Forescout XDR

eXtended Detection and Response

FORESCOUT

Forescout XDR

eXtended Detection and Response

真の脅威の検出・対応能力が向上し、SOCの効率が450倍アップ

セキュリティオペレーションセンター（SOC）には、重要なコンテキスト情報が欠けた不完全で不正確なアラートが日々大量に押し寄せます。しかし、その多くは誤検出です。その結果、重大な脅威を見逃して調査・対応に時間がかかり、侵害リスクが高まってしまっています。実際、一般的なSOCが1日に受け取るアラートは約11,000件とされており、1時間あたり450件[1]にも上りますが、そのほとんどが忠実度と信頼度の低い誤検出です。

Forescout® XDRなら、検出数を1時間あたり1件とSOCで対応できる数にまで減少させ、分析担当者による調査が本当に必要な確度の高い脅威だけを検出します[2]。

ソリューションの概要

Forescout XDRは、テレメトリとログから、SOCで対応可能な忠実度と確度の高い脅威を検出します。

キャンパス、クラウド、データセンター、エッジにいたるまで、IT、OT/ICS、IoT、IoMTのあらゆる接続デバイス全体にわたって、高度な脅威の検出、調査、ハンティング、対応を自動で行います。SOCに欠かせない技術と機能をクラウドネイティブな統合プラットフォームに集約し、脅威の可視化と対応を一元的に行うことができます。

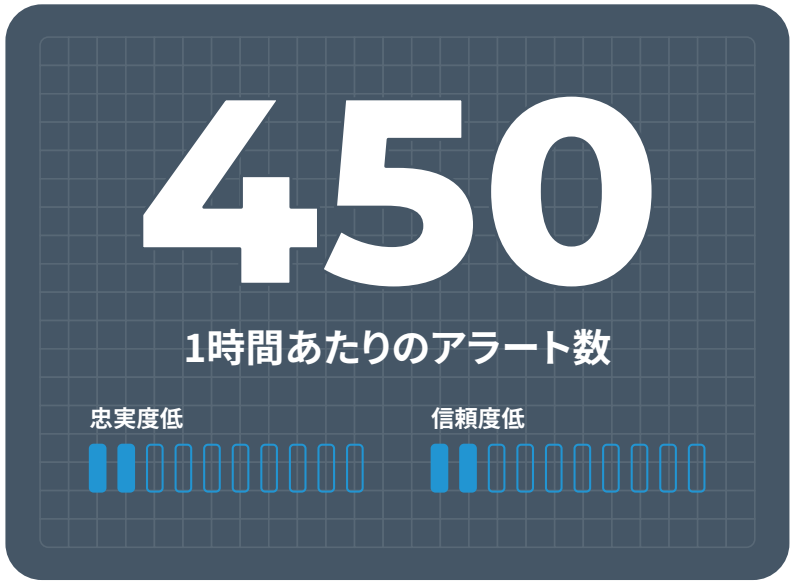
**管理デバイスも非管理（エージェントレス）デバイスも含め、
あらゆる対象から企業全体のデータを活用します。**

Forescout XDR なら、テレメトリとログを基に対応可能な脅威を検出、一般的な SOC と比べて効率が450倍アップします。

Forescout XDR

VS

一般的なSOC



＊検出とは：分析担当者による調査が本当に必要な、
SOC で対応可能な確度の高い脅威の検出を指します。

規模・業界の異なる代表31社の1年間（2021年12月～2022年12月）の
平均データ集計に基づく結果です。

1日あたり11,000件のアラート＝1時間あたり450件
出典：『The 2020 State of Security Operations』Forrester Consulting

SOC が実際どのくらいの数のアラートを受け取るかは、
導入しているセキュリティソリューションの数、種類、場所や
そのチューニング（分析担当者のキャパシティ、リスク許容度、専門性の高さによる）、
従業員とデバイスの数、業界など、多くの要素によって変わります。

導入のメリット

ビジネスリスクを低減

サイバー攻撃やデータ侵害のリスクや被害規模を低減。アラートの「ノイズ」をほぼ全て除去するため、多様化する高度な脅威をこれまで以上に迅速かつ正確に検出、調査し、対応できるようになります。

これにより、サイバー攻撃やデータ侵害による業務の中断や金銭的損害を防ぐことができます。

セキュリティ運用業務を最適化

重要データのエンリッチメントと正規化、シグナルの相関解析を自動で行い、分析担当者による調査が本当に必要な忠実度と信頼度の高い脅威のみを検出します。情報やコンテキストデータの漏れが少なくなり正確性も増すため、複雑な調査や脅威ハンティングがシンプルかつスムーズに。Forescoutの他のソリューションや、サードパーティのSIEM、ケース管理システム、対応ソリューションもまとめて一元的に管理することができます。

Forescout XDRは、分析担当者/IR、エンジニア、SOC管理者、コンプライアンス/リスク管理者、経営幹部などそれぞれの立場に合わせて重要パフォーマンス指標（KPI）を設け、事前に設定、カスタマイズしたダッシュボードを用いて、脅威ライフサイクル全体を強力に可視化します。これにより、SOCチームは重要度の高いセキュリティ業務に注力できるようになります。

コストを削減

以下に関連するSOC費用を削減します。

- データレイク、セキュリティ解析、セキュリティオーケストレーション・自動化・レスポンス（SOAR）、ユーザとエンティティの行動分析（UEBA）、脅威インテリジェンスプラットフォームなど、複数のSOCポイントソリューションのライセンスと管理
- ログストレージ
- 過剰労働による分析担当者の離職に伴う人材の採用と研修
- 新しいデータソースの維持
- ルールの作成とチューニング

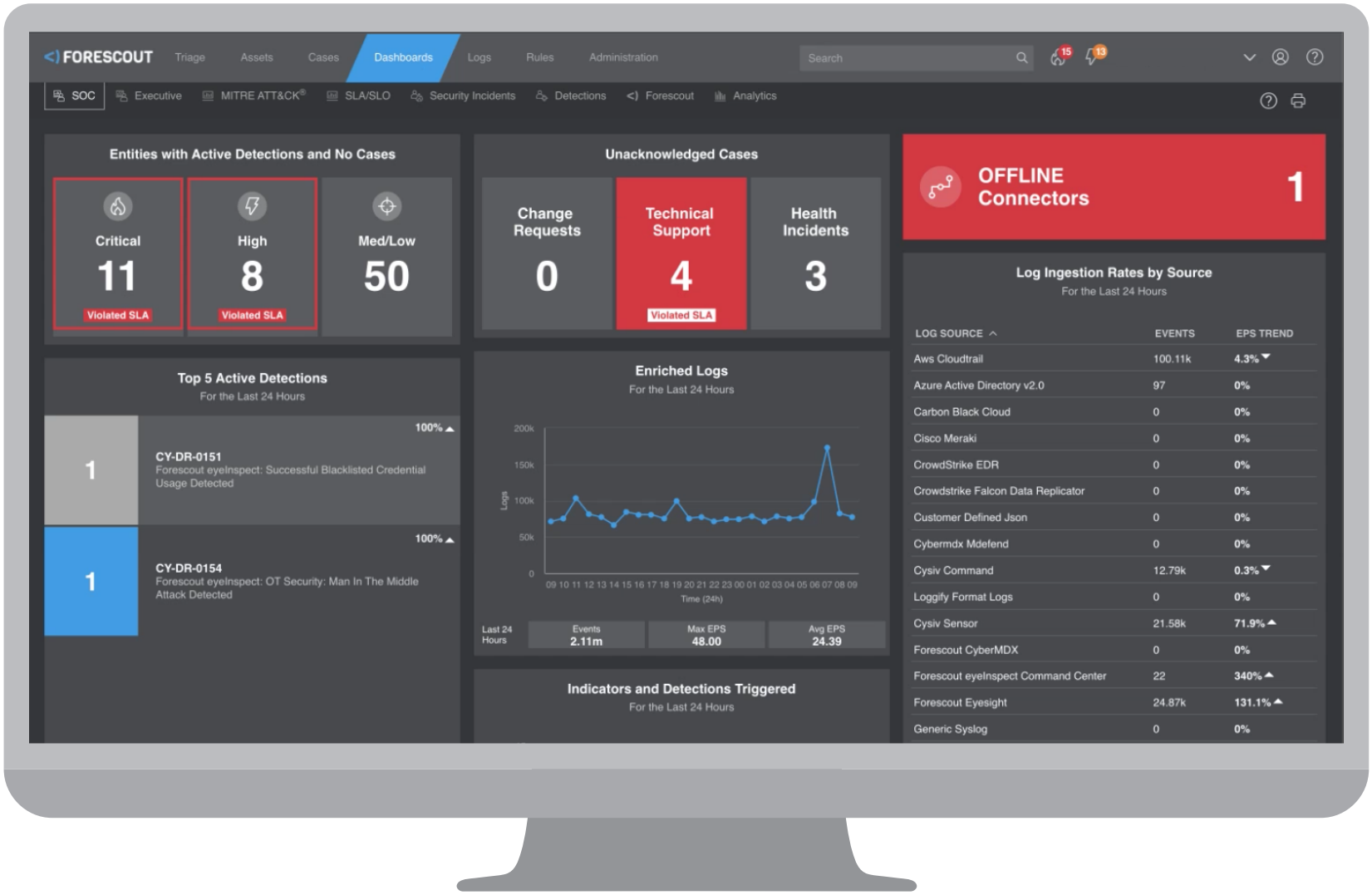
コンプライアンスに対応

ログストレージ、脅威の自動検出、脅威インテリジェンスにより、主要な規制や基準を守りコンプライアンスに対応。侵害や業務中断が通知されてから対応措置を取るまでの空白時間を短縮することができます。

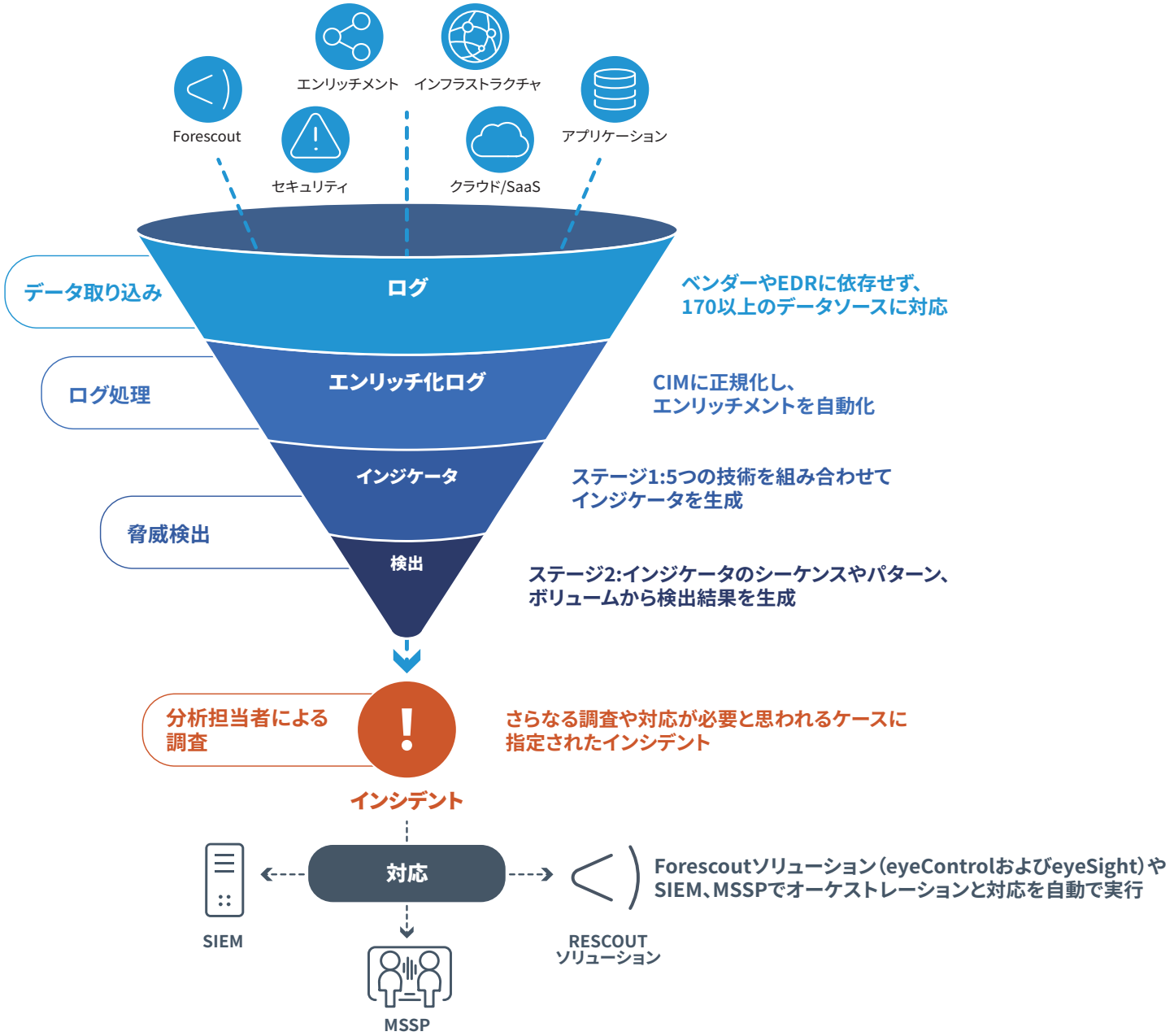
既存のセキュリティ資産を活用

導入済みのForescoutソリューションだけでなく、既存のネットワークやエンドポイント/クラウドセキュリティセンサ、エンフォースメントポイントも、ベンダーに関係なく有効に活用することができます。ベンダー固有のソフトウェアやハードウェアを新たに導入する必要はありません。

キーメトリクスとトレンドを監視することで、SOC のパフォーマンス管理をより最適化。



事前設定や個別にカスタマイズが可能なダッシュボードで、分析担当者 /IR、エンジニア、SOC 管理者、
コンプライアンス / リスク管理者、経営幹部など各役割に適した KPI を設定することができます。


エンリッチメント
インフラストラクチャ
Forescout
セキュリティ
クラウド/SaaS
アプリケーション
データ取り込み
ログ
ベンダーやEDRに依存せず、
170以上のデータソースに対応
ログ処理
エンリッチ化ログ
CIMに正規化し、
エンリッチメントを自動化
脅威検出
インジケータ
ステージ1:5つの技術を組み合わせて
インジケータを生成
検出
ステージ2:インジケータのシーケンスやパターン、
ボリュームから検出結果を生成
分析担当者による
調査
!
さらなる調査や対応が必要と思われるケースに
指定されたインシデント
インシデント
対応
SIEM
RESCOUT
ソリューション
Forescoutソリューション（eyeControlおよびeyeSight）や
SIEM、MSSPでオーケストレーションと対応を自動で実行
MSSP

Forescoutを選ぶ理由

Forescout XDRは、他のForescoutソリューションと共に独自の機能を提供します。
ベンダーやEDRに依存せずにデータを取り込み、検出効率が450倍アップ。
脅威に漏れなく対応し、リスクも前もって低減。費用も予測しやすい手頃な価格で提供します。

ベンダーやEDRに依存しないデータ取り込み

- 既に導入済みの製品やベンダーにも対応
- あらゆる管理・非管理デバイス（IT、OT/ICS、IoT、IoMT）からデータを取り込み可能
- 脅威検出の範囲、能力、柔軟性、効率性が向上

検出効率が450倍アップ

- 高度なデータパイプラインにより共通情報モデル（CIM）を適用。取り込んだデータを正規化し、ユーザ情報、IP属性、ジオロケーション、重要資産情報を基にデータのエンリッチメントを自動で実施
- 5つの技術を組み合わせた2段階の脅威検出エンジンにより、ノイズを減らし、忠実度を向上

脅威に漏れなく対応

- 強力な調査ツール
- ケース管理ソリューションとのネイティブ統合
- Forescoutソリューションを介して、管理・非管理デバイスに対して脅威対応を自動化

事前にリスクを低減

- 他のForescoutソリューションと一体化させることで、攻撃対象領域を縮小し、侵害されたデバイスやコンプライアンス違反のデバイスが自社のネットワークに接続するそもそものリスクを低減
- 動的なアクセスポリシーにより、あらゆる接続デバイスを常時監視

費用を予測しやすいシンプルで手頃な価格設定

- 検出精度を上げるために送信するログを増やしても追加料金の発生なし
- ライセンス料は社内のエンドポイント（IP/MACアドレス）の総数で決定
- 価格には31日分のログストレージ費用が含まれており、オプションでストレージ期間を延ばすことも可能

主な特長

Forescout XDR は、SOC に欠かせない技術と機能をクラウドネイティブな統合コンソールに集約しています。

データの取り込み

Forescout の eyeSight、eyeInspect、Medical Device Security のデータに加え、ベンダーや EDR に依存しない、次のような170以上のデータソースにネイティブ対応しています。

- **セキュリティ:** ファイアウォール、ネットワークIDS/IPS、EDR、エンドポイント保護プラットフォーム(EPP)、サーバ/ワークロード/コンテナセキュリティ、ウェブプロキシ、Eメールセキュリティ
- **インフラストラクチャ:** Windows セキュリティ、AD 認証、IAM、DHCP、DNS、クラウド監査証跡、ネットワークメタデータ
- **エンリッチメント:** 認証(LDAP)、資産のインベントリと分類、構成管理、脆弱性スキャン結果、脅威インテリジェンス(IOC)
- **アプリケーション:** データベース、ERP、CRM、API
- **クラウド/SaaS:** AWS、Microsoft Azure、Google Cloud、Microsoft 365、Google Workspace、その他 SaaS アプリケーション

データオンボーディング

最も重要なユースケースに対応するため、検出に必要なデータを最大限抽出できるようにします。オンボードするデータソースの計画と優先順位付け、さらにデータパイプラインの構成を Forescout のデータエンジニアがサポート。データの分析、精錬、正規化、エンリッチメントが適切に行われるようにします。

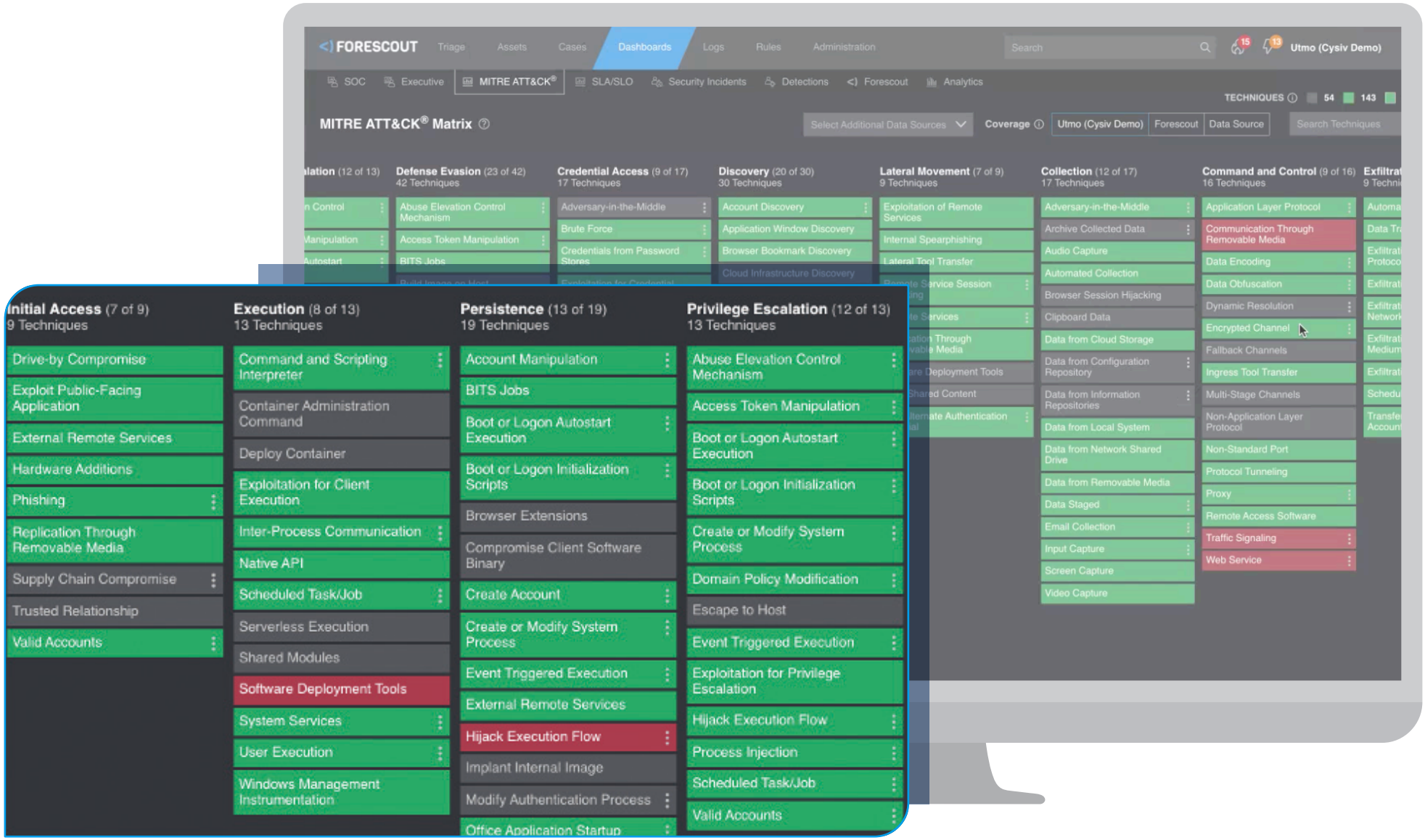
高度なデータパイプライン

企業全体のデータソースから高度な脅威検出エンジンへのデータフローの管理方法に関して、厳格なデータサイエンスを中心としたアプローチを採用しています。まず、共通情報モデル(CIM)を適用し、取り込んだデータを正規化。次に、IP アドレスやジオロケーション、ADObject プロパティ、構成など、セキュリティコンテキストに関するコンテキストデータを基にデータのエンリッチメントを自動で行います。これにより、アノマリ検出が最大化され、複数のデータソース全体にわたって迅速な相関分析と脅威ハンティングを行えるようになります。最後に、ETL(抽出・変換・格納)プロセスによって、より一般的である ELT(抽出・格納・変換)プロセスよりも迅速で安定した効率的なデータ分析を可能にしています。

MITRE ATT&CK® フレームワークの統合

MITRE ATT&CK フレームワークは、サイバー攻撃のライフサイクル全体を通じた攻撃者の戦術と技術を体系化したものです。Forescout の XDR はこのフレームワークを統合しました。広範、または特定のカバレッジを実現するために取り込むべきデータソースとの違いを即座に把握、攻撃者に悪用されるおそれのあるブラインドスポットを特定し、カバレッジを強化するにはどのデータソースを追加すべきか判断できるようにしました。

MITRE ATT&CKフレームワークの統合により、潜在的なブラインドスポットがどこにあるのか、どのデータソースを追加すれば脅威検出をさらに強化できるのかを可視化。



高度な脅威検出

Forescout XDRで検出可能な脅威の例

- アプリケーションの悪用
- ブルートフォース攻撃
- バッファーオーバーフロー攻撃
- クラウドリソーススキャニング
- クラウドサービスの誤設定
- クラウド:不正アクセス
- クラウド:安全性の低いストレージの検出
- コマンド&コントロールの接続
- コンプライアンス違反
- クロスサイトスクリプティング
- クリプトジャッキング
- データ窃取
- ファイルアクセスエラー
- リソースへの不正アクセス
- インサイダー脅威
- ラテラルムーブメント
- マルウェア/アウトブレイク
- ネットワークスキャニング
- パスワードクラッキング
- フィッシング攻撃
- ポートスキャンと脆弱性スキャン
- ランサムウェア
- SQLインジェクション
- 不審な振る舞い
- システムへの不正アクセス
- ファイアウォールルールの不正変更
- サービスの不正再始動
- サービス/プロセスの不正作成
- 脆弱性の悪用
- ウェブアプリケーションの誤設定
- ウェブアプリケーション攻撃(レイヤ7集中攻撃)
- ワーム/ウイルスアウトブレイク

クラウドベースのデータレイク

大幅に拡張可能でインデックス化された専用のデータレイクは、データストレージが階層化(ホット、ウォーム、コールド)されており、迅速な全文検索が可能です。これにより、生のテレメトリでもエンリッチメントしたデータでも、ログの保持・管理が短期間から長期間(7日〜1年以上)低コストで可能になり、セキュリティやコンプライアンス要件に対応することができます。

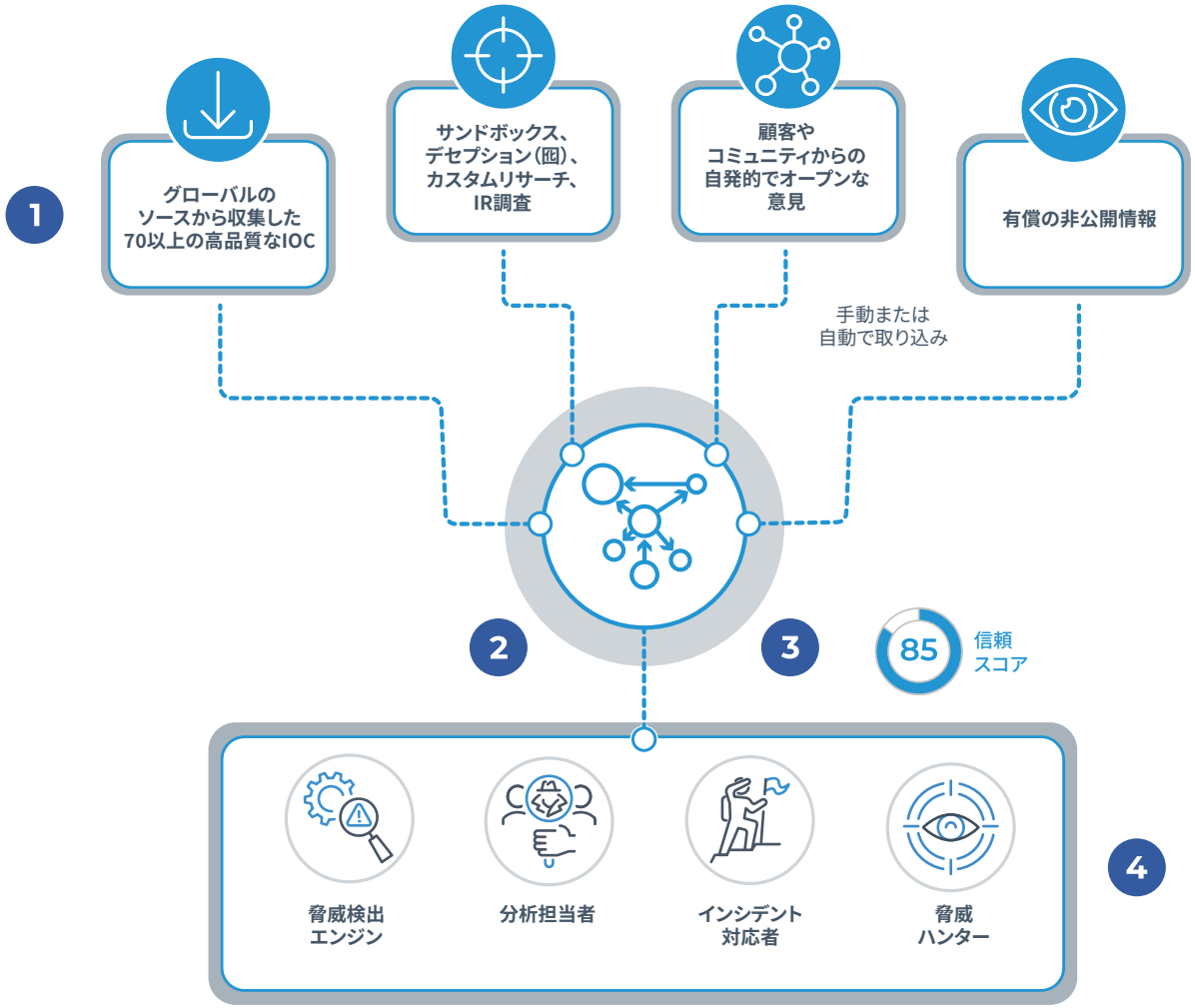
検出ルール

Forescout XDRには、データソース用にすぐに使える検証済みの検出ルールとモデルが1,500以上含まれています。これらのルールは、導入初日から効果的に運用して価値を発揮できるよう、本番データで試験済みの状態になっています。また、ルールは柔軟にカスタマイズできるため、自社独自の要件に対応できるインジケータや検出、正常性に関するルールを、ユーザーの経験に基づきながら迅速に作成することができます。

脅威検出エンジン

以下の5つの技術を採用した2段階の脅威検出エンジンにより、調査が本当に必要な忠実度と信頼度の高い真の脅威を自動で検出し、誤検出(ノイズ)を除去します。

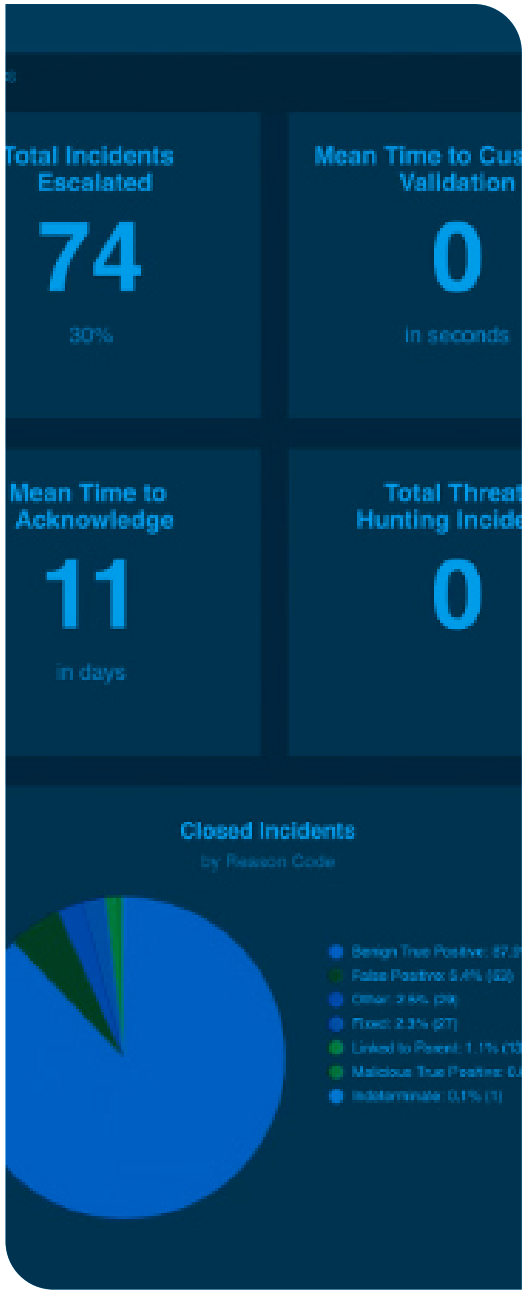
- **シグネチャ:** オブジェクト属性を既知の悪質なオブジェクトと照合し、生テレメトリ内の脅威や駆除できないマルウェア、ランサムウェアなどを特定します。
- **UEBA:** デジタルパターンやフットプリント、人の行動、ネットワークの振る舞いを既知の悪質な振る舞いと照合し、異常な振る舞いを検出します(例:営業担当者がCRMの記録を大量にダウンロードしている、通常の勤務時間外に異常な行動をしている、ビーコン通信を行っている、ありえない距離を移動している)。
- **統計と外れ値:** クラスタリング、グルーピング、スタック計算、基準値と変動値の比較、外れ値の検出、ロジスティック回帰などの方法により、異常な行動を検出します(例:ログソースの低下、サービス拒否(DoS)攻撃)。
- **アルゴリズム:** 教師あり/教師なし学習やディープラーニングなど、コンテキストアウェアなAIやML技術を用いて、悪質・異常な活動を検出したり、攻撃を予測したりします(例:プロセスパスやドメイン生成アルゴリズム(DGA)の特定)。
- **脅威インテリジェンス:** 70以上のサイバーインテリジェンスソースを活用して、バックドアやC&Cトラフィックといったモノや、悪質なフィッシングサイトに接触しようとしている人を検出します。



脅威インテリジェンス

Forescout XDRは、Forescoutの専門家による国際調査チームであるVedere Labsなど、世界各地の70以上の優れたソースからIOC情報を収集しています。これらのIOCは、分類、実証してスコアを付けた上で、完成した情報として提供され、脅威の検出からハンティング、調査プロセスまであらゆる段階で自動的に活用されます。主な脅威アクターや脅威について記した、Forescout調査員作成の詳細な脅威レポートもご参照いただけます。また、匿名化したIOCデータを、業界別のISACなどあらかじめ許諾を得たコミュニティ間で、コミュニティ固有の脅威インテリジェンス共有プラットフォームを介して共有することもできます。

1. Forescoutは信頼できる幅広いソースからのIOCデータを活用しています
2. IOCインテリジェンスは、「既知の悪質な」ドメインやURL、IPv4/IPv6アドレスをグラフモデル化した検索可能なデータベースに落とし込み、相関分析されます
3. 各IOCには、ソースの品質評価に基づいて信頼スコアが動的に付与されます
4. この信頼スコアが付与されたIOCインテリジェンスは、脅威検出エンジンやユーザのSOCチームによって、脅威の検出や調査プロセスを加速・向上させるために活用されます



UEBA

振る舞いを基にした分析手法で、エンティティの振る舞いの大きな変化や異常な行動を検出します。ユーザやホストのプロファイルと振る舞いを時間をかけて収集。それを標準モデルとして組み込み、標準から外れるような異常な行動が見られた場合は、不審な行動としてトリガーします。

ダッシュボード

事前設定や個別にカスタマイズが可能なダッシュボードで、分析担当者/IR、エンジニア、SOC管理者、コンプライアンス/リスク管理者、経営幹部など各役割に適したKPIを設定することができます。

SOAR

組み込み型のケース管理と通知機能により、検出から調査、対応までのSOCプロセスを一つにまとめます。IPジオロケーションやユーザ/資産情報、複数のインテリジェンスソースとの相関性といったエンリッチメントソースを通じてセキュリティを自動化。Forescoutの eyeSight と eyeControl を活用して、オーケストレーションから対応までのワークフローを自動化し、企業全体にわたり管理デバイスにも非管理(エージェント不可能)デバイスにも漏れなく接触することができます。また、Palo Alto Cortex XSOAR などの他の SOAR と統合することで、既に導入済みの SOAR を引き続き活用することもできます。

SIEM統合

Forescout XDRによって特定された真の脅威を既存のSIEMに取り込み、オーケストレーションとインシデント対応を一元化することができます。

ソフトウェアとコンテンツの継続的なアップデート

新しい機能や修正点、新しい検出ルールやモデルが2〜3週間ごとに切れ目なく提供されます。アップデート作業にサポートは不要で、業務が中断することもありません。

マルチテナントアーキテクチャ

国、オフィスの場所、事業部門などをベースに論理的分離(またはテナント)を簡単に作成することができます。また、世界全域のテナントや事業部門全体にわたり、集計ビューの生成やクエリ・分析の実行も可能になるため、大企業や多国籍企業、MSSP、各地にSOCを置く企業には特に役立ちます。

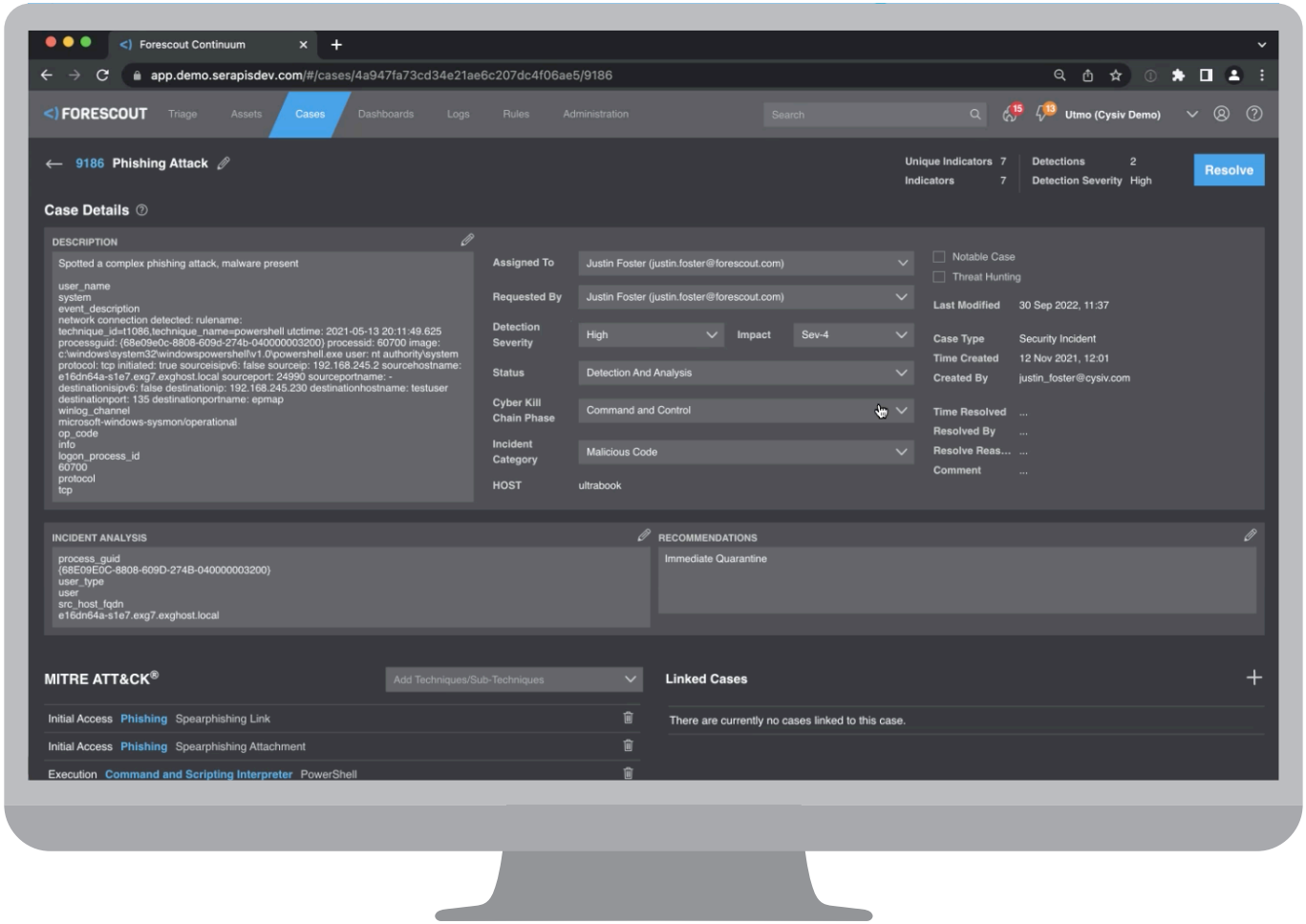
世界共通アーキテクチャ

データレジデンシーとコンプライアンスの要件に即座に対応し、各地域のセキュリティ業務を低コストでサポートします。アメリカ、ヨーロッパ、アジア太平洋など25の地域の中からログを保管したい場所を指定できる一方、データの一括表示や一括クエリも引き続き行うことができます。

クラウドネイティブ

デプロイは一切不要で、新しい機能や修正点、ルールが隔週で切れ目なく提供されます。

ケース管理画面では詳細が一括表示されるため、調査や対応を
これまで以上に迅速かつ効果的に行えるようになります。

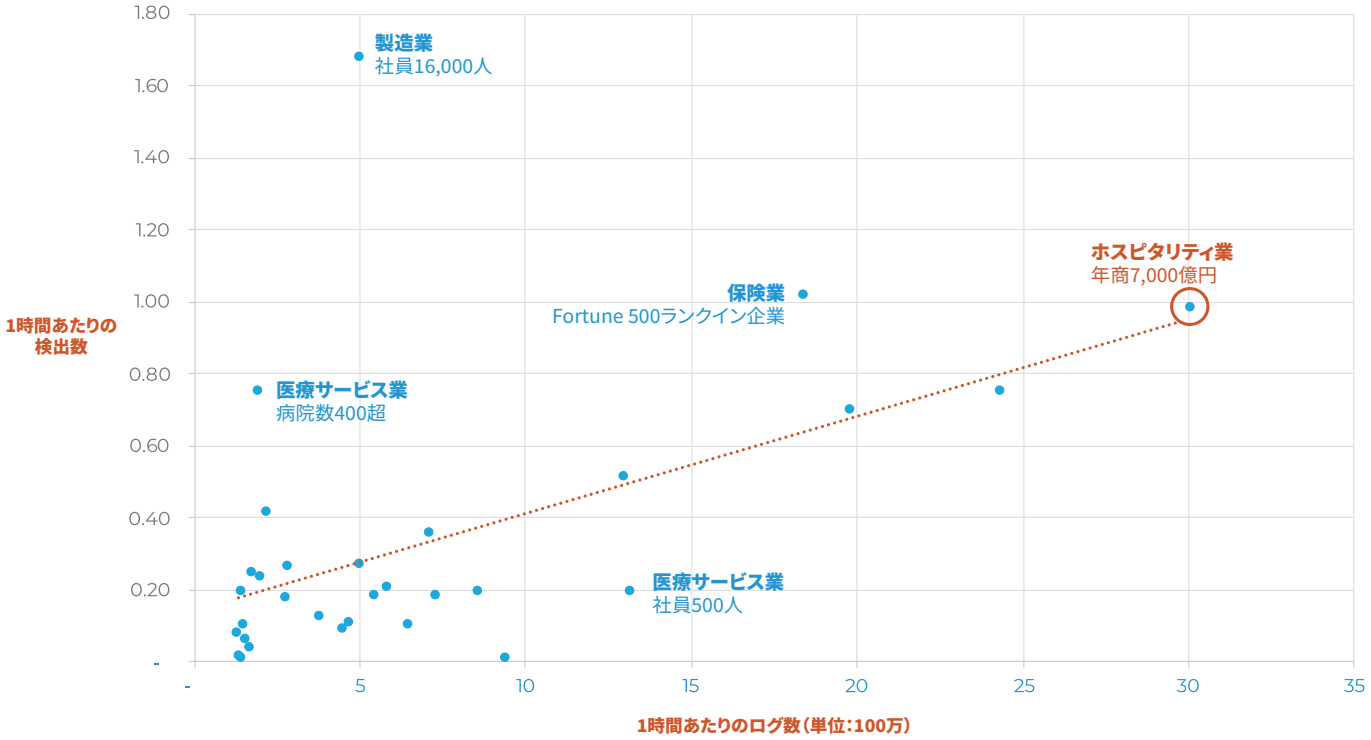


Forescout XDR は、検出処理中やインシデント管理中も、ワークフローや緊密な統合、透明性、シームレスなコミュニケーション/コラボレーションを実現。
NIST インシデント対応ライフサイクルに基づき、ServiceNow、RSA Archer、Jira Software、ManageEngine ServiceDesk Plus、
Palo Alto Cortex XSOAR、TheHive、ConnectWise との統合にも対応しています。

まとめ

Forescout XDR なら、ログの数が100万単位でも1,000万単位でも億単位でも、ノイズを即座に自動で除去して、人間の分析担当者による調査が必要な忠実度と信頼度の高い脅威のみを検出します。

以下のグラフは、2021年12月15日からの1年間にわたり集計した31社のデータを示したものです。例えば、年商7,000億円のホスピタリティ企業は1時間あたりのログ件数が平均で3,000万件でしたが、ノイズを除去し、1時間あたりの検出数を0.98とSOCで対応可能な数にまで減らすことができました。



備考：

- 規模・業界の異なる以下の企業を調査対象としました。
  - 建設
  - 小売
  - エネルギー/公益事業
  - フィンテック
  - 医療
  - 保険
  - 製造
  - 鉱業
  - 出版
  - テクノロジー
  - 物流/ロジスティクス
- 各結果は、ユースケース、ログの内容、ログの総数、ルールのチューニング状況など、複数の要素によって変動します。

1『The 2020 State of Security Operations』Forrester
2 エンドポイントとは、ユーザデバイス、ネットワークインフラストラクチャデバイス、非ユーザデバイス、クラウドインフラストラクチャコンポーネントに割り当てられている各MACアドレスおよびIPアドレスを指します。

Forescout XDR

eXtended Detection and Response

デモをご覧ください

forescout.com/xdr-demo-request

フォアスカウト・テクノロジーズ株式会社

東京都港区西新橋1-1-1
日比谷フォートタワー10階
詳しくは、Forescout.jpへ

フォアスカウト・テクノロジーズ株式会社

住所：〒105-0003 東京都港区西新橋1-1-1
日比谷フォートタワー10階
電話：050-1746-6455
詳しくは、Forescout.jp をご覧ください。