ゼロトラスト

エッセンシャルガイド

splunk>

turn data into doing™

目次

今日、組織のデータとシステムを守るための戦略として「ゼロトラスト」がこれまで以上に注目を集めています。新型コロナウイルスの感染拡大は、規模や業種を問わず、ゼロトラストに対する組織の認識を高めました。さらに、SolarWindsのような高度な脅威の出現、クラウド移行の加速、攻撃対象の拡大により、アプローチ転換の重要性が一層増しています。

しかし、この種のイニシアチブに躊躇する組織も多いでしょう。特にこの場合、組織全体だけでなく、組織内の個々のデバイス、アプリケーション、ユーザーのセキュリティ対策を見直す必要があるため、負担に感じるのも無理はありません。さらに問題を難しくしているのは、ゼロトラストの適用対象が従来のITシステムだけでなく、ハッカーのターゲットになりやすいOT/ICS (運用技術/産業用制御システム)やIoTにも及ぶ点です。

しかし、導入する価値があることは確かです。ゼロトラストモデルを実現すれば、防御を境界のみに依存する従来の仕組みを変えることで組織のセキュリティ体制を抜本的に改善し、運用の負担を軽減できます。ゼロトラストでは、境界で防御する代わりに、各アクセスポイントで一定の信頼性を確保することにより、ユーザー、資産、リソースを効果的に保護します。といっても、境界での防御が不要になるわけではありません。重要な資産を境界だけでなく組織全体で守ることが目標なのです。

大切なのは、ゼロトラストは単なるアーキテクチャのフレームワークではなく、何を監視し、トリアージし、修復すべきかを一から考え直すマインドセットだということです。このエッセンシャルガイドでは、ゼロトラスト戦略が求められる背景、その推進に必要な要素、実際の構築手順を紹介し、最終的に、セキュリティの本質を明らかにしたいと思います。

ゼロトラストとは

ゼロトラストの基本原則は、組織のデータがどこにあっても保護し、リソースや資産へのアクセスを正当なユーザーとエンティティにのみ許可することです。逆に言えば、組織のネットワークにアクセスするユーザー、デバイス、サービスはすべて、正当だと証明されるまで、信用できないものと見なします。

具体的には、アクセスを要求するユーザーとそのデバイスを認証した後、アプリケーションや情報単位でアクセスポリシーと照合します。つまり、従業員のデバイス、資格情報、行動に基づいてアクセスの可否を判断するホワイトリスト方式です。セッションごとに常にデバイスレベルとユーザーレベルで認証を行うことで、継続的できめ細かい適応認証を実現します。

ゼロトラストセキュリティプログラムを成功させるための心構え：

- ネットワークには常に悪意が潜んでいると見なす。
- ネットワークには常に外部および内部からの脅威があることを認める。
- ネットワークローカリティが示す場所だけでは信頼性を判断してはならないことを理解する。
- あらゆるデバイス、ユーザー、ネットワークフローを認証と許可の対象にする。
- 動的で、かつできるだけ多くのデータソースから導き出したポリシーを実装する。

この仕組みを例で説明しましょう。ある従業員が、新しく割り当てられたデバイスから組織のケース管理システムを使用することを許可されたとします。この従業員がこのデバイスからリクエストを行うと、アクセスが許可されます。しばらくして従業員は、仕事に役立つと考えて、あるWebサイトからドライバをダウンロードします。このデバイスはゼロトラスト戦略で継続的に監視されているため、このアップデートにはフラグが付けられます。

ドライバの追加によってデバイスの構成が変化したため、デバイスの信頼スコアが変更されます。これにより、従業員が次にシステムにアクセスする際、新しい信頼スコアと適用されるポリシーに応じて、権限が下げられ、アクセスが拒否される可能性があります。このように、複数の要素(この例ではユーザー、デバイス、リソースのスコア)を組み合わせることで、組織のリソースに対するリスクに柔軟に対応できます。つまり、ゼロトラストシステムでは、状況の変化を考慮に入れて継続的に評価を行い、リソースを保護するのです。

ゼロトラストの進化

2010年にForrester社によってゼロトラストが初めて提唱されるまで、組織のセキュリティは、従来型のネットワークセキュリティソリューションを使用したネットワークベースのセグメンテーションモデルが主流でした。その基本的な考え方は、重要なリソースやデータをすべてネットワーク内に置き、ネットワークの境界、いわば組織のネットワークを取り囲む城壁の防御力を強化することです。しかし、ひとたび脅威が境界を破ってネットワーク内に侵入してしまうと、攻撃者はネットワーク内を縦横無尽に移動し、ネットワークに接続するシステムに侵入して資産を侵害できるため、甚大な被害につながる可能性があります。

境界防御からゼロトラストへ

その後、組織のセキュリティは、ネットワーク境界を重視するアプローチから、組織の内外を問わずすべてのデバイス、ユーザー、システムは信頼できないという前提に立ち、すべてのリソースへのアクセスを明示的に認証および認可すべきであるという考え方を基本とするアプローチへと移っていきました。ただし以前は、その実現は容易ではありませんでした。従来のツールでは統合機能が不十分で、組織のリソースのセキュリティを包括的かつ一元的に監視することができず、かえってサイロ化が進んで、実装を手掛けるセキュリティエンジニアの負担が増すことになりました。

今日では、アクセス制御に重点を置くツールが増え、制限された場所や重要情報へのユーザーアクセスの可否を判断するルールを細かく設定できるようになりました。ゼロトラストアーキテクチャでは、これらのツールを連携することで、複数のセキュリティコントロールを個別に管理する複雑さを軽減できます。

アクセス制御に役立つツールの例：

- アイデンティティ /アクセス管理(IAM)
- 多要素認証(MFA)
- データ漏えい防止(DLP)
- クラウドアクセスセキュリティブローカー (CASB)
- クラウドインフラ権限管理(CIEM)

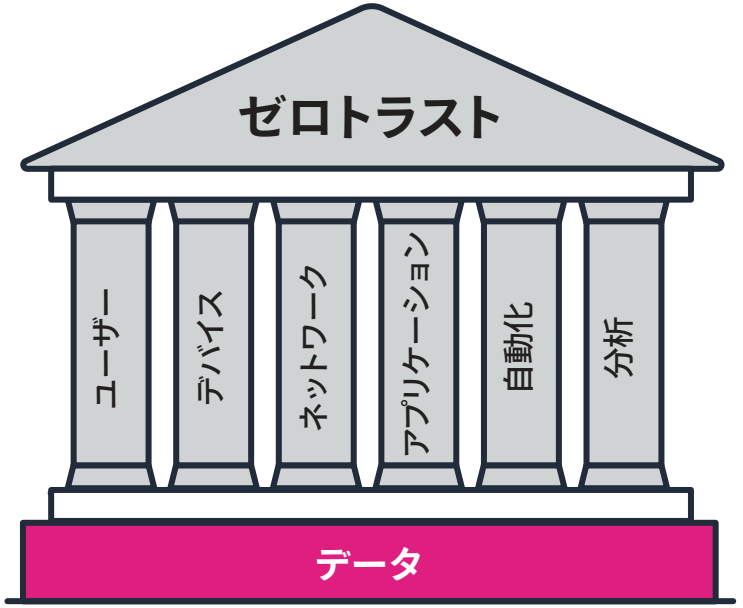
こうしたテクノロジーの進化によって、ゼロトラストの実現は以前よりも容易になりました。ゼロトラストへの流れをさらに後押ししたのが、新型コロナウイルスの感染拡大による世界的なデジタルトランスフォーメーションの加速です。一夜にして、従業員はリモートワークを余儀なくされ、ITインフラやセキュリティインフラには多大な負荷がかかりました。保護すべき領域が広がり、境界防御に限界が見え始めたことで、ゼロトラストの導入は世界的に緊急課題となったのです。

ゼロトラストモデル

ITを通じて政府の改善を目指す非営利の官民提携団体、ACT-IAC (American Council for Technology and Industry Advisory Council)は、ゼロトラストセキュリティモデルの6つの柱を定義しています。どの柱も、その土台にはデータがあります。

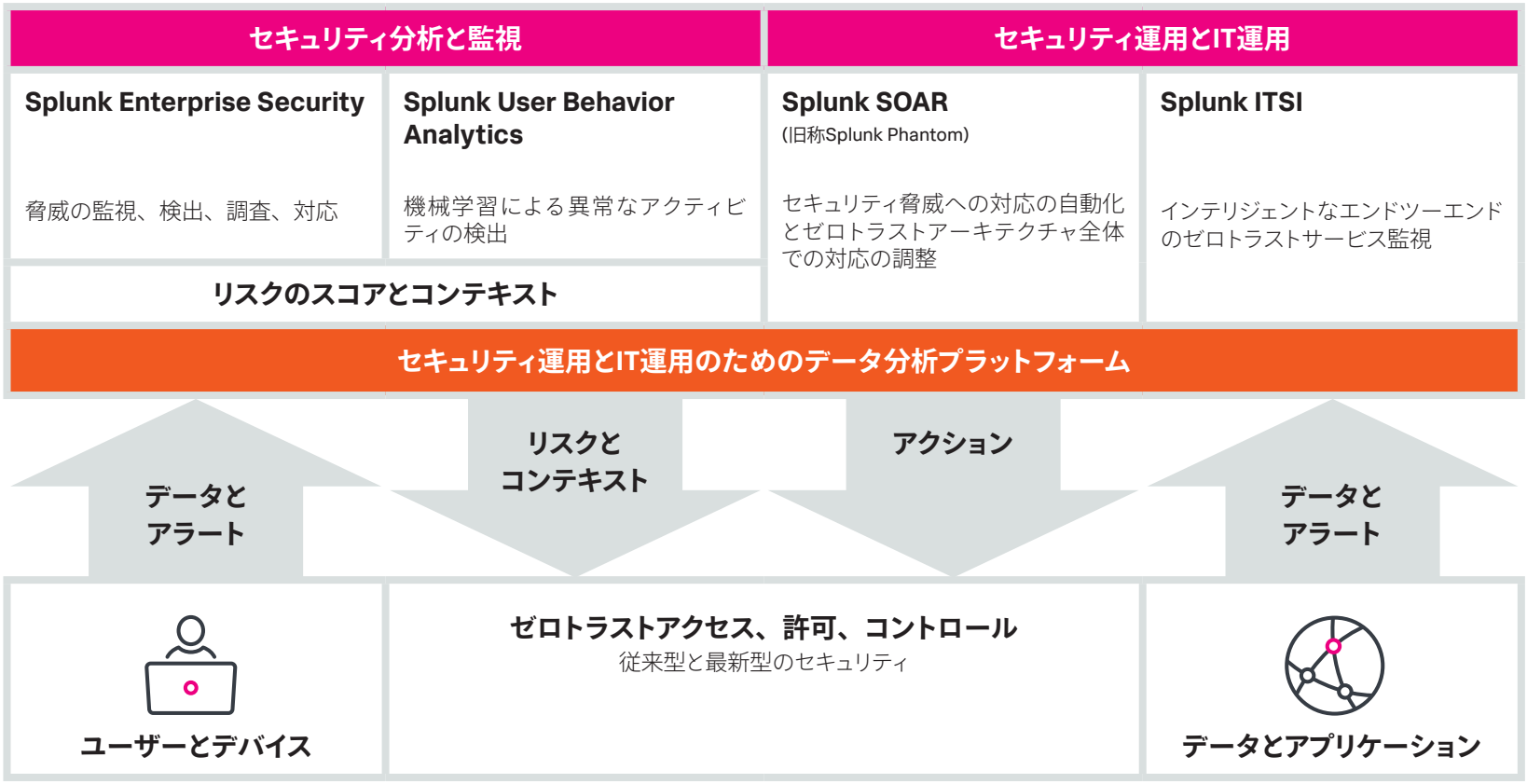
各柱の概要は次のとおりです。

- **ユーザー：**信頼済みのユーザーを継続的に認証し、ユーザーの信頼性を継続的に監視、確認して、アクセスと権限を管理する。
- **デバイス：**デバイスのサイバーセキュリティ対策と信頼性をリアルタイムで評価する。
- **ネットワーク：**ネットワーク(ソフトウェア定義のネットワーク、ソフトウェア定義の広域ネットワーク、インターネットベースの技術を含む)をセグメント化、分離、制御する。
- **アプリケーション：**アプリケーションレイヤー、コンテナ、仮想マシンを保護し、適切に管理する。
- **自動化：**SOAR (セキュリティのオーケストレーションと自動化によるレスポンス)によって、複数の製品にまたがるタスクをワークフローで自動化し、エンドユーザーをインタラクティブに監督する。
- **分析：**SIEM (セキュリティ情報/イベント管理)、高度なセキュリティ分析、UEBA (ユーザーとエンティティの行動分析)など、可視化ツールや分析ツールを使用して現状を把握し、状況に応じた防御策を実行する。



ゼロトラストチェックシート

☐	ゼロトラストモデルでは、すべての資産とリソースへのユーザーアクセスを認証および認可し、組織の適切なポリシーに基づいてセッション単位でアクセス権を付与する。	
☐	ゼロトラストのコントロールを洗い出し、組織のシステム、ユーザー、データと整合させる。その際は、次の2つの観点を考慮する。	
	☐	オンプレミス/クラウドのインフラ、ネットワーク、システム、アプリケーション、データ(総称して「オブジェクト」)を保護するためのセキュリティコントロール
	☐	リソースにアクセスするユーザーとエンドポイント(管理アクセスを含む。総称して「サブジェクト」)を保護および認証するためのセキュリティコントロール
☐	外部リソース(SaaSなど)を含むすべてのシステムのユーザーとデバイスのアイデンティティと信頼スコアを管理するための共通のポリシー、プラクティス、手順を定める。	
☐	ゼロトラストコントロールの管理を一元化し、従来のセキュリティルール(IPベースのコントロールなど)ではなくビジネスレベルのロジックに基づいて、動的なエンドツーエンドのアクセスを設計する。	
☐	エンドツーエンドのデータ分析環境を構築して、ITとセキュリティの両方の運用要件に対応した、アーキテクチャ全体の監視と脅威検出を実現する。	
☐	一元的なセキュリティ体制を確立し、アクセス許可について、コンテキストに沿ったリスクプロファイルと高度なポリシーロジックを作成する。	
☐	既存のセキュリティコントロールとプロセスを確認し、より広範なゼロトラストアーキテクチャ内でのそれらの適合性と互換性を評価する。	



ゼロトラストの歴史と基本知識を学んだら、次は実践です。以下のセクションでは、最新のSOC (セキュリティオペレーションセンター)を構築してゼロトラストのセキュリティ監視体制を確立する方法と、Splunkを活用して組織のゼロトラスト戦略目標をすばやく実現する方法について詳しく説明します。

ゼロトラスト実現のための Splunkデータ分析ジャーニー

セロトラスト戦略を導入するには、まず、ゼロトラストコントロールとポリシーに沿ってセキュリティインシデントを監視、検出、調査するための体制を整備する必要があります。特に、ユーザー、システム、アプリケーション、データを保護するための仕組みが重要です。

Splunkは、データ分析ソリューションの導入を長年支援してきた経験、業界のベストプラクティス、これまで蓄積してきた知識に基づいて、「セキュリティデータ分析ジャーニー」と呼ぶモデルを確立しました。

この成熟度モデルでは、組織のセキュリティジャーニーを複数のステージに分けています。各ステージで段階的に改善を重ねることでステージの目標を達成し、次のステージに進みます。このジャーニーはセキュリティの成果に重点を置いていますが、データを再利用したり置き換えたりすることで、IT監視能力の強化にも役立ちます。

このアプローチを実践することで、最終的に、1.IT/セキュリティ運用とゼロトラスト戦略の整合性を高める、2.ゼロトラストアーキテクチャに対応した最新のSOCを構築して既存のギャップを埋める、という2つの大きなメリットを実現できます。以下のセクションでは、データ分析ジャーニーの各ステージを順に紹介しながら、組織のIT/セキュリティ運用に沿ってゼロトラスト要件に対応する方法について説明します。

Splunkセキュリティデータ分析ジャーニー

ステージ6

高度な検出
機械学習などの高度な検出メカニズムを導入する

ステージ5

自動化とオーケストレーション
一貫性のある繰り返し可能なセキュリティ運用機能を構築する

ステージ4

強化
セキュリティデータをインテリジェンスで補強し、イベントのコンテキストや影響について理解を深める

ステージ3

拡張
エンドポイントでの活動やネットワークメタデータなど、追加のデータソースを収集し、高度な攻撃の検出を促進する

ステージ2

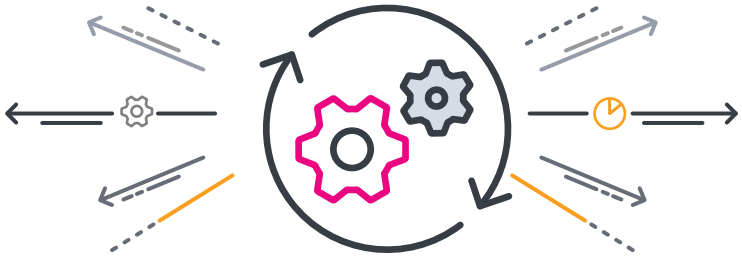
正規化
標準的なセキュリティデータの形式を適用し、資産データとアイデンティティデータを追加する

ステージ1

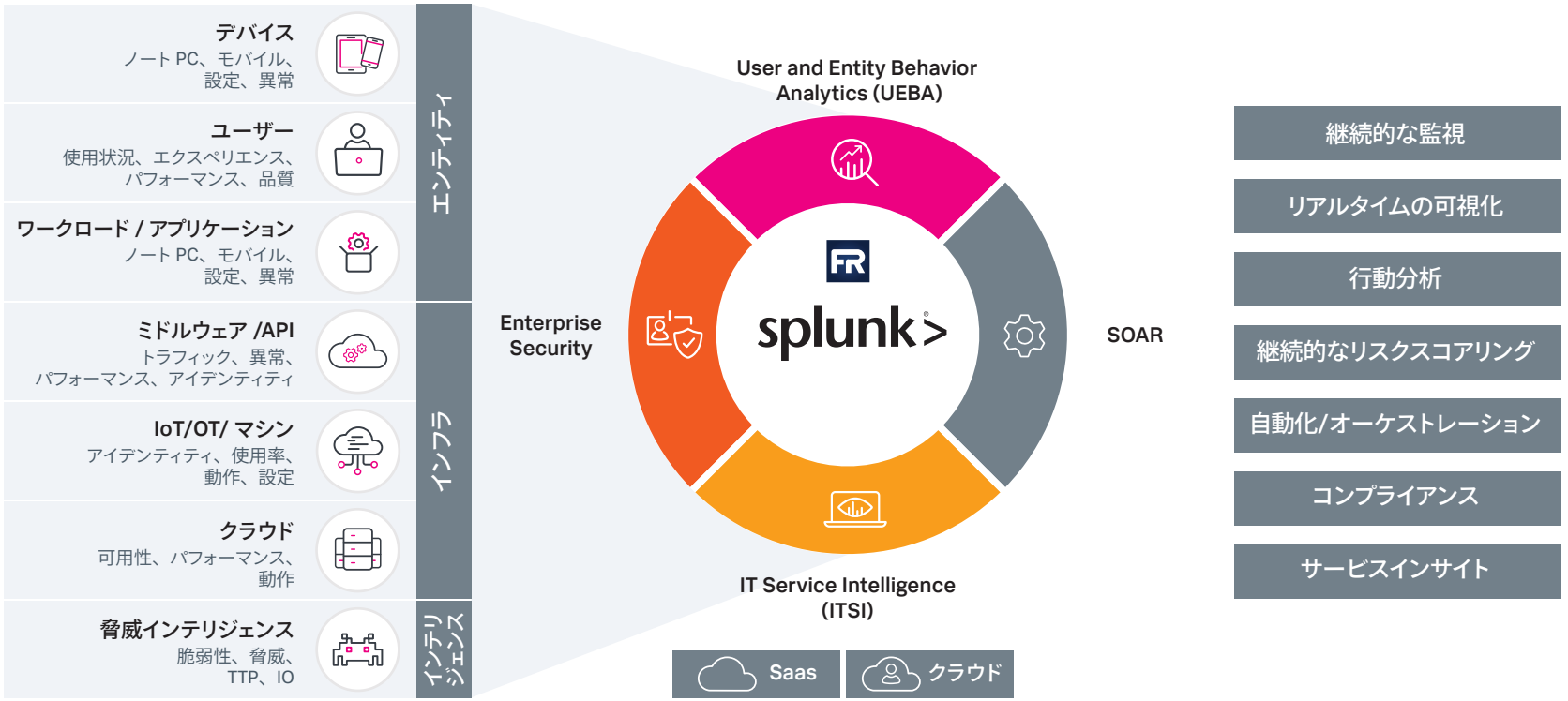
収集
環境内の基本的なセキュリティログやその他のマシンデータを収集する

ゼロトラストジャーニーの各ステージの説明では、ゼロトラストに対応したセキュリティ /IT監視を実現するための各種要件に適合する製品も紹介します。これには、以下の製品が含まれます。

- Splunk Enterprise：データ分析/調査プラットフォーム
  - ゼロトラストアーキテクチャでのIT、セキュリティ、不正検出のユースケースに対応する、拡張性の高いデータ分析プラットフォーム
  - 幅広い構造化データと非構造化データを収集可能
  - 包括的なパートナーエコシステムにより、ゼロトラストに必要な統合、迅速なデータソースオンボーディング、データ正規化に対応
- Splunk Enterprise Security：SIEM (セキュリティ情報/イベント管理)
  - Splunk Security Essentials (SSE)やEnterprise Security Content Update (ESCU)と併せて、セキュリティ監視と検出に関する幅広いユースケースライブラリを提供
  - 資産データとアイデンティティデータの補強とコンテキスト追加、リスクスコアリング、ゼロトラスト目標に沿ったセキュリティ体制の整備に対応するための主要なフレームワークを提供
  - リスクベースのアラート(RBA)により、MITRE ATT&CKフレームワークに沿った高度なリスクスコアリングと複数指標による検出を実現。ゼロトラストコントロールを監視して、悪質な行動につながる可能性のある一連のアクティビティを検出
- Splunk User and Entity Behavior Analytics (UEBA)
  - 教師なし機械学習で、高度な行動検出とアイデンティティの自動照合をすばやく実現
- Splunk SOAR (旧称Splunk Phantom)：セキュリティのオーケストレーションと自動化によるレスポンス
  - ゼロトラストアーキテクチャでのセキュリティインシデントやサービスインシデントに対応するための包括的なケース管理、調査、オーケストレーション、自動化を実現
- Splunk IT Service Intelligence (ITSI)
  - ゼロトラストコントロールと、関連アプリケーションおよびサービスの基盤となるインフラを、エンドツーエンドで監視



ゼロトラストのIT/セキュリティ運用に対応するSplunkソリューション



ステージ1：関連データの収集

まずは、保護および監視する必要のある組織内の資産を洗い出し、優先度を判断します。資産の優先度を明確にしておけば、リソースの割り当てや取り込むデータソースを決める際に参考になります。

ゼロトラストではさまざまなテクノロジーを組み合わせます。一部はすでに導入済みである場合もあります。それらのシステムはIT監視とセキュリティ監視の重要なデータソースになると同時に、エンドツーエンドの包括的なゼロトラストプログラムの土台となります。

ゼロトラスト実現に役立つテクノロジーの例：

- 次世代ファイアウォール(NGFW)
- ソフトウェア定義ネットワーク(SDN)とマイクロセグメンテーションソリューション
- クラウドアクセスセキュリティブローカー (CASB)
- リモートアクセス
  - 仮想プライベートネットワーク(VPN)
  - 仮想デスクトップインフラ(VDI)
  - ゼロトラストアクセス(ZTA)
- アイデンティティ /アクセス管理(IAM)とディレクトリサービス
- 多要素認証(MFA)
- 特権アクセス管理(PAM)
- エンドポイント検出/対応(EDR)
- セキュリティポスチャソリューション(パッチと脆弱性管理など)
- Webプロキシ、Webフィルタリング、セキュアWebアクセスサービス
- データ漏えい防止(DLP)
- セキュアアクセスサービスエッジ(SASE)
- 統合エンドポイント管理(UEM)とモバイルデバイス管理ソリューション

システムやサービスの基盤となるインフラを構成する要素(ストレージ、ネットワーク、IT管理機能を支えるコンポーネントなど)も重要なデータソースであり、この段階でデータの収集対象に加えます。

データソースの例：

- **ネットワーク:**データセンターとクラウドのネットワークインフラ(スイッチ、ルーター、ロードバランサーなど)、および仮想ネットワークサービス
- **ストレージ：**データセンターとクラウドのストレージシステムおよびサービス(ストレージアレイ、システムディスク、NAS/SAN、クラウドストレージサービスなど)
- **コンピューティング：**データセンターとクラウドのコンピューティングリソース(物理コンピューター、仮想コンピューター、オペレーティングシステムなど)
- **管理：**管理機能を支えるシステムとアプリケーション(監視システム、ジャンプホスト、管理者認証/特権アクセス制御など)

組織の資産の洗い出しと優先度の判断は大掛かりな作業に思えるかもしれませんが、Splunkのデータ分析ジャーニーで重要なのは、システムまたはサービス単位で、その時点で実践する必要のあるユースケースに合わせて、段階的に進めることです。重要度の高い資産とエンティティを洗い出して明確化すれば、それに基づいて、IT/セキュリティインシデントのアラートにコンテキストを追加し、優先順位を判断できます。また、データソースを確立しておけば、次の段階の成熟度を目指す際に、そのデータを再利用できます。

ステージ2：データの理解とコンテキスト追加

データのコンテキスト追加はゼロトラスト戦略の要です。データを理解するには、すべてのデータソースに共通の分類基準を定める必要があります。この作業を行わないと、大量のノイズに悩まされることになります。データの分類基準を定めておけば、特にセキュリティジャーニーのステージを進む中で、多くの混乱を解消できます。

たとえば、ファイアウォールのログ形式やデータ構造はベンダーによって異なります。一元監視を実現するには、ファイアウォールのログデータの構造を変換して、フィールド名と値の組み合わせに正規化し、他のデータと形式を統一する必要があります。

構造化データも非構造化データも一網打尽

Splunkは、共通の分類基準を確立するためのオープンで拡張性のあるアプローチとして、CIM (共通情報モデル)を開発しました。Splunk CIMを使用すれば、Rawデータから抽出したフィールド名と値を構造化および標準化して、幅広いカテゴリに対応するデータモデルに変換できます。Splunkでは、取り込み後のデータにこの処理が行われるため、元のRawデータは変更されません。

Rawデータが変更されないため、要件が変化した場合でも、すべてのデータを取り込み直す手間をかけずにデータ構造を更新できます。また、データモデル高速化を有効にすれば、ピボットサーチを利用してデータセットの作成を迅速化することもできます。これにより、構造化データのサーチパフォーマンスが向上し、最終的に、ゼロトラストモデルの全体的な健全性を判断するために必要な結果をすばやく得られるようになります。

Splunk CIMは、Splunk Enterprise Security (ES)のネイティブの監視および検出機能でサポートされ、特定したすべてのゼロトラストデータソースに適用できます。Splunkのパートナーおよびユーザーエコシステムでも、データのオンボーディングと正規化に利用できる幅広いSplunkアドオンが提供されています。

Splunkアドオンは、さまざまなゼロトラストデータソースに対応するだけでなく、継続的なアップデートによって新機能の追加や機能の改善が行われる点も魅力です。

データ活用のニューノーマル

次に、正規化したデータを活用するためのユースケースを実装します。セキュリティ検出の出発点として最適なのは、Splunk Security Essentials (SSE)で利用できるユースケースライブラリです。SSEには、セキュリティ分析ジャーニーの各段階に対応する幅広いユースケースが用意されています。

SSEにはさらに、MITRE ATT&CKフレームワークに従ってジャーニーの各ステージにマッピングできる、ゼロトラストに適したユーケースカテゴリが新しく追加されました。MITRE ATT&CKフレームワークは、実際の脅威で使われた戦術や技法をまとめた広範なナレッジベースを提供し、多くのセキュリティチームに幅広く利用されています。

MITRE ATT&CKの使い方

Splunkは、ゼロトラスト戦略で防止すべき脅威を評価し、関連するMITRE ATT&CK戦術に基づいて、一連のセキュリティユースケースをまとめました。ゼロトラストを徹底するための複雑さと範囲の広さを考えれば、ゼロトラストに適したセキュリティ検出および監視ユースケースを適用することは、コントロールベースのアプローチを強化するために役立ちます。

ただし、現実には他の多くのタイプの脅威にも対応する必要があるため、このガイダンスは、より包括的なセキュリティ監視戦略の一部として検討してください。

SSEのゼロトラスト向けの主なセキュリティ検出ユースケースは、以下のMITRE ATT&CK戦術に基づいて分類されています。

- **初期アクセス：**攻撃者がネットワークに侵入しようとしている
- **永続化：**攻撃者が攻撃拠点を築こうとしている
- **権限のエスカレーション：**攻撃者がより高いレベルの権限を獲得しようとしている
- **資格情報へのアクセス：**攻撃者がアカウント名とパスワードを盗もうとしている
- **ラテラルムーブメント(横展開)：**攻撃者が環境内を移動しようとしている
- **データ流出：**攻撃者がデータを盗み出そうとしている

また、以下のユースケースは、セキュリティジャーニーのステージ2 (データの正規化)に適用できます。これらのユースケースでは、認証、ネットワーク、エンドポイントなどのデータ(ステージ1で取り込んだデータ)のデータソースが使用されます。

- アカウント管理の変更
- 新しいアカウントの作成
- セキュリティポリシーまたはコントロールの変更
- 認証のブルートフォース攻撃
- 管理ログまたはセキュリティログの消去
- システム設定の不正な変更

このステージでデータが正規化されるため、Splunk Enterprise Security (ES)でゼロトラスト関連のアクティビティを監視およびレポートできます。対象になるアクティビティには以下のものが含まれます。

- エンドポイントとサーバーのマルウェアおよびシステム設定変更の監視
- エンドポイントとサーバーの脆弱性とパッチの管理
- ユーザーのアクセスとアカウントの管理
- ユーザーのWebアクティビティの監視
- ネットワークトラフィックの監視

次に、保護するシステムのリスクプロファイルなどの情報と、ユーザーアイデンティティに関するコンテキストを組み込みます。これはセキュリティ分析において重要な作業です。これらの情報がセキュリティアラートのリスクスコアと優先順位の基礎となります。ステージ1で特定した保護対象の資産とエンティティのデータにコンテキスト情報を追加します。

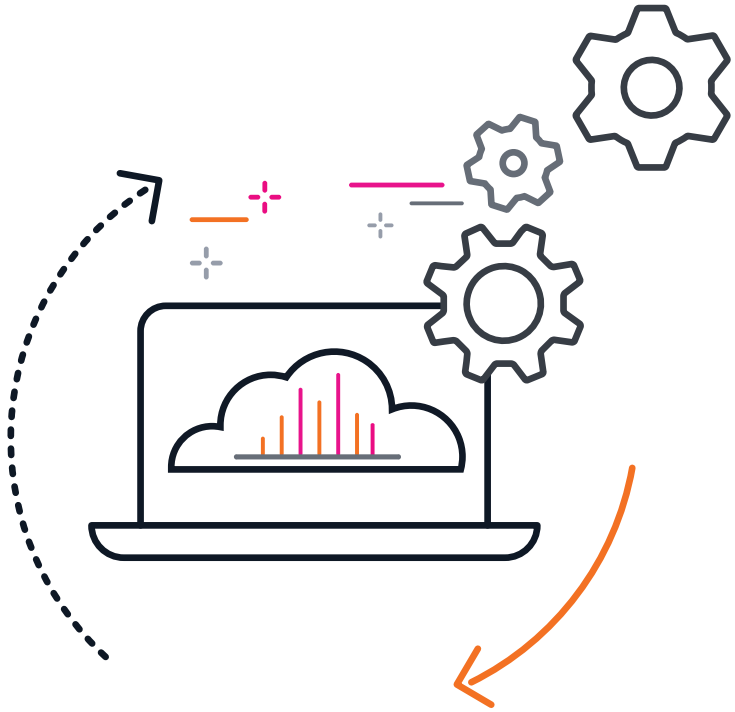
重要なコンテキスト情報の例：

- **資産のリスクプロファイル：**この資産に影響するインシデントのビジネスインパクト、この資産に影響するインシデントが起きる可能性、この資産に対するセキュリティ対策、このシステムで処理または保持されるデータの機密性と重要度、このシステムをよく使用するユーザーのタイプ
- **アイデンティティのリスクプロファイル：**このアイデンティティの重要度、このアイデンティティのアカウントのタイプ(サービスアカウント、管理者アカウント、経営幹部レベルのユーザーアカウント、請負業者のアカウントなど)、そのアカウントは攻撃のターゲットになりやすいか、そもそも信頼できないアカウントであるか、このアイデンティティが侵害を受けた場合の影響、ユーザーに離職リスクがあるかどうか

Splunk ESに組み込まれた資産とアイデンティティのフレームワークは、このステージの調査に不可欠で、リスクスコアの基礎にもなります。ESで登録された資産やアイデンティティはすべて、関連するセキュリティイベントとその重大度、資産やアイデンティティの重要度に基づいて継続的に記録されます。この情報は、セキュリティジャーニーの最後のステージ(高度な検出)で導入するリスクベースのアラートで重要な役割を果たします。

資産とアイデンティティのフレームワークに取り込まれて、集約、構造化されるデータソースには以下のものが含まれます。

- 構成管理データベース(CMDB)
- ネットワーク資産検出ツール
- ディレクトリ/認証サービス
- 人事システム
- クラウド環境



ステージ3：データソースの拡張

セキュリティコントロールを継続的に監視していても、高度なセキュリティ脅威を検出するのは難しいものです。この課題を解消するには、対象のシステムの動作状況だけでなく、システムが正しく使用されているかどうかも監視する必要があります。また、システム、データ、ユーザーを包括的に監視することも重要です。そのためには、行動やインフラレベルの監視が不可欠です。

なぜそこまでする必要があるのでしょうか。ゼロトラストでは、正当な手段を使用した不正行為、内部脅威、高度な攻撃(盗んだアカウントによるなりすましなど)を完全に防ぐことはできないからです。しかし、インシデントを封じ込め、被害を最小限に抑えることはできます。ただし、監視対象を誤れば、このタイプの脅威の検出が後手に回る可能性があります。ゼロトラストポリシーと正規ユーザーの正しい行動を考慮に入れることで、監視すべき異常な状態を想定して、悪質なアクセスをより迅速に検出できます。

データが増えればストレスが減る

セキュリティコントロール以外のデータソースからもデータを取り込めば、ユーザーの行動をより詳細に可視化できます。たとえば、ネットワークフローデータを取り込んで、ネットワークアクティビティとアプリケーションやプロセスのアクティビティを相関付けます。これは、正規のネットワーク通信を使用する不正なアプリケーションの検出や、アプリケーションやユーザーアカウント間のラテラルムーブメントの検出に役立ちます。

ゼロトラストを前提にコントロールとポリシーを定めて監視範囲を広げるだけでなく、アクセスが許可された正規のユーザーの行動やシステムの正しい動作にも細心の注意を払う必要があります。セキュリティコントロールの関連情報にも目を向ければ、盗まれた資格情報によるなりすましやデバイスの乗っ取りにも対応できます。

以下のタイプのデータソースは、ユーザーの行動やデバイスの動作の異常を検出するために役立ちます。

- **エンドポイント：**SysmonやosqueryなどのEDR (エンドポイント検出/対応)拡張機能またはツールを使用して、アプリケーションとプロセスの実行状況、ファイルの整合性、ネットワーク接続を把握します。
- **アプリケーション：**まずは、ビジネスに重要なアプリケーションの情報を収集します(財務システムや、機密データ、顧客データ、ユーザーアクティビティのログを処理するシステムなど)。
- **データベース：**監査ログとトランザクションログを分析して、異常な行動パターン、レコードの変更や削除、機密レコードや制限されたレコードへの不正アクセスを識別します。
- **クラウド：**中心となるのはSaaS (Software-as-a-Service)ビジネスアプリケーションでのユーザー監視ですが、ゼロトラストポリシーに違反する可能性のある不審な管理者アクティビティを検出するには、IaaS (Infrastructure-as-a-Service)やPaaS (Platform-as-a-Service)環境も監視します。
- **クラウドベースのファイルストレージサービス：**機密データの動きや異常なデータ移動パターンを監視します。

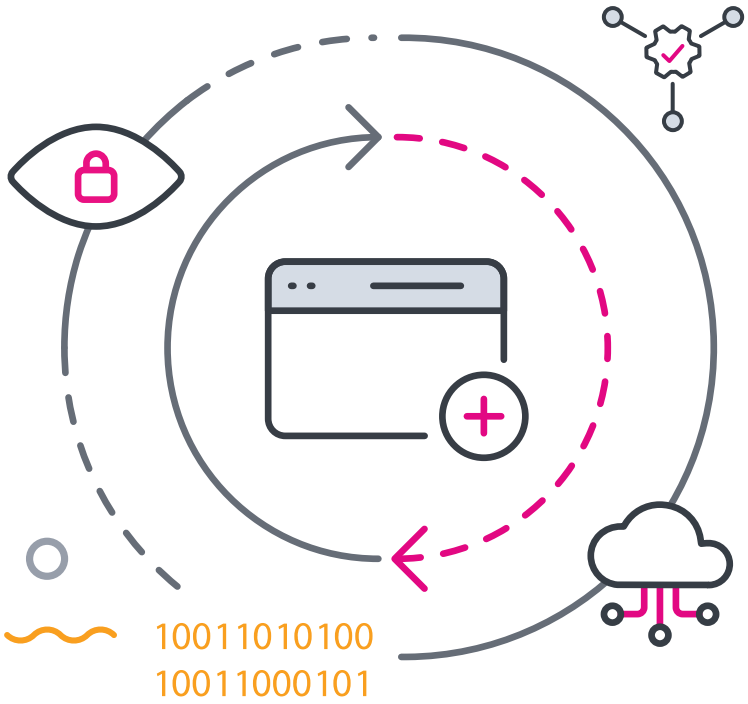
ステージ2で始めた初期の検出と監視を拡張し、ステージ3で追加したデータソースを使用すれば、より高度な検出が可能なユースケースを追加できます。これには、SSEに用意されているユースケースのほかに、Splunk Enterprise SecurityやEnterprise Security Content Updates (ESCU)で利用できるユースケースも含まれます。

分析ストーリー

ESCUのユースケースは「分析ストーリー」として定義されています。分析ストーリーは、インシデントと検出のライフサイクル全体に対応し、ユースケースの背景、データソースの詳細、インシデントの検出と調査に役立つサーチで構成されます。

ステージ3のユースケースの例：

- ラテラルムーブメント
- 時刻や場所が異常なユーザー認証またはアクセス
- システムまたはアプリケーションへの新規のユーザーアクセス
- 新しいリムーバブルメディアデバイス
- 新しいローカルアカウントの作成
- デフォルトアカウント、システムアカウント、サービスアカウントのインタラクティブな使用
- 異常であるか、過去にほとんどまたはまったく実行例のないプロセス/アプリケーション
- 異常なコマンドラインアクティビティ (難読化されたPowerShell)
- 異常であるか、ほとんど使用例のないクラウドアプリケーションの使用(ファイル共有)
- エンドポイントの変更と状況変化(ソフトウェアのインストール、システムファイルの変更)



ステージ4：データの補足と強化

このステージでは、脅威インテリジェンス、脆弱性とパッチの管理ツール、攻撃対象領域管理ソリューションなど、さらに多くのコンテキストを提供するデータソースを追加します。

脅威の状況を把握する

脅威インテリジェンスは、ゼロトラストコントロールや保護対象システムで侵害の痕跡(IoC)を特定するのに役立ちます。Splunk Enterprise Securityの脅威インテリジェンスフレームワークを介して、またはSplunk SOARの自動化機能で情報補強のプレイブックを使用することで、脅威インテリジェンスシステムにリアルタイムでアクセスできます。

脅威インテリジェンスを活用すれば、保護対象のシステムやユーザーが影響を受ける脅威を把握できます。また、ゼロトラストセキュリティコントロールでこれまで検出できなかった既知のIoCを検出することもできます。たとえば、フィッシング攻撃で使用されるIPアドレス、URL、ファイルハッシュや、悪質な目的に使用される既知のSSL証明書情報を調査できます。

また、保護対象の資産のセキュリティ対策や、これらのリソースにアクセスするシステムを把握すれば、リスクスコア、セキュリティインシデントの優先順位、アクセス許可の判断に役立ちます。たとえば、必要なパッチが適用されていないユーザーデバイスから重要なシステムへのアクセスを制限したり、既知の脆弱性に関連するセキュリティインシデントの優先順位を上げたりできます。

さらに、攻撃対象領域管理ソリューションを使用すれば、セキュリティコントロールの最適化とエンドツーエンドの可視化を徹底することで、全体的なセキュリティを強化できます。コントロールにセキュリティギャップがある場合は、ギャップを軽減したり監視を強化したりできます。

強化のステージでは以下のデータの追加を検討します。

- **リアルタイムの脅威インテリジェンス：**Splunk Enterprise Securityの脅威インテリジェンスフレームワークでは、商用のソースとオープンソースを含む複数の脅威インテリジェンスフィードを取り込み、キュレーションできます。情報のやり取りにはSTIXやTAXIIなどのプロトコルが使用されます。その後、ゼロトラストデータソースに対してIoCを照合することで、既知の脅威をプロアクティブに検出できます。

脅威インテリジェンスの一般的なIoCには以下のものが含まれます。

  - IPアドレス
  - FQDN/URL
  - ファイル名とファイルハッシュ
  - SSL証明書情報

- **脅威の状況の監視：**Splunk Enterprise Securityの脅威インテリジェンスフレームワークには、組織の環境の脅威の状況や傾向をより的確に把握するための監視機能も用意されています。脅威インテリジェンス監視では、さまざまなタイプの脅威の発生率や、環境内のIoC、各種のフィードを調査できます。
- **リアルタイムのセキュリティ体制：**Splunk Enterprise SecurityとSplunk CIMには、脆弱性とパッチの管理ソリューションからデータを取り込んで活用するための幅広い機能が用意されています。このデータを使用すれば、組織のセキュリティ体制に関する集計データを可視化すると同時に、セキュリティインシデントの優先順位付けに役立つコンテキストを抽出できます。

ステージ5：高度な自動化とオーケストレーション

ここまでで、データの集約、正規化、補強の3つの工程を経てセキュリティの監視と検出のための強力な基盤を築きました。次のステージでは、調査と対応の強化に取り組みます。

Splunk SOARでは、オーケストレーションと自動化によって、インシデントの調査と修復を効率的かつ迅速に行うことができます。高度なプレイブックまたは独自のリクエストを通じて、ゼロトラストコントロールのセキュリティインシデント対応を自動化し、問題をすばやく封じ込めて解決できます。

対応を効率化

Splunk SOARのプレイブックでは、意思決定ロジックにより、必要な対応のコンテキストに応じて異なるアクションが実行されます。これを活用すれば、高度なポリシーロジックでゼロトラストのポリシー実行ポイント(PEP)とネットワークアクセスコントロール(NAC)機能を拡張し、リアルタイムのリスクスコアを組み込んで、ゼロトラスト認証をさらに強化できます。

Splunk SOARでは、NIST 800-61などの業界フレームワークに沿った標準運用手順を定義することもできます。これにより、アナリストは、発生したインシデントのタイプに応じて適切なワークブックまたはケーステンプレートを実行して作業を効率化し、本来の仕事であるデータ分析に集中できます。

SOARを実装

データ分析を行うときと同様に、SOARの実装も段階的な手順で行います。

1. まずは、アナリストが普段手動で実行している定型作業を洗い出します。これらを自動化することは非常に効果的です。
2. 全体のプロセスを確認して文書化します。使用するテクノロジーやタッチポイント、各ステップにかかる時間も記録します。このプロセスはSplunk SOARワークブックを使って文書化できます。
3. プロセスフロー図を作成します。意思決定や承認が必要なすべてのステップを含めます。この図がプロセス自動化のプレイブックの基になります。プロセスの中で、モジュール化してサブプレイブックとして再利用できそうなセクションを抜き出します。
4. 必要なコンポーネントを洗い出し、Splunk SOARアプリケーションとのインテグレーションを導入して、統合のための設定を行います。
5. ワークブックで定義したプロセスを実行してみます。必要に応じて手動で機能を実行しながら、インシデントを調査し、対応します。
6. プレイブックを作成および修正しながら、プロセスの中で自動化する部分を増やし、再利用できる部分は別のプレイブックとしてモジュール化します。
7. プレイブックをレビューし、アナリストのパフォーマンスをしばらく監視して成否を判定し、同時に、改善点を探ります。

Splunk SOARの高レベルのゼロトラストユースケースの例：

- ゼロトラスト関連のインシデント対応と調査を定義したワークブック/ケーステンプレート。たとえば以下の対応が含まれます。
  - アカウント侵害
  - データ漏えい
- ゼロトラスト関連のインシデント対応を自動化するプレイブック。たとえば以下の対応が含まれます。
  - Active Directoryのパスワードリセット/アカウントロック
  - 侵害されたメールの隔離と対応
  - フィッシングメールの調査と対応
  - 紛失/盗難デバイスの隔離
  - 悪意のある内部者の隔離
  - マルウェアの隔離と対応
  - 悪質なWebリソースの隔離と対応

Splunk SOARの導入にはさらに良い点があります。それは、アナリストがゼロトラストコントロールに直接ログオンする必要がないことです。Splunk SOARでは、特権アクセス管理(privileged access management - PAM)ソリューションと統合することで、SOAR内からアクションを実行できます。

また、ゼロトラストPEP/NACソリューションよりも高度な認証を実装できます。Splunk SOARなら、リスクの対策状況とスコアをリアルタイムで把握できるため、より多くの情報に基づいてユーザーアクセスの可否を判定することで、従来のゼロトラストアクセス/認証ポリシーを拡張できます。ユーザーとユーザーがアクセスしようとしているシステムの両方のリスクを組み合わせて評価すれば、エンドポイントのリスクプロファイルをより正確に理解できます。

手動のSOCタスクを自動化する

認証の際(と認証後)、Splunk SOARで、Splunk ESに登録された資産とアイデンティティのリスクプロファイルを評価して、アクセスの可否と、実行すべきその他のアクションを判断できます。その後、この情報をゼロトラスト対応NACまたはポリシーエンジンと共有して、最終的にアクセスを許可するか、拒否するか、または無効にできます。アクセスが拒否された場合でも、その理由に応じてSplunk SOARで措置を講じることができます。

たとえば以下の対応が含まれます。

- ユーザーアクセスを拒否し、リスクスコアが上がったことを通知する。
- 初期の認証後、異常な動作またはリスクのある動作が検出された場合はユーザーアクセスを制限する。
- 認証後、システムの脆弱性スキャンや資産のインベントリスキャンを実行して異常な動作の証拠を調査する。
- アクセスが拒否されたコンプライアンス違反のシステムに関するITサポートチケットを自動作成する。
- 修復措置を自動的に実行する(パッチ適用、未許可ソフトウェア/サービスの無効化、セキュリティコントロールの適用または再適用など)。

ステージ6：高度な脅威検出

いよいよゼロトラストアーキテクチャ構築の最後のステージです。ここでは、リスクベースのアラート(RBA)による高度なセキュリティ検出を定義します。これは、脅威に関するアラートの忠実度を保証し、アラートの全体量を最小限に抑えるために役立ちます。また、このステージでは、Splunk UEBAを使用してSplunk Enterprise Securityの機能を強化します。

このステージの目標は、1.ゼロトラストに関するポリシーを強化すること、2.ユーザーがアクセス先のシステムで通常行う操作を把握すること、そして3.異常または悪質なアクティビティを示唆する行動パターンの識別方法を確立することです。

まずは、前のステージで構築した検出のユースケースを見直します。セキュリティインシデントをキルチェーンの段階に従って分類し、段階ごとに不審なアクティビティの兆候に基づいてアラートを生成できるようにします。

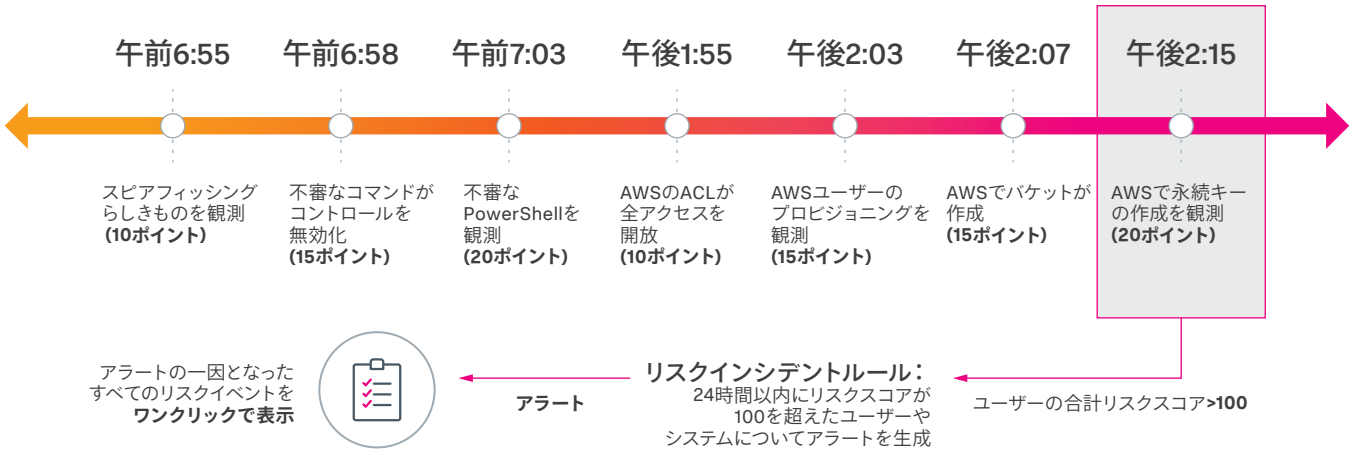
RBAでアラートの忠実度を高める

脅威の最初の兆候を検出した時点でアラートを生成するのではなく、リスクベースでアラートを生成すれば、イベントをより効率的に記録できます。リスクのあるイベントに続いて、悪質なアクティビティの兆候が検出されたら、フラグを立てます。これにより、資産やアイデンティティにリスクをもたらす一連のイベントまたはイベントのパターンを把握し、1つのアラートにまとめることができます。

下の図の例では、データ流出の前にいくつかの異常なイベントが発生しています。RBAを使用しない場合、イベントごとに個別のアラートが生成されるため、イベント間の関連性がわからなくなる可能性があります。一方、キルチェーンに沿って複数の兆候を関連付ければ、忠実度の高い単一のアラートを生成できます。

ゼロトラストのリスクベースのアラート

複数のゼロトラスト関連イベントを1つのコンテキストとして忠実度の高いアラートを生成



より高度なリスクスコア機能を導入して、アラートの優先順位の正確性を高めることもできます。たとえば、Splunk ESの標準的なリスクスコアフレームワークでは資産やアイデンティティの重要度が基準になりますが、アラートの重大度も考慮してリスクスコアを動的に決めることができます。

RBAでは、ゼロトラストを強化するためにディメンション層を追加できます。関連するユースケースには以下のものが含まれます。

- 複数のゼロトラストMITRE戦術に含まれる技法を24時間以内に検出
- 単一の戦術に含まれる複数のMITRE技法を24時間以内に検出

RBAとUEBAでは、仕組みは異なりますが、いずれも複数の兆候に基づいて不審なアクティビティや悪質なアクティビティを特定できます。これらのツールによって多くの評価基準が提供されるため、アラートの忠実度の高めると同時に誤検知の数を減らすことができます。

ユーザーとエンティティの行動分析

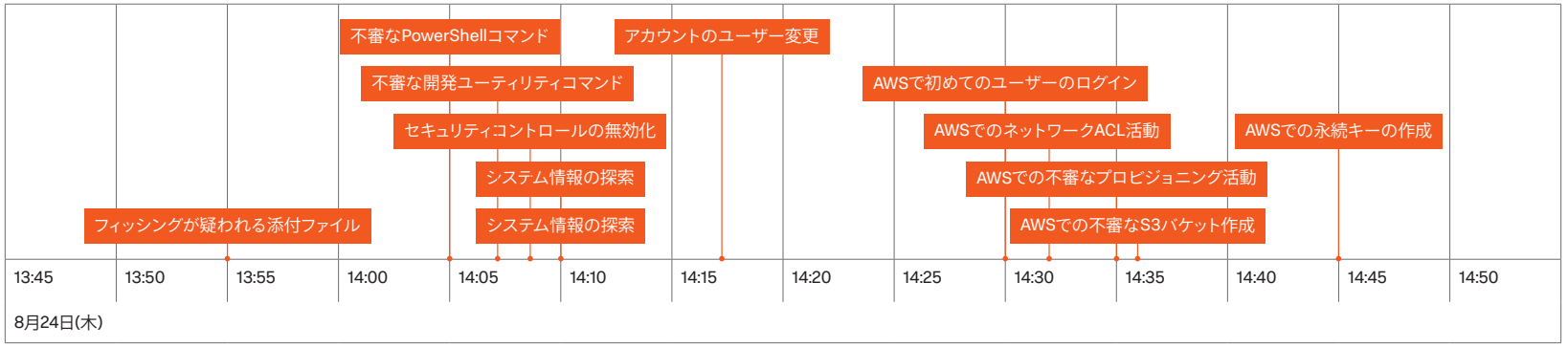
Splunk UEBAでは、教師なし機械学習により、ユーザーアクティビティ、デバイス、アプリケーションの逸脱を検出できます。多くの場合、これらのイベントは異常であっても無害です。UEBAでは、RBAと似たようなアプローチで、1つのセキュリティインシデントの段階をまたぐパターンや連続性が検出され、該当する異常なイベントが1つのアラートまたは脅威に自動的にまとめられます。

RBAの場合と同様、これによってアラートの忠実度が上がるとともに、関連するイベントをアナリストが手動で識別する手間を省くことができます。Splunk UEBAでは、行動の分析はもちろん、コンテキストを補強したり、ユーザーのアクティビティをアクセス先のシステムやデータとマッピングしたりできます。

内部脅威と高度な脅威に適用できる行動ベースのゼロトラストアプローチには以下のものが含まれます。

- ユーザーアカウントの乗っ取りによるデータ流出
- 内部者または離職リスクの高いユーザーによるデータ流出
- 高度なラテラルムーブメント
- 高度な権限のエスカレーション

RBAによるゼロトラスト脅威タイムライン



ゼロトラストの
エコシステムアプローチ

包括的なゼロトラストポリシーを実現するには、さまざまなコンポーネントを統合する必要があります。これらのコンポーネントは、一元監視に必要なデータとインサイトを提供します。

Splunkのパートナーエコシステムを活用してゼロトラスト手法を確立すれば、組織のセキュリティ体制とセキュリティ運用全体を大幅に強化できます。

このセクションでは、ゼロトラスト機能を提供するSplunkパートナーとゼロトラスト目標の達成におけるその役割をご紹介します。

Zscaler

Splunkの重要戦略パートナーであり、セキュリティ業界をリードするZscaler社は、インターネットや社内アプリケーションへのユーザーアクセスを保護するための革新的なソリューションを提供しています。Zscaler社のZero Trust Exchangeは、外部への露出を増やすことなくユーザーやアプリケーションを社内リソースと直接つなぐクラウドネイティブのプロキシアーキテクチャです。このアーキテクチャは、SSL (Security Sockets Layer)インスペクション、強力な認証、ポリシーベースの幅広い制御によって強化されています。

2つの主要ゼロトラストソリューション

Zscaler Internet Access (ZIA)：ユーザーがどこにいてもインターネットアクセスを包括的に保護します。世界150カ所のデータセンターからサービスが提供されるため、ユーザーは高速で安全なアクセスを快適に利用できます。

Zscaler Private Access (ZPA)：ローカルユーザーとリモートユーザーが従来型のアプリケーションとクラウドベースのアプリケーションのどちらにも最小限の権限でシームレスにアクセスできるようにします。ネットワークのセグメント化やリモートアクセスといった複雑な設定は必要ありません。アプリケーションは公開チャネルから隠されるため、攻撃にさらされる領域を大幅に縮小できます。

Splunkでは、すぐに使えるクラウド間インテグレーションを使って、Zscalerソリューションから高精度なテレメトリデータを取り込むことができます。これにより、クラウドとネットワークのトラフィックを可視化して、組織全体での新たな脅威の検出と対応に役立てることができます。Zscaler社が提供するAPIを使用して、Splunk SOARでZscalerプラットフォームやその他のセキュリティツール間でアクションを調整し、Splunkbaseで提供されるAppとテクノロジーアドオンを介して、ユーザーアクセスとポリシーの管理を統合することもできます。

DTEX Systems

DTEXは、世界初で唯一のワークフォースサイバーインテリジェンスプラットフォームです。エンドポイントから行動に関するテレメトリデータを収集し、動的な「悪意の痕跡(Indicators of Intent)」を特定して、組織のすべてのユーザーのアクティビティを、個人のプライバシーを守りながらリアルタイムで包括的に監視します。

複合的なスコアリングフレームワークによって、コンテキストに応じたインテリジェンスを確認、理解し、アクションにつなげることで、内部脅威やデータ喪失を防ぎ、ソフトウェア投資を最大化して、従業員を効果的に保護できます。このレベルの可視化は内外の高度な脅威に対応するために非常に重要であり、異常な行動を検出するための包括的なデータソースとしても活用できます。

SplunkbaseでAppアドオンとして提供されるDTEXとSplunkのインテグレーションを使用することで、ゼロトラスト関連の高度なセキュリティ検出と監視のユースケースを強化できます。

CloudKnox

クラウドネイティブサービスでは、新しいアイデンティティやポリシーが次々に追加されるため、異なるタイプのユーザーを管理および保護し、アクセスレベルを適切に保つことが次第に難しくなります。その結果、ユーザーは多くの権限を許可される一方、実際に使用する権限は一部に限られ、ほとんどのユーザーがリスクの高い権限の5%程度しか使用していないという状況に陥りがちです。そうなると、最低限のポリシーすら適用するのが難しくなり、組織全体のリスクが高まるだけでなく、ゼロトラストアクセスを適切に管理できなくなります。

CloudKnox Permissions Management Platformは、マルチクラウド/ハイブリッドクラウドで権限を管理および監視するためのプラットフォームです。権限の包括的な可視化、修復の自動化、継続的な監視を実現して、クラウドの重要インフラリソースとアイデンティティを保護します。CloudKnox社独自の「アクティビティベース認証(Activity Based Authorization)」技術により、単一の運用モデルですべてのクラウドのゼロトラストポリシーを一元的に管理できます。CloudKnoxプラットフォームは、VMware vSphere (オンプレミス版とクラウド版の両方)、AWS、Azure、GCPに対応しています。

CloudKnox社はSplunkのゼロトラスト分野での戦略的セキュリティパートナーであり、Splunkbaseでアドオンが提供されています。CloudKnox Permissions Management Platformは、数多くのFortune 500企業を含む世界中の企業でSplunkとともに利用されています。

Okta

Oktaは、顧客から従業員まですべてのアイデンティティを保護する、信頼性の高いクラウドネイティブプラットフォームです。1万社以上の企業がOktaのアイデンティティソリューションを使用して、ハイブリッド環境で重要なアプリケーションとデータへのユーザーアクセスを認証、認可、管理しています。もちろん、ゼロトラストアプローチに必要な重要機能もサポートされています。Oktaプラットフォームが提供するアイデンティティの認証/認可データとコンテキストは、Splunkでゼロトラストに対応したセキュリティ監視を実現するために重要なデータソースです。Splunkbaseで提供されるOkta用アドオンを使用すれば、Splunkと統合してデータをすばやく取り込み、ゼロトラスト目標の達成に活用できます。

Illumio

Illumio社は、先進的なアプローチによってセキュリティに変革をもたらしています。その優れたソリューションは、アプリケーション、接続状況、エンドポイント、ワークロードのマップを作成し、ゼロトラストのマイクロセグメンテーションを実現して、クラウド、ハイブリッド、マルチクラウド、オンプレミス環境での通信の信頼性を保証します。Splunkbaseで提供されるIllumio Appでは、包括的なネットワークセキュリティテレメトリなど、Illumioソリューションの幅広いゼロトラスト機能を利用できます。このAppでは、ITチーム、セキュリティチーム、コンプライアンスチームに役立つ高度な監視およびレポート機能も提供され、Splunkでアプリケーショントラフィックを包括的に可視化して、不審なワークロードをワンクリックですばやく隔離できます。

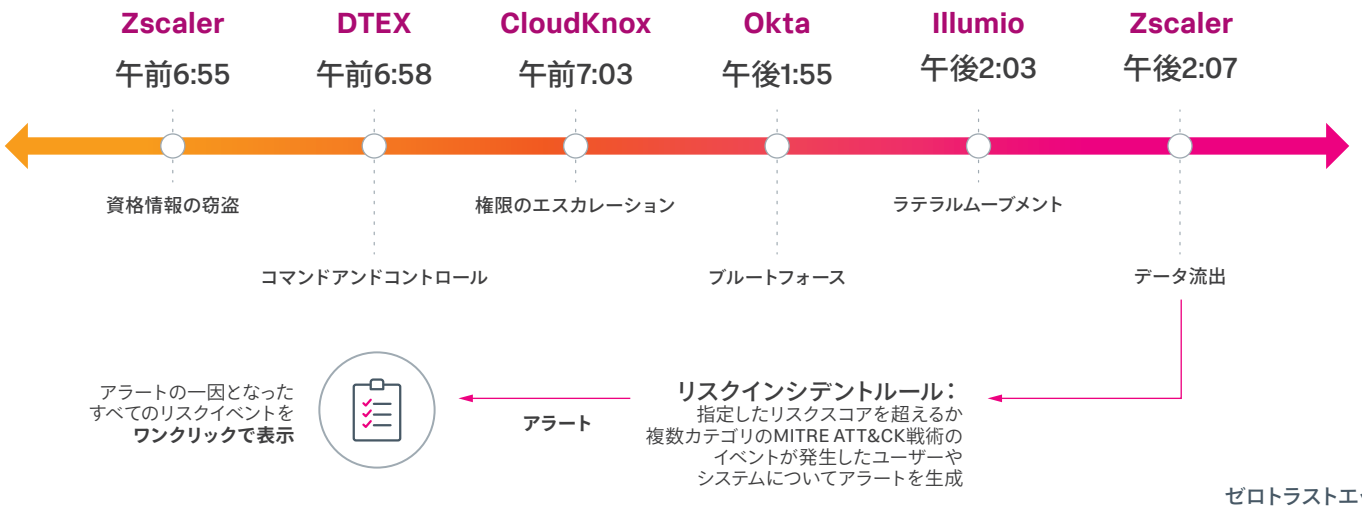
ゼロトラストエコシステムの活用例

前述のMITRE ATT&CKカテゴリとセキュリティジャーニーのステージに沿って、Splunkのエコシステムに含まれるゼロトラストテクノロジーを各種のユースケースで活用できます。下の図は、この統合アプローチで実現できるユースケースの例を示します。パートナーソリューションはそれぞれ、ゼロトラスト関連のMITRE ATT&CK戦術の検出範囲を幅広くカバーし、他のデータソースと組み合わせることで、より高い可視性を実現します。

- **初期アクセス：**Zscaler Private Accessが提供するテレメトリを使用して、保護されたアプリケーションに対する不審または異常なアクセス(盗まれるか乗っ取られた資格情報を使用したアクセス)を検出できます。
- **永続化：**DTEXプラットフォームが提供する詳細なエンドポイントデータを使用して、コマンド&コントロールへの足場を確立しようとする攻撃技法を検出できます。
- **権限のエスカレーション：**CloudKnoxプラットフォームの高度な監視機能を使用して、ハイブリッドクラウド環境で管理者や開発者の権限に対する変更(クラウド管理者の正当な資格情報の異常な使い方など)を検出できます。
- **資格情報へのアクセス：**Oktaソリューションが提供する詳細な認証/認可データを使用して、Splunkで、資格情報を不正使用している可能性のあるアクセス(ブルートフォース攻撃など)を示す異常なアクティビティを検出できます。
- **ラテラルムーブメント：**Illumioソリューションのマイクロセグメンテーションアプローチに基づいてハイブリッド環境のネットワークアクティビティを詳細に可視化することで、ラテラルムーブメントを防止するか迅速に検出できます。
- **データ流出：**Zscaler Internet AccessのWebアクティビティ監視機能を使用して、Splunkで幅広いWebサービスを対象にデータ流出の可能性のある異常を検出できます。

MITRE ATT&CK戦術の広範にわたる検出

複数のソースから複数の痕跡を検出し、RBAで忠実度の高いゼロトラストアラートを生成

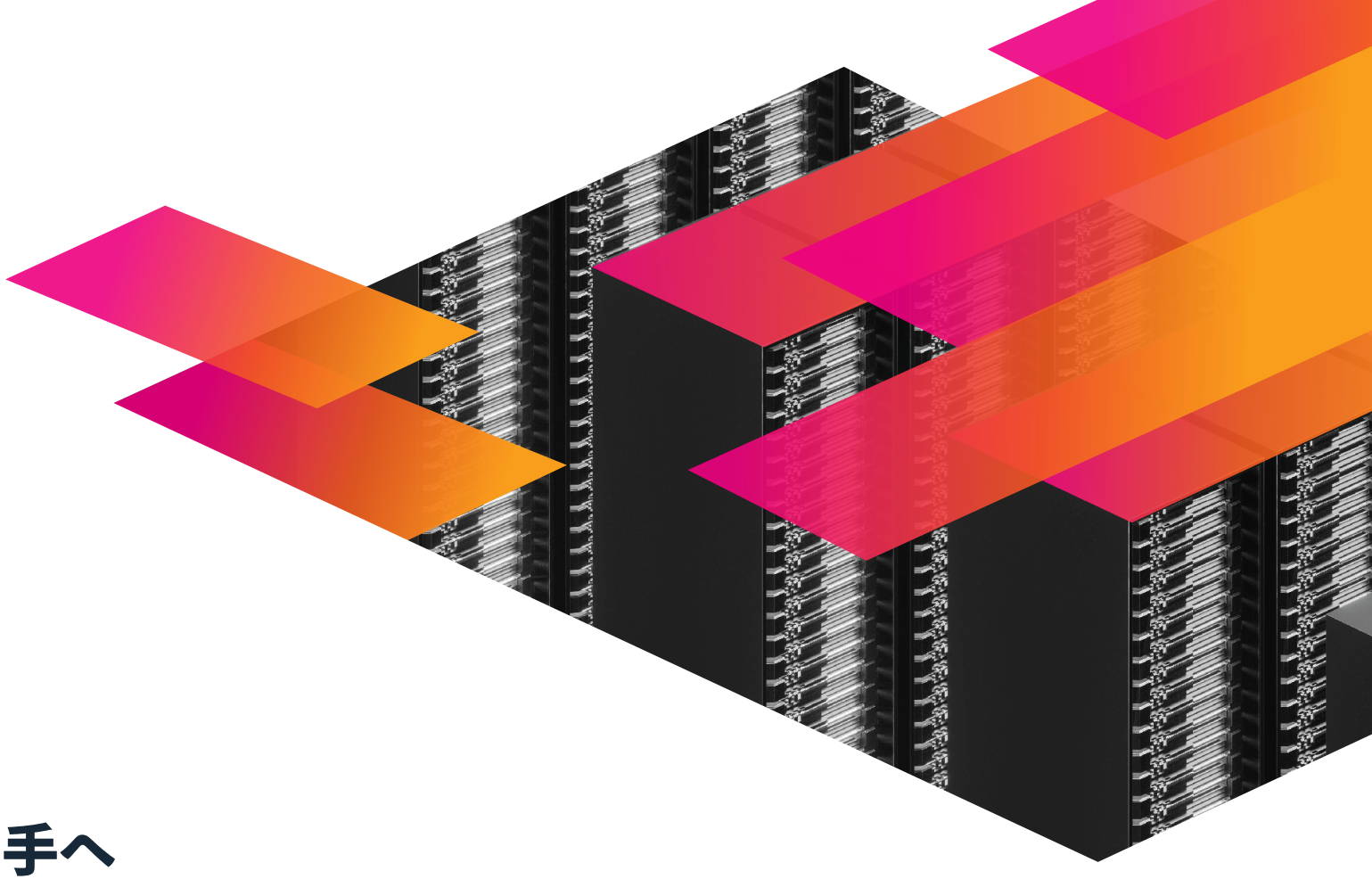


データファーストのアプローチからゼロトラストへ

これで、ゼロトラスト実現のためのジャーニーは終わりです。重要なのは、セキュリティに対するデータファーストのアプローチが、とりわけゼロトラストアーキテクチャを構築する上で、幅広いメリットをもたらす点です。

データはあらゆる戦略、特にセキュリティ戦略の成功に中心的な役割を果たします。しかし、多くの企業では、連携しないシステムや複雑な構成のせいでデータがサイロ化し、分断されています。これでは、データが持つ計り知れない価値を引き出すことは非常に困難です。

この課題を乗り越えるにはどうすればよいでしょうか?組織のゼロトラストポリシー、その役割、必要なリソースを正しく理解し、データを適切に分析すれば、データを分断する壁を取り払い、豊富なインサイトと機会を発見できます。柔軟でオープンなSplunkポートフォリオを活用して、個別に運用されていたテクノロジーを連携させ、アクションの精度を高めることで、組織全体の意思決定の質、スピード、効果を向上させ、最終的に確固としたゼロトラスト戦略を築くことができます。



Splunkで後手から先手へ

ゼロトラストジャーニーのどのステージでも、Splunkがあれば、未知の脅威と既知の脅威の一歩先を行くことができます。セキュリティ運用をモダナイズし、組織のセキュリティ体制を強化する方法について詳しくは、Splunk Security Essentialsでご確認ください。

21-18251-Splunk-The Essential Guide to Zero Trust-EB-JA-202109

splunk> turn data into doing™