セキュリティ・スポットライト：人的ミスのコストと自動化のメリット

政府機関がセキュリティ管理に対する手作業のアプローチを見直している理由と、インテリジェントな自動化でコストの高いセキュリティギャップから生じる潜在的な脅威を防止する方法

次へ

この e ブックの内容

01 はじめに：増大するサイバー犯罪の脅威

サイバー犯罪は増加しています。実際に、サイバーセキュリティのインシデント数は 2021 年には 15.5% 増加し、重大な侵害は 24.5% 増加しています。[1] にもかかわらず、公共セクターの組織の 34% が、急速に変化する脅威の状況に適切な準備ができていないと回答しています。[1]

政府機関が新しいテクノロジーを取り入れてハイブリッドモデルの働き方に適応していくにしたがって、サイバー犯罪者もその能力を変革させています。従業員やコンピューティング・リソースの分散化が進み、IT インフラストラクチャを取り巻く環境が急速に進化したことで、悪意のある人物がセキュリティのギャップや脆弱性を悪用する新たな機会が生じています。そのため、データ漏洩による組織上のコストが上昇しています。このような環境にあっては、強力なセキュリティ体制を構築した組織であっても、リスクの増大は避けられません。

サイバー犯罪に対するプロアクティブなセキュリティ

保護されたシステムやデータを侵害する新たな方法をサイバー犯罪者が考え出しているため、組織はより戦略的でプロアクティブな保護を開発するよう、内外からのプレッシャーを受けています。事実、組織のデータセキュリティやプライバシー対策は、より包括的な規則および法令に順守しなければなりません。

こうしたセキュリティやプライバシー規制の強化傾向は、業界や地域を問わず、あてはまります。たとえば、EU の一般データ保護規則 (GDPR) は、個人データの収集、使用、保護の方法に対する厳格なルールを規定しています。シンガポールのサイバーセキュリティ法が規定するフレームワークでは、重要な情報インフラストラクチャの所有者が、ガバナンス、アクセス制御、インシデントの検出と対応、その他の領域に対する特定のベストプラクティスに従うことを要求しています。アルゼンチンの Dirección Nacional de Ciberseguridad も、重要な情報インフラストラクチャを保護し、セキュリティインシデントの防止、検出、対応、修復を国家レベルで向上するポリシーを発行しています。さらに、米国政府機関は、2024 年末までにゼロトラスト・アーキテクチャをデプロイして、連邦政府のサイバーセキュリティの目標を達成する必要があります。

防御機能の強化

サイバーセキュリティの強化を目指すには、まず既存の脆弱性を特定する必要があります。包括的な戦略がすでに実施されていても、人的ミスと認識不足がセキュリティ侵害を招くことが多々あります。小さなミスを放置しているとシステムへのリスクが生じ、すでに複雑な問題をさらに悪化させます。この結果、信頼性の向上とリスクの低減を目的として、セキュリティ戦略への自動化の導入が進んでいます。

この e ブックでは、人的ミスによって生じたリスクがサイバー犯罪に対する対応にどのように影響するかを確認します。また、サイバーセキュリティの主要なリスク軽減戦略を自動化すると、セキュリティが強化され、IT チームの負担となる時間のかかるタスクの量が低減されることを説明します。

サイバー犯罪が世界にもたらすコスト

24.5%

2021 年における重要な侵害数の増加率[1]

43.5 億米ドル

データ漏洩の世界的な平均コスト[2]

60%

データ漏洩を理由としてサービスや製品の価格を上げた組織の割合[2]

1. ThoughtLab、「Cybersecurity Solutions for a Riskier World」、2022 年
2. IBM、「2022 年データ侵害のコストに関する調査レポート」、2022 年 7 月。

02 効果的なセキュリティ戦略には全員の関与が必要

人間にミスはつきもの

IT チームのメンバーであっても、システムの脆弱性やそれによるセキュリティリスクを過小評価したり誤解したりすることがあります。リスクを正確に評価できないと、組織にコスト面で大きな損害を与えかねません。

例を取って考えてみましょう。ファイアウォールが原因でプロダクションの障害が発生し、ファイアウォールのエンジニアが重圧の中でポリシーを手作業で更新せざるを得ないとします。変更によって障害は修復されますが、サイバー犯罪者が悪用できる新たな攻撃ベクトルも導入されてしまいます。

このシナリオでは、手動でファイアウォール構成を急いで変更したことから、データの漏洩、業界および政府のデータセキュリティ規制への違反、サービス停止、システムのダウンタイムなど、さまざまな好ましくない結果が引き起こされ、そのコストはすべて組織に降りかかります。

セキュリティにはアプリケーションへのパッチ適用、ファイアウォールの更新、管理者権限の設定と適用など数多くの要素がありますが、これらを手作業で処理するとエラーの入り込む余地が生まれます。また、脆弱性を特定して悪用するサイバー犯罪者の能力が高くなっているため、手作業の運用のみに頼ってこれらのセキュリティタスクを処理していると、好ましくない結果や修復できない結果に至る可能性があります。

人材不足はセキュリティギャップを悪化させる

サイバーセキュリティスキルを持つ人材は需要に追いつかず、手作業による人的ミスの発生確率は高まるばかりです。セキュリティリスクの評価と対処のスキルを持ち、トレーニングを受けた人材が不足しています。(ISC)^2 Cybersecurity Workforce Study によると、世界的なサイバーセキュリティのギャップを解消するには 272 万人以上の IT セキュリティ担当者が必要です。[4]

このようにサイバーセキュリティ専門家が慢性的に不足しているため、組織がリスクを適切に管理することが一層難しくなっています。IT チームはすでに手一杯で、セキュリティプロセスを組織全体に適用する時間がありません。そもそも、プロセスを確立させることすら困難です。

セキュリティチームへの自動化の導入

手動のセキュリティプロセスとスキル不足の双方から高まるリスクへの対処は、サイバー犯罪への対策にとって必須となりました。そして、それに対する有望な解決策が自動化ソリューションです。これから見ていくように、セキュリティプロセスを自動化することで、組織が望んでいた一貫性、精度、スケーラビリティが手に入ります。

手作業でセキュリティ対策を行うことのリスク

「セキュリティ AI と自動化の導入を完了している組織は、それらを導入していない組織よりもはるかに迅速に侵害を検出し、封じ込めることができます」[4]

3. (ISC)^2 Cybersecurity Workforce Study、「A Resilient Cybersecurity Profession Charts the Path Forward」、2021 年。
4. IBM、「2022 年データ侵害のコストに関する調査レポート」、2022 年 7 月。

03 リスク管理の一般的な課題

政府機関にはより優れたリスク管理が必要

公的な情報の機密保持、整合性、可用性を確保するため、政府機関はリスクを正確かつ効率的に特定し、管理できなければなりません。セキュリティ脅威は絶えず進化しているので、組織のリスクプロファイルとセキュリティ体制もそれに常時対応できなければなりません。このような課題に迅速に対応するには、運用の自動化が極めて重要です。

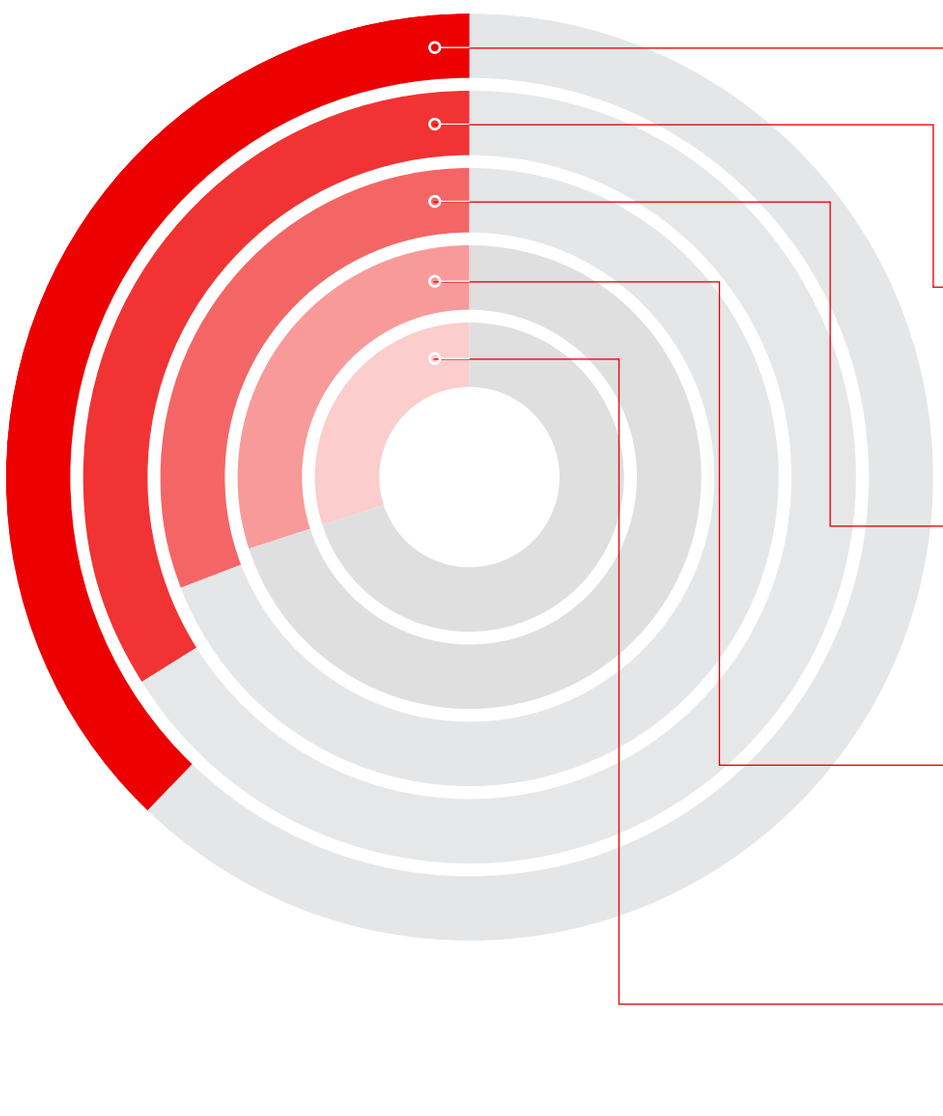
セキュリティ手法の変更を阻む要因

セキュリティを強化しようとする政府機関にはさまざまな課題が立ちはだかり、中でも特徴的な課題は変化の管理に関連するものです。一般的な問題は次のとおりです。

- 新しいサイバーセキュリティの取り組みを実装するには、チームをどのように拡大するのか
- 新しいセキュリティプロトコルに準拠させるには、組織のさまざまな部門をどのようにサポートするのか
- 重要なサービスを提供する既存システムのセキュリティを向上させ、組織が必要とする先進的なセキュリティ戦略を導入するには、何ができるか
- 現在のアーキテクチャでゼロトラストなどの戦略を実装できるか

しかし、これらの検討事項を負担と考えるのではなく、セキュリティの状況の変化を活用してセキュリティ手法を見直し、より厳格なプロトコルを実装するチャンスと捉えることもできます。

サイバーセキュリティの一般的な課題



38%
急速に変化する脅威の状況の把握[5]

34%
リスクや行動に関する教育[5]

31%
内部のサイバーセキュリティ体制の強化[5]

30%
サイバーセキュリティのトレーニングが必要[5]

30%
データ漏洩による法的/財政的影響[5]

5. 「State of the Channel 2021」、CompTIA、2021 年 8 月。

04 自動化によるセキュリティ体制の強化

セキュリティ規制の共通テーマ

あらゆる業界や地域を通じて、データプライバシー、アクセス制御、インシデント対策、検出、対応は、サイバーセキュリティ規制およびイニシアチブ全体で共通のテーマとなっています。実装方法を細かく指定する規制もありますが、多くの規制はガイドラインと必須の成果を規定するだけであり、現在の状況、人員配置レベル、インフラストラクチャに応じた最適な準拠方法の判断は各組織に任されています。

セキュリティ自動化は、政府機関および組織がサイバー犯罪に対応し、規制に準拠するのに役立ちます。定型的な繰り返し作業を自動化すると、セキュリティチームはより重要で戦略的なタスクに専念できます。さらに自動化は、人的ミスが発生しやすく、セキュリティ上のリスクを増加させるタスクや仕事量を減らし、IT チームが過負荷にならないようにする手助けにもなります。

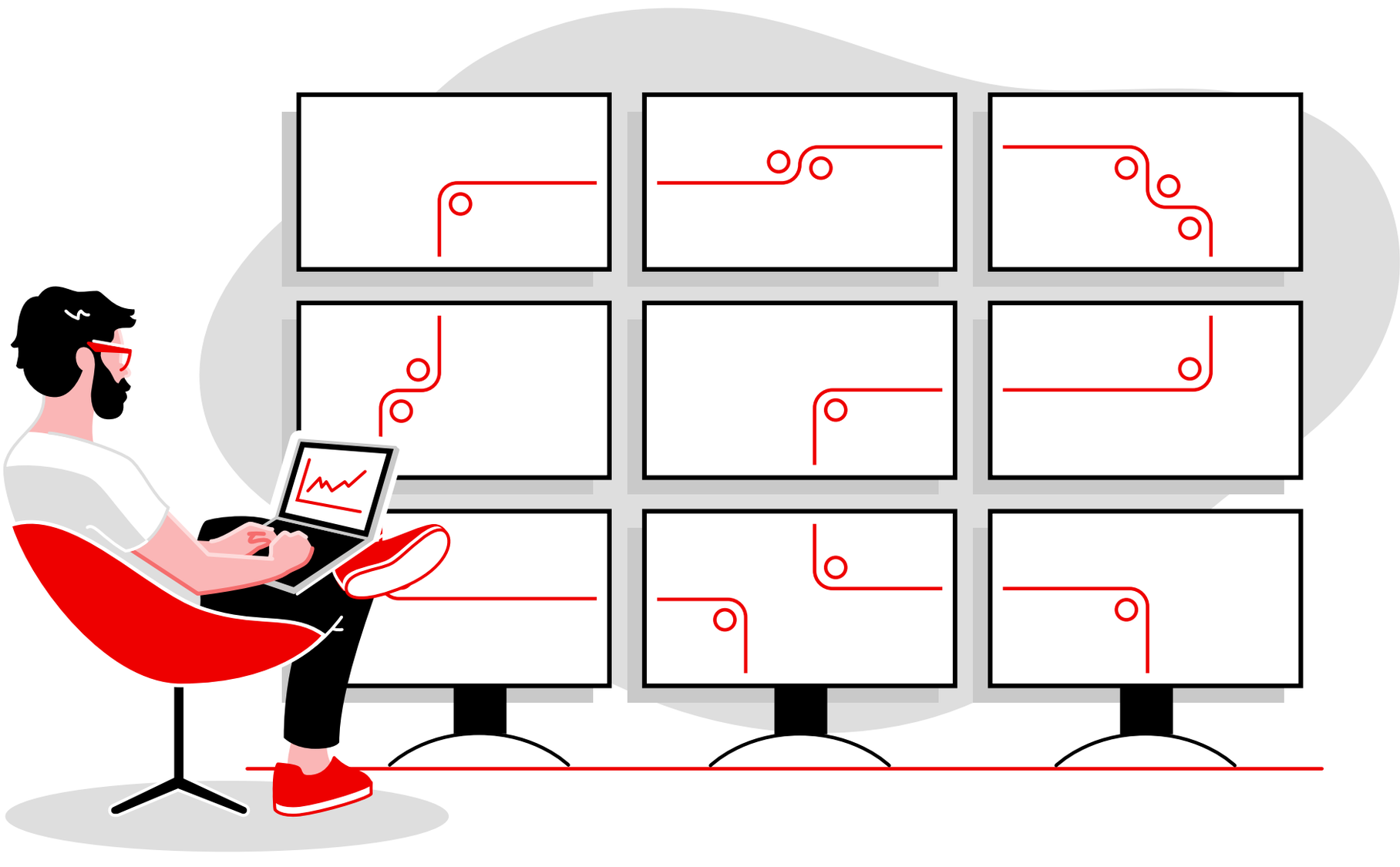
セキュリティ自動化がチームをつなげる

セキュリティ自動化は、組織全体でチームとドメインを連携させて、リスク管理、サイバー脅威への対処、インシデントの軽減を改善するための、さまざまなプラクティスで構成されます。たとえば、セキュリティアナリストはインシデントの対応および修復プロセスに自動化を適用できます。IT 運用チームはパッチをシステムに自動的に適用させてコンプライアンスを施行できます。ネットワーク管理者はネットワークアクセス制御をセットアップして維持できます。

セキュリティ自動化は、IT チームとセキュリティチームが、人事、顧客ケア、法務チームなど、セキュリティ規制の影響を受ける組織内の他の部門とより効率的に共同作業するためにも役立ちます。たとえば、ほとんどの組織はそれぞれのセキュリティ統制を検証し、サイバーインシデントを報告して、法的要件に準拠する必要があります。規制監査担当者にはコンプライアンスの証明が必要ですが、組織のセキュリティシステムを直接操作することはない場合があります。セキュリティ自動化を外部のログ記録システムと統合してアクションを記録すると、監査担当者が必要とするレポートや証拠を提供することができます。

自動化を適用してリスクを管理する

組織内の主要なプロセスを自動化すると、能動的および受動的なセキュリティ体制の強化に役立ちます。以降のセクションでは、どの地域であっても、規制に準拠して組織に実際のインパクトを与えるためにセキュリティ自動化が役立ついくつかの領域について説明します。



インシデントの対応と対策

2022 年には、データ漏洩を特定して封じ込めるまでに平均して 277 日間が必要でした。[6] 200 日以内にセキュリティ侵害の検出と阻止ができれば、侵害の平均コストが 26.5% 削減されます。[6] しかし、侵害の検出と修復を複数のプラットフォームやツール、環境にわたって手作業で行うと、複雑で時間がかかり、ミスが発生しやすくなります。

インシデント対応では、侵害の継続を阻止するためのアクションを取ります。侵害が発見されると、セキュリティスタッフはそれを阻止するために迅速かつ大規模に対応する必要があります。しかし、多くの場合、対応アクションには、接続されていないシステムで実行される複数の手動タスクが含まれているので対策の実施に時間がかかり、組織が脆弱な状態が長時間続くことになります。

修復アクションを反復可能な承認済みの Playbook として体系化すると、セキュリティ自動化を利用してインシデントへの対応を迅速化できます。IP アドレスやドメインへの攻撃のブロック、脅威ではないトラフィックの許可、悪用された資格情報の凍結、インシデントに関連する損害を最小化するためにさらに調査をする際の疑わしいワークロードの分離などのタスクをスピードアップできます。

パッチ適用とシステムアップデート

攻撃防止を支援するため、多数のサイバーセキュリティ標準では、システムとアプリケーションに定期的にパッチを適用してアップデートすることを推奨しています。とはいえ、手作業でパッチ適用やアップデートを行うと人的ミスが発生しやすくなり、大規模組織では特に、長時間を要することになります。

迅速な対応の重要性

277 日間

2022 年のデータ漏洩の特定と封じ込めにかかった平均時間[6]

26.5%

200 日以内に検出および特定されたデータ漏洩のコスト削減[6]

パッチ適用は自動化ワークフローのまたとないユースケースです。手作業によるテスト、プレフライトチェック、パッチデプロイメントに頼るのではなく、 検証と評価を自動化できます。このようにすると、これらのすべてのステップがスムーズかつ効率的に進行し、その裏側では適切なセキュリティが適用されます。

特権および認証情報の管理

データ漏洩の最も一般的な原因は、認証情報の盗難または漏洩です。[6] 特権アクセスと認証情報を一元化および管理すると、リスクが軽減され、データプライバシーおよびセキュリティの規制に準拠しやすくなります。

最小権限の原則を使用して、実際に必要なアクセスだけをユーザーに付与します。各ユーザーの現在のアクセス権を監査して再評価する必要がありますが、このアプローチをとることで、盗難または漏洩した認証情報の影響を最小化できます。

アクセス認証情報を一元的に保存すると、アプリケーションに直接挿入するという、脆弱性が高まる操作を行う必要性がなくなります。特権アクセス管理ワークフローを自動化すると、プロセスが管理しやすくなり、信頼性と一貫性が向上します。ゼロトラスト・アーキテクチャおよびアプローチの基盤ともなります。

コンプライアンスとポリシー適用

組織の最大のセキュリティ侵害のうち 44% の主な原因は、構成ミスです。[7] 構成が不適切なシステムは、攻撃に対して脆弱になります。プロビジョニング時点で適切に構成されたシステムも、組織に強力な変更管理機能がないと、時とともに攻撃を受けやすくなります。

システムおよびアプリケーションのライフサイクル全体を通じてポリシーを適用すると、システムが使用開始時に適切に構成され、その構成がその後も維持されるようになります。自動化は、これをすばやく大規模に行い、分散したシステムおよび環境に対して一貫性を向上させるのに役立ちます。自動化を変更管理プロセスに適用すると、変更要求が承認され、変更アクティビティがログに記録され、監査用のレポートが生成されることを検証することもできます。

6. IBM、「2022 年データ侵害のコストに関する調査レポート」、2022 年 7 月。
7. ThoughtLab、「Cybersecurity Solutions for a Riskier World」、2022 年

ゼロトラスト・アーキテクチャ

以前の領域をそれぞれ自動化していくと、組織に貴重な経験が蓄積され、ゼロトラスト・アーキテクチャの基盤が構築されます。ゼロトラストは、ネットワーク境界でセキュリティを排他的に管理するのではなく、各アセットにセキュリティを適用するアーキテクチャパターンです。セキュリティ境界の内外で動作する当事者、システム、ネットワーク、またはサービスを暗黙に信頼しません。あるユーザーまたはサブジェクトをリソースに接続するには、そのセッションが認証および認可され、明示的な信頼を確立する必要があります。

ID とアクセス管理はゼロトラスト・アーキテクチャの中核をなすものです。アセットとのやり取りを希望するすべてのサブジェクトは、その特定のやり取りに対するアクセスを要求しなければならず、アクセスを許可する前に、そのやり取りのリスクが評価される必要があります。この評価では、サブジェクトの ID と属性を理解することが重要です。誰がアクセスを要求しているのか、どのアセットにアクセスする必要があるのか、そのトランザクションの目的、アクセスをどのように制限するべきかなど、コンテキスト情報を決定する必要があります。

アクセスの決定が下されたら、ID と ID 属性の保存、管理、キュレート、および更新を一貫性のある保護された方法で行わなければなりません。ほとんどの組織では、この情報を管理するために、ID および特権アクセス管理のためのシステムを少なくとも 1 つ使用しています。また、これらのアクセスの決定を継続的に再評価して、時間が経過しても有効であることを確認する必要もあります。

インタラクションごとにリスク評価が必要になるので、ゼロトラストアプローチでは、インフラストラクチャと組織から大量のデータと情報を収集する必要があります。ここで重要になるのが自動化です。まず、インタラクションの数自体が多すぎて、IT スタッフが手作業では処理しきれません。各インタラクションを手作業で評価しなければならないとしたら、あらゆるリソースにタイミングよくアクセス権を付与することは不可能です。

次に、自動化は、統合されていないシステムからのデータ収集に役立ちます。たとえば、従業員が社内アプリケーションへのアクセスを希望した場合、少なくとも、人事システムから雇用情報を収集して検証し、IT システムから情報を特定し、従業員のコンピュータからステータスと位置情報を更新するという作業をする必要があります。自動化プラットフォームは、通常は相互に連携しない、または連携できないシステムとドメインを接続できるので、情報をすばやく容易に収集、相関付け、分析できます。さらには必要に応じて、この情報をセキュリティ情報イベント管理 (SIEM) やその他の一元化されたセキュリティシステムに送信することもできます。

最後に、自動化することでユーザーイベントやステータス変更に動的に対応できます。ユーザーがロールを退任したり組織内の新しいロールに就任したりした場合、手作業のアクションを待つことなく、変化が起きた時点で、イベント駆動型の自動化を使用して全システムについてその従業員のアクセス権を更新できます。

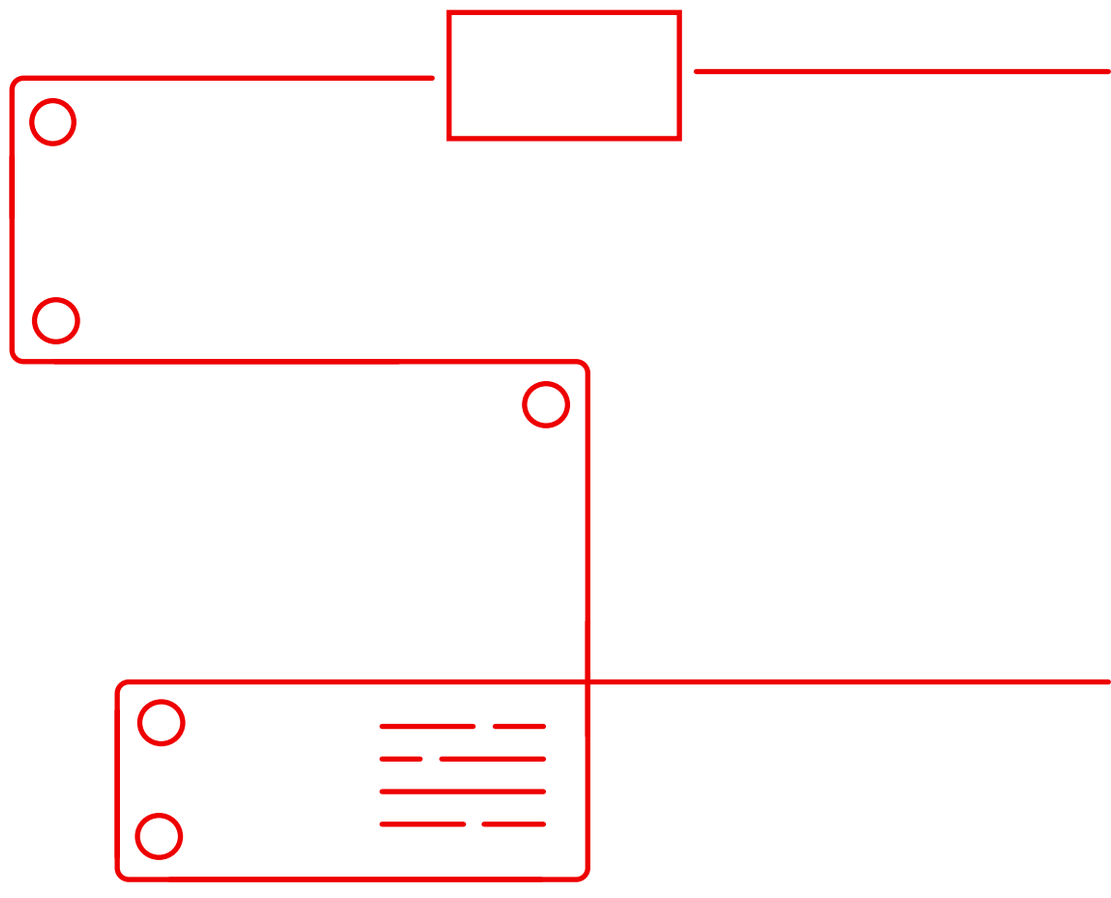
ゼロトラストアプローチのメリット

20.5%

ゼロトラストをデプロイした組織におけるデータ漏洩コストの削減率[8]

165 万米ドル

ゼロトラストをデプロイしていない場合と比較した、成熟したゼロトラストデプロイによるデータ漏洩コストの平均削減額[8]



8. IBM、「2022 年データ侵害のコストに関する調査レポート」、2022 年 7 月。

05 サイバーセキュリティのアプローチにおける Red Hat の役割

将来を見据えたサイバーセキュリティ手法の構築

サイバーセキュリティの成熟度モデルの基盤に自動化を据えることで、すばやく反復的に手作業のプロセスを置き換え、リスクを管理し、セキュリティ体制を向上させる実用的なステップを踏み出せます。Red Hat® ソリューションは、既存の手作業のプロセスの自動化をサポートできるので、人員不足の IT チームが過負荷で見落しを起こすリスクを低減できます。Red Hat のオープンソース製品は、クラウド環境およびアーキテクチャに柔軟性とスケーラビリティをもたらし、現在のセキュリティを強化し、将来の不確実性に備えることができます。

Red Hat Ansible Automation Platform

Red Hat Ansible® Automation Platform は、複雑な手作業のプロセスを自動化ワークフローに転換する、人間が読める形式の自動化言語で構築されています。Ansible Automation Platform により、IT チームは組織内のセキュリティプロトコルを自動化し、統合できます。このプラットフォームを使用すれば、精選された認定済みの自動化コンテンツを通じて、調整かつ統一された方法で脅威を調査し、対応できます。次のものも自動化できます。

- 共通脆弱性識別子 (CVE) のアップデートおよびパッチ適用
- アプリケーション制御のロールアウト
- バックアップ、リストア、検証のプロセス

Ansible Automation Platform は、ハイブリッドクラウドからエッジ環境まで、大規模な IT 自動化を構築して運用するための、セキュリティ重視で安定したエンタープライズ・フレームワークを提供します。この自動化ソリューションにより、開発者や運用チームから、セキュリティおよびネットワークチームに至るまで、組織中のユーザーが自動化コンテンツおよび Playbook を作成、共有、管理できるようになります。IT 管理者は、自動化を個々のチームにどのように適用するかのガイドラインを規定することができ、自動化クリエーターは、既存の知識を利用したタスクを作成できます。

さらに、Ansible Automation Platform には CyberArk、IBM、Splunk などの認定パートナーからのコンテンツが含まれているので、これらを使用してセキュリティ・ソリューションの統合ポイントとして機能できます。これらのコンテンツはセキュリティ・テクノロジーの管理や統合の自動化に使用できます。

Red Hat Ansible Automation Platform の詳細はこちら ›

Red Hat Enterprise Linux

Red Hat Enterprise Linux® は、既存のアプリケーションを拡張し、ベアメタル、仮想化、クラウド、およびエッジにわたるフットプリントで一貫してセキュリティを適用して先進テクノロジーを展開するための基盤を提供します。

Red Hat Enterprise Linux では、セキュリティ上の課題への実用的な対応策として、3 つの側面からなるアプローチを採用しています。

- 軽減：会社のデータやシステム、あるいは評判が危険にさらされる前に、セキュリティを管理し、侵害のリスクを軽減します。
- 保護：最小限のダウンタイムでセキュリティ制御を大規模に自動化し、長期にわたって維持します。
- 準拠：規制の厳しい環境を備えた組織のコンプライアンス基準を最適化します。

Red Hat Enterprise Linux には、コモンクライテリア (CC)、連邦情報処理標準 (FIPS) 140、セキュリティ技術導入ガイド (STIG) などの多数の規制および標準に準拠する組み込みのセキュリティポリシーも含まれており、セキュリティ制御を新しいデジタルサービスに自動的に一貫して適用することで、リスク管理の改善に役立てることができます。

Red Hat Enterprise Linux の詳細はこちら ›

Red Hat

前へ

Red Hat でセキュリティを強化

Red Hat はデジタルサービスのセキュリティ向上をお手伝いします

Red Hat は、規制基準およびガイダンスを自動化し、自動化されたセキュリティ統合によってリスク管理の向上を支援します。

詳細については、今すぐお問い合わせください ＞