コンプライアンスを管理するためのセキュリティ運用のブループリント

資産とID管理のインテリジェンスを
継続的に活用してセキュリティギャップを
プロアクティブに解消するための5つの方法

splunk>

アナリストの重要な職務となったコンプライアンス監視

規制コンプライアンスは今や、セキュリティ担当者にとって、死や税金と同じくらい避けられないものになっています。Splunkの『2024年セキュリティの現状』レポートでは、91%の組織が、セキュリティチームの全員がコンプライアンス対応を業務に組み込んでいると回答しています。実際、そうせざるを得ないのです。今日では、組織の資産が増加し、環境が複雑化する中、すべての資産の状況を把握するだけでなく、コンプライアンスを確保し、かつてないほど幅広い関係者にそれを証明することが求められ、より多くの人手、ツール、資金、時間が必要になっています。

さらに、米国証券取引委員会(SEC)のサイバーセキュリティ開示に関する新しい規則では、サイバーセキュリティインシデントが発生したときに、検出後「不当に遅れることなく」重大度を評価し、重大であると判断された場合は、その時点から4営業日以内にForm 8-KのItem 1.05において情報を開示することが組織に義務付けられています。セキュリティチームにとって、インシデントの影響を受けた資産を特定することは、可能であったとしても相当慌ただしい作業になるでしょう。

資産の状況把握に苦心するセキュリティチーム

ユーザー、デバイス、アプリケーション、規制要件が急激に変化しながらその規模と複雑さを増しています

不完全で不正確な資産データ

52%の組織が1万以上の資産を管理[1]

時間のかかるセキュリティ調査

69%の組織が未把握の資産または管理が行き届いていない資産を標的とした攻撃を経験[2]

コンプライアンスの不備

コンプライアンス監査に不合格だった場合の収益損失額は平均400万ドル[3]

1『Security Hygiene and Posture Management Survey』12ページ、ESG、2021年10月
2『Security Hygiene and Posture Management Survey』13ページ、ESG、2021年10月
3 ホワイトペーパー『The True Cost of Compliance』12ページ、Ponemon Institute、2017年12月

パズル状態の資産管理

包括的な資産インベントリを作成し、常に最新の状態に保つことの重要性は、誰もが容易に理解できます。しかし、その実現は容易ではありません。組織のデジタルインフラがクラウド環境、ハイブリッド環境、オンプレミス環境、OTシステム、IoTシステムへと拡大するにしたがって、保護対象となるデバイス、ユーザー、アプリケーションなどの幅広い資産すべてを正確かつ効率的に把握することが困難になっています。

資産管理ツール：略語集

多くの組織が、資産の状況を把握するために以下のような多数の異なるツールを使用していますが、それがサイロ化や非効率化につながります。

CMDB：構成管理データベース(Configuration Management Database)

ITOM：IT運用管理(IT Operations Management)

CAASM：サイバー資産攻撃対象領域管理(Cyber Asset Attack Surface Management)

CSPM：クラウドセキュリティ態勢管理(Cloud Security Posture Management)

多数のシステムを使って各種の資産を管理し、さまざまなコンプライアンスツールを使って資産を検出していても、一元的かつ包括的な可視化機能を欠いていては、重要な資産情報が各ツールに分散したままです。セキュリティチームが必要とするインサイトが各ツールで収集されていたとしても、不完全または不正確であったり、すでに古くなっているかもしれません。そんなジグソーパズルは誰もやりたくありませんよね。

正確な資産管理はコンプライアンスと監査に不可欠です。以降2ページにわたって、資産検出の最新アプローチを提唱する6つのコンプライアンスフレームワークをご紹介します。

検出
資産の
継続的な検出

管理
資産分類の
管理

特定
資産とユーザー IDの
関連付け

保護
アラートとインシデントの集約と
優先順位付け

追跡
脆弱性の追跡と
コンプライアンス体制の維持

CMDB

ITOM

CAASM

CSPM

ベストプラクティスのフレームワーク

以下のベストプラクティスのフレームワークは、資産の検出と管理を通じてセキュリティとコンプライアンスの取り組みを強化するための基盤として利用できます。

- **CISクリティカルセキュリティコントロール® v8**

  概要：バージョン8では、組織の資産のインベントリと管理の重要性が強調されています。このフレームワークを取り入れれば、ネットワーク内のすべてのハードウェア、ソフトウェア、データ資産を正確に把握し、状況を包括的に把握できます。

  導入のメリット：セキュリティの基盤となるこのコントロールは、資産の継続的な検出と管理を実現し、脆弱性の特定と軽減、コンプライアンスの徹底、不正アクセスの防止につなげることができるため、セキュリティを維持するうえで非常に重要です。

- **ISO 27001:2022**

  概要：ハードウェア、ソフトウェア、データなどの情報資産の正確なインベントリを作成、維持することで、効果的なリスク管理と機密情報の保護を実現することが組織に求められます。

  導入のメリット：この規格で求められる要件に従って資産の継続的な検出と管理を実現することで、すべての資産を適切に特定、分類し、セキュリティ脅威から保護できます。

- **NIST CSF 2.0**

  概要：IT資産管理を重視したフレームワークであり、ハードウェア、ソフトウェア、データ資産の詳細なインベントリを作成、維持してサイバーセキュリティリスクを効果的に管理することが組織に求められます。

  導入のメリット：このガイダンスでは、組織の資産を継続的に監視および管理することが推奨されます。これにより、リスク評価、脅威検出、セキュリティ標準への準拠を強化できます。

大規模で複雑かつ動的な組織が、急速に変化し複雑化が進む環境の管理に苦心するのは当然です。しかし攻撃者は、自らの能力、忍耐力、意欲を総動員して、組織の「インベントリの作成と管理」を極めて大掛かりに実行することで攻撃のチャンスを掴もうと狙っています。

— CISクリティカルセキュリティコントロールv8

規制コンプライアンスのフレームワーク

以下の規制コンプライアンスのフレームワークは、組織の間で、すべての資産を把握しインシデントの影響を受けた資産を特定しなければならないという重圧がかつてないほど高まっていること、そして継続的な資産管理が求められていることを反映しています。

- **PCI DSS V4：セクション5.2.1a**

  概要：悪質なソフトウェアの影響を受けると考えられるすべてのシステムにウイルス対策やマルウェア対策ソリューションを積極的に導入して、既知のタイプのマルウェアを検出、除去、防止できるようにすることが組織に求められます。

  導入のメリット：ウイルス対策ソリューションの導入は必須です。この対策は、ペイメントカードデータを継続的に監視し、進化を続ける脅威から保護することで、データのセキュリティと整合性を維持するために不可欠です。

- **PCI DSS V4：セクション5.2.3c**

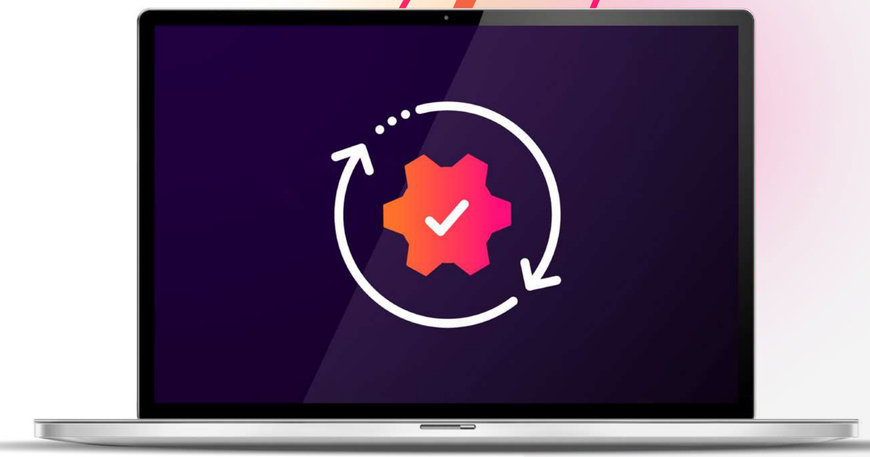
  概要：権限のないユーザーがマルウェア対策を無効にしたり変更したりできないようにすることが組織に求められます。

  導入のメリット：ウイルス対策ソリューションを最新の状態に保つことは必須です。これは、セキュリティ態勢を弱体化させたりシステムをセキュリティ脅威にさらしたりする可能性のある不正な変更を防止して、マルウェア防御の効果を維持するうえで非常に重要なコントロールです。

- **HIPAA：セクション164.310(d)(2)(iii)**

  概要：医療データのセキュリティに関するフレームワークであり、電子保護対象医療情報(ePHI)が不要になったときの的確で安全な廃棄を担保する手順を実装することが組織に義務付けられます。

  導入のメリット：適切な廃棄方法を通じて患者のプライバシーを保護し、機密性の高い医療情報を不正アクセスから守ることは必須です。



コンプライアンス管理に重要な5つの機能

資産を包括的に把握して管理することは、セキュリティに関する効果的な意思決定と効率的なコンプライアンス管理に不可欠です。このセクションでは、セキュリティチームがセキュリティギャップをリアルタイムで検出して解消することでリスクをプロアクティブに緩和するために役立つ、5つの重要な機能をご紹介します。

資産の可視化は、以前から多くの組織で重要な課題でした。見えないものは守れません。セキュリティに関するコンプライアンス規制が厳しさを増し、サイバー保険会社から組織のセキュリティ態勢の透明化が求められる中、資産の可視化の重要性はかつてないほど高まっています。

— IDC社セキュリティ &トラスト担当リサーチディレクター、
Michelle Abraham氏

1. 資産全体の継続的な可視化

課題：データサイロがセキュリティチームに多くの課題をもたらしています。しかも課題は雪だるま式に増えています。情報が分断され、分散していると、資産を可視化して潜在的な攻撃対象領域をあぶり出し、資産について問い合わせ、その回答に基づいて対策を講じることが難しくなります。また、資産データを手動で追跡および調整することが必要となり、プロセスに時間と労力がかかるため、チームを疲弊させることになります。

さらに、資産管理ツール自体の非効率性がこれらの課題を悪化させます。多くのツールが部分的なインサイトしか提供せず、組織のインフラ全体を把握するのが困難になります。見えないものは守れません。組織のすべての資産を包括的かつ一元的に可視化できないと、十分なセキュリティ対策を取れなくなります。

重要機能：今日の規制状況(前述のNIST CSF 2.0などの説明を参照)に対応するには、最新のデータを把握することが不可欠です。データが古いと、規制違反に陥るリスクがあります。そのため、セキュリティチームには、ネットワーク、エンドポイント、クラウド、スキャンツールなど、**さまざまなソースから提供される資産インベントリを継続的に更新**する機能が必要です。古いデータを排除することで、チームは、資産インベントリが常に正確で完全であることを前提に行動できます。信頼できるインサイトが得られることは、リスクを軽減し、盲点を解消するために非常に重要です。

2. コンプライアンスメトリクスを測定するための事前構築済みのフレームワーク

課題：セキュリティチームが直面する最大の課題の1つは、端的に、時間がないことです。セキュリティコントロールに対するコンプライアンスの不備を見つけるには、通常、多くの時間がかかります。しかし、こうした不備は早期に特定して解消する必要があります。さもないと、監査で不合格になるリスクがあります。

そのリスクを冒したい組織はないでしょう。コンプライアンス監査で不合格になれば、多額の収益損失につながる可能性があります(コンプライアンス違反1件あたりのコストは平均587万ドルにのぼります)。さらに、サイバー攻撃に対する脆弱性が増大することも大きな問題です。しかし、そもそも、組織の環境内にあるすべての監視対象資産の追跡と状況把握ができていないと、セキュリティコントロールに対するコンプライアンスを測定することは困難です。その結果、セキュリティチームは、四半期ごとに外部監査のため、さらに、最近急速に増えている、コンプライアンスに深い関心を持つ組織内の関係者のために、資産インベントリやコンプライアンスレポートの準備に長い(かなり長い)時間を費やすことになります。

重要な機能：ボタン1つですべての作業が完了する機能は非現実的ですが、NIST、PCI DSS、HIPAAなど、すぐに使える**主要なコンプライアンスフレームワークを基準にコンプライアンスを測定**できれば、セキュリティチームは貴重な時間を無駄にすることなく組織のコンプライアンス状況をすばやく把握できます。これにより、チームはより戦略的でプロアクティブな業務に時間を使うこともできます。

3. コンプライアンスメトリクスを測定するためのカスタマイズ可能なフレームワーク

課題：まったく同じアーキテクチャは2つと存在しません。そのため、資産インベントリを包括的に可視化し、さらに最新の状況も把握できるようにするために、セキュリティチームは多くの時間を費やさねばならないでしょう。また、組織では可視化が必要な領域ごとに専用ツールを導入することがよくありますが、こうしたツールは互いの連携が不十分であるかまったく連携がないため、手動プロセスが必要となり、夜間の動作確認作業が増えることになります。

重要な機能：セキュリティチームには、ノートPCの暗号化、脆弱性スキャンのカバー率、アプリケーションの適用、マルウェア対策の状況などを確認するための**独自のコンプライアンスメトリクスを構築**する機能が必要です。これにより、リスクを低減し、セキュリティコントロールに対するコンプライアンスレポートをリアルタイムで生成できます。

取締役会は何でも数字で示すことを求めますが、サイバーセキュリティに関しては1つの数字で良し悪しを語るのは非常に難しいのです。

— ある運輸・輸送・物流企業のCISO、『CISOレポート』

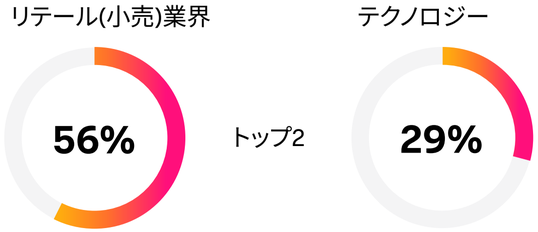
4. リアルタイムのコンプライアンスレポートの生成

課題：組織のコンプライアンスに関心を持つ関係者がかつてないほど増えており、静的なリスク評価やコンプライアンス評価だけでは対応しきれなくなっています。コンプライアンス体制についての個人の説明責任が以前よりも重視されるようになり、将来、特定のコード行を書いた開発者が誰なのかを知りたがるようなステークホルダーが現れてもおかしくありません。

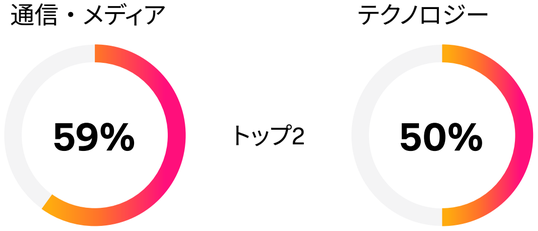
多くのセキュリティチームはこれまで、監査のための資産インベントリの準備に長い時間をかけてきましたが、今日のステークホルダーは、最新のコンプライアンス体制を迅速かつ明確に把握することを望んでいます。そのためセキュリティチームは、コンプライアンスの不備をプロアクティブに特定し、継続的な改善状況を明確に示さなければならないという、かつてない重圧にさらされています。

重要な機能：セキュリティチームには、**組織のコンプライアンス体制に関するリアルタイムのレポートを生成**する機能が必要です。複数のメトリクスを組み合わせてコンプライアンスに不備がある資産をすばやく特定し、経営幹部向けのメトリクスに基づいてコンプライアンス状況を可視化するレポートを作成して、問題のある資産にプロアクティブに対処するための計画を示すことが重要です。これにより、誰もが安心して夜眠れるようになるでしょう。

CISOの最優先事項として規制コンプライアンスを挙げた割合



CISOの最優先事項としてデータプライバシーを挙げた割合



5. 資産に関する正確なコンテキストデータの提供

課題：セキュリティチームは、インシデント調査でアラートのデータと特定の資産やIDを相関付けられないという重大な課題に直面しています。これは、資産をリアルタイムで包括的に把握できていないことが原因です。相関付けのために複数のツールを相互参照する必要があり、仮定に基づいて調査を行わなければならないことも少なくありません。これにより、調査プロセスが長引くだけでなく、アラートのトリアージやインシデント対応が遅れることになります。

アラートに関係する資産のIPアドレス、ネットワーク上の位置、ユーザーの関連付けなどの属性が変わっていると、調査が一層複雑になります。その変更が長期間把握されていないかった場合はなおさらです。では、セキュリティチームが、調査対象となる資産をいつでも正確に特定できるようにするにはどうすればよいでしょうか？

重要な機能：ゲームであれば、仮定や推測で答えを導き出すのもよいでしょう。しかし、現実の世界では**資産とIDに関する正確なコンテキスト**を手に入れましょう。セキュリティチームはこれを基に調査の焦点を絞り込み、作業時間を短縮できます。さらに、資産とIDの関係をマッピングすれば、**いつ**、**どの**資産に、**誰**が関連付けられたかをすばやく特定できます。

最新の包括的な資産インベントリを構築することは、セキュリティギャップの迅速な解消と、コンプライアンスの継続的な改善の証明に役立ちます。Splunk Asset and Risk Intelligenceを使用すれば、継続的な資産検出とコンプライアンス監視を実現して、リスクをプロアクティブに緩和できます。詳しくは、こちらをご覧ください。

splunk>

© 2025 Splunk Inc. 無断複写・転載を禁じます。Splunk, Splunk>, およびTurn Data Into Doingは、米国およびその他の国におけるSplunk Inc.の商標または登録商標です。他のすべてのブランド名、製品名、もしくは商標は、それぞれの所有者に帰属します。

24.CMP.ebook.the-secOps-blueprint-to-navigating-compliance_v9-JA-202503