可視性と分析のピラーを通じてゼロトラストの成熟度を進める

エグゼクティブサマリー

拡大し続けるサイバーセキュリティの世界では、脅威はさまざまな形で現れ、しばしば目立たないようにシステムに侵入する。侵入のリスクは常に存在するため、迅速な検知と軽減が極めて重要である。

このサイバーセキュリティ・インフォメーション・シート（CSI）は、ゼロトラスト（ZT）モデルの可視性と分析の側面を中心に、エンタープライズ全体の環境におけるデータの特性とイベントを包括的に観察することの重要性を強調している。サイバー関連のデータ分析に優先順位をつけることで、政策決定への情報提供、対応措置の促進、セキュリティ対策を積極的に強化するためのリスクプロファイルの構築に役立つ。

可視化と分析は、あらゆる ZT 戦略の礎石を形成し、組織がインフラ、ツール、データ、テクニックを活用してリスクを事前に低減し、新たなサイバー脅威を迅速に特定、検知、対応できるようにする。従来のシグネチャベースのアプローチから進化し、検知（可視化と分析）および対応機能は、現代のサイバー脅威の高度化に対抗するために、行動ベースの手法を採用するようになってきている。このピラーは、継続的なモニタリングの利点を強調し、潜在的なセキュリティリスクを特定して低減し、認可されたユーザーとデバイスのみが機密リソースにアクセスできるようにするために不可欠な洞察を提供する。

この CSI は、ZT フレームワークの中で可視化と分析を進めるための推奨事項を提示している。この CSI は、NSA の出版物「Embracing a Zero Trust Security Model」[1] に詳述されているように、これらの機能がどのように包括的な ZT フレームワークにシームレスに統合されるかを説明している。[国家安全保障システム（NSS）、国防総省（DoD）、防衛産業基盤（DIB）の関係者は、このガイダンスを補完的なリソースと併せて活用することで、概略の機能を実装することで可視性と分析を強化することができる。

序文

人間のコミュニケーションパターンを驚くべきスピードで模倣できる生成的人工知能の出現は、フィッシングの脅威を悪化させている。[2]フィッシングと効果的に戦うためには、様々な指標を掘り下げ、関連情報を包括的に把握するために必要な可視性を理解することが極めて重要である。いったんこのデータが収集されると、最初のフィッシングの試みによって引き起こされた攻撃パターンをつなぎ合わせるために、異種ソース間の融合が不可欠となる。従来の IT アーキテクチャでは、フ

ィッシング手口の動的な性質に迅速に対応することができないため、この脅威の検知に失敗することが多く、可視性と分析機能の強化が急務となっている。

研究者たちは、悪意のあるサイバー行為者の行動が衝動的で無計画であることは稀であることを繰り返し学んできた。これらの事業体は、しばしば意図的かつ計画的な方法で行動する。この概念は、MITRE® ATT&CK® の知識ベースにおいて、敵対的行動の具体的な分類法に焦点を当てて捉えられている。[潜在的な脅威を検知・識別するには、ネットワーク全体を理解し、侵入のシグナルとなり得る異常な変化を検知し、インシデントが発生した場合に迅速かつ適切に対応するために、人的要素と技術的要素の両方が必要となる。

この CSI に含まれる個々の概念は、まったく目新しいものではないが、完全なゼロトラスト（ZT） 枠組みを通じてサイバーセキュリティを支援する上で、それぞれ固有の相互依存的な役割を識別する 方法で提示されている。これらは、国防総省のゼロトラスト戦略で定義されているように、能力と活動のピラーである可視性と分析により直接的に焦点を当てながら、ZT の主要原則を支持するために協働する。[4]

想定読者

本 CSI は、主に国家安全保障システム（NSS）、国防総省（DoD）、防衛産業基盤（DIB）ネットワークを 対象としたガイダンスを提供するが、巧妙な悪意のある行為者に狙われる可能性のある他のシス テムの所有者や運用者にとっても有用であろう。システム所有者および運用者向けのガイダンスは、国立標準技術研究所（NIST）[5]およびサイバーセキュリティ・インフラセキュリティ庁（CISA）[6]を通じて入手することもできる。[このガイダンスは、国防総省のサイバーセキュリティ・リファレンス・アーキテクチャー（CSRA）バージョン 5.0、 [7]国防総省のゼロトラスト・リファレンス・アーキテクチャ（ZT RA）バージョン 2.0、[8]および本文書の末尾で参照されている国防総省のゼロトラスト戦略 [4]と互換性がある。

背景

国家のサイバーセキュリティの改善に関する大統領令（EO 14028）[9]と国家安全保障覚書 8（NSM-8）[10]は、連邦文民行政機関（FCEB）と NSS の所有者・運営者に対し、ZT サイバーセキュリティの枠組みを採用する計画を策定するよう指示している。

Embracing a Zero Trust Security Model では、ZT の概念が定義され、7 つのピラーの基礎となる原則とともに文脈化されている。ピラーは、包括的な ZT フレームワーク全体にわたって漸進的な成熟を可能にする能力で構成されている。この CSI に記述されている能力は、時間の経過とともにサイバーセキュリティの防御、対応、運用を継続的に成熟させることを意図している [1] 。7 つの

ピラーのそれぞれにおける能力の進歩は、脅威の評価と監視に基づく継続的な改善のサイクルと見なすべきである。

本 CSI は、国防総省の ZT RA 成熟度尺度である「準備」、「基本」、「中級」、「上級」に従ったガイダンスを提供する。また、ZT Portfolio Management Office (PfMO)のガイダンスである「目標」及び「上級」レベルを補完するものである。[4]

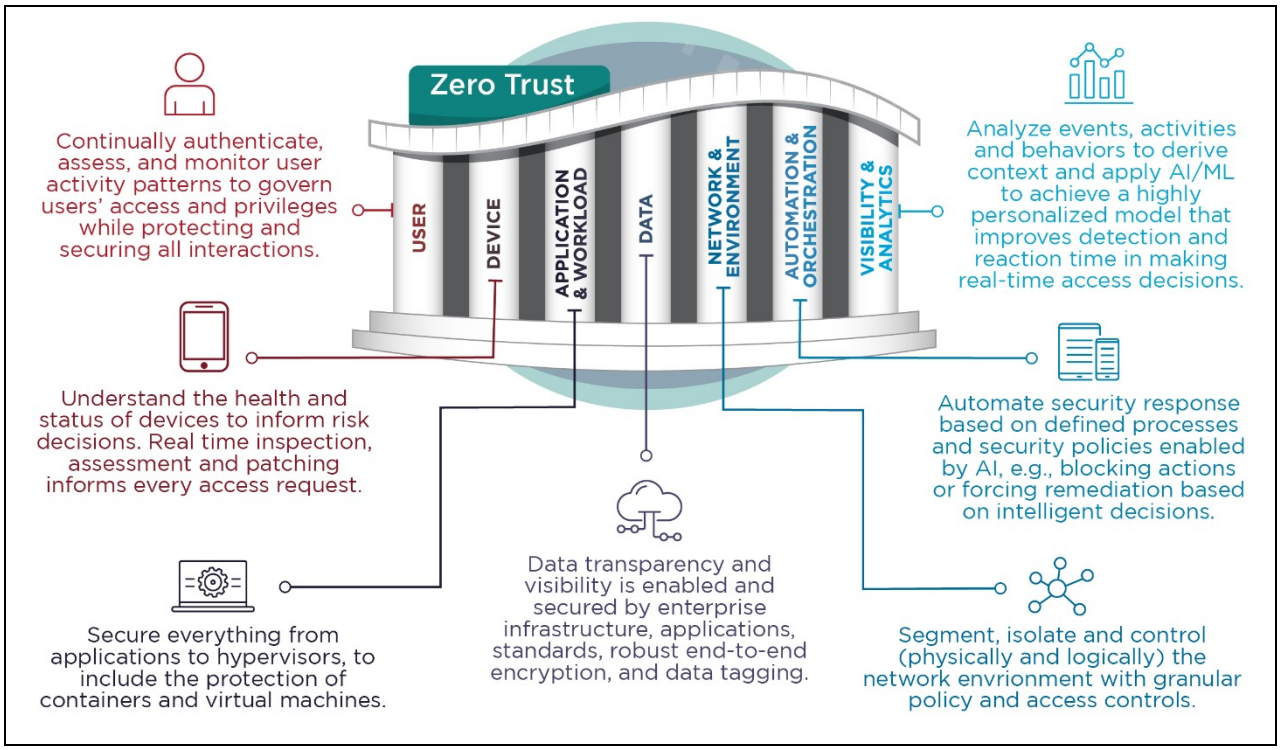

図 *1*：ゼロトラストの *7* つのピラーの説明

図 1 は、可視性と分析のピラーを含む 7 つの ZT のピラーを示している。ZT 成熟度モデルの可視性とアナリティクスのピラーの能力とマイルストーンについては、本文書を通じて詳しく説明する。ZT の 7 つのピラーは独立しているわけではなく、それぞれのピラーは他のピラーの能力に依存したり、他のピラーの能力と連携したりしている。

可視性と分析のピラー

国防総省の ZT RA によると、可視性は異常な動作の検知を改善し、セキュリティポリシーの動的な変更とリアルタイムのアクセス決定を行う能力を提供する。[NSS ガイダンスと整合するサイバーセキュリティ・インフラセキュリティ庁（CISA）のゼロトラスト成熟度モデル バージョン 2.0 は、可視性を企業全体の環境の特性とイベントから生じる観察可能な成果物としている。[ZT フレ

ームワークの「可視性と分析」のピラーは、すべてのネットワーク・コンポーネントで発生するリアルタイムのコミュニケーションとセキュリティ関連の活動を観察することによって、インフラ全体の健全性、ステータス、パフォーマンス、行動、脅威に関する洞察を提供する。このピラーは、他のピラーに必要なデータをベースライン化するために必要である。なぜなら、このピラーは、ネットワーク全体で何が起きているかの包括的な全体像を構築するために、すべてのピラーからのログ・データを活用するからである。このピラーは他のピラーに依存するだけでなく、収集されたデータをまとめて意味を持たせるために独自の機能を採用し、異常で潜在的に悪意のある活動に関する重要な洞察を生み出す。

これは、以下に詳述する主要機能によって達成される：

- 関連するすべての活動の記録
- セキュリティ情報とイベントの一元管理
- セキュリティとリスク分析
- ユーザーと事業体の行動分析
- 脅威インテリジェンスの統合
- 自動化された動的ポリシー

これらの機能により、可視性と分析のピラーを適切に実装することで、イベント、活動、行動の分析が促進され、人工知能と機械学習テクノロジーに供給して、さらに実用的な分析が可能になる。可視性とアナリティクスのピラーを成功させることで、サイバーセキュリティの脅威に対する検知と対応が迅速に行われ、脅威の探索、フォレンジック、調査の迅速化、コンプライアンス・イニシアチブのサポートが可能になる。

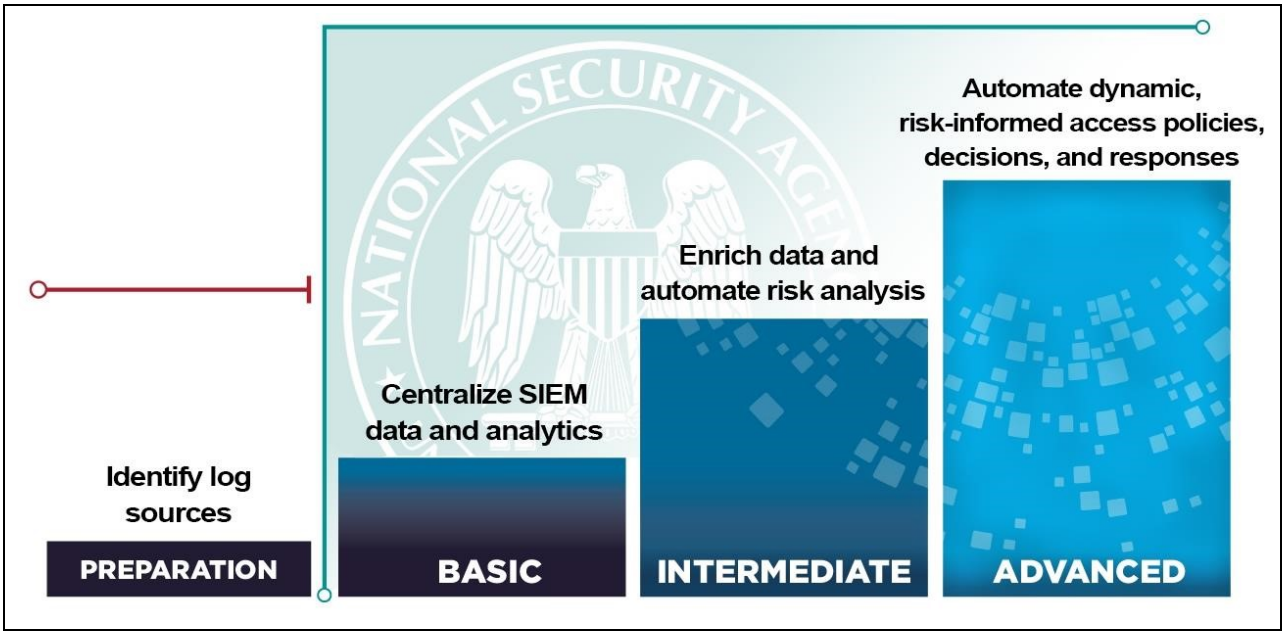

図 2：ゼロトラストの可視性とアナリティクスのピラーの成熟度

関連するすべての活動の記録

ネットワーク上で何が起きているかを理解するための最初のステップは、ネットワークデバイス（スイッチ、ルーター、無線アクセスポイント、ネットワーク監視ソフトウェアなど）、ユーザーデバイスおよびアプリケーション（オフィス製品、開発ツール、オペレーティングシステムなど）、認証サービス（使用される ID および認証情報、アカウントディレクトリ、フェデレーションゲートウェイなど）、リソースおよびデータアクセス（ファイルシステム、ホストされたサービス、電子メールサービス、ウェブサイトなど）から、関連するアクティビティログをキャプチャすることである。ログデータの量を考慮し、すべてを無差別に収集するのではなく、適切なビューポイントを優先して、環境全体で発生している適切なアクティビティのみをキャプチャする。利用可能なすべてのログソースと潜在的なログイベントを特定することから始め、関連する有用な情報を持つものを選んで取り込む。これらのログは、SIEM のような中央リポジトリに集められ、疑わしい活動や悪意のある活動の指標を分析できるワークフローにまとめられるべきである。

従来、このデータは、コンピュータ・セキュリティまたは情報技術の取り組み（例えば、運用、監査、ユーザー行動、規制遵守）において、年次アセスメントや侵入テストのようなスナップショット活動として、または必要に応じて補足的な情報源として使用されてきた。ログを通じてアクティビティを収集し理解することで、ベースラインを作成し、ネットワーク上の正常なアクティビティとは何かを決定することができる。いったん確立されれば、標準からの逸脱を調査し、その活動が

良性（偶発的な設定ミスなど）か悪性かを判断することができる。ログは収集、保存され、業界標準に従って標準化され、ネットワーク・セキュリティの目的のために継続的に分析され、ネットワーク上で何が起きているかを常に把握できるようにしなければならない。

表 *1*：関連するすべての活動の成熟度を記録する

準備	基礎	中級	上級
組織は、すべての関連するネットワーク、データ、アプリケーション、デバイス、およびユーザーのログを収集し、保存する。 ネットワークのベースラインが確立され、スナップショットが最新の状態に保たれるように更新スケジュールが設定される。	ログは解析され、正規化され、適切なネットワーク防御者やセキュリティ・オペレーション・センター（SOC）と共有される。	ハントおよびインシデント対応業務に関連するログを特定し、保存と分析の優先順位をつける。 必要に応じて追加のロギングが行われる。	ロギング活動は、新しいソースから関連するログを自動的に取り込み、フォーマットし、正規化するために自動化される。これにより、ネットワーク・アクティビティとユーザー行動のより完全な全体像が得られ、規模に応じたセキュリティ防御の自動化が促進される。

セキュリティ情報とイベントの一元管理

組織は、セキュリティ情報・イベント管理（SIEM）技術を活用して、ネットワークに関するセキュリティ情報を集約・一元化し、異なるセンサーの視点からのイベントを相関させ、データ分析を実行して、ネットワーク環境内の潜在的なサイバーセキュリティ脅威に関するアラートを生成する必要がある。SIEM は、実行可能なプレイブックを備えたインタラクティブなユーザーダッシュボード、検索クエリのための高速インデックス、脅威の前処理と検知のための高度な処理機能（例えば、スケールの大きなイベントを管理するための機械学習や高性能コンピューティング（HPC）機能）を提供することによって、このデータを管理する。SIEM の目的は、セキュリティ上の脅威を識別し、それらが組織に損害を与える機会を得る前に低減できるようにすることである。

表 2：一元的なセキュリティ情報・イベント管理（*SIEM*）の成熟度

準備	基礎	中級	上級
ネットワーク防御担当者やセキュリティ・オペレーション・センター（SOC）は、SIEM ツールに記録されたデータを手動で監視、検知、分析している。	ユーザーとデバイスのベースラインは、セキュリティ・コントロールを使って作成され、SIEM と統合される。 SIEM 内の分析とアラートが成熟し、より高度なデータポイントをサポートする（サイバー脅威インテルによるエンリッチメント、自動ベースライン比較など）。	より多くのデータが自動的に取り込まれ、処理され、分析され、異常なユーザー行動、悪意のある活動のアラート、一般的な脅威事象に対するインシデントレスポンスに関連する関連情報の収集が自動化される。	未知の脅威の行動を識別するために機械学習を使用する。 ハイパフォーマンス・コンピューティング（HPC）機能を利用することで、これまで達成できなかった規模のデータをより高速に処理する。

セキュリティとリスク分析

企業は、自社の構成、ネットワーク資産、既知の脆弱性に関する情報を使用して、自社の データとインフラに対するリスクをアセスメントする分析を開発することを目指している。リスク像は、初期のリスクアセスメントを低減する要因として、システムとデータを保護するために実装されたセキュリティ機能に関する情報を活用すべきである。リスクの見積もりは、想定されるインシデントの潜在的な影響を判断する際に、重要なファイル、重要なサーバ、重要なサービス、または高度な特権を持つユーザなど、ネットワーク内の資産の価値と重要性も考慮すべきである。共通脆弱性エクスポージャー（CVEs）、既知のエクスプロイト（ExploitDBs）、共通脆弱性スコアリングシステム（CVSS）などの外部データは、脅威環境の変化に応じて動的なリスクスコアを充実させるために活用されるべきである。

表 3：セキュリティリスク分析の成熟度

準備	基礎	中級	上級
CVE からの脆弱性、ExploitDB からのエクスプロイトなどのデー	既知の脆弱性、コンフィギュレーション情報、アセットデータを	CVE からの脆弱性情報、既知の悪用された脆弱性データ、資産情	包括的なリスクアセスメントスコアリングシステムがネットワーク

準備	基礎	中級	上級
タが収集され、CVSS スコアを作成するために使用される。	組み合わせて、シンプルなリスクアセスメントを作成する。	報、リスク低減策が分析され、ローカルに調整された CVSS スコアと、より包括的なリスクアセスメントが開発される。 初期の内部脅威リスクを評価する。	に適用され、データの機密性、資産やサービスの重要性に関する情報が含まれる。 新たな脆弱性に関する追加情報は、リスクをより適切に判断するために、権威ある情報源からかき集められる可能性がある。 自動リスクアセスメントシステムが確立されている。

ユーザーと事業体の行動分析

ユーザーと事業体の行動分析（UEBA）は、ログデータを利用してネットワーク上で発生する異常な行動を検知する。特に、通常のネットワーク活動や変動のノイズの中に隠れようとするサイバーアクターによる悪意のある行動を検知するには、単一のログソースや限られたログソースでは不十分なことが多いからである。行動分析は、基本的なユーザーパターンの分析とともに、ユーザーのピラーで最初に説明された。組織内の UEBA は、収集されたデータを利用し、従来のアプローチと機械学習（ML）人工知能（AI）アプローチを使用して、膨大なネットワーク活動を分析し、悪意のある活動を示す可能性のある異常値を抽出することで、ここでその拡張を完了する。当初、AI ベースの検知は教師あり学習で行われるが、ニューラルネットワークのような高度な技術を使えば、UEBA オペレータは学習プロセスに参加する必要がなくなるかもしれない。しかし、これらのモデルは常に確率的なものである。完全に説明できないモデルは証拠で裏付けられる必要があり、運用上の決定には常に人間のオペレーターが必要となる。

UEBA の目的は、脅威を示す異常で潜在的に危険な行動を識別することである。内部脅威の特定は、悪意のある内部関係者や、漏洩した内部関係者の認証情報を操作するハッカーを特定する上で重要な目的である。これらの内部脅威は、正当な許可を得て行動したり、ネットワーク上で認可された活動を模倣したりするため、他のセキュリティ・ツールによる気づきを逃れる能力を持っている。

MITRE のサイバーセキュリティ対策の D3FEND™分類法には、潜在的な悪意のある活動を示す可能性のある異常な行動を特定するさまざまな方法について、12 個のサブテクニックを持つユーザー行動分析[D3-UBA]という技術カテゴリー全体が含まれている。[11]

表 4：ユーザーと事業体の行動分析の成熟度

準備	基礎	中級	上級
UEBA のベースライン化とプロファイリング戦略を策定する。リスクの高い分野を特定し、具体的なユースケースを設定する。	組織はまず、ユーザーと事業体のアクティビティと行動をプロファイリングし、ベースラインを設定し、それらのベースラインを相関させて異常検知に役立てるためにアナリティクスを採用する。	異常で潜在的に危険なユーザーとデバイスの動作の脅威が自動的に識別される。	異常なユーザー、デバイス、その他の事業体の行動や高度な脅威の検知をサポートする高度な AI ベースの自動分析が作成され、使用される。

脅威インテリジェンスの統合

脅威インテリジェンスは、組織の意識を高め、脅威や脅威行為者の活動を狙ったツールや技術を開発するのに役立つ。脅威インテリジェンス情報には、脅威指標、戦術、技術、手順（TTP）、セキュリティアラート、脅威インテリジェンスレポート、ツール構成、その他の情報源が含まれる。脅威インテリジェンスは、組織が重大性と関連性に基づいてセキュリティイベントとアラートに優先順位を付け、これまで検出されなかった可能性のある潜在的脅威を特定し、AI/ML モデルの精度を高め、セキュリティアナリストの意思決定プロセスに情報を提供するのに役立つ。政府またはセクターの共有イニシアティブによる指標共有サービスや、NSA が発行するサイバーセキュリティ・アドバイザリ（CSA）、または他のサイバーセキュリティ当局によるアラートの利用を検討する。多くの勧告やアラートには、サイバーセキュリティ・ツールや SIEM で使用できる指標が含まれている。さらに、脅威情報は、最新の敵対者の TTP をネットワーク所有者に知らせ、ロギングや低減などの優先順位を設定するために、集約、変換、分析、または解釈することができる。

表 5：脅威インテリジェンスの統合成熟度

準備	基礎	中級	上級
組織は、重要な資産、既知の脅威、脅威インテリジェンスデータの利用などを組み込んだ脅威インテリジェンスの要件を定義する。	脅威インテリジェンス・プラットフォーム（TIP）が導入され、データは標準化と機械可読性のために正規化される。 SOC は脅威インテリジェンス情報とストリームを収集する。	SOC は、脅威インテリジェンス情報を組み合わせて、SIEM で収集されたデータと照合可能な ID、特性、TTP に焦点を当てる。	結果として得られた脅威インテリジェンスデータは、他の SIEM データと直接統合され、自動化された検知と対応の取り組みを強化する。

自動化された動的ポリシー

可視性とアナリティクスのピラーにある他の機能から情報を得て、組織は、これまでのルールベースのアクセスを活用して、AI/ML アルゴリズムに様々なリソースへの自動的なアクセス決定を教えることで、動的なポリシーを確立する。セキュリティ態勢の継続的なモニタリング、リスクアセスメントとスコアリング、自動パッチマネジメントは、すべてこのプロセスで使用される。

ZT の最終的な目標の 1 つは、リアルタイムのセキュリティプロファイルを使用してモデル化された動的なポリシーの自動化を確立し、それらのポリシーが変化する脅威環境と信頼度スコアに基づいて継続的に適応するようにすることである。同じことが、パッチやコンフィギュレーション・ポリシーなど、アクセス管理以外のポリシーにも当てはまる。

組織のポリシーやリスク許容度にもよるが、動的ポリシーでは、多くの場合、事前に承認されたポリシー・オプションを動的に実装することで、ポリシーの変更を承認する必要がある。

表 6：自動化された動的ポリシーの成熟度

準備	基礎	中級	上級
既存の方針が見直され、どの方針が自動化に適しているかが決定される。	AI/ML ソリューションが確立され、リスクレベルによって決定される限定されたデータセットに対して、適用さ	組織の AI/ML ソリューションは、セキュリティの継続的なモニタリング、リスクと信頼性のスコアリング、自動	実行可能で適切な場合は、自動化されたリアルタイムのセキュリティプロファイルに基づいてユーザーアクセス

準備	基礎	中級	上級
新たな脅威に対処するため、必要に応じて新たな動的ポリシーを策定する。	れるポリシーが自動化される。	パッチマネジメントを通じて、セキュリティプロファイルとデバイス構成を動的かつ自動的に更新する。	を確立する。進化する状況、リスクと信頼性のスコアに基づいて、継続的にポリシーを策定する。

ガイダンスの概要

以下は、可視性とアナリティクスの ZT のピラーに特化した関連ガイダンスの要約である：

- ログ収集計画を策定し、優先順位の高いログ（ファイアウォール、エンドポイント検知・対応、Active Directory、スイッチ、ルーターなど）を共通の SIEM に統合し、優先順位の低いログがそれに続くようにする。業界標準のオープンなログフォーマットを採用する。
- SIEM の分析・検知機能を開発する。
- 外部の脅威情報や脆弱性情報を活用し、リスクや潜在的な脅威活動の検知能力を強化・充実させる。
- これらの分析プロセスに可能な限り AI/ML を組み込んで、規模、範囲、効率を改善する。

ここで紹介する情報は、すべての組織のニーズに適合する標準的な解決策を示した決定的なガイドではなく、ZT フレームワークの中で効果的な可視化と分析を実施するための提案と考慮事項である。組織のミッションを発見・定義し、セキュリティ確保が必要なサポート資産を特定することは、ZT の 7 つのピラーの CSI における推奨事項と比較した、現状のアーキテクチャの明確なイメージを構築するのに役立つ。この比較は、すべての利害関係者が組織のリスクとギャップを特定するのに役立つと同時に、特定の組織のための成熟した ZT アーキテクチャを形成する。各組織は、ZT セキュリティ要件を評価し、どれが自組織に適用可能かを判断する必要がある。政府全体の目標は、組織の ZT 目標に沿った戦略を持つ ZT ロードマップを策定することである。

さらなるガイダンス

NSA は、ZT 機能を試験的に導入している NSS コミュニティ全体の顧客を支援し、NSS コミュニティ、NIST、CISA、DoD と ZT 活動を調整している。NSA はまた、NSS、DoD、DIB 環境の中で ZT を統合するという課題を通してシステム開発者を支援するため、追加の ZT ガイダンスの開発を支援している。今後予定されている追加ガイダンスは、エンタープライズ・ネットワークに ZT の原則と設計を組み込むことを整理し、ガイドし、簡素化するのに役立つ。

引用文献

[1] 国家安全保障局。ゼロトラスト・セキュリティ・モデルの採用。2021. https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF

[2] Z.エイモス 2024 年のフィッシング：期待されるものはこれだ。2024. https://cybersecurity magazine.com/phishing-in-2024-heres-what-to-expect/.

[3] MITRE.org.MITRE ATT&CK.2024. https://attack.mitre.org/

[4] 国防総省。国防総省ゼロトラスト戦略。https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf

[5] 国立標準技術研究所.NIST 特別刊行物 800-207.2020. https://csrc.nist.gov/publications/detail/sp/800-207/final

[6] サイバーセキュリティ・インフラセキュリティ庁.CISA ゼロトラスト成熟度モデル第 2.0 版。2023. https://cisa.gov/zero-trust-maturity-model

[7] 国防総省。DoD Cybersecurity Reference Architecture (CSRA) Version 5.0。2023 年。https://dodcio.defense.gov/Portals/0/Documents/Library/CS-Ref-Architecture.pdf

[8] 国防総省。DoD Zero Trust Reference Architecture Version 2.0.https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf。

[9] ホワイトハウス大統領令 14028: 国のサイバーセキュリティの改善。2021. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-onimproving-the-nations-cybersecurity/

[10] ホワイトハウス National Security Memorandum 8: Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems.2022. https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on Improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence community-systems/.

[11] MITRE.org.MITRE D3FEND.2024. https://d3fend.mitre.org/

推薦の免責事項

本文書に含まれる情報および意見は、「現状のまま」提供されるものであり、いかなる保証も行わない。本書に記載されている、商号、商標、製造事業者、その他による特定の商用製品、プロセス、またはサービスへの言及は、米国政府による推奨、推薦、または支持を意味するものではなく、本ガイダンスを広告または製品推奨の目的で使用してはならない。

商標

ATT&CK および MITRE は、The MITRE Corporation の登録商標である。D3FEND は The MITRE Corporation の商標である。

目的

本文書は、国家安全保障システム、国防省、防衛産業基盤の情報システムに対する脅威を識別し広 報する責任、サイバーセキュリティ仕様と低減策を策定し発行する責任など、NSA のサイバーセキュリティ 任務を推進するために作成された。この情報は、すべての適切な利害関係者に届くように広く共有されることがある。

連絡先

サイバーセキュリティレポート フィードバック CybersecurityReports@nsa.gov

サイバーセキュリティに関する一般的なお問い合わせまたはお客様のご要望：Cybersecurity_Requests@nsa.gov

防衛産業基盤に関するお問い合わせとサイバーセキュリティサービス：DIB_Defense@cyber.nsa.gov

メディアお問い合わせ / プレスデスク NSA メディアリレーション：443-634-0721, MediaRelations@nsa.gov