jamf

Appleエンドポイント テレメトリ実務ガイド

見えなければ、守れない

可視性はテレメトリから始まる

真っ暗な部屋に入ったことはありますか?光がなければ、壁がどこで終わり、家具の角がどこにあるかといった状況をはっきりと判別することはできません。エンドポイントセキュリティ、ひいてはコンプライアンスも、これによく似ています。テレメトリデータがなければ、見えないものを守ることはできません。

当たり前のことを言っているように思えるかもしれませんが、管理対象のAppleデバイスから現在のエンドポイント健全性データを取得できないことが、現代の組織が直面している最大の課題の一つになっています。確かに、IT部門はmacOS、iOS、iPadOSデバイスの登録台数を簡単に把握できますし、セキュリティ部門は6ヶ月前の移行プロジェクトで何台のデバイスがmacOSの最新メジャーバージョンにアップグレードされたかを詳細に記したレポートを作成できます。

しかし、IT部門やセキュリティ部門は、まさに今この時点のMac・モバイルデバイス全体のコンプライアンス状態を検証できるでしょうか。**言い換えれば、以下のような項目の検証に使用しているデータに、どれほどの確信を持てているでしょうか。**

- どのプロセスが実行されているか?
- システムの整合性に影響が出ているか?
- 誰がその変更を行ったか?
- エンドポイントはコンプライアンス要件を満たしているか?

「識別」と「検証」の間には、些細なようで重要な違いがあることに注意してください。なぜなら、この2つの間に、登録済みデバイスとコンプライアンスを満たしたエンドポイントとの違いがあるからです。前者は、モバイルデバイス管理(MDM)ソリューションに記録があり、定期的なチェックイン時にのみ更新されるデバイスです(識別)。後者は、常時監視によって豊富なテレメトリデータが収集・分析され、エンドポイントの健全性をリアルタイムで把握できるデバイスです(検証)。

前者は最新のチェックイン時点のデータに基づいており、スケジュールやリソースによっては情報が古くなっていて、組織に未知のリスクをもたらす可能性があります。後者は最新の健全性データに基づいてエンドポイントのコンプライアンスをリアルタイムで検証し、監査人にタイムスタンプ付きのデバイスコンプライアンス証明を提供できます。

あらゆる規模の組織にとって、識別と検証のギャップを埋める鍵となるのが、テレメトリです。**このガイドでは、現代の管理・セキュリティ戦略においてテレメトリが果たす重要な役割を紹介するとともに、以下の点も解説します。**

- テレメトリの内容とテレメトリには含まれないもの
- デバイスの状況を深く理解するうえでのテレメトリの役割
- 可視性がもたらす効果:
  - 包括的なIT運用の実現
  - 期待されるビジネス成果の達成
  - 連携の強化による価値の創出
  - 組織のセキュリティ状態の強化

誤解のないように言えば、専用のセキュリティオペレーションセンター、アナリストによる専門チーム、脅威インテリジェンスのバックグラウンドがあれば確かに役立ちますが、これらは必須ではありません。必要なのは、テレメトリが何を提供するのかを理解することだけです。そうすれば、各部門は古くて時代遅れの情報に基づく事後対応的なプロセスに頼るのではなく、リアルタイムのデータに基づく意思決定に即した、先回り型のワークフローを構築できるようになります。

テレメトリとは

テレメトリ（Telemetry）の語源を調べると、ギリシャ語の「tele」（遠く離れた）と「metron」（測定）に由来する2つの単語の組み合わせであることがわかります。大まかに訳すと「遠隔測定」です。

エンドポイントセキュリティの文脈では、テレメトリとは、デバイスが自身の健全性やアクティビティに関して絶え間なく送る測定データを指します。具体的には、何が実行されたか、何が変更されたか、誰が変更したか、いつ何に接続したかなどの情報です。

macOSエンドポイントの場合、テレメトリには一般的に以下のものが含まれます。

- **アクセス追跡：**誰が、いつ、どこからログインしたか、どのリソースを要求したか、権限昇格の要求など、どの権限が許可または拒否されたかを記録します。
- **プロセス実行：**アプリの起動、バックグラウンドタスク、関連する子プロセス、カーネルやユーザ空間との相互作用を追跡します。
- **システムイベント：**構成のずれ、アップデートの成否、システムファイルの変更、ハードウェアやソフトウェアの状態の変化を記録します。
- **ネットワークアクティビティ：**暗号化強度やネットワークの種類、IP情報、ポート、プロトコル、データ送信アプリケーションなど、接続の詳細を記録します。
- **診断ログ：**システムの動作やパフォーマンスのデータに加え、クラッシュレポート、コード状態、メモリダンプを収集します。

テレメトリを確認する際、個々のデータは軽視され、忘れられたり見落とされたりしがちです。しかし、パズルのピースが1つだけでは意味をなさないのと同様に、すべてのテレメトリデータを組み合わせて初めて全体像が明らかになります。これらが一体となることで、特定の時点におけるエンドポイントの健全性を検証するための詳細な分析データがIT/セキュリティ部門に提供されるのです。

脅威ハンティング、パッチ管理、コンプライアンス検証など、各部門がそれらの測定データをどのように活用するかは、また別のステップです。

テレメトリには含まれないもの

多層防御戦略における他のセキュリティ対策と同じく、できる限り効果的に抜けが内容に防御を多層的に構築するには、管理者はどこにギャップが存在するかを理解する必要があります。同様に、テレメトリを効果的に活用するためには、その利点だけでなく、限界についても十分に理解しておく必要があります。

以下のものは、テレメトリに含まれません。

- ユーザの個人的な活動や閲覧習慣の監視
- 管理タスクやセキュリティ修復ワークフローを実行するツールの代替物
- エンドポイントのライフサイクル全体にわたる包括的なコンプライアンスの証明

テレメトリデータは、デバイス（またはデバイス全体）から収集され、ログに保存された情報にすぎません。それ以上の処理を適用しなければ、テレメトリ自体はほとんど役に立ちません。テレメトリが価値を発揮するのは、組織がそれを活用したときです。まず、テレメトリをレビューするか、セキュリティ情報イベント管理（SIEM）ソリューションにストリーミングして分析し、そのコンテキストをデータに基づく意思決定として管理、セキュリティ、コンプライアンスのワークフローに適用することが必要です。

ここが大きな分かれ目です。

収集してもMDMやエンドポイントセキュリティソリューションに活用されないテレメトリデータは、Apple MacBookの製造に使用されるアルミニウムの塊と大差がありません。アルミニウムそれ自体は、ユーザが業務を遂行するうえで何の役にも立ちません。しかし、Appleはそのアルミニウムを製造プロセスに活用することで、ユーザが職務を果たしたり、クリエイティブな活動を行ったりできるノートパソコンを製造しているのです。

この例えにおいて、テレメトリは原材料（アルミニウム）に相当します。組織は、テレメトリを活用して初めて、コンプライアンスプログラムを構築できるようになります。それは、包括的な可視性と、個々のデータポイントを組み合わせることで浮かび上がるパターンの把握から始まります。

テレメトリの働き：クエリからインサイトへ

テレメトリとは何かを説明したところで、視点を少し変えて、エンドポイントに存在するテレメトリデータが、デバイスや組織のセキュリティ状態に関する意思決定をどのように変革するかを見ていきましょう。

テレメトリの流れについて理解を深めるために、パイプラインの4つの段階をそれぞれ詳しく見ていきます。

1 収集

macOSプラットフォームは、デバイス上で発生するすべての事象をリアルタイムで捉えるシステムレベルのイベントストリームを生成します。この健全性データは、カーネルレベルやハードウェアセンサーから収集され、AppleのEndpoint Security APIによって監視されるパフォーマンスメトリックが記録されます。

2 集約

ローデータを収集した次のステップは、統合ログシステム（ULS）を介してこの情報を解析することです。この段階では、収集されたデータが各デバイスの構造とストレージ要件に合わせた形式へ変換されます。

3 処理

データがログに記録された後、XProtectやMRTなどのmacOSネイティブツールが、サードパーティのセキュリティエージェントとともに、リアルタイムでログストリームにアクセスします。これらのツールはデータストリームを読み取って分析し、最終段階に向けて高シグナルイベントを優先的に処理します。

4 レポート

この段階では、処理・構造化が完了した質の高い詳細なテレメトリデータが、ファーストパーティの標準プロトコル（クラッシュレポートや使用状況分析を確認するAppleの診断サーバなど）やサードパーティのデータ分析ツールを介して送信されます。

テレメトリデータをパイプラインに送り込んだ後は、一般的にはIT部門やセキュリティ部門がデバイスログをレビューしてエンドポイントの健全性を評価し、潜在的な問題を識別します。デバイス1台で生成されるログの数は多く、しかも社内の全デバイスでログが延々と生成されるため、データを常時SIEMソリューションに送り、重大度や組織のコンプライアンス要件に基づいて整理することが推奨されます。つまり、「干し草の山から針を探し出す」ように膨大なエントリを苦労して選り分けるのではなく、テクノロジーを活用し、レビューが必要な重大度順にイベントを並び替えるのです。

貴社の規模や人員によって、この段階が部門横断型のチームでテレメトリデータを細かく調査し、確認された問題に対処するかどうかの分かれ目になります。

例えば、専任のIT部門とセキュリティ部門を配置している組織の多くは、これらの部門を1つの部門として連携させ、それぞれの強みを活かし、重大なパッチの適用漏れが発覚したエンドポイントにコンプライアンスポリシーを適用するようになっています。セキュリティ部門が検出結果が本当であるか検証し、IT部門が検証結果に基づいてMDM内でコンプライアンス違反のデバイスをグループ化します。この連携が転換点となり、エンドポイントセキュリティソリューションで修復を自動化して、最新のテレメトリデータを収集しコンプライアンスを検証できるようになります。

つまり、テレメトリで得られるどのようなインサイトが得られるか把握するうえで、その基盤プロセスで使用するプロトコルやデータタイプ、API呼び出しを丸暗記する必要はありません。重要なのは、データがパイプラインを移動する仕組みと、IT部門とセキュリティ部門が現在のデバイスの状態を把握するうえ役立つ内容を知り、コンプライアンスを確保する道筋を理解することです。

可視性：テレメトリが実現する成果

テレメトリと可視性には大きく異なる点が1つあります。テレメトリは入力で、可視性は出力です。これらの言葉はよく似ているので同じ意味で使われがちですが、その差異は区別が必要になるほど大きいため、混同しないように注意する必要があります。

これらの違いを簡単につかむ方法が、「原因」と「結果」です。テレメトリは問題の「原因」、つまりデバイスの構成ミスなどを示します。可視性は、構成の誤りの具体的な内容とその影響を受けるデバイス、つまり「結果」を明らかにします。

業務の観点で見ると、可視性とは、社内のデバイス全体で現在起きていることを正確に評価したものです。同時に、表面化した問題に対処するための有用な方針を定めるものでもあります。可視性は、次のような疑問に答えを提供します。

- ベースライン挙動は監視されているか？
- どのデバイスが健全か？
- どのデバイスが危険か？
- 進行中の脅威はあるか？

テレメトリは、この可視性を実現するデータの集まりです。社内のあらゆる管理対象エンドポイントから収集した情報で構成され、以下のようなデバイスの健全性に関する詳細な情報をリアルタイムに提供します。

- 適用されていないシステムまたはセキュリティのパッチ
- インストールされている未承認アプリ
- ベースラインから変更された構成

テレメトリがあれば可視性を確保できますが、ひとりでにそうなるわけではありません。エンドポイントを絶えず監視し、大量のテレメトリを収集しても、デバイスの健全性やコンプライアンス状態を可視化できないということは起こり得ます。

テレメトリ = 入力

可視性 = 出力

テレメトリを収集しても可視性を実現できない理由

テレメトリ ≠ 可視性。

前者は後者を実現する要素であり、その材料でもあります。しかしその関係が成立するのは、データをレビューし、コンテキスト化して決断や行動に活かしたときだけです。データのレビューも意思決定もなければ、テレメトリは読まずに積まれた本と同じです。有用な情報が豊富に記載されていますが、ユーザの役に立つことはありません。

可視性をオン/オフ式のスイッチと考えるのはやや不正確で、連続的なスケールとして捉えた方が正確です。スケールの一端は可視性が100%実現された状態、もう一端は可視性がゼロの状態です。これを踏まえ、貴社の現状が可視性スケールのどこに位置するかを考えてみてください。

この検討の参考として、以下に可視性スケールの両端に位置する企業の例を示します。

可視性ゼロ：MDMへのデバイス登録を義務付け、12時間間隔のチェックインでデバイスレコードを更新している組織。この場合、デバイスの健全性の情報は限定的で、リアルタイムの可視性はまったく得られません。チェックインに時間差があるため、収集したデータはどれだけ新しくても12時間前のものになります。デバイスが定期チェックインを実行できなかった場合、次の予定時刻まで収集が行われないので、集まる情報はさらに古くなります。

また、MDMは多彩な機能を備えていますが、エンドポイントセキュリティソリューションの代わりとなるようには設計されていません。つまり、マルウェアの兆候や不審な挙動などのリスク指標は収集されません。加えて、封じ込めワークフローを自動的に実行することができないので、可視性不足によりセキュリティ状態も損なわれます。

可視性100%：MDMへのデバイス登録を義務付け、12時間間隔のチェックインでデバイスレコードを更新し、かつエンドポイントセキュリティを統合して能動的にエンドポイントを監視している組織。これらすべての措置により、デバイスの健全性に関する包括的なインサイトを得て、リアルタイムの可視性を確保できます。MDMの定期チェックインには時間差があるものの、能動的に監視によりセキュリティエージェントからパイプラインにテレメトリデータが継続的に送られるので、社内のデバイス一つのエンドポイント健全性がリアルタイムで正確にわかります。

エンドポイントセキュリティがMDMソリューションと統合されているため、リスクの可能性がある挙動、アプリ、コードがないか常時監視し、検出した際には自動で阻止できます。さらに、侵害されたエンドポイントの隔離やリスクの軽減のようなワークフローを実行することもできます。並行して各部門に最新の健全性データを提供して、ポリシーベースの管理でコンプライアンスの確保を進めたり、監査でのコンプライアンスの証明としてタイムスタンプ付きの証拠を用意したりすることも可能です。

つまり、可視性とは、テレメトリをセキュリティに役立つものとして利用することで得られる成果です。重要なのは、人員やツールを増やすことではなく、現在運用中のmacOS、iOS、iPadOSデバイスで得られるテレメトリをインサイトに変えることです。このインサイトがあれば、推測や1日前や2日前の最終チェックイン時の情報ではなく、全デバイスの正確な健全性状態に基づいて、大規模に意思決定や行動を進められます。

検出・調査・対応には可視性が役立つ

可視性が有益である理由は、単にコンプライアンスに関するインサイト、さらにコンプライアンスのセキュリティ状態への影響がわかることだけではありません。その価値は、以下のような日々のIT・セキュリティ業務にまで及びます。

検出

IT部門は、ベストプラクティスに基づき、自社に合わせてベースラインから標準の業務手順やパフォーマンスレベルを策定しています。テレメトリ、ひいては可視性を利用すると、構成がベースラインに合っているか、それとも逸脱しているかなど、デバイスの健全性に関するインサイトが得られます。さらに可視性は、ベースラインからの逸脱など、異常な挙動を見つけるうえでも役立ちます。これにより異常性をできる限り早期に検出できるので、多数のデバイスを運用する際に特に有用です。言い換えると、リアルタイムの可視性があれば、従来であればインシデントへと発展するまで見過ごしていた問題を、未然に検出できるようになります。

調査

可視性が一番効果を発揮するのは、ほぼ間違いなくこの業務です。異常が検出されると、セキュリティ部門はすぐさま調査モードに切り替わり、問題を検証して、以下のような大量の質問に答えることになります。

- 何が起きたのか？
- いつ起きたのか？
- なぜ起きたのか？
- 影響はどの程度か？

率直に言うと、テレメトリがない場合、上記やそれ以外の重要な質問への返答は、ユーザの説明に基づく推測、憶測、伝聞証拠に頼るほかありません。ここで言いたいのは、こうした説明が間違っているということではなく、説明の検証にあたる技術担当者に大きな負担がかかるということです。これに対し、テレメトリはエビデンス、つまりイベントの時系列に沿って何が起きたかを説明する明確な証拠となります。

対応

この業務に対する可視性の影響を最もよく表すなら、「理解が行動に変わるポイント」と言えます。問題の検出、およびセキュリティ部門でのエビデンスのレビューが終わると、テレメトリ主導のインシデント対応ワークフローを通じて、再現性のある手順でリスクの抑制と最大限の修復を両立するために必要なインサイトが提供されます。

- 侵害されたエンドポイントを隔離して影響を封じ込める
- 深刻度/重大度で脅威を優先順位付けする
- リスクを軽減して、長引く脅威を根絶する
- エンドポイントを修正し、ベースラインのパフォーマンスに復旧する

> > >

対応：可視性の有無の影響

前述の通り、可視性100%の組織と可視性ゼロの組織には対照的な違いがあります。決定的なポイントは、前者が収集したテレメトリデータを積極的に活用しているのに対し、後者は収集しただけで役立てていない（または古いデータに頼っている）ことです。本書ではこうした例をはっきりと示していますが、この違いが最も明確に認められるのは、技術部門がインシデント対応に追われているケースです。

以下に、「会社支給のデバイスに脆弱性のある未承認アプリがインストールされ、ランサムウェア攻撃を受けた」インシデントへの対応を例に、2つの部門（AとB）の相違点を示します。

部門A：可視性ゼロ

- **対応用の情報が不完全：**インストールされたアプリはわかるが、脆弱性の程度は不明
- **問題の兆候が出てから対応：**まずデバイスのパフォーマンスが低下し、その後データがアクセス不能に
- **データソースの裏付けなし：**情報は影響を受けたユーザから提供され、裏付けを取れない
- **解決作業の手間がかさむ：**裏付けとなる指標がなく、根本原因の修復作業の手間が増える
- **デバイス数の拡大に追随不可：**デバイスが増えると作業の負担、さらにはリスク要因や露出期間も大幅に増加

部門B：可視性100%

- **包括的なデータで隙間なし：**インシデントを内側から確認し、原因、推移、影響を明確化
- **検出から解決まで実施：**推測に頼ることなく、時系列を完全に把握してインシデントを修復
- **最新、正確、裏付けあり：**エンドポイントの健全性状態を社内各部門や監査人向けに情報で証明
- **状況に照らしてデータをレビュー：**カーネルやセンサーからのインジケータも情報として収集し、全体像を解明
- **デバイスが増加しても作業増なし：**拡張性が念頭に置かれているので、管理者の負担を増やすことなくプロセスおよびワークフローが自動的に順応

負担を増やさずに業務をスマート化

テレメトリには、自動化を促進する効果があります。

テレメトリ駆動型のワークフローにモバイルデバイス管理、エンドポイントセキュリティ、アイデンティティベースのアクセス管理を組み込むと、これまでにない形で多岐にわたる面倒な作業をテクノロジーにまかせ、デバイス管理とセキュリティ戦略を拡張できます。管理者は、自身のスキルを存分に発揮して環境を拡充し、ビジネス成果に合わせて業務を調整できるようになります。

例として、エンドポイントセキュリティで脆弱なアプリを検出し、MDMソリューション経由で修復をトリガするポリシーベースの自動化を考えてみましょう。このワークフローはシンプルですが、ユーザの業務に影響を及ぼしたりインシデント化したりすることなく、IT部門のサポートなしでセキュリティ状態を維持し、リスクを軽減できます。

現代の組織では、人工知能（AI）/機械学習（ML）テクノロジーにあらゆる規模の部門の力を何倍にも強める効果があることが認められています。プロセスにAIを利用すると、社内デバイス全体にわたりきわめて迅速に高度な脅威を探し出すことができます。このプロセスは各エンドポイントから収集したテレメトリデータの関連性を調べ、複数のオープンソース/クローズドソースの脅威インテリジェンスデータベースと照らし合わせて分析することで、未知の脅威を検出し、各部門に通達します。また、拡張性に優れた自動化オプションを利用すれば、重大度の低い問題を自律的に処理するポリシーベースのワークフローも、人の判断が必要なインシデントについては人を介在させる仕組みも簡単にワークフローに組み込めます。

ソリューションは貴社固有のニーズに合わせてカスタマイズできるため、質の高い情報に基づいてインシデントを迅速に解決可能です。これにより、効率を最適化し効果を最大限に高めながら、リスクと手作業を最小限に抑えられます。

状況別のテレメトリ：コンプライアンス、業務、組織にとっての価値

先述した脅威の調査およびインシデント対応におけるメリットに加えて、組織でのテレメトリの扱いについて同じく重視すべき領域はさらに2つあります。

コンプライアンス

世界的に、医療、金融、教育などの業界にはますます法規制で厳しい監視の目向けられるようになっています。連邦政府および地方の指令により、データのセキュリティが確保されていること、データにアクセスするデバイスの構成がコンプライアンス要件に準拠していることの立証が義務付けられています。

ここで強調しておくべきは、コンプライアンス要件が満たされているという主張には証明が必要であることです。多くの監査人の基本的な判断基準は、「証明できないのであれば、デバイスはコンプライアンスに準拠していない」ということに尽きるからです。

テレメトリは、この立証を可能にする「秘伝のソース」です。先に述べたように、テレメトリそれ自体は、ただのデータの集まりにすぎません。レビューし、コンテキスト化して意思決定や行動に活かさなければ、可視性は得られません。同じように、まず適切なセキュリティ対策とポリシーを導入していなければ、テレメトリでコンプライアンスを確保することもできません。

背景情報と結びつけ、セキュリティ対策を実装することで、テレメトリは評価時点で適切に動作していたことを証明する（またはそうでないと証明する）原動力になります。公的な監査以外でも、エビデンスとなるデータ（テレメトリ）は他のコンプライアンス関連の領域でも重要です。具体的には、次セクションで説明する業務や、サイバーセキュリティ保険が挙げられます。後者では、ほとんどの保険業者において、保険期間の開始前または更新前、または請求時にセキュリティを実施していたと示す証拠が求められます。

業務

先ほどの「検出・調査・対応」の例で示したように、このテレメトリデータはIT業務にもメリットをもたらします。IT部門およびセキュリティ部門の職務に役立つのはもちろんですが、IT責任者と幹部陣にとっては、別途プロセスを実施したり、タスクを増やしたり、個別のレポートを生成したりすることなく、組織の健全性およびコンプライアンス状況をリアルタイムに把握する材料となります。

テレメトリには様々な側面があり、リアルタイムのテレメトリを基にレポートを作成すれば2つの効果を同時に実現できます。1つは、技術部門の日常業務を支援すること。もう1つは、コンプライアンス状態およびリスク評価をエビデンスに基づく信頼性の高い文書にまとめて様々なビジネス事例をサポートし、最新の正確なデータに基づく意思決定を可能にして、今後の事業展開に関する議論を促進することです。

つまり、テレメトリの基本的な価値は、人員数や組織構造に左右されません。レビューを行うのが単独のIT管理者であっても、セキュリティアナリストのチームであっても、その効果は同じです。ただし、テレメトリは広い範囲で使われるべきものです。「セキュリティチームだけが使う」ものではなく、質問者に応じて様々な役割を果たします。

テレメトリと可視性の現状の評価

テレメトリおよび可視性について、その概念を理解するのは有用です。これらが組織の現状把握にどう役立つかを知るのは、さらに有用です。第一歩としては、新しいツールを購入することも、特別なトレーニングを実施することも、既存テクノロジーの構成を変更することも必要ありません。まずは、組織のテレメトリおよび可視性の運用状況を自身で評価しましょう。

まずは、以下の質問について考えてください。

1. エンドポイントのログデータをデバイス上に保存していますか？それとも、解析用に一箇所（SIEMソリューション）にストリーミングしていますか？
2. 社内の全デバイスについて、自信を持って現在のセキュリティ状態を判断できますか？
3. エビデンスに基づいてインシデントの時系列を再現できますか？それとも、影響を受けたユーザの事態に関する説明のみに頼っていますか？
4. 本日求められた場合に、監査用にタイムスタンプ付きのコンプライアンス証明を生成できますか？
5. コンプライアンス違反が検出された場合に、自動で修復されますか？それとも、手動での対応が必要ですか？

上記の質問に対する答えでわかることは、貴社のセキュリティ状態の詳細だけではありません。さらに重要なこととして、**リスクを未然に軽減できるのか、インシデントが起きてから受動的に対応せざるを得ないのか**を特定できます。以下に、注意すべきよくある落とし穴をいくつか示します。

- 豊富なテレメトリがあっても、エンドポイントに保存しているか既存テクノロジーと共有している場合、気づかないうちに可視性に穴が生じる
- クロスプラットフォーム環境で一部イベント（Windows）は転送し、他は孤立させている場合、組織にリスクが生じる
- テレメトリの収集はソリューションの一端に過ぎず、その真の価値を発揮させるには定期的にレビューし行動に活かす必要がある

逆に言うと、以下の特性を備えていればセキュリティ体制が成熟しています。

- テレメトリは誰かが思い出したときだけレビューされるのではなく、絶えずパイプラインを流れ、ワークフローに組み込まれている
- 収集したデータを複数のソースに照らして分析し、関連付け、重大度に応じて優先順位を設定している。手作業で整理していると、重要な情報を見逃す可能性がある
- コンプライアンスプログラムに成功する鍵は、人員や予算の多さではなく、生成されたテレメトリを活用して意思決定や行動を進めること
- ほぼすべての場合において、新しいツールを導入して可視性を実現しようとするより、既存データを材料に可視性を構築する方が早く先へと進める

まとめ

何度でも繰り返します。レビューをしなければ、テレメトリはただのデータの集まりです。

デバイスの動作、構成状態、脆弱性に関する情報をタイムスタンプ付きで常時ストリーミングしても、軽微な問題が多大な損害をもたらすコンプライアンス違反へと静かに発展する前にその情報から得られた知見に基づいて行動を起こさなければ、何の役にも立ちません。

得られたテレメトリデータをデータに基づく意思決定の材料へと変え、リアルタイムの健全性状態に基づいた速やかな対処へつなげること。それが「可視性」です。データが正確かつ最新のものであれば、パイプラインからゴールである意思決定者へ、信頼性のある情報を届けられます。

管理と保護の間にある溝は埋められるものです。ただし、必ずしもそのために資金を追加したり、チーム全体に専門知識を広めたり、既存環境に大幅な変更を加えたりする必要はありません。現在お使いのデバイスはそれぞれの動作を記録するように設計されており、現在の状況を残らず伝えています。

本当の問題は、貴社がそうしたデバイスの声に耳を傾け、行動に活かす準備ができているかどうかです。

ぜひお試しください

トライアルに申し込む