エクスポージャー管理準備体制のチェックリスト

エクスポージャ管理は、効果的に組み合わせることで、多くの組織がすでに投資しているさまざまな機能を活用します。その結果、あなたは自分が思っている以上にエクスポージャ管理の取り組みを進めている可能性があります。

このチェックリストでは、エクスポージャー管理に含まれる製品カテゴリーと、それらが提供するコア機能の概略を説明しています。可視性、優先順位、検証、修正の4つのカテゴリーに整理されたこのチェックリストは、サイバーセキュリティの技術スタックにすでに備わっている関連機能を説明し、どこにギャップがあるかを特定するのに役立ちます。

リストアップされている製品タイプの多くは複数のカテゴリーに当てはまっており、各項目にはその旨が記載されています。

可視性

サイバー攻撃者があなたの環境に侵入するには、たったひとつの盲点があれば十分です。このセクションのテクノロジーは、アタックサーフェスを構成するすべてのサイバー資産、エクスポージャー、その他の要素を可視化するものです。なお、このセクションに記載されている技術をすべて導入する必要はないことにご留意ください。一部の機能は重複する特徴を持っています。また、あなたの環境には関連性のない機能も掲載されている可能性があります。必要なのは、むしろ、アタックサーフェスを完全に可視化できる、適切な組み合わせを見つけることです。

IT資産の検出

可視性	**X**
優先順位付け	
検証	
修復	

これらのツールは、組織のIT環境内のハードウェアおよびソフトウェア資産を自動的に識別し、インベントリを作成します。しかし、特定のタイプの資産を検出しにくいツールも存在するほか、エクスポージャーを検出するように設計されていないツールもあります。このため、アタックサーフェスを包括的に可視化するにはその他のツールも必要となります。

統合エンドポイント管理 (UEM)

可視性	**X**
優先順位付け	
検証	
修復	**X**

UEMツールは、ITチームがデスクトップ、ラップトップ、モバイルデバイス、その他のインターネット接続デバイスなどのエンドポイント環境を包括的に理解し、各エンドポイントを管理、設定、保護するのに役立ちます。

モバイルデバイス管理 (MDM)

可視性	X
優先順位付け	
検証	
修復	X

MDMツール (ここでは「モバイルデバイス管理」の略) は、スマートフォンやタブレットなどのモバイルデバイスの検出と管理に特化したUEMツールです。

モダンデバイス管理 (MDM)

可視性	X
優先順位付け	
検証	
修復	X

このタイプのMDMツール (ここでは「モダンデバイス管理」の略) では、他のタイプのMDMツールよりも広範囲な接続済みネットワークデバイスのリモート監視、プロビジョニング、パッチ適用、セキュリティの確保を行えます。対象となるデバイスには、デスクトップPC、IoTセンサー、ウェアラブル (スマートウォッチなど)、医療機器、そして産業機械などが含まれますが、これらに限定されるものではありません。

ネットワーク検出

可視性	X
優先順位付け	
検証	
修復	

これらのソフトウェアソリューションは、ネットワーク上のハードウェア、ソフトウェア、仮想の資産を自動的に検出してマッピングします。これらのツールは、ネットワークインフラの包括的なビューを作成するのに役立ちます。

ネットワーク脆弱性スキャナ

可視性	X
優先順位付け	
検証	
修復	

ネットワーク脆弱性スキャナは、ネットワークデバイスやシステムにおけるセキュリティ脆弱性を自動的に検出・評価し、組織が潜在的なリスクを特定するのに役立ちます。

IoT (モノのインターネット) セキュリティツール

可視性	X
優先順位付け	
検証	
修復	X

IoT資産とエクスポージャーを検出するツールの業界標準の名称や定義はありませんが、そのようなツールは数多く存在します。「IoTセキュリティツール」をオンラインで検索すると、さまざまな選択肢が見つかるはずです。

サイバーフィジカルシステム (CPS) 保護プラットフォーム

可視性	X
優先順位付け	
検証	
修復	X

CPS保護プラットフォームは、サイバーフィジカルシステムを発見、分類、マッピング、保護するように設計されています。これには、物理的コンポーネントと計算コンポーネントを統合した産業用制御システム (ICS) やスマートビルディングソリューションが含まれます。

クラウド・セキュリティ・ポスチャー管理 (CSPM)

可視性	X
優先順位付け	
検証	
修復	X

大規模なクラウドインフラを持つ組織は、CSPMツールでそれらの環境の可視性を管理することを選択できます。これらのツールは、プライベート・クラウド、パブリック・クラウド、ハイブリッド・クラウド、マルチクラウドのいずれの環境であっても、組織のクラウド資産を識別してカタログ化します。また、セキュリティとコンプライアンスのフレームワークに対してこれらを継続的に監視し、脆弱性と脅威を特定します。

クラウド・ワークロード・プロテクション・プラットフォーム (CWPP)

可視性	X
優先順位付け	
検証	
修復	X

CWPPソリューションは、仮想マシン、コンテナ、サーバーレス機能といった、クラウド上で実行されるアプリケーションやプログラムなど、クラウドベースのワークロードに影響を与える脅威、脆弱性、エラーを自動的に検出し、対処します。

クラウドネイティブ・アプリケーション保護プラットフォーム (CNAPP)

可視性	X
優先順位付け	
検証	
修復	X

CNAPPソリューションには、CSPMやCWPPツールの機能に加えて、クラウド・インフラストラクチャ・エンタイトルメント管理 (CIEM) ツールのようなクラウドに特化したツールも含まれています。それらは基本的に、クラウドセキュリティのワンストップショップといえる存在です。

外部アタックサーフェス管理 (EASM)

可視性	X
優先順位付け	
検証	
修復	

「外部アタックサーフェス」- 言い換えれば、インターネットに面したすべての資産 - は、組織によって見過ごされがちですが、攻撃者にとってはそうではありません。EASMツールは、ドメイン、IPアドレス、オープンポート、関連するエクスポージャーなど、インターネット上で発見可能なすべての資産を特定し、攻撃者の視点を組織に提供します。これらのツールは、ベンダーや買収ターゲットなど、組織が関与するサードパーティのインターネットに面した資産やエクスポージャーを、非侵襲的な方法で特定するのにも使用できます。

デジタルリスク保護サービス (DRPS)

可視性	X
優先順位付け	
検証	
修復	X

DRPSテクノロジーは、ドメイン、クレデンシャル、知的財産、クレジットカード情報など、従来のIT資産とは見なされないものの、組織のブランド、評判、セキュリティに影響を及ぼす可能性のある、侵害された企業資産に関連するデジタルリスクを特定します。これらのソリューションは、オープン・ウェブ、ディープ・ウェブ、ダーク・ウェブ、ソーシャルメディアにわたるエクスポージャーの監視機能と、それらのエクスポージャを修正する修復機能を提供します。

サイバー資産アタックサーフェス管理 (CAASM)

可視性	X
優先順位付け	
検証	
修復	

CAASMツールは、API統合を利用して、既存の資産管理ツールやセキュリティツールから資産やエクスポージャーデータを集約します (CAASMツールはネイティブのスキャン機能は提供しません)。これらのツールは、こうしたデータを関連付けることで、組織の資産とエクスポージャーの全体像を把握します。

SaaSセキュリティポスチャー管理 (SSPM)

可視性	X
優先順位付け	
検証	
修復	X

SaaS (Software-as-aservice) アプリケーションのセキュリティ設定と構成を継続的にスキャンして評価することで、SSPMツールは潜在的な脆弱性と誤った構成を特定することができます。これらのツールは、セキュリティ上の問題を修正し、ベストプラクティスを実施するために、自動修復機能も採用しています。

静的アプリケーションセキュリティテスト (SAST)

可視性	X
優先順位付け	
検証	
修復	

SASTツールは、コードを実行することなく、コードのセキュリティ脆弱性を分析します。これらのツールは実際に機能するアプリケーションを必要としないため、ソフトウェア開発ライフサイクル (SDLC) の初期に使用されます。

動的アプリケーションセキュリティテスト (DAST)

可視性	X
優先順位付け	
検証	
修復	

DASTツールは、実行中のアプリケーションを分析し、セキュリティの脆弱性や弱点を特定します。通常、動的アプリケーションセキュリティテストは、SDLCのテストフェーズ中、または生産環境においても、実際の運用環境でアプリケーションが安全であることを確認するために実施されます。

モバイルアプリケーションセキュリティテスト(MAST)

可視性	X
優先順位付け	
検証	
修復	

MASTツールは、静的解析、動的解析、ペネトレーションテストを組み合わせて、AndroidやiOSといったプラットフォーム上のモバイルアプリの脆弱性を特定します。

ソフトウェア構成分析 (SCA)

可視性	**X**
優先順位付け	
検証	
修復	

SCAツールは、コードベース内のオープンソースコンポーネントを特定し、それらのコンポーネントを既知の脆弱性データベースと照合して、セキュリティ上の問題や既知のエクスプロイトをチェックします。

IDおよびアクセス管理 (IAM)

可視性	**X**
優先順位付け	
検証	
修復	

IAMツールの主なユースケースは、ユーザーIDを安全に管理し、重要な企業情報、アプリケーション、ネットワークへのアクセスを制御することです。エクスポージャー管理の観点から、IAMツールは組織のIDアタックサーフェスの全体像を把握するのに役立ちます。これらのツールには、ユーザープロフィール、クレデンシャル、ロール、権限といったIDおよびアクセスデータが含まれています。また、これらのツールのいくつかは、ログイン試行、アクセスパターン、不審なアクティビティに関するリスクデータを提供します。

アイデンティティプロバイダ (IdP)

可視性	**X**
優先順位付け	
検証	
修復	

IdPはIAMのコンポーネントです。IdPソリューションは、ユーザーIDを検証し、認証サービスを提供することに主な重点を置いています。フル機能のIAMシステムを入手できない、または利用できない状況では、IdPソリューションを使用して組織のIDアタックサーフェスを可視化できます。

データ損失防止 (DLP)

可視性	**X**
優先順位付け	
検証	
修復	

DLPツールは、個人情報、財務データ、知的財産など、保護が必要な機密データを特定します。これらのツールは、組織の内外でデータがどのように使用され、アクセスされているかを監視し、不審なアクティビティが検出された場合にはアラートやレポートを生成することができます。

データセキュリティポスチャー管理(DSPM)

可視性	X
優先順位付け	
検証	
修復	X

DSPM製品は、データベース、クラウドサービス、その他の場所など、すべてのデータがどこに保存されているかを特定し、脆弱性、設定ミス、アクセス制御の弱さなど、データに関連するセキュリティリスクを評価することができます。これらの製品はまた、セキュリティ上の問題を修正して全体的なデータセキュリティを向上させるための推奨事項やツールを提供します。

API保護製品

可視性	X
優先順位付け	
検証	
修復	X*

API保護製品は、組織のアプリケーションプログラミングインターフェース (API) を検出し、インベントリを作成します。また、APIのエクスポージャーに対し推奨される改善策のリストも提供します。

*API保護製品は、修復のガイダンスは提供しますが、修復アクションは行いません。その代わり、手動でできる対応を推奨します。

APIセキュリティポスチャーツール

可視性	X
優先順位付け	
検証	
修復	X*

APIセキュリティポスチャーツールは、文書化されていないAPIやシャドーAPIを含め、環境内のすべてのAPIを自動的に識別し、マッピングします。これらのツールは、静的および動的な脆弱性スキャンを使用して脆弱性やその他のセキュリティ問題を検出し、その上で修復のための推奨事項を提供して、組織がそれらの問題を修正して全体的なAPIセキュリティを向上させるのを助けます。

*APIセキュリティポスチャーツールは、修復のガイダンスは提供しますが、修復アクションは行いません。その代わり、手動でできる対応を推奨します。

優先順位付け

優先順位付けツールは、可視化ツールから引き出された資産とエクスポージャーのデータを活用し、組織にとって実行可能なものに作り変えます。見えないものは守れないということわざがあるように、まずは全体像を把握する必要があります。その後に優先順位付けツールが、見つけた問題に関して何をすべきかを判断する手助けをします。

いくつかの可視化ツールは、優先順位付けを提供すると主張しており、その主張はある程度正確だと言えます。多くの可視化ツールは、サイロ化された範囲内のエクスポージャーの修復に優先順位をつけるために使用することができますが、組織がアタックサーフェスで直面しているすべてのエクスポージャーの修復には使用できません。たとえばEASMツールは、外部に面した資産に関連するエクスポージャーのみに優先順位をつけます。いくつかの可視化ツールは、優先順位付けを提供すると主張しており、その主張はある程度正確だと言えます。多くの可視化ツールは、サイロ化された範囲内のエクスポージャーの修復に優先順位をつけるために使用することができますが、組織がアタックサーフェスで直面しているすべてのエクスポージャーの修復には使用できません。たとえばEASMツールは、外部に面した資産に関連するエクスポージャーのみに優先順位をつけます。

エクスポージャー評価プラットフォーム (EAP)

可視性	X
優先順位付け	X
検証	
修復	X

EAPは、エクスポージャー管理の分野で新たに登場した製品です。エクスポージャー管理が既存のテクノロジーの融合に根ざしたものであるのに対し、EAPは複数のエクスポージャー管理機能を組み合わせた専用プラットフォームです。これらのプラットフォームは、ネイティブのスキャン機能によって検出発見されたものであれ、サードパーティのツールから取り込まれたものであれ、アタックサーフェス全体にわたって資産とエクスポージャーを可視化します。さらに、資産の重要性とビジネスコンテキストを考慮したエクスポージャー修復活動の優先順位付けと、それらの活動を調整または実行する機能を提供します。

リスクベースの脆弱性管理 (RBVM)

可視性	X
優先順位付け	X
検証	
修復	

その名が示すように、RBVMツールはリスクに基づいて脆弱性の修復に優先順位を付けます。これらのツールは、スキャナやその他のセキュリティツールから得られた知見を取り込んで集約し、脅威インテリジェンスや資産の重要性などのデータポイントと関連付けることで、組織が十分な情報に基づいた攻撃計画を立てるのを助けます。また、一部のツールはネイティブのエクスポージャースキャン機能を提供しています。

アプリケーションセキュリティポスチャー管理(ASPM)

可視性	X
優先順位付け	X
検証	
修復	

基本的に、ASPMツールとは、アプリケーションセキュリティ向けのRBVMツールです。これらのツールは、アプリケーションスキャナー (SAST、DAST、SCA、コンテナなど) から資産やエクスポージャーのデータを収集し、脅威インテリジェンスや資産の重要度と関連付けることで、エクスポージャーの修復活動の優先順位付けを行います。一部のベンダーは、RBVMとASPMの機能を組み合わせて、アタックサーフェス全体のサイバーリスクをより統合的に把握し、これを顧客に提供しています。また、ASPMツールにはネイティブなエクスポージャースキャン機能 (SASTなど) を搭載しているものもあります。

脅威インテリジェンス

可視性	
優先順位付け	X
検証	
修復	

脅威インテリジェンス製品は、広く脅威の全体像に関する情報を提供するものです。本書に含まれる他の優先順位付け製品とは異なり、脅威インテリジェンス製品は、組織の環境に特化したデータは扱いません。むしろ、グローバルな視点を提供することで、組織の環境内で脅威が特定される前に、セキュリティチームが潜在的な脅威に予防的に優先順位をつけることが可能となっています。

検証

検証は、優先順位付けをチェックする役割を果たします。潜在的な攻撃者が、特定されたエクスポージャーを実際にどのように悪用する可能性があるのか、また、そのような事態が発生した場合に、監視・制御システムがどのように反応する可能性があるのかを検証します。これにより、組織はどのエクスポージャーが本当に必要なのかを判断し、組織のリスクレベルとリスク選好との整合性を維持することができます。

検証は、敵対的エクスポージャー検証 (AEV) 技術と総称される製品を使用して行うこともできますし、委託を受けたベンダーまたは社内チームが手動プロセスで実施することも可能です。ベストプラクティスは、様々な検証方法を組み合わせ、最大限に包括的な結果を得ることです。

どのような方法で検証を行うにしても、バイアスがかかっていない結果を得るためには、優先順位付けに使用するサードパーティとは別のサードパーティが検証作業を行うようにすることもベストプラクティスに含まれます。検証は、手術を受ける前にセカンドオピニオンを得るようなものだと考えてください。

アタックパス分析 (APA)

可視性	
優先順位付け	
検証	X
修復	

アタックパス分析 (APA) ツールは、攻撃者が組織の環境をナビゲートするために使用できる経路を視覚的にマッピングします。これらのツールにより、セキュリティチームは、サイバー敵対者が攻撃を実行するために環境内でどのような「パス (経路)」をたどるかを判断することができます。またこれらのツールは、どのようなエクスポージャーが悪用不可能な行き止まりであるかも示します。

侵害攻撃シミュレーション

可視性	
優先順位付け	
検証	X
修復	

BASツールは、多種多様なサイバー攻撃をシミュレートすることで、組織のエクスポージャーを継続的に検証します。手作業によるレッドチーミングやペネトレーションテスト (ペンテスト) とは異なり、BASソフトウェアは検証を完全に自動化したアプローチを提供します。

レッドチーム

可視性	
優先順位付け	
検証	X
修復	

レッドチーミングとは、レッドチームと呼ばれる倫理的ハッカーのグループが、組織の防御力をテストし、脆弱性を特定し、セキュリティ対策の有効性を評価するために、実際のサイバー攻撃をシミュレートすることです。

継続的自動レッドチーミング (CART)

可視性	
優先順位付け	
検証	X
修復	

レッドチーミングでは倫理的ハッカーが手作業でサイバー攻撃をシミュレートするのに対し、CARTツールはシミュレートされたこれらの攻撃を自動化し、よりスケーラブルで費用対効果の高いリアルタイムのテストを頻繁に提供します。また、BASツールが既知の攻撃手法に対するセキュリティ対策の有効性をテストするのに対し、CARTツールは脆弱性を発見し、安全に悪用することで、攻撃者が組織の防御を突破できるかどうかを確認することに重点を置いています。

ペネトレーションテスト

可視性	
優先順位付け	
検証	X
修復	

レッドチーミングと同様、ペネトレーションテスト (しばしば「ペンテスト」と略されます) は、倫理的なハッカーが組織のシステムに対して模擬攻撃を行うものです。両者が異なる点は、ペンテストが特にエクスポージャーの検出と悪用に重点を置くのに対し、レッドチーミングは全体的なセキュリティ態勢を評価する点です。ベンダー、パートナー、その他のサードパーティにペンテストの結果を求めるのも賢明です。これは、彼らのアタックサーフェスはあなたのアタックサーフェスの一部でもあるためです。

自動ペネトレーションテスト

可視性	
優先順位付け	
検証	X
修復	

自動ペネトレーションテストのソフトウェアは、その名の通り、自動化されたペンテストを実施することで、手動による方法よりも迅速かつ定期的にテストを実施することができます。

サービスとしてのペネトレーションテスト (PTaaS)

可視性	
優先順位付け	
検証	X
修復	

PTaaSは、組織がオンデマンドでペネトレーションテストサービスにアクセスできるクラウドベースのモデルです。PTaaSは、自動と手動の両方のテスト手法を組み合わせて提供します。また、PTaaSプロバイダーがテストプロセスを管理することで、組織は独自のセキュリティ専門家チームを置くことなく、定期的なセキュリティ評価を実施できるようになります。

バグバウンティ

可視性	
優先順位付け	
検証	X
修復	

一部の組織では、倫理的ハッカーが組織内のシステム、ソフトウェア、ウェブサイトの脆弱性を発見し、責任を持って開示することを推奨しています。そのような開示情報に対しては報酬や承認の印が与えられますが、この仕組みは「バグバウンティ」と呼ばれています。

サイバーレンジ

可視性	
優先順位付け	
検証	X
修復	

サイバーレンジは、組織が実際のサイバー攻撃をシミュレートし、制御されたサンドボックス環境でセキュリティインシデントへの対応を練習できる仮想環境です。

修復

修復はエクスポージャー管理プロセスの最終段階です。リスク選好に基づいて修正すべきエクスポージャーを決定すると、修復ツールがそれらのエクスポージャーの修正を支援します。

パッチ管理

可視性	X
優先順位付け	
検証	
修復	X

パッチ管理製品は、ソフトウェアにアップデートやパッチを適用し、脆弱性を修正したり、機能を改善したりします。一部の製品は、オペレーティングシステムやサードパーティのアプリケーションを可視化するディスカバリー機能も備えています。

構成管理

可視性	
優先順位付け	
検証	
修復	X

構成管理ツールは、一貫したシステム構成の維持および適用プロセスを自動化するものです。また、一貫したシステム構成により、IT環境内のすべてのデバイスとシステムが、事前に定義されたセキュリティポリシーとベストプラクティスに従って設定され、動作することが保証されます。

Ivanti について

Ivantiは、ITとセキュリティ部門間の障壁を取り除きEverywhere Work（場所にとらわれない働き方）を実現します。IvantiのCIOとCISO向けに特化したプラットフォームは、ITとセキュリティ部門へ組織のニーズに合わせて拡張できる包括的なソフトウェアソリューションを提供し、セキュアに従業員体験を向上させます。Ivantiプラットフォームは、クラウドスケールのインテリジェントなハイパーオートメーションレイヤーであるIvanti Neuronsを搭載しており、組織全体でプロアクティブな修復とユーザーフレンドリーなセキュリティを実現し、ユーザーが満足するような従業員体験を実現します。Ivantiのエンドツーエンドのソリューションは、Fortune 100社のうち85社を含む40,000社以上の顧客によって採用されています。Ivantiは、すべての視点が聞き入られ、尊重され、評価される環境づくりに尽力し、顧客、パートナー、従業員そしてよりサステイナブルな未来を実現するために取り組んでいます。詳細については、www.ivanti.com/jaや@GoIvantiをフォローしてください。

ivanti

詳細について、またはIvantiへのお問い合わせは、ivanti.com/jaにアクセスしてください。