FORCEPOINT

Forcepoint Behavioral Analytics

情報セキュリティ：知的財産を保護し、侵害されたアカウントを検出し、インサイダーリスクを軽減

Forcepint Behavioral Analyticsを使用すると、セキュリティチームは企業内でのリスクの高い行動を事前に監視できます。当社のセキュリティ分析プラットフォームは、構造化データと非構造化データを融合させて悪意のある、危険にさらされた、過失のあるユーザーを識別するとで、比類のないコンテキストを提供します。アカウントの侵害、企業のスパイ行為、知的財産の窃盗、詐欺などの重大な問題を発見できます。

なぜForcepint Behavioral Analyticsがセキュリティに役立つのか

私たちのクライアントは、企業内での人間の行動を分析するため私たちを頼っています。 Forcepoint Behavioral Analyticsのみが、セキュリティアナリストがビジネスにとって最も重要な問題に取り組むための構成可能な分析を提供します。 セキュリティチームを支援しながら、私たちは規模に合わせて構築できます:

- インサイダー攻撃を検出するための時間を短縮
- セキュリティチームがアラートの海で溺れているときに、関連する警告を表示します
- SIEMや他のツールを超えて、インサイダー活動についてきめ細かく理解する
- インシデント対応および違反後のフォレンジックのための調査効率の向上

プラットフォームの柱

Forcepint Behavioral Analyticsは、異常なアラートだけでなく、リスクの高い行動や個人に対する洞察を提供します。人、データ、デバイス、およびアプリケーション間の微妙なやり取りを評価することにより、Forcepintはセキュリティチームのためにタイムラインに優先順位を付けます。私たちのソフトウェアは4つの柱の上に構築されています:

- **豊富なコンテキスト**› SIEM、エンドポイント、および従業員 関連情報フィードとともに、コミュニケーションの内容を組み合わせて意図を分析し、異なるデータソースを1つの物語へ融合します。
- **ハイブリッド分析**› 洗練された攻撃をより適切に検出するために、変化、パターン、および異常の検出に焦点を当てた、複数の種類の厳密な行動およびコンテンツベースの分析を適用します。
- **検索と発見**› 継続的な監視および徹底的な調査のためのコンテキスト豊富なユーザーインターフェースを介して強力なフォレンジックサーチおよび発見ツールを用います。
- **直感的なワークフロー**› ヒューマンワークフローおよび既存のクライアント情報アーキテクチャと完全に統合して運用効率を合理化するプロアクティブレポートを提供します。

主な利点

- 活動の前兆を検知
- コンテンツアウェアDL
- 不正なアカウントの検出
- データの偵察行為を検出
- 特権ユーザーの悪用検知
- セキュリティ分析

セキュリティ分析の再定義

- **コンテキスト主導の可視性** › Forcepoint Behavioral Analyticsは、構造化されていないコンテキスト豊富なデータストリームを構造化データと統合することで、従業員の活動、行動、および関係に対する可視性を独自に提供します。 当社の分析モデルを使用すると、これまでセキュリティチームには利用できなかった、すべてのデータストリームにわたって複数のレンズを使用してエンティティとイベントのスコア付けと優先順位付けを行うことができます。また、Active Directory、SIEM、EDRおよび主要なデータソースと統合して、真の状況認識、および内部調査を大幅に強化する強力なフォレンジックプラットフォームを提供します。
- **設定可能なアナリティクス** › 伝統的なブラックボックスのUBAツールは、固定された分析構成を持つ、異なるシステムで分析された構造化データソースに限定されることがよくあります。これとは対照的に、Forcepintは、セキュリティチームが進化するセキュリティユースケースに対処し、すべてのデータセットにわたる高度な検索を含むリアルタイム詳細分析を実行することを可能にする強力な分析機能を提供します。

私たちの分析は追加のプログラミングなしで調整することができ、セキュリティの脅威に対するより機敏な対応を可能にします。

- **スケール** › 私たちは基本的に規模に合わせて構築しています。エラスティックサーチを使用して大量のデータに瞬時にアクセスできるのはForcepointだけです。当社のプラットフォームは、構造化データと非構造化データの両方をシームレスに保存し、クライアントと共に成長するように水平方向に拡張します。 Forcepointはさまざまなレベルのアクセスと管理制御も提供しているため、あらゆる種類の展開で、私たちのテクノロジを使ってビジネスに役立つことができます。

エンタープライズ向けの能力

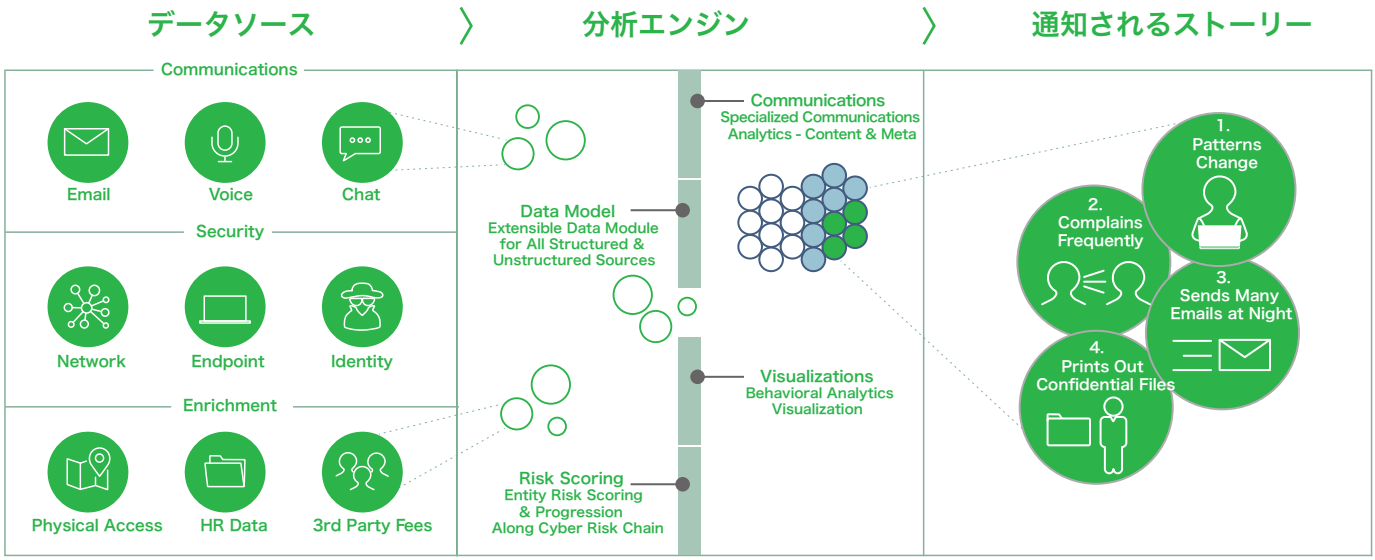
- **ロールベースのダッシュボードとワークフロー** › 直感的なユーザーインターフェイスを介して、準拠していないアクティビティを迅速にレビューできるようにすることで、アナリストやマネージャはすばやく調査、レビュー、エスカレート、そして対応を実施することができます。
- **堅牢なデータ要求** › 内部統制と外部からのデータ保護に関する懸念の両方に必要とされる複雑なデータ要求を完全にサポートします。
- **拡張可能なプラットフォーム** › 構成可能な分析、ダッシュボード、ユーザーグループ、およびワークフローは、すぐに使えるセキュリティユースケースをサポートし、あらゆるリスクユースケースに拡張できます。柔軟なプライバシー管理により、ワークグループ間の機密性が保たれます。

高度なデータサイエンスモデルを専門的なサービス契約なしで提供します。

- **柔軟な導入オプション** › オンプレミス、仮想プライベートクラウド、またはForcepointアプライアンスを使用して容易に導入できます。

高度な機能

- **行動に関する洞察** › 感情およびコンテンツ分析を使用して、従業員による現在または潜在的な違法、不要または不適合な行動を示す可能性のある行動の変化を特定します。
- **インテリジェントな優先順位付け** › コンテンツとメタデータのパターンの分析に基づいて、関心のあるイベントとアラートに優先順位を付けます。
- **自然言語処理(NLP)** › NLPのスマートで実用的なアプリケーション、あらゆる言語の複雑な用語集、およびスレッド化された電子メールからの免責事項と引用テキストを認識するテキスト識別テクノロジによって、誤検知を大幅に削減します。
- **オーダーメイドの視覚化** › アナリスト自身の推論機能を解き放ち、関連する活動について最大限のコンテキストを提供するために、視覚化は特に開発されました。誰が、何を、いつ、どのようにして従業員の行動を理解するかを素早く理解します。
- **コンテンツ分類** › Forcepointのコンテンツ分類エンジンを使用して、バルクメール、サードパーティのメーラーなどの関連性のない通信を識別してフィルタ処理することで、DLPの導入効果を加速します。



お問合せ先
ForcepointJapan株式会社
〒105-0003　東京都港区西新橋1-2-9　日比谷セントラルビル14階
Tel:03-5532-5602
Email: Japan@forcepoint.com
Web: www.forcepointcom/ja