cloud security alliance

CSA

CISCO

公開資料

「AI の嵐」に備えてネットワークを準備する

ネットワークを堅牢化し、AI が加速する攻撃に対抗

謝辞

執筆者

Rich Mogull

グラフィックデザイン

Stephen Smith

スポンサーについて

Cisco（NASDAQ：CSCO）は、世界的なテクノロジーリーダーであり、人工知能（AI）時代の組織に導入される接続および保護の技術を変革し続けています。40 年以上にわたって世界をつなぎ安全を確保しており、AI を活用した業界最先端のソリューションとサービスを通じて、お客様、パートナー、コミュニティのイノベーション実現、生産性向上、デジタルレジリエンス強化に貢献しています。

www.cisco.com/site/jp/ja/solutions/artificial-intelligence/security-in-ai-era.html

目次

はじめに

AI モデルの進歩によって、攻撃者と防御者の関係が変化したことで、セキュリティプログラムの開発にこれまで使用してきたリスク想定が損なわれつつあります。Mythos や ChatGPT 5.5 などの高度な機能を持つモデルのリリースからもわかるように（「AI Vulnerability Storm」で詳述）、モデルは、急速に進化し、これまでにない脆弱性の発見や新しいエクスプロイトの作成だけでなく、複雑な多段階攻撃の自動実行まで行えるようになりました。この数年間の進歩から判断すれば、今日の最先端モデルの能力に、広く利用されている基盤モデルが追い付き、ローカルで動作するオープンウェイトモデルもやがて同じ能力を備えるようになると考えられます。

セキュリティプログラムの構築に基準として使用していたリスクモデルは、もはや通用しません。これまでにない脆弱性を発見したり、新しいエクスプロイトを作成したりする場合、以前は数ヵ月から数年かかっていましたが、今では数時間で済みます。こうした発見やエクスプロイトに必要とされた高度な技術スキルという壁が急速に崩壊しつつあるのです。サイバー防御の経済性も変化しています。攻撃に必要な時間やスキルが減少し、これまで防御に想定していたタイムラインが有効ではなくなったため、プログラムを見直す必要があります。

AI は、攻撃者にも防御者にも有用です。しかし、両方に同じように有効というわけではなく、「Core Collapse」で述べたように、根本的な数学的非対称性が存在しています。つまり、攻撃者は、脆弱性を発見、その問題のエクスプロイトを開発、特定の標的を攻撃などのように、1 つの問題に注力できる一方、防御者は、常に、あらゆる攻撃者、あるいはあらゆる潜在的エクスプロイトから、すべてのリソースを保護しなければならず、それらが組み合わさった複雑な状況に直面しています。

この点は、1 件の脆弱性が新たに公開されたときの影響を考えれば簡単に理解できるでしょう。攻撃者は、AI を利用してエクスプロイトをすぐに開発し、自動化した攻撃を開始できます。防御者は、パッチを入手したとしても、適用が必要なリソースをすべて特定しテストしたうえで展開しなければならず、稼働中のアプリケーションも停止できません。高い技術力があったとしても、異なる物理法則に基づいて競争しているようなものです。

こうした不均衡をなくすために有効な既存の戦略があります。今後、新しいソフトウェアは、すべて、リリース前に LLM を使用して評価および堅牢化されるため、ソフトウェアに存在する脆弱性の全体数は減少すると予測できます。さらに、今日では、セキュリティ境界を追加して、攻撃の成功までに突破が必要な壁を混在させ、さらに複雑にすることも可能です。

AI を活用する攻撃者に対抗可能なレジリエンスを構築するには、技術のさまざまな側面を考慮しなければならず、その規模は、セキュリティチームが自力で管理できる範囲をはるかに超えています。アイデンティティから、ワークロード、コンテナ、API、エンドポイントに至るあらゆる領域で、セキュリティを確保する壁を増やす必要があるからです。

ネットワークは、こうした境界を配置するうえで、最も重要なツールの 1 つと言えますが、ほとんどの本番環境ネットワークのセキュリティ、設計、運用モデルでそうした境界が十分には設定されていません。高度化や投資が長年行われてきたにもかかわらず、現在もフラットなネットワークが非常に多く、古いハードウェアへの依存が見られることも少なくありません。ネットワークの運用プロセスとセキュリティプロセスも、迅速な対応や自動化がすぐには行えない状態にあります。ファイアウォールのルール変更といった単純な作業でも、ネットワークが複雑な場合、数週間から数ヵ月かかる可能性があります。

攻撃者が突破する必要のある複雑さ（と攻撃にかかるコスト）を増大させるには、ネットワークに以下が求められます。

- すぐにパッチ適用の頻度を上げ、継続的に適用を行います。
- 影響範囲が縮小されるよう、ネットワーク セグメンテーションを改善し、価値の高いデータの公開場所を限定します。
- 複数の境界の突破が必要となるよう、複数の防御層を、並列ではなく直列に追加します（単一のアプリケーションスタック内の異なる層に複数のファイアウォールを配置するなど）
- 応答性の高い運用プロセスを基盤にし、脅威環境の変化に迅速に適応できるようにします。

高度な AI 機能を防御目的で使用すると、AI に長けた組織は、最終的に、エクスプロイトの開発スピードに耐えうる競争力を持つようになります。それまでの間、セキュリティ境界は、攻撃を遅らせ、展開の更新に必要な時間を確保するためのツールとして機能します。

このホワイトペーパーでは、ネットワークおよびセキュリティの管理者にガイダンスを提示します。ネットワーク防御だけでは、レジリエンスの新たな要件に対応することはできません。しかし、ネットワークセキュリティの境界を増やすことは、最も効果的な出発点の 1 つと言えます。

ネットワーク モダナイゼーションによる対応型防御

私たちの業界では、10 年以上にわたり、ネットワークのモダナイゼーションが進み、境界防御が改善され、ネットワーク セグメンテーションも強化されてきました。そうした動きは、この数年間、さらに加速しており、クラウドへの移行によって、ますます顕著になっています。なぜなら、クラウドネットワークはデフォルトでソフトウェア定義型であり、ソフトウェア定義型ネットワークの場合、境界とセグメンテーションの作成と変更がはるかに簡単になるからです。

しかし、こうしたネットワークの大規模な更新では、現実的で当然起こり得る課題が生じました。ほとんどではないにせよ、物理ネットワークの多くは、内部が比較的フラットな状態にあります。クラウドネットワークは、柔軟性に優れ、セグメンテーションが容易で、常にソフトウェア定義型の技術が使用されますが、必ずしも、ほかより優れているとは限りません。その主な要因は、古いデータセンター設計をコピーしたリフトアンドシフト移行が行われていることにあります。ゼロトラストの導入では、非常に多くの場合、従業員とキャンパスエッジの保護が重視され、データセンターやアプリケーション間（水平方向）のトラフィックの保護はあまり重視されていません。必ずしもネットワークが自社で所有、管理されているとは限らず、サードパーティのオブザーバビリティにも制限があります。

多くの組織で、マイクロセグメンテーションが開始されましたが、通常、その適用は、ネットワークのごく一部に限定されていました（実装が複雑であるため）。また、ハードウェアの多くが古く、それらの更新には時間も手間もかかっています。運用プロセスは、意図的に慎重に行われてきました。境界の外側については、内部ネットワークへの迅速なパッチ適用は求められなかったため、このプロセスでは、エッジが重視され、内部ネットワークへのパッチ適用は、はるかに遅いペースで進められています。

いずれの対応も間違っておらず、直面しているリスクへの合理的な対応です。このホワイトペーパーで紹介している推奨事項のほとんどはよく知られており、現在も運用されています。問題は、AI によってリスクとタイムラインが変化していることです。こうした境界だけでなく、社内ネットワークの障壁もセキュリティ境界の拡張として重要な役割を果たすようになり、攻撃者の AI の優位性を抑制するために不可欠なものとなりました。フラットなネットワークの場合、何らかの侵害が生じると、その影響は広範囲に及びます。時間をかけ慎重に変更を行っていては、数時間で終わるエクスプロイト開発に追い付けず、パッチをすぐに適用できないハードウェアは、ファイアウォールの内側にあっても、かなり大きなリスク要因となります。

幸いなことに取るべき対策はわかっているものの、その実行方法が新たな課題となります。必要なのは、迅速なアクションです。なぜなら、これまでの優先順位やスケジュールを決定する際に基準としてきたリスク想定が通用しなくなったからです。ネットワークセキュリティの基礎であるセグメンテーション、パッチ適用、応答性の高い運用は、不均衡の修正に効果がありますが、今後はそれらの粒度を高め、優先度順に厳しいスケジュールで実行しなければなりません。

こうした問題に対処するには、ネットワークの設計、運用、セキュリティを担当する各チームの連携も必要です。このソリューションは、組織をまたいでいるため、基本的なアーキテクチャ、パッチ適用、脆弱性管理に加え、セキュリティに特化した防御策（NGFW、WAF など）も同時に考察する必要があります。以降は、モダナイゼーションの構成要素を取り上げ、それを達成するためのフェーズについて説明します。

構成要素とプロセス

敵対的な AI リスクに対応するネットワーク モダナイゼーションは、次の 3 つで構成されます。

- **運用モデルと運用プロセス：**以前はまず、機器の配線を行い、変更の少ない IP アドレスを保護していたため、ネットワークプロセスと、そのセキュリティプロセスは慎重に行われる傾向がありました。特に、ハードウェアの更新や構造上の変更にそうした傾向が見られますが、こうしたプロセスは、物理的な依存関係が存在する環境向けに構築されたものです。パッチ適用について言えば、エッジに重点が置かれ、内部のハードウェアはリスクが低いという理由で後回しにされていました。ネットワークのほとんどに 1 層または 2 層の防御が実装され、インターネットの脅威から防御するために、垂直方向のトラフィックが重視されました。クラウドは、ダイナミックであるものの、成熟度、リフトアンドシフトへの依存、ハイブリッドの依存関係によっては、不均衡の要因となります。また、定期的なプロジェクトから継続的な運用への移行も見られるようになりました。これは、パッチの適用や更新だけではなく、セグメンテーションにも言えることです。つまり、一度展開して終わりではなく、構築時に境界を追加し維持するようなアーキテクチャを形成します。次の 2 つのループを並行して行う運用と考えるとよいでしょう。
    - **ネットワークにパッチを適用し、最新の状態にする**：ここでの目標は、継続的なパッチ適用と、優先順位を付けた更新です。そうすれば、修復不可能なものを防御し続ける必要がありません。ネットワークデバイスへのこうした運用は、これまで非常に困難でした。そのため、これを新しい運用プロセスとして扱い、外部から見えるリソースにまず対処することをお勧めします。これは、VulnOps プログラムに統合可能であり、統合が必要な運用でもあります。詳細は、前述の「Vulnerability Storm」レポートで説明していますが、VulnOps では、継続的な自動化によって、脆弱性管理を DevOps スタイルのプログラムのように扱います。

    - **セグメンテーションおよび分離の方法を更新する**：マイクロセグメンテーションに移行し、アプリケーションの変化に応じて、複数の境界（水平方向、垂直方向）を継続的に追加、維持し、トポロジとセキュリティ防御の両側面からそれらを実装します。

- **インフラストラクチャ**：ネットワーク自体が標的にされています。ネットワークハードウェアおよびソフトウェアの脆弱性とエクスプロイトは今後も増加し、自動攻撃への利用が続くと予想されます。こうした攻撃はすでに発生しており、このホワイトペーパーを執筆していた数週間の間に、ネットワーク インフラストラクチャを標的にした攻撃が複数見られました。ネットワークでは次の状態を維持する必要があります。
    - **最新**：サポート終了の状態になく、現在もサポート対象のハードウェアを更新する。
    - **パッチ適用可能**：ハードウェアの更新だけでなく、パッチ適用プログラムへの統合も行い、数週間ではなく数時間以内に更新可能な状態にする
    - **ソフトウェア定義型**：クラウドの例を見るとよくわかるように、ソフトウェア定義型ネットワーク（SDN）は、アジリティに優れ、多くの場合、デフォルトですべてのアクセスを拒否します（ソフトウェア定義型境界（SDP）などのプラットフォームによって異なる）。セグメンテーションは、後付けではなく、既定で実装されます。
- **アーキテクチャ**：アーキテクチャによって、攻撃時に複雑さとコストが増大するよう、境界を定義します。必ずしも、各資産の全レベルに今すぐファイアウォールを配置する必要はありませんが、以下の要素を使用して構築します。
    - **境界セキュリティ**：一般的に最も効果があり、今後も必要な対策です。しかし、これまでよりも継続的な運用モデルに合うよう変更しなければならず、状況によっては、プラットフォームの多様性と、境界セグメンテーションの強化が必要な場合もあります。
    - **マクロセグメンテーション**：これにより、ビジネスユニット、アプリケーションスタック、運用環境のセグメンテーションを強化します。その目的は、攻撃の影響範囲がネットワーク内の単一「スタック」に限定されるようにすることです。
    - **マイクロセグメンテーション**：アプリケーションスタックのレイヤ内に境界を追加すると同時に、アプリケーションとサービス間の境界数を増やします。
    - **ゼロトラスト**：そうした境界と、アイデンティティおよびコンテキスト認識型ポリシーを組み合わせ、それらを常に検証することで、ネットワークの場所ではなくリクエストごとにアクセスを許可します。信頼は、IP や VLAN によってではなく、ダイナミックに判断し、最小権限を付与します。また、トポロジではなくアイデンティティとリスクに関連付けます。これには、ソフトウェア定義型境界（SDP）などの技術が含まれます。

そうしたすべての要素の基盤となるのは、可視性（ネットワーク上の各要素、その存在場所、設定状況などの把握）と属性（各要素の所有者や、ビジネスまたは技術上の判断を下す責任者などの特定）であり、さらにリアルタイムのテレメトリが可能であれば理想的です。こうした推奨事項を実現するうえで

の複雑さは、重々承知していますが、最新技術によって、それらは達成しやすくなっており、特にプロジェクトごとの実現可能性が高まっています。

防御側でも、AI ツールを活用して、継続的なテストおよび改善を行えます。たとえば、自社ネットワーク上の社内 LLM をポイントして（安全な）アセスメントツールを持たせ、その結果を使用して、攻撃側から見た強みと弱みを把握します。

こうしたどの対策にも、時間がかかり、場合によっては数年が必要です。一方で、AI を活用した敵対的な攻撃はすでに始まっています。段階的で優先順位を付けた、リスクベースのアプローチを推奨しているのはそのためです。この方法なら現実的で、目に見える成果をすぐに得られ、長期目標を達成するための強固な基盤も形成できるでしょう。

重要なポイント：以下のフェーズは、継続的な運用プロセスの一部として、並行して実行できます。次のフェーズに進む前に、1 つのフェーズを完了する必要はありません。

フェーズ 1：優先順位付け、的を絞った更新、堅牢化

攻撃は、到達可能な範囲から開始されます。防御側としては、侵害された場合の最も大きな損害に注意を払う必要があります。そのため、最初のステップは、外部の攻撃対象領域を特定し、組織の優先事項と紐付けることです。

このフェーズでは、「外から内に向かって、重要なアセット優先」で考察を進めます。最初に、インターネットに面した攻撃対象領域を判断し、クラウンジュエル（最重要デジタル資産）を特定します。攻撃対象領域の特定では、該当領域をすべて洗い出してください。セキュリティおよびネットワークのデバイスとサービスを含め、すべてのデバイスとサービスを確認します。インターネットに接続され、外部から到達可能と思われるあらゆる要素のほか、VPN サーバー、リモートオフィス、エッジルータ、クラウドベースの仮想セキュリティアプライアンスといった資産も忘れてはなりません。

重要なデジタル資産、つまり「保護対象領域」は、データ侵害や破壊的な攻撃を受けた場合にビジネスに最も大きな損害が及ぶアプリケーションやサービスを指すことになります。こうしたサービスには、接続とデータフローを包括的に示すマップが必要ですが、その作成は、多くの場合ビジネス部門への確認を伴うため、ネットワークチームとセキュリティチームだけでは内容を決定できません。

次に、相互の関連付けを行います。特定の重要な資産について、外部から内部に向かう 1 つの経路上にどのようなネットワークデバイスが配置されているかを確認します。これには、ファイアウォール、WAF、ルータ、スイッチ、VPN（これも重要な要素です）などがすべて含まれます。次の表を使用して、取るべきアクションを決定しましょう。

ステータス	推奨アクション
サポートが終了している（EoL）	ハードウェアを更新する（完全に交換）
サポートが延長されている	可能な限り早く交換する
最新のパッチが適用されていない	ただちに、パッチを適用する
HA 構成で展開されていない（物理または仮想）	HA ペアを追加して、ダウンタイムなしでパッチを適用する
プロセスまたはハードウェア/ソフトウェア上の制約により、リリース当日にパッチを適用できない	リリース日にパッチ適用が可能な VulnOps プログラムに当該デバイスを追加するか、リリース日にパッチ適用が可能なハードウェアに更新する

こうしたすべてのデバイスに取るべきアクションは、ほかにもあります。先ほどと同様、これらが、容易でないことは認識しています。しかし、非常に価値ある防御策であり、実際に使用されている複数の攻撃手法を防ぐのに有効です。

- 管理上の操作には少なくとも MFA を求めます。また、管理者には PAM によるブローカリングを行うことが理想的です。
- インターネットまたは DMZ に公開されている管理インターフェイスを無効にします。デバイス、SDN コントローラ、その他の管理ステーションへの管理アクセスも無効化の対象にし、信頼できないネットワークからのトラフィックはすべて拒否する必要があります。
- 出力トラフィックをフィルタリングします。これにより、コマンドアンドコントロールが実行された際のコールバックの可能性を減らすことができます。IP だけでなく、DNS ベースのフィルタリングも行うようにしてください。
- ネットワーク/セキュリティ管理に関わる自動化スクリプトやコードを使用する場合は、これらを評価し、シークレットが埋め込まれていないかを確認します。また、LLM を使用してセキュリティ上の不備がないかを評価します。
- インターネットに面したすべてのアプリケーション（デバイス、仮想デバイス、クラウドサービスなど）の前に WAF を配置します。

この 1 つ目のフェーズでは、既存のリソースを堅牢化し、今後も最新の状態を維持できるようにすることに重点を置いています。最も侵害される可能性が高い、高リスクのネットワークおよびセキュリティツールは排除します。攻撃のエントリポイントになったセキュリティ境界は無意味だからです。

二重の防御：OT ネットワークと重要度の高いネットワークを保護する

運用技術/産業用制御システムでは、一定サイクルでのパッチ適用は、難しいか、まったく行えない場合があります。OT は、これまで、独立した環境に置かれていましたが、数十年間で、IT ネットワークとの接続が増え、インターネットからのルートも開拓されています。こうしたシステムは、重要なインフラストラクチャであり、格好の標的とされますが、AI による脆弱性の発見、エクスプロイト、攻撃を防御する機能をあまり備えていません。

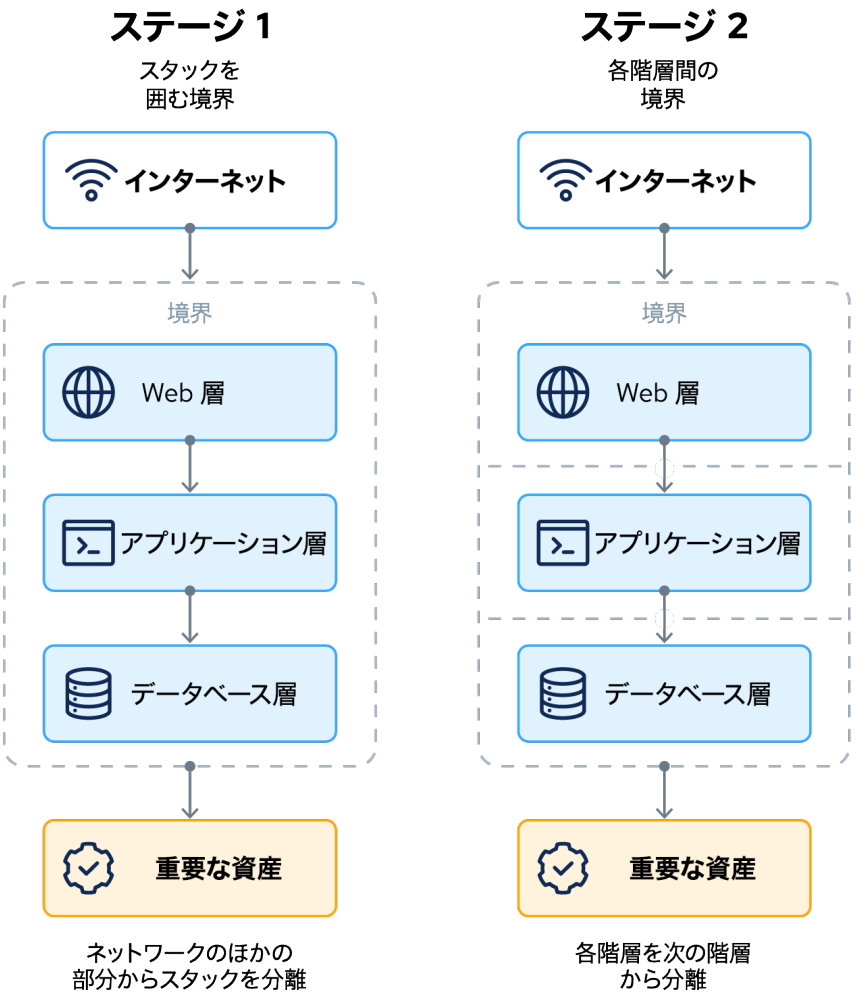
これらのネットワークは、インターネットに向かうすべてのルートから切断する必要があります。それが不可能な場合は、通信を一方向に限定する技術（データダイオードなど）によってテレメトリを収集します。それも不可能な場合は、最新状態に保たれ、ベンダーが異なる複数の次世代ファイアウォールを通信経路上に配置します。これにより、OT ネットワークに侵入しようとする攻撃者に複数のゼロデイエクスプロイトを強いることになります。

フェーズ 2：優先順位付けされ、焦点が絞られた境界の追加

フェーズ 1 では、既知の資産を堅牢化し、パッチを適用できない、または AI 主導のパッチ適用のペースに対応できない古いハードウェアとソフトウェアを排除することに重点を置きました。フェーズ 2 では、まず、セキュリティ境界を追加して、攻撃を防げるよう障壁の混在による複雑さを高め、成功した攻撃の影響範囲が縮小されるようにします。

最初のステップでは、実質的に、マクロセグメンテーションを行います。スタックを分離することで、同じネットワーク上にあり、あまり価値がなく、防御策が手薄なリソースが侵害されても、それが、優先度の高いスタックに容易に到達可能な経路とならないようにします。適用できるネットワーク手法は複数あり、たとえば、ファイアウォールの追加、サブネットおよびルートの分離、分離された仮想ネットワークへの移行、SDN 制御を使用した障壁の作成、ゼロトラストへの移行などが挙げられます。
フェーズ 1 で垂直方向の上（インターネット）から下への攻撃に対し堅牢化が済んでいるなら、水平方向の攻撃からの分離を最優先にしてください。

ホスト内のツールを使用して分離する場合、ツールは低レイヤ（理想的には、オペレーティングシステムの外部（ハイパーバイザ））で動作する必要があります。または、堅牢化した外部管理型エージェントを使用します。これにより、当該ホストへの侵入者によってネットワークセキュリティを無効化されないようにします。



2 番目のステップでは、通信経路上に追加のセキュリティ境界を設けます。このステップはさらに時間がかかり、新しい技術が必要にもなるでしょう。これまでのステップでは、侵入しやすい経路の削減に焦点を当てていましたが、このステップでは、実際の攻撃に必要なコストを増大させます。アプリケーションの各階層は、想定されているポートおよびプロトコルのみを介して、上位と下位の階層とのみ通信する必要があります。これに最適な選択肢は SDN です。しかも、このパターンは、多くの場合、クラウド環境や完全仮想化環境に、かなり簡単に実装できます。

フェーズ 3：拡張と高度化

フェーズ 1 と 2 では、最も重要な資産を迅速に保護することに焦点を当てています。つまり、古いハードウェアやソフトウェアの交換、あらゆる要素の最新状態の維持、防御策が手薄なリソースからの分離を行ったほか、セキュリティ境界を増やし、攻撃時のコストおよび複雑さを増大させました。しかし、これはネットワークとセキュリティの観点から不均衡に対処したにすぎません。CSA の「AI Vulnerability Storm Ready」のガイダンスに従うとすれば、それらと同様に重要で、並行して実装すべき対策がほかにもあります。

フェーズ 3 では、こうした防御策をほかのネットワークに拡張して高度化します。理想的には、フラットネットワークから、マクロセグメンテーション、マイクロセグメンテーション、ゼロトラストへと移行します。最善策は、ゼロトラストに直接移行することですが、短期間での完了は難しいでしょう。マクロセグメンテーションでは、まず、事業部門とトラストゾーンの間に障壁を設けます。

マイクロセグメンテーションでは、個々のワークロードとサービスに至るまで、境界を設定し、それぞれにとって実際に必要な通信のみ行うようにします。これを、大規模に行う場合、時間もコストもかかる可能性があるため、一般的には、プロジェクトごとに実装します。これには、何年もかかる可能性があり、どのような変更にも、実際のフローや依存関係のマッピングが事前に必要となりますが、実装を急ぐと本番環境に支障をきたす恐れがあります。

CSA では、マイクロセグメンテーションをゼロトラストの一部と定義していますが、これらは異なる概念であるものの多少の重複はあると考えるネットワークやセキュリティ管理者もいます。マイクロセグメンテーションは、最初にネットワークのみへの実装、次に資産やアプリケーションごとの分離といった順に進めることができます。その後、ゼロトラストを実装し、アイデンティティとコンテキストに基づいて接続許可を判断することも可能です。

ゼロトラストでは、これらをすべて一体化させます。境界を細かく設定し、ネットワークの場所ではなくワークロードとアイデンティティに基づくポリシーを設定したら、接続ごとにアクセスを許可するようにします。これが、攻撃者を阻む強力な障壁として機能します。その効果は、クラウドで実証済みです。チョークポイントには常に注意が必要です。アイデンティティ プロバイダーなどの統合コントロールポイントは、あらゆるネットワーク要素から信頼されるため、高価値な標的になります。つまり、これには、厳格な監視とより多くの境界が必要です。

このフェーズできわめて重要なのは、技術的な管理プロセスおよび管理インターフェイスを綿密に調査することです。ネットワークには、パッチ適用だけでなく、定期的なアップデートが必要であり、管理インターフェイスは格好の標的となります。

どのフェーズにも終わりはありません。これが重要なポイントです。1 つのフェーズが完了すれば、AI 主導の攻撃に耐えうるネットワークが実現するわけではなく、その実現には、継続的なセグメンテーション、パッチ適用、可視化が必要です。これにより、どの新規アプリケーションも境界が設定済みの状態で出荷できるようになります。新たなエクスプロイトが発生するたびに、防御側以上に攻撃側にコストがかかるネットワークがそれらの障壁となるのです。インシデントは今後も発生するでしょう。しかし、ネットワークテレメトリを改善することで、インシデント対応チームも強化されます。

困難な移行を乗り越え、明るい未来を手に入れる

このホワイトペーパーで示した手法は、いずれも新しいものではありません。しかし、その実装の規模、範囲、タイムラインが、これまでの運用とは異なっています。ここで取り上げた概念や技術は、すべてセキュリティの基本原則であり、その多くは、さまざまな環境で防御の効果を試されたものです。しかし、ネットワークとセキュリティの専門家である私たちは、常に摩擦とリスクのバランスを取る必要があります。セキュリティ上の管理を追加すれば、コストと複雑さが増し、ビジネスの一部に遅れが出ることもあるでしょう。ここでの推奨対策は、必ずしも簡単ではなく、無償で提供されることもありませんが、ほかに選択肢がないため、実行するしかありません。

現在のプラクティスを構築する際に行う基本的なリスク想定が、AI の影響で変化しています。たとえば、スキルがあまりない攻撃者でも、AI を活用すれば、優秀なバグハンターやペネトレーションテスターに近い高度な操作を行えるようになりました。もはや、エッジのパッチ適用に数週間から数ヵ月をかけたり、何年もかけて内部インフラストラクチャにパッチを適用したりはできません。社内のアーキテクチャは複雑なためあちこちに侵入されることはない、あるいは、パッチ未適用でも 1 ヵ所の分散拠点でしか使用されない VPN サーバーは狙われないため安全、などとは想定できなくなっています。

現在のところ、計算上は攻撃側が有利かもしれません。しかし、優位さの不均衡を修正するための道すじは明らかです。攻撃側と同等の AI 機能をソフトウェア開発とセキュリティ評価に全面的に統合すれば、結果的に、リリース前のソフトウェアの安全性が本質的に高まります。さらに、ネットワークのモダナイゼーションを行い、ゼロトラストを推進するなかで、突破が必要なセキュリティ境界の数を増やし、コストと複雑さを増大させます。継続的にパッチ適用と更新を行えば、攻撃活動に適した時間も短縮できます。

以上の組み合わせこそ、計算上の優位さを取り戻す手段であり、わずかな変更であっても、大きな効果を得られる可能性があります。具体的には、運用モデルを更新して応答性を高めるとともに、VulnOps を統合します。また、最も重要な資産を最初に保護するよう注力します。ハードウェアとソフトウェアを常に最新の状態にし、それらのパッチはリリース当日に適用できるようにします。可能な限り SDN に移行します。SDN は、セグメンテーションの実装と管理が非常に容易なため、ほとんどの仮想ネットワークとクラウドネットワークに導入されています。次に、水平方向のセグメンテーションによって個々の

スタックを分離します。さらに、通信経路上の垂直方向の境界を増やし、最終的な到達点であるゼロトラストと SDP を実現します。

ゼロトラストを実現するか、ゼロデイに甘んじるのか、選択を迫られています。

AI 時代に成功する組織とは、脆弱性をすべて排除した組織ではありません。勝者となるためには、エクスプロイトされうる未対策領域を継続的に減らし、それらの悪用を未然に防ぎます。さらに、時間稼ぎのための障壁を配置し、攻撃コストを増大させます。攻撃対象領域の縮小、対応の迅速化、セキュリティ境界の追加を組み合わせた対策こそが、真のレジリエンス実現につながるのです。