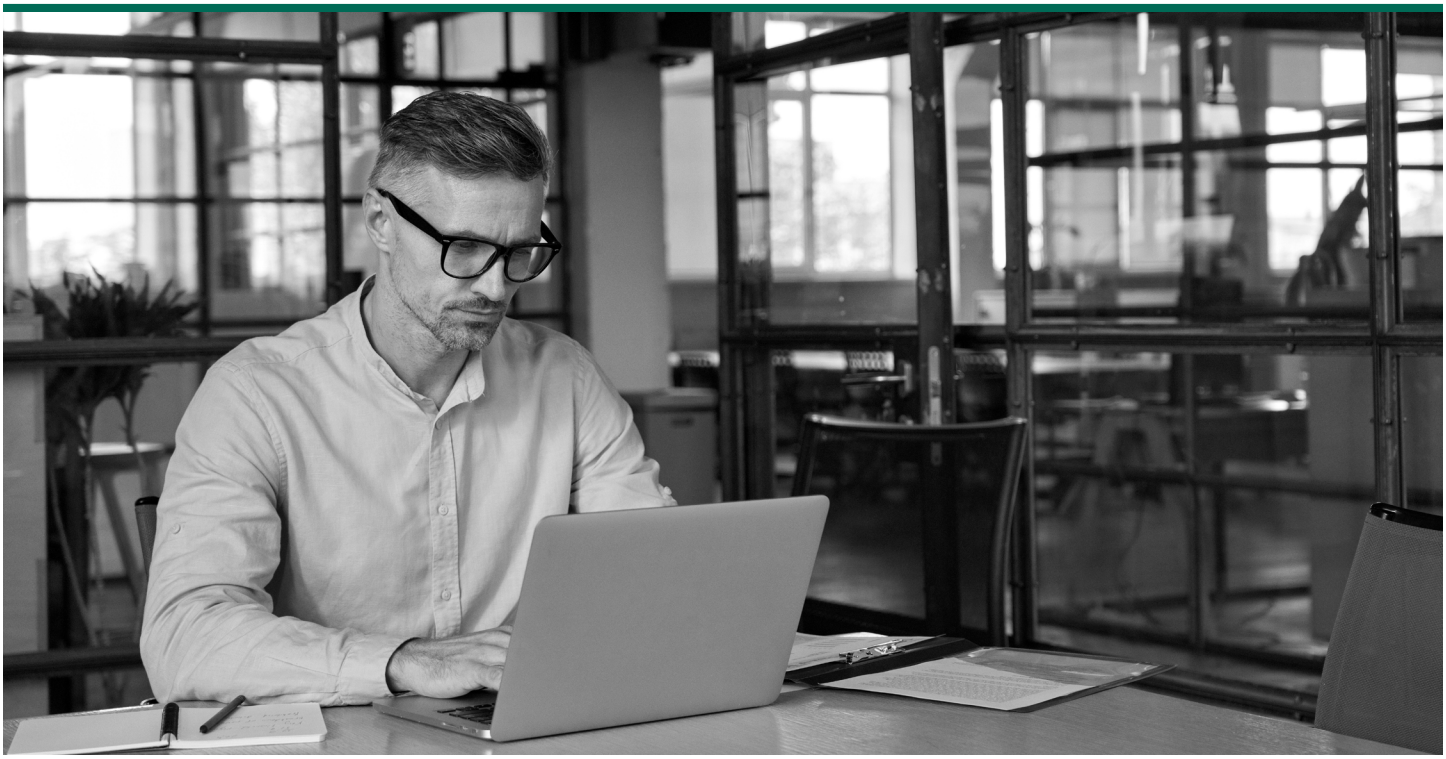
FORTRA™

ガイド (TRIPWIRE)

基本的なコントロール製品購入者ガイド



はじめに

あなたがセキュリティのプロであれば、おそらく、企業のサイバーセキュリティ対策に関する情報や、悪質なハッキングが企業や政府機関、社会に与える深刻な影響に関する資料が氾濫していると感じていることでしょう。さまざまなハイテクツールやセキュリティオプションが出回っており、どれを選べば良いのか分からないというのが本音ではないでしょうか。最近流行りの、高度なAIを使った機械学習ベースのマルウェア検知システムがよいのでしょうか？それとも、クラウドを利用したビッグデータセキュリティ分析が必要でしょうか。あるいは、情報漏洩対策を備えた優れたネットワークフィルタリング機能を採用して、組織の安全性とコンプライアンスを確保すべきでしょうか。間違いなく必要とされているのは、今日の企業のセキュリティに関する余計な情報や誇大広告を排除し、世の中に存在する数多くのフレームワークやセキュリティ規制を端的に説明しているガイドです。

自分の組織のセキュリティ対策が「強固なセキュリティコントロールを基盤として構築される」ようにすることが明らかな正解です。それでは、基盤となる「基本的なコントロール」とは何でしょうか。

基本的なコントロールには次のものが含まれます。

- 資産の検出
- セキュリティコンフィギュレーション管理
- ファイル整合性監視
- 脆弱性管理
- ログ管理

この「基本的なコントロール製品購入者ガイド」は、組織がセキュリティおよびコンプライアンスプログラムの基盤となるソリューションを新規導入する際、あるいは入れ替えの際に役立ちます。本ガイドの目的は、さまざまな機能の相違点を探り、最も重要な機能を特定することです。

資産の検出

大規模ネットワークでは、最善を尽くしているにもかかわらず、保護すべき資産に対する可視性が不完全であったり、時代遅れであることがよくあります。多くの場合、企業のセキュリティチームは、保護対象の資産を直接管理しておらず、これらのデバイスの深い知見を得ることは困難です。クラウド、仮想およびモバイルデバイスの導入が進むにつれ、企業ネットワークも複雑化しており、その結果、セキュリティリスクの可視性に死角が生じています。そして、そのような死角は、攻撃者が侵入し、攻撃を拡大するのにうってつけの場となります。基本的なコントロールを配備するための第一歩は、ハードウェアとソフトウェアの正確なインベントリの作成です。このステップは非常に重要です。なぜなら、資産のインベントリの完全ビューは、その後に続く基本的なコントロール（脆弱性管理など）で必要となるからです。

CISコントロール1 – 許可されたデバイスと無許可のデバイスのインベントリでは、資産のインベントリ情報が不完全であることがなぜ問題となるかを説明しています。

資産の検出プロセス

資産の検出を開始すると、次のようなタスクがバックグラウンドで実行されます。これらは、使用しているソリューションとその構成によって異なります。

- **名前解決：**DNSサーバーを使用して、IPアドレスからホスト名を解決します。
- **PING：**ホストへのPing実行は、ホスト検出プロセスの一部ですが、通常1つのタスクとして分類されます。一般的に、ICMP timeoutやMax requestsなど、製品に適用できるデータベース固有の設定が存在します。
- **ホスト検出：**特定のTCPポートとUDPポートを使用して、あるホストが稼働中かつ応答可能であるかを判断します。
- **NetBIOSの名前解決：**特定のNetBIOSパケットを使用して、ホストのNetBIOS名を割り出します。
- **資格情報セットの作成：**ユーザーインターフェイス経由で入力されたクレデンシャルが特定の資格情報セットに変換されます。これらは、要求時にルールに適用されます。
- **CIFS共有の列挙：**ホスト上の利用可能な共有場所の列挙が実行されます。
- **ポートスキャン：**構成可能な既知のポートリストに基づいてポートスキャンが行われます。通常は、ユーザーインターフェイス経由でリトライ試行回数およびタイムアウト時間に関する設定を行えます。
- **アプリケーションスキャン：**検出されたオープンポートに対し、アプリケーションルールが実行されます。高度なソリューションでは、さまざまなプロトコルを特定のポートに関連付けてそれらのプロトコルとポートのペアのみをスキャンし、プロトコル、アプリケーション、およびルールを特定の順序で実行することにより、スキャンによる影響を低減しています。一般的には、非標準ポート上のプロトコルやアプリケーションのスキャンも可能になっています。
- **OSフィンガープリントスキャン：**従来のスタックフィンガープリント技術を使用して、OSの特定を行います。ホストに対してスタックフィンガープリントルールを実行します。これらの結果を、既知のOSの応答データベースと比較します。
- **OSの計算：**以前のテスト結果に基づいて、最も可能性の高いOSが決定されます。

> ある日の夜に新しいハードウェアをネットワーク上に設置して、翌日まで未設定のまま適切なセキュリティ更新パッチを適用しなかった場合、そのハードウェアは攻撃に利用されてしまう可能性があります。攻撃者が内部アクセスをすでに取得しており、内部のジャンプポイントや標的を物色していれば、インターネット側からは見えないデバイスですらも悪用されてしまいます。」
>
> www.cisecurity.org/critical-controls/

考慮すべき点

- **動的なホスト追跡機能：**正確で信頼性の高いデータ収集を実現するには、異なるネットワークに接続、切断、再接続するシステムを一意に識別することによりポータブルホストを追跡する機能が不可欠です。多くのソリューションでは、IPアドレスを使用してホストを経時的に追跡します。しかし、IPアドレスは頻繁に変更されるため、不正確な結果を招きかねず、ネットワークリスクの状態を正確に把握することができません。たとえば、あるホストのIPアドレスが変更されると、一部のソリューションでは、2つのホストがあるように報告してしまうことがあります。最先端の資産検出ソリューションでは、ホストを追跡し、一意に識別するために、エージェントや追加の動的情報（DNS名、NetBIOS名、OS、IPアドレス、ポートシグネチャ、OSフィンガープリント、MACアドレスなど）を使用することでこの問題を克服しています。このようなソリューションは、そのような詳細データを利用して、グループ間で移動するホストを動的に追跡し、その変更をレポートおよび資産管理データに即座に反映させます。このような方法により、特定のホストまたはグループから収集されたデータの正確性を維持しています。
- **資産のタグ付け：**ソリューションは、グループ、技術的な所有者、地理的な位置、または重要度に基づいて資産のタグ付けを行う機能を提供する必要があります。ルールベースの資産タグをデバイスに自動的に割り当てて、ワークフローを自動化し、組織固有の特性を把握可能にする高度なソリューションも存在します。
- **クレデンシャル使用のスキャン：**ソリューションでは、クレデンシャル使用および不使用の両方の評価機能を備えてユーザーが選択できるようにし、経時的なニーズの変化に対応できることが理想です。
- **資産の階層的構成：**業務に適した構造でホストとネットワークを構成できると便利です。たとえば、ビジネスユニットのカテゴリー（財務と営業、あるいは北米、ヨーロッパ・中東・アフリカなどの地理的分類）別に資産をグループ化する機能があると良いでしょう。セキュリティデータの計算やトレンド分析の際に、ビジネスコンテキストを適用しやすくなります。
- **デバイスのサポート：**ソリューションは、有線および無線デバイス、仮想マシン、クラウドインスタンスなど、環境内のすべてのデバイスタイプの検出をサポートする必要があります。
- **ソフトウェアおよびアプリケーションのサポート：**デスクトップアプリケーション、OS、ポート、サービス、プロトコルなど、環境内で使用中のすべてのソフトウェアとアプリケーションの検出にも対応すべきです。

セキュリティコンフィギュレーション管理

セキュリティコンフィギュレーション管理（SCM）は、ITセキュリティとITオペレーションが交わるポイントに存在します。脆弱性評価、自動修復、コンフィギュレーションアセスメントの要素を組み合わせたソフトウェアベースのソリューションがSCMです。ITセキュリティのプロは、SCMを使用してOS、アプリケーション、およびネットワークデバイスのセキュリティ構成をプロアクティブかつ継続的に監視・強化することによって、ネットワーク内の攻撃対象領域を縮小できます。またSCMにより、コンプライアンス監査官は、所定のポリシーに照らしてコンプライアンス監査を行えるようになります。

セキュリティコンフィギュレーション管理のプロセス

SCMのプロセスは大まかに次の4つのステップで構成されます。

1. **検出：**まずは、管理が必要なデバイスを探します。統合された資産検出リポジトリを備えたSCMプラットフォームを活用するのが理想です。また、カテゴリー分類機能と資産のタグ付け機能を活用して、不要なサービスを開始しないようにすることもできます。たとえば、エンジニアリング部門のワークステーションと金融部門のシステムでは、異なる構成が必要となるはずです。
2. **コンフィギュレーションベースラインの確立：**まず、管理対象のデバイスのタイプ別に、許容される安全な設定を定義します。多くの組織では、デバイスの構成方法についての詳細をCISまたはNISTのベンチマークから得ています。
3. **評価、アラート、レポートに関する変更：**デバイスを検出し、カテゴリー分けしたら、評価の頻度を決定します。ポリシーチェックの頻度はどれくらいにしますか？リアルタイムアセスメントを実行できるとしても、すべてのケースにおいて必要というわけではありません。
4. **修正：**特定された問題は、修正するか、誰かが例外として認める必要があります。すぐに処理しきれないほどの作業を抱えている可能性があるので、優先順位付けが成功の鍵となります。また、監査に備えて、予期していた変更が実際に発生したことを確認する必要もあります。

考慮すべき点

- **OSおよびアプリケーションのサポート：**コンフィギュレーション管理機能は、御社の環境内で使用中のOSとアプリケーションをサポートしている必要があります。
- **標準およびベンチマークのサポート：**ソリューションが提供するポリシーとコンフィギュレーションの数が多いほど、御社の要件に簡単に適合するものが見つかる可能性が高まります。
- **ポリシーの編集：**一般的にポリシーは、要件を満たすためにカスタマイズが必要となります。コンフィギュレーション管理ソリューションには、ポリシーを定義し、新しいベースライン構成やベンチマークを追加するための柔軟なポリシーエディタが必要です。
- **拡張性：**各デバイスにおいてコンフィギュレーションの変更を検出する際には、エンドポイントやネットワークに多大な負荷がかかります。そのため、スキャナーの効率的な配置方法を理解し、スキャンの頻度、影響、範囲を柔軟に調整できるようにしましょう。
- **リモートデバイス：**リモートデバイスの評価はどのように行われますか？営業担当者のノートPCや、帯域幅が限られた遠隔地にあるデバイスなどがこれに当たります。適切な修復を確実に行うために、どのようなリカバリー機能が組み込まれていますか？、（たとえば、接続されていないなどの理由で）最近評価が行われていないデバイスがあればアラートを受け取ることができますか？
- **運用プロセスとの統合：**特定されたコンフィギュレーション上のあらゆる問題が中央のヘルプデスクシステムに確実に報告されるようにして、変更を承認・適用するための適正なプロセスが実行されるようにします。
- **例外ポリシーの処理プロセス：**前述のように、コンフィギュレーションの変更が、例外として承認されるケースがあります。厄介なことに、コンフィギュレーション管理機能が変更を検出した後（場合によってはそれを取り消した後）に承認されることもよくあります。このような誤検出の可能性は、低減しなければなりません。

ファイル整合性監視

変更監視とも呼ばれるファイル完全性監視（FIM）機能は、ファイルを監視して、変更の有無、発生日時、および誰がどのような変更を行ったのかを識別し、変更を戻す方法を特定することを意味します。当然のことながら、定期的なパッチ適用などにより、多くのファイルには、時間の経過とともに正当な変更が加えられます。しかし、ファイルの大半は静的なものであり、中核となる機能（IPスタックやEメールクライアントの設定など）を変更することにより、何らかの問題が発生することがよくあります。FIMのアクティブなセキュリティコントロール機能では、ファイルのセット（システムファイルやその他のファイル）を定義し、ベースラインとなる構成を取得して、変更を監視することができます。FIMは、不正な変更やマルウェアの検出に多大な効果を発揮するとともに、PCIなどの規制遵守にも役立てることができます。

ファイル整合性監視のプロセス

ファイル整合性監視の実行には、通常次のプロセスが含まれます。

- **ポリシーの設定：**まずはポリシーを定義し、どのデバイス上のどのファイルにモニタリングが必要かを特定します。
- **ファイルのベースライン作成：**次に、評価するファイルが既知の正常な状態にあることを確認します。ファイルのバージョン、作成日、変更日、その他のファイル属性を評価することにより、ファイルが正当なものであることを保証します。
- **モニタリング：**その後、変更をアクティブに監視します。1台のシステムでも、通常1日に数百件ものファイルの変更が発生するため、これは、簡単な作業ではありません。そのため、正当な変更と不正な変更を見分けることが不可欠です。予想される変更を自動プロモートすることで誤検出を最小限に抑える方法が必要となります。
- **アラート：**不正な変更が検出されたら、担当者に通知する必要があります。
- **レポート：**FIMはPCIのコンプライアンス遵守に必要です。そのため、御社の監査官が効果的に利用できることを立証する必要があるでしょう。コンプライアンス監査のためのレポート生成機能が提供されるかを確認しましょう。

考慮すべき点

- **軽量なエージェント：**FIMを実装するには、保護された各デバイスにエージェントをインストールする必要があります。エージェントでは、使用していない機能をオフにしたり、必要に応じて機能を追加したりできることが重要です。
- **監視頻度：**ファイルには継続的な監視が本当に必要か、それともスケジュールに基づいた監視で十分かを判断しなければなりません。
- **脅威の情報ソースとの統合：**内部調査から得た情報に、サードパーティ提供の脅威情報を統合します。通常サードパーティは、攻撃手法や侵害の兆候などに関する最新情報を持っています。
- **調査とインテリジェンス：**潜在的に悪質な変更のなかから、正当な変更を特定できれば、FIMはほぼ成功したと言えます。脅威インテリジェンスの情報ソースとの統合の他にも、オペレーショナルインテリジェンスとの統合が必要です。
- **変更検知のアルゴリズム：**変更検知は、ファイルのハッシュ、バージョン、作成日、変更日あるいは権限をベースに行われますか？それとも、それらすべてでしょうか。ファイルが変更されたことをベンダーがどのように判断しているかを理解すれば、あらゆる脅威モデルをカバーできるでしょう。
- **バージョン管理：**正当なファイルであっても、それが適切ではない場合もあります。たとえば、システムファイルの更新をする際に、古いバージョンがインストールされてしまうこともあるでしょう。
- **フォレンジック機能：**侵害の発生時には、すべてのファイル操作のログなどのフォレンジック機能が必要となるでしょう。それぞれのファイルにいつ、どのプログラムがアクセスし、何を行ったかを知ることは、攻撃の被害を評価したり、データ損失を招くイベントの連鎖を究明する上で非常に役立ちます。
- **クローズドループ変更監査：**ファイルの追加、削除、変更は何千件も発生しています。そして、そのほとんどが、許可された正当なものです。しかし、コンプライアンスと運用の両方の信頼性を確保するためには、実際に起こった変更と予想される変更とを照合する必要があります。
- **プラットフォームの統合：**検知、レポート作成、エージェントのデプロイ/更新/保守といったクロスファンクショナルな機能をわざわざ一から開発しなおす必要はありません。FIMプラットフォームを活用して、導入を合理化し、運用を容易にしましょう。
- **ポリシーの管理：**システムは、ポリシーの作成を開始するために使用できるベースラインを提供する必要があります。環境にはそれぞれ独自の特徴がありますが、プラットフォームベンダーは既成のポリシーを提供し、素早く簡単にカスタマイズできるようにする必要があります。すべてのポリシーは、新しいポリシーのテンプレートとして利用できなければなりません。ポリシーが複雑であるほど、内部の不一致が生じたり、誤った是正措置が定義されたりしやすくなります。ほとんどの管理者は、明確でグラフィカルなレイアウトでポリシーを設定できるインターフェイスを求めています。見やすいグリッドがあり、ポリシーごとに適切な情報が表示されることを望んでいます。
- **ポリシーの粒度：**製品では、デバイスごとに異なるポリシーがサポートされることが求められます。たとえば、（PCIの適用対象の）店舗のPOSデバイスは、特定のファイルを管理する必要があります。一方で、セグメント化されたインターネット専用ネットワークに接続された企業ロビー内の情報キオスク端末に対しては、それと同じレベルの監視は不要でしょう。
- **サポートされる標準およびベンチマーク：**PCI DSS、NERC CIP、SOX、HIPAA、NIST 800-53、MAS TRM、IRS 1075、CISコントロール、Mitre ATT@CK、COBIT、ISO 27001など。ツールが対応する標準や提供するコンフィギュレーションベンチマークが多いほど、御社の要件に簡単に適合するものが見つかる可能性が高まります。
- **ポリシーの編集：**一般的にポリシーは、要件を満たすためのカスタマイズが必要です。コンフィギュレーション管理ツールでは、ポリシーを定義し、新しいベースライン構成やベンチマークを追加するための柔軟なポリシーエディタが提供されるべきです。
- **ポリシーの更新：**規制のポリシーは常に更新されています。システムは、その内容を速やかに（むしろ自動的に）ソリューションにダウンロードしてアップデートする必要があります。

脆弱性管理

企業ネットワークに新たな物理・仮想デバイスが追加されたり、変更あるいは削除されるスピードがこれまで以上に加速するなか、企業ネットワークは絶え間なくかつ急速に変化しています。このような変化のなかには不正なものがあり、新たな脆弱性を生じさせることがあります。このような脆弱性が（ダイナミックコンテナやエラスティックなクラウドインスタンスに存在する）一時的なものであっても、あるいはリモートネットワークやビジネスパートナーのネットワーク上に存在するものであっても、攻撃者に隙を与えていることに変わりはありません。脆弱性の是正を任務とするITセキュリティチームは、リスクの正確な評価を行い、セキュリティ上の脅威を最小化して、コンプライアンスを維持するために、複数の視点から脆弱性評価を行うことを求められます。

脆弱性管理のプロセス

脆弱性管理プログラムには、大まかに次の4つの段階があります。

1. **脆弱性スキャンプロセス：**このプロセスでは、資産の重要度、資産の所有者、スキャンの頻度を判断し、是正に向けたタイムラインを決定します。
2. **資産の検出とインベントリ：**ネットワーク上の資産の検出とインベントリ作成を行います。
3. **脆弱性の検知：**検出した資産上の脆弱性を検知します。
4. **レポートおよび是正機能：**発見された脆弱性のレポート生成と是正を行います。

考慮すべき点

- **リスクスコアリング：**優先順位、リスク許容度、組織を標的とする脅威の種類は組織ごとに異なります。CVSSなどの標準の脆弱性スコアリングシステムで、ある脆弱性が（1～10のスケールで）「8」と評価される場合でも、同じ脅威が特定の組織ではそれ以上またはそれ以下のリスクを呈する場合があります。定量的なスコアは必要なベースラインですが、多くの企業は、特定のビジネスや業界固有の要件に基づいて脆弱性を評価する能力を求めています。セキュリティチームが自社のネットワーク上で最も重要なリスクを迅速に特定し、是正できるようにするには、各社固有のリスクプロファイルに応じて脆弱性管理データをカスタマイズできる自動化ツールが必要です。このデータを利用すれば、優先順位付けを行った包括的な是正情報を取得できます。リスクスコアリングは、組織が脆弱性管理データを特定のビジネス要件に合わせてカスタマイズできることを示す良い例です。多くの脆弱性管理システムでは、「1～10」あるいは「高/中/低」のスコアが使用されます。数千、数万もの脆弱性が存在する組織の場合、そのような大まかな脆弱性スコアでは意味をなしません。高度な脆弱性管理ソリューションは、非常に大規模なネットワークにも適応できる柔軟かつきめ細かなスコアリングシステムを提供します。
- **クレデンシャルを使用する脆弱性評価：**アセスメントの深度は結果の精度に大きく影響します。深い脆弱性評価を行えば、より詳細な情報が得られ、システムはそれを使用して正確性を向上できます。クレデンシャルを使用する脆弱性評価では、管理用のクレデンシャルを使用して、ファイルシステム、レジストリおよびコンフィギュレーションファイルの検査を行います。クレデンシャルを使用する脆弱性評価は、クレデンシャルを使用しない評価より長い時間を要します。しかし、収集された追加情報によって、脆弱性の検出および評価の正確性が劇的に向上します。対照的に、クレデンシャルを使用しない基本的な脆弱性評価では、ホストが公開する簡単な情報を取りまとめて評価を行うため、不正確な結果や誤検出を招く可能性があります。どちらにも、それぞれの利点があります。最良のソリューションは、クレデンシャルを使用する評価と使用しない評価の両方を提供します。脆弱性管理製品は、両方の方法を提供するのが理想です。それにより、評価のスピードと深さのバランスを組織の要件に合わせて最適化することができます。
- **ID管理とアクセス管理：**組織のディレクトリサービスと脆弱性管理システムが緊密に連携されていない場合、変更が発生するたびに、管理者が手動でアカウントを作成、更新、削除しなければなりません。人事管理上の変更が脆弱性管理システムに反映されていない場合には、脆弱性データへのアクセスが必要な従業員がアクセス権を持っていなかったり、逆に、アクセスの必要がない従業員がアクセス権を持っているといった状況が発生します。規模の大きな複合型の企業や、マネージドサービスプロバイダーでは、マスターアカウントからのサブアカウント管理を最適化できるマルチテナント機能が必要となります。この付加機能により、データを分離し、ユーザーアクセスを分離させることが容易になります。
- **正確性：**脆弱性評価の結果が正確であることは極めて重要です。しかし、脆弱性管理製品が提供する評価結果の精度はさまざまです。なかには、存在もしない脆弱性を検出したり、深刻なセキュリティ上のリスクをもたらす脆弱性を見逃してしまうソリューションもあります。脆弱性管理コントロール製品は、「疑わしい」脆弱性の検出を大幅に低減するために、さまざまな技術を備えている必要があります。そうすることで、時間とリソースを最も効率的に使用できるようになります。
- **無差別型のテスト：**この古い脆弱性評価方法では、脆弱性管理製品は定義されたホストIPアドレスの範囲をスキャンし、脆弱性管理ベンダーが管理している既知の脆弱性のリストに照らして、各ホストを無差別にチェックします。この方法では脆弱性のチェックに時間がかかるだけでなく、評価対象のデバイスにチェックが行われない可能性もあります。Linuxマシンに対して、Windows向けの脆弱性チェックが実行されてしまう場合もあるでしょう。このようなシナリオは、デバイスとアプリケーションのインベントリが不正確な場合にも発生する可能性があります。たとえば、Unix系OSを実行するNetAppファイラーが、Windows SMB/CIFSサービスを実行しているためにWindowsデバイスとしてプロファイルされているようなケースです。
- **ターゲットを絞ったテスト：**この脆弱性評価方法ではまず、各ホストのインベントリ作成とプロファイリングを行い、デバイス、OS、およびアプリケーションの種類を特定します。その後、その情報を使用して、特定のホスト、OS、またはアプリケーションのバージョンに不要なチェックはスキップして、関連する脆弱性のみをインテリジェントかつ効率的にチェックします。
- **ITチームとセキュリティチームの連携：**セキュリティチームとITオペレーションチームが変更情報および脆弱性データを共有すれば、特定のビジネス目標に向けて簡単にリソースを最適化できるでしょう。しかし、ほとんどの脆弱性管理データは簡単に共有できるものではありません。また、多くの脆弱性管理ツールでは、他のチームがデータを利用できるように、手動でデータをエクスポートおよびフォーマットする必要があるため、貴重なリソースが浪費されます。
- **リアルタイムのデータナビゲーション：**高度な脆弱性管理製品は、リアルタイムのデータナビゲーションやデータ統合機能を提供します。このような高度なツールによって、セキュリティ担当者は容易にネットワークリスクを評価できるため、より重要な作業に注力できるようになります。たとえば、特定の脆弱性が存在するホストのリストを作成したり、過去2回のホスト評価結果を比

較して、新しい脆弱性や変更が発生したアプリケーションを特定するといったことが可能になります。

- **過去の傾向：**脆弱性の特定と経時的な修正の傾向を明示することで、リソースの計画と分配に活かせる知見が提供されます。トレンドデータは、ネットワーク内のセキュリティリスクが緩和されている領域、あるいは悪化している領域に関する重要な知見を提供します。
- **スキャンから分離されたレポート機能：**高度なソリューションでは、複数の評価から得られた情報を1つのレポートにまとめることができます。能力の劣るソリューションでは、評価とレポートを結合させています。一方、高度なソリューションでは、評価データを経時的に収集および保存し、将来的にオンデマンドレポートとして簡単に利用できるようにしています。個々のスキャンごとにレポートを作成している場合は、次のスキャンのための設定を行い、新しいレポートが作成されるまで待機しなければなりません。
- **データの保持：**そのソリューションは、管理者が指定した期間内のすべての評価結果を保持し、あるホストの最近および過去の評価結果をユーザーが簡単に確認できるようになっていますか？
- **レポート：**そのソリューションでは、さまざまな利用者に適した詳細度でレポートを提供できますか？たとえば、コンプライアンス達成の証拠を確認したいと考える監査官や、組織のリスク状況の概要やリスクトレンドのグラフ表示、あるいは組織の階層別や地域別のリスクデータの可視化を求める経営幹部といった利用者が考えられます。すべてのユーザーがレポートフィルターを作成、保存、共有できますか？ホストのスコア、脆弱性の種類、重大度、OSグループなどの特性に基づいてデータを含めたり除外したりする「レポートのフィルタリング」を行えますか？ユーザーの役割に応じたレポートの自動配布を行えますか？
- **是正に向けたアドバイス：**そのソリューションは脆弱性の正しい是正方法に関するアドバイスを提供してくれますか？たとえば、正確かつ包括的な是正策の詳細、脆弱性緩和策、パッチへのリンク、ベンダーのアドバイザリ情報、適切な脆弱性情報などは提供されますか？
- **脆弱性インスタンスデータ：**「脆弱性がどのように検出されたか」という詳細情報は、システム管理者が手動で脆弱性の存在を確認する際に役立ちます。パッチやフィックスを適用後（もしくは誤適用後）も、マシンにまだ脆弱性が内在しているために、レポート内に脆弱性情報が再表示されることもあります。パッチを有効にするためにデバイスを再起動する必要がある場合にも、脆弱性が再び報告されることがあります。「どのように脆弱性が発見されたか」という情報は、組織にもたらされるリスクの根本的な原因をチームが協力して究明する際に役立ちます。

> *『セキュリティロギングと分析が欠如していると、攻撃者の所在や悪意のあるソフトウェア、マシンが受けた被害痕跡の隠ぺいを許してしまいます。システムが侵害されたことを被害者が認識した場合でも、保護された完全なロギングレコードがなければ、攻撃の詳細やそれに続く攻撃者の行動を知ることができません。しっかりとした監査ログがなければ、いつまでも攻撃に気づくことができず、受けたダメージを修復することすらできないかもしれません。』*

ログ管理

インフラストラクチャの安全は、環境内で何が起こっているのか、そして過去に何が起きたのかを正確に判断する能力に大きく依存しています。環境内のアクティビティに関するデータの多くは、さまざまな種類のログに記録されます。ログは、OS、アプリケーション、その他ほとんどのデバイスによって生成されます。ログの収集、保管、分析は、CISのクリティカルセキュリティコントロールに含まれています。CISでは、セキュリティのためのログ管理の妥当性を非常に簡潔に説明しています。

組織内のすべての資産のログデータの収集、保存、分析を怠たれば、可視化されるセキュリティの状態との間に大きな隔たりが生じます。

ログ管理のプロセス

ログ管理のプロセスでは、5つの基本的なパラメータを考慮しなければなりません。

1. **収集：**暗号化された接続を介し、さまざまなプラットフォームからエージェント/エージェントレスの方法を使用してログを収集します。
2. **ストレージ：**ログは、保存、圧縮、暗号化、記憶後、アーカイブされます。
3. **検索：**ログは、プレーンテキスト、REGEX、およびAPIクエリによる検索用にインデックス付けされます。
4. **コリレーション：**コリレーションルールを適用して、目的のイベントを検出し、自動化されたアクションを実行します。
5. **出力：**情報は、ダッシュボード、レポート、電子メール、およびイベント転送機能を使用して他のシステムに配信されます。

考慮すべき点

- **収集：**安全で信頼性の高いログ収集を行うためには、多くの考慮事項があります。もちろん、欠落しているログデータは解析できないため、ログを確実に収集できることは、どのようなログ管理プロジェクトでも最重要です。どのログ管理製品でもログを収集する手段は複数用意されていますが、最も信頼性の高い方法が推奨されるべきです。

  リモートでのログ収集が必要な場合もありますが、エージェントベースの手法よりも信頼性は著しく低下します。エージェントを使用したログ収集のほうが、オペレーションの安全性と信頼性が高くなります。可能な限り、リモートでのログ収集よりもエージェントベースのログ収集を優先させます。
- **ストレージ：**収集されたログはどこかに保管する必要があります。どのような展開においても、ログデータの量によってストレージが重大な問題となります。ログストレージは、少なくともログデータの保存と圧縮の要件に対応している必要があります。コンプライアンス要件および拡張性に対応するために、データの地理的な格納場所を柔軟に設定できる高度な機能も存在します。
- **検索：**データは使用することを目的に収集するものです。ログの検索は前述のどのようなケースでも行われるアクティビティです。ログの検索を効果的に行うためには、柔軟性とパフォーマンスのバランスが適切でなければなりません。ユーザーが分類タグを使用して、適切なフィルタリングを行うことにより、検索に直接影響を与えられるようにします。インデックス付きの正規化されたログデータを検索することが推奨されますが、生ログを確認できることも重要な要件です。ログ検索では、アナリストが結果を絞り込めるような幅広いクエリだけでなく、非常に直接的なクエリも

容易にする必要があります。ユーザーが複数のクエリの結果を同時に見て、比較できることが重要です。

- **コリレーション：**どのようなユースケースでも、1つのホスト上の1つのログエントリ内に複数のイベントが発生していることは稀です。アナリストの仕事の大部分は、それぞれのイベントを点と点で結ぶことにあります。この手作業のすべてを自動化できるわけではありませんが、ログ管理ツールのコリレーション機能により、最も顕著な例の負担を軽減できます。コリレーション機能は、生成されるイベントを環境に合わせてカスタマイズする機能をユーザーに提供することを目的としています。多くのイベントは、ベンダーが提供するルールを使用して事前設定できますが、強力なコリレーション機能では、個々の組織または部門に固有のイベントパターンを利用します。ユーザーは、事前に構築されたコリレーション機能のライブラリに加えて、新しいコリレーションルールを作成するための直感的なインターフェイスを探す必要があります。もちろんコリレーションの機能は、コリレーション処理を実行するデータエレメントに左右されます。

  ユーザーは、収集されたログデータのエレメントについて、どのようにコリレーションが行われたかを評価する必要があります。ログにはコリレーションに必要となるすべてのデータが含まれているわけではありません。より完全なイベントコリレーションが容易に行えるように、ログ管理ツールが、追加のデータソースのインポートをサポートすることが重要です。脆弱性スキャンの結果や、別のシステムからの資産情報などがこれに該当します。

- **出力：**ログ検索やイベントコリレーションの実行結果をシステムから取り出す機能は、ログ管理システムの中核となる要件です。ベンダーは、ベンダー提供のシステムをデータの最終的な行き先とみなしたいようですが、実はそうであるケースは稀です。その次の行き先が人間であろうと、別のシステムであろうと、ログ管理ツールがデータのやりとりを促進することが不可欠となります。ユーザーは、検索結果がどのようにエクスポートされるのか、スケジュール設定できるのか、コリレーションイベントはどう配信されるか、またどのような送信先を選択できるのかを考慮する必要があります。ログを転送する機能もまた重要な要件です。昨今、ログやその他のデータの複雑な分析に対する投資が増えています。ログ管理システムは、データの収集とコリレーションという中核的な要件に焦点を当てるべきです。そのうえで、ログデータ（データ全体あるいは特定のイベントに絞ったもの）を他のシステムに配信する機能も維持しなければなりません。

まとめ：

ベンダーに確認すべき10項目

1. セキュリティとコンプライアンスに関し、具体的にどのようなコントロールを提供しているか？すべてのコントロール用のポリシーは、ベンダーのコンソール経由で管理できるか？
2. ベンダーの製品では、どの製品、デバイス、アプリケーションがサポートされるのか？
3. ベンダーの製品は、どのような基準やベンチマークに対応しているか？
4. どのような種類のレポートが提供されるのか？特定のレポートをカスタマイズするには、どうすればいいのか？
5. ベンダーには社内リサーチチームがあるか？そのチームは製品の向上にどのように寄与しているか？
6. 製品にはどのようなエージェントが必要か？エージェントは持続型か？それとも自動消滅型か？更新はどのように管理対象デバイスに配信されるのか？エージェントが改ざんされないようにどのような対策が施されているか？
7. リモートデバイスや接続していないデバイスはどのように扱われるか？
8. 管理コンソールはどこで実行されるか？専用のアプライアンスが必要か？ベンダーの環境では、どのような階層管理がサポートされるか？管理用インターフェイスは、どの程度カスタマイズ可能か？
9. 仮装デスクトップ（VDI）への対応予定は？
10. ベンダーのプラットフォームには、どのようなセキュリティ対策が講じられているか？強力な認証方式がサポートされているか？ベンダーのコンソールでは、アプリケーションのペネトレーションテストが行われたか？ベンダーのエンジニアリングチームでは、安全なソフトウェア開発プロセスが実行されているか？

あと10件は、追加の質問を続けることができますが、以上の質問は、対応するデバイスとアプリケーション、リサーチ/インテリジェンス、プラットフォームの整合性と統合、および管理コンソールの機能といった重要な側面を明らかにするものです。このリストは、総合的なRFIやRFPの代わりになるものではありませんが、ベンダーの製品ファミリーが御社の要件を満たしているかどうかを簡単に知るための助けとなるでしょう。

デモのご予約

TripwireがFortraの基本的なコントロール用ソリューションのデモを行い、御社のご質問にお答えします。**www.tripwire.com/ja/demo**からご予約ください。

FORTRA™

Fortra.com

Fortraについて

Fortra は、他に類を見ないサイバーセキュリティ企業です。私たちはお客様のために、よりシンプルで強力な未来を創造します。当社の信頼できるエキスパートと統合されたスケーラブルソリューションは、世界中の組織にバランスとコントロールをもたらします。私たちはポジティブ・チェンジメーカーであり、サイバーセキュリティの旅路のあらゆる段階において、お客様の味方となります。詳細については、fortra.com をご覧ください。

　(fta-tw-gd-ja-0124-r1-hm)