワーク中心のアプローチによる脅威の検知と対応）」の中で、Augusto Barros、Anton Chuvakin、Anna Belakの各氏が、SOC可視化トライアド（SOC Visibility Triad）の概念について紹介しています。

このレポート内で、ガートナーは次のようにアドバイスしています。「企業がより高度化する脅威に対抗するためには、複数のデータソースを使用して脅威の検知と対応を行う必要があります。ネットワークベースのテクノロジーであれば、エージェント不要で、システム環境全体から素早く脅威を可視化することができます[1]」

調査結果によれば、現代のセキュリティ運用ツールは、冷戦時代の主要概念であった「核のトライアド（三本柱）」に例えることもできます。トライアドは、戦略爆撃機、大陸間弾道ミサイル（ICBM）、潜水艦発射ミサイルで構成されています。右の図1に示すように、最新のSOCは、以下のように「核のトライアド」のような可視化のためのアプローチを持っています。

1. **SIEM/UEBA**が、ITインフラストラクチャーやアプリケーション、その他のセキュリティツールによって生成されたログを収集して分析する機能を提供。（詳しくは「SIEM Technology Assessment」を参照）

2. **エンドポイントの検知と対応**によって、エンドポイントにおける実行、ローカル接続、システム変更、メモリの状態、その他のオペレーションの内容を把握することができます。（詳しくは「Endpoint Detection and Response Architecture and Operations Practices」を参照）

3. **ネットワークセントリックの検知と対応（NTA、NFTおよびIDPS）**は、本調査結果の説明にあるように、ネットワークトラフィックのキャプチャや分析にフォーカスしたツールによって提供されます[2]。

この3つの異なるアプローチによって、SOCは脅威の可視化、検知、対応、調査、そして修復のための能力を向上させることができます。

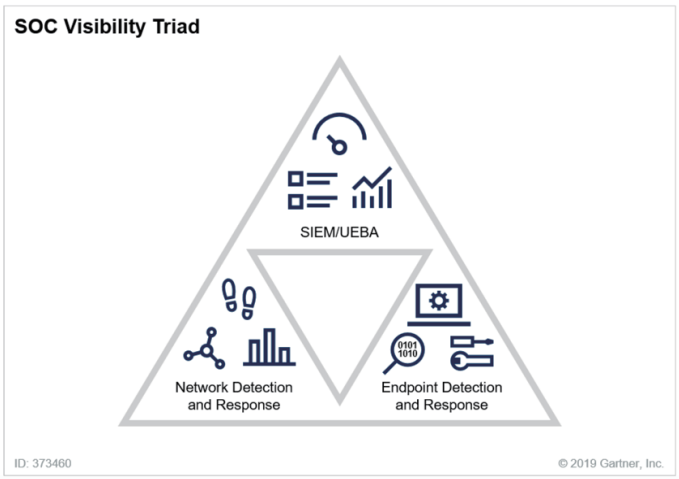

図1：SOC可視化トライアド（SOC Visibility Triad）

出典：Gartner, Applying Network-Centric Approaches for Threat Detection and Response, Augusto Barros et al., March 18, 2019, ID G0037346

Microsoft Defender Advanced Threat Protection

マルウェア、パッチ未適用の脆弱性、設定ミス、そしてユーザーの不注意に至るまで、エンドポイントの侵害はごく当たり前のように発生します。モバイルデバイスは、パブリックネットワークにおいて簡単に侵害を受け、企業ネットワークに再接続された際にその感染を拡大します。

Microsoft Defender Advanced Threat Protection（ATP）は、予防的保護、侵害後の検出、自動調査/対応のための、統合エンドポイントセキュリティプラットフォームです。

Microsoft Defender ATPの振る舞いベースでクラウドを使用した脅威およびマルウェアの防御機能によって、感染デバイスから広がる高度で未知の脅威を防ぐことできます。Microsoft Defender ATPは、メモリやカーネルを含むオペレーティングシステムの深部まで目を光らせ、高度なゼロデイ攻撃やデータ漏洩を検知します。

[1] *出典：Gartner, Applying Network-Centric Approaches for Threat Detection and Response, Augusto Barros et al., March 18, 2019, ID G0037346*

[2] *Ibid.*

このような可視化によってアナリストは、パターンや振る舞い、侵害の痕跡、その他の隠された手掛かりを特定できるようになります。このデータを他のセキュリティ・インテリジェンス・フィードに紐付けすることで、ホストの内部でしか確認できない脅威も検知できるようになります。

Vectra 製品におけるネットワーク検知と対応

ネットワークメタデータは、脅威の検知に対して、最も信頼できるソースとなります。隠れた脅威を明らかにできるのは、完全性、信頼性、および独立性を兼ね備えたネットワーク上のトラフィックだけです。ログの分析など、粒度の粗いソースからは、目に見える不正が把握できるだけで、攻撃者によるスパイ行為や拡散、窃盗に伴う、避けることのできない、基本的な脅威に関わる振る舞いを把握することはできません。

Vectra AI社のプラットフォームでは、ネットワーク上の全てのデバイスに関わるやり取りを俯瞰することができます。セキュリティリサーチとデータサイエンスの要素を取り込んだVectra AI社の振る舞いに関するモデルは、活動中の攻撃を検知し優先付けを行って、侵害を受けたホストデバイスとの関連付けを行います。主要なネットワークメタデータを収集および保存し、機械学習と高度な分析機能を使って強化することで、企業ネットワークに存在する不審な活動を検知することができます。

Microsoft Defender ATPとのネイティブな連携により、セキュリティチームは、Vectra AI社によるトップダウンな視点と、Microsoft Defender ATPのボトムアップ的な視点の両方を組み合わせることが可能となります。アナリストは、Vectra AI社のプラットフォーム内でMicrosoftから提供されるコンテキストを確認し、アカウントを自動的に無効化したり、Vectra製品のコンソールからMicrosoft Defender ATPのホスト隔離機能を実行することができます。さらにセキュリティチームは、Vectra製品から得られたローカルコンテキストを、Microsoft Defender ATPでのスコープおよびスケール用パラメータとして使用し、Microsoft Defender ATPへ即時に切り替えを行いながら、調査を迅速化することができます。

Microsoft Azure Sentinel

十数年もの間、セキュリティチームはIT環境全体のセキュリティアクティビティを管理するためのダッシュボードとして、SIEMに依存してきました。SIEMは、他のシステムからのイベントログ情報の収集や、データ分析機能、イベントの関連付け、さらに集約やレポーティングを行います。

Azure Sentinelでは、Vectra CognitoとMicrosoft Defender ATPのsyslogを取り込むことができます。インシデントが発生すると、アナリストは組込み済みのアプリケーションとVectra製品のダッシュボードウィジェットを使って、影響を受けたホストデバイスとアカウントを素早く特定することができます。また、簡単な調査によって、攻撃の性質やその攻撃が成功したかどうかを判定することができます。

SIEMは、ファイアウォールやNACの実施ポイントといった、他のネットワークセキュリティコントロールと通信して、不審なアクティビティをブロックするよう指示することができます。またSIEMでは、脅威インテリジェンスのフィードを使用して、攻撃を予防的に防ぐこともできます。

MicrosoftとVectra AI社 ー SOC可視化トライアドのビジョンを具現化

セキュリティチームは、Vectra Cognitoプラットフォーム、Microsoft Defender ATP、Azure Sentinelをネイティブに統合することで、SOC可視化トライアドのビジョンを具現化することができます。この連携によって、それぞれ単独では対応できない、様々な質問への回答が可能になります。例えば：

- 他のアセットが、侵害を受けた可能性のあるアセットと通信した後で、異常な振る舞いを始めていませんか？
- どんなサービスやプロトコルが使われたのでしょうか？
- 他のどのようなアセットまたはアカウントが関係している可能性がありますか？
- 同じ外部のC&C IPアドレスにコンタクトした、他のアセットはありますか？
- ユーザーアカウントが、他のデバイス上で想定外の使われ方をしていませんか？

各データソースから得られるコンテキストをネイティブに統合したり、アカウントの無効化やホストの隔離、さらに組込み済みのSOC可視化ダッシュボードといったソリューションを組み合わせることで、十分に連携がとれた対応が可能となり、セキュリティ運用の効率を高めると共に、最終的には、ビジネスリスクを高める可能性がある攻撃者の滞在時間を短縮することができます。

VECTRA AI, INC.

お問合せ：
製品、ソリューションなどに関するお問い合わせは、info-japan@vectra.ai までお願いします。