ESG 経済性検証

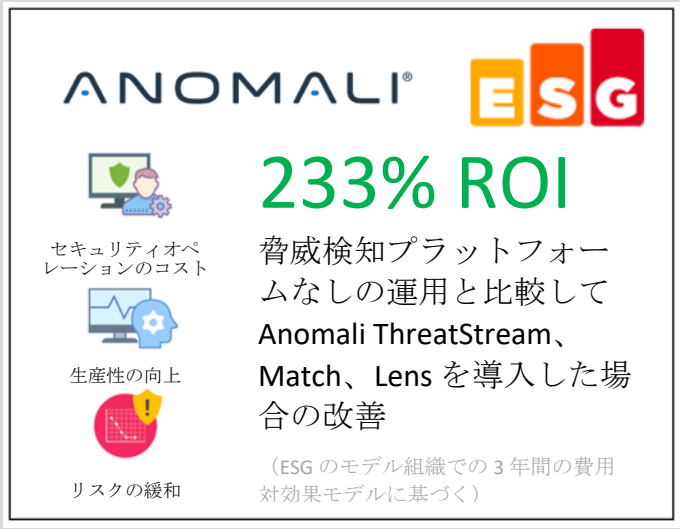
Anomali 脅威インテリジェンスプラットフォームの経済的メリットの分析

著者：Aviv Kaufmann/Alex Arcilla、シニア検証アナリスト

2020 年 7 月

エグゼクティブサマリー

ますます増加するリモートワークの効率的な支援は、企業にとってこれまで以上に重要な責務です。この責務を果たすには、地域、ネットワーク、デバイスを問わずアプリケーションやリソースに確実にアクセスできる体制を整える必要があります。企業は、組織と資産を保護するための効果的かつ効率的なオペレーションをセキュリティチームに求めています。セキュリティチームには、ソリューションを迅速に導入し、制限とポリシーを緩和し、参入への障壁を排除するというプレッシャーがかけられています。脅威を特定して修正するために、よりスマートかつ効率的に、できるだけ多くの脅威インテリジェンス情報を取り込む必要があります。



ESG は、Anomali のインテリジェンス駆動型セキュリティ製品スイートを検証し、セキュリティオペレーションの合理化、ワークフローの自動化、誤検知の減少、社内外のコラボレーションの改善、検知・修正時間の短縮に効果があったことを確認しました。ESG は、Anomali の顧客が得たメリットを一連のヒアリング調査を通じて明らかにし、その情報に基づいてモデルシナリオを作成しました。このシナリオは、生産性の向上、リスクの回避、製品群がもたらす価値からどのようにして組織が毎月 9 万 3,000 ドルを節約できるのかを示します。ESG のモデルでは、10 人のセキュリティチームで Anomali の導入を選択した場合と脅威インテリジェンスプラットフォームなしで運用した場合を比較した結果、233% の投資収益率とわずか 11 ヵ月での投資回収という結果を得ました。

はじめに

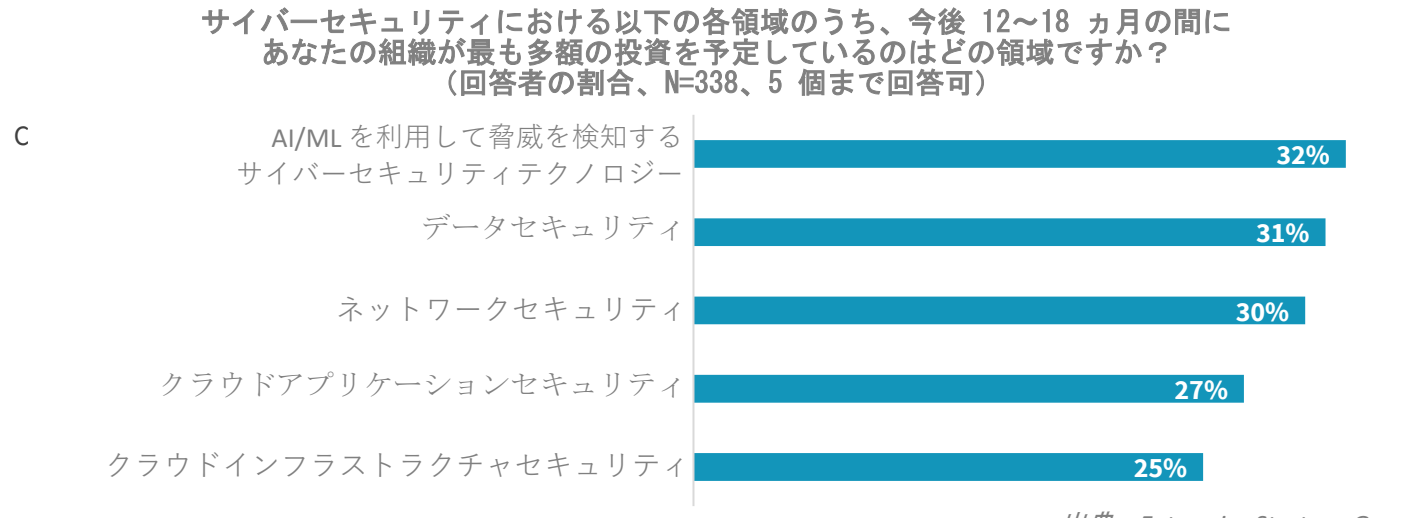
この ESG 経済性検証では、セキュリティオペレーションチームが Anomali のインテリジェンス駆動型セキュリティ製品スイートを導入して潜在的な脅威を迅速かつ効率的に分析、検知、調査、対応することで期待できる量的および質的なメリットに焦点を合わせます。製品スイートには、Anomali ThreatStream（脅威インテリジェンスプラットフォーム）、Anomali Match（脅威検知）、Anomali Lens（脅威ナレッジ）が含まれます。

課題

サイバーセキュリティは、あらゆるビジネスにとって最大の懸案事項です。セキュリティオペレーションチームは、アラートに受動的に対応して「穴を塞ぐ」体制から、爆発的に増大する脅威インテリジェンスを能動的に活用して保護を常に強化する体制へと進化してきました。ESG の調査によると、62% の組織は今後 12～18 ヵ月間にサイバーセキュリティサービスの支出が増加すると予想しています。[1]脅威インテリジェンスのデータソースは増加の一途をたどり、セキュリティ担当者への負担は増すばかりです。彼らは、こうしたインテリジェンスを効率的に取り込み、管理し、分析して、それらの情報に基づき適切な行動を取る方法を見つけなければなりません。組織に人材がどれだけいても、利用可能なインテリジェンスのすべてを活用することはできないでしょう。膨れ上がる脅威インテリジェンスの山に対して、効率的に優先度を判断し、行動に直結するインテリジェンスを選り分けるには、自動化と分析が不可欠です。

多くの大手組織は、時間をかけてさまざまなセキュリティテクノロジーを導入し、こうしたソリューションをサポートするためにセキュリティ専門チームの規模を拡大してきました。セキュリティオペレーションセンター（SOC）を導入することにより、チームの知識と経験を組み合わせて共通のオペレーションを構築し、脅威の検知および対応能力を高めることができます。しかし、セキュリティエキスパートは無限にいるわけではなく、こうした人材を発掘してトレーニングし、維持するのは困難でコストもかかります。同様に、セキュリティ情報およびイベント管理（SIEM）も、多数のサーバーやデバイスが生成したインテリジェンスと情報を統合することで脅威をより効率的に検知します。ただし、SIEM が効率的にログを検索し管理できるデータ量には限りがあり、チームが対処すべき誤検知も非常に多いことから、脅威に対する組織の可視性は限定的になります。組織が、負担の大きい SOC チームを支援するために、本当の脅威を効果的に突き止めて対応を加速する方法を探すのは当然のことです。ESG の調査では、人工知能（AI）と機械学習（ML）を脅威検知に利用するテクノロジーを使用することがサイバーセキュリティの最も一般的な防御策で、組織が 2020 年に最も多額の投資を行う領域であるという結果が出ています（図 1 を参照）。

図 1.2020 年におけるサイバーセキュリティ支出の上位 5 領域



出典：Enterprise Strategy Group

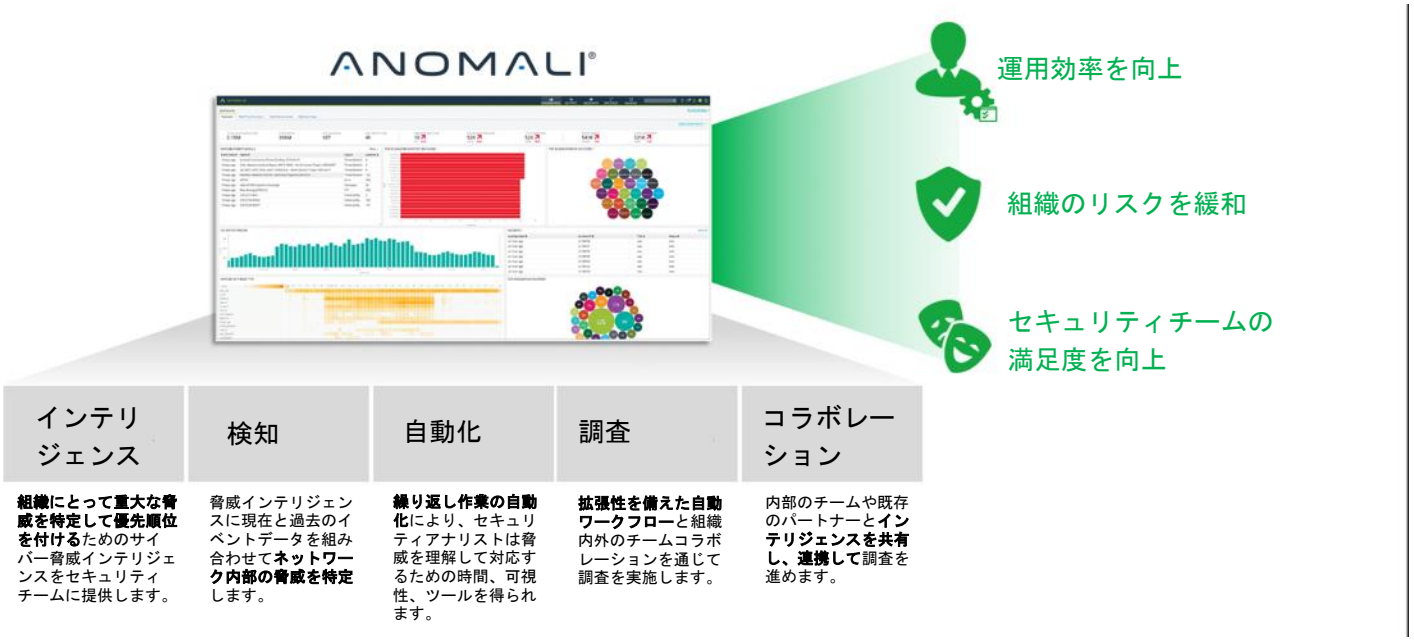
[1] 出典：ESG Master Survey Results：*2020 Technology Spending Intentions Survey*、2020 年 1 月。本書のすべての ESG 調査リファレンスおよび図は、このマスター調査結果セットから引用しています。

膨大な量の脅威インテリジェンスとログデータを活用できれば、セキュリティが強化されることは確実です。ただし、より効果的な保護を実現するには、組織で最も価値ある武器、つまり、SOC とサイバー脅威インテリジェンスを担当する人材に猶予を与えてコミュニケーションを最適化するしかありません。

Anomali のソリューション

Anomali は、インテリジェンス駆動型のセキュリティ製品を提供して、脅威に対する優れた可視性、迅速な検知、機敏な対応、生産性の向上をもたらします。Anomali の製品により、組織は内外のさまざまな脅威インテリジェンスフィードの収集、管理、導入を自動化し、誤検知を排除し、環境内の脅威を特定し、運用を効率化して最も重要なセキュリティニーズに集中できます。

図 2.Anomali 脅威インテリジェンスプラットフォーム



出典：Enterprise Strategy Group

Anomali は、クラウド、オンプレミス、またはエアギャップ環境（オンプレミスであるがパブリックデータとは完全隔離されている状態）に導入できます。プラットフォームは Anomali ThreatStream、Anomali Match、Anomali Lens の 3 つの主要製品で構成されます。

Anomali ThreatStream：脅威に関するデータと情報を質の高いインテリジェンスとしてまとめ、セキュリティ制御に自動配信し、調査ツール群と統合することで、効率的な脅威調査をサポートします。ThreatStream では、オープンソースの脅威インテリジェンス、有償の脅威フィード、共有インテリジェンス、調査結果から得た内部インテリジェンス、サンドボックス解析結果（管理された環境内でのマルウェアの爆発的拡散シミュレーション）など、組織内外の数百に及ぶ情報源から脅威インテリジェンスデータを自動収集します。こうしたフィードを共通のタクソノミーに標準化して複製し、機械学習アルゴリズムにより誤検知を排除し、データをリッチ化し、インテリジェンスの重大度と確度を示すリスクスコアを設定します。その後、機械で読み取り可能な脅威インジケータをセキュリティ制御（SIEM、ファイアウォール、EDR、IPS、SOAR など）に自動配信することのによりインテリジェンスを活用します。また、Diamond、Kill Chain、STIX、MITRE ATT&CK フレームワークを使用したモデルベースの調査を実施するアナリストおよび SOC チーム向けのツールを提供します。調査ワークベンチには、包括的なデータリッチ化ソース群、インジケータの拡張や切り替えを行うパワフルなビジュアルエクスプローラーツール、マルウェアやフィッシング URL をシミュレーションするための統合サンドボックスデトネーション、脅威速報のコラボレーション/オーサリング/パブリケーションなどがあります。

Anomali Match：利用可能なあらゆる脅威インテリジェンスをすべてのネットワークアクティビティログと照合することで、ネットワーク内の脅威を自動検知します。Match では、すべての SIEM ログとその他のイベントソースをインデックス化して 1 年分以上の履歴データを保持し、新旧の脅威インテリジェンスと照らし合わせて継続的に分析し、対応と修正のために SIEM、SOAR、チケットシステムにアラートを自動通知します。リアルタイムフォレンジックにより、アナリストは過去のセキュリティ侵害の証拠を追跡して「ペイシェント・ゼロ（最初の感染）」発見を実現し、アクター、脆弱性、TTP に基づいて脅威を探索し、リスクスコアと資産の重要性に基づいて対応の優先度を決定します。

Anomali Lens：脅威の知識をすぐに使えるようにまとめ、自然言語処理（NLP）を使用して Web コンテンツの文脈を自動識別します。Lens では、Web ページ、ソーシャルメディアプラットフォーム、SIEM などのセキュリティログをスキャンして、セキュリティ侵害インジケータ（IOC）、脅威アクター、マルウェアファミリー、攻撃手法を特定します。Lens で識別された脅威インテリジェンスは、MITRE ATT&CK フレームワークに自動的に関連付けられ、Anomali ThreatStream にインポートされ、ボタンをクリックするだけで調査や分析に利用できます。また、Lens は Anomali Match と統合されているため、ネットワーク内に存在するスキャンされた脅威インテリジェンスが強調表示され、環境における深刻度と影響度を瞬時に把握できます。

ESG 経済性検証

ESG では、量的な経済性検証を行い、Anomali 製品スイートの分析をモデル化しました。

ESG の経済性検証プロセスは、製品やソリューションの経済的バリュープロポジションの把握、検証、数値化、モデル化に定評のある手法です。このプロセスでは、ESG の市場/業界分析、将来に関する調査、技術的/経済的検証におけるコアコンピテンシーを活用します。ESG は、既存のケーススタディとエンドユーザー調査の結果を確認し、エンドユーザーとの詳細なヒアリング調査を実施しました。特に、Anomali 導入前の運用状況や他の組織での以前の状況との比較を重視して、組織に Anomali が与えた影響について理解を深め、定量化しました。量的および質的な調査結果をシンプルな ROI モデルの基本データとして使用し、モデル組織で予想される節約効果とメリットを Anomali 導入で予想されるコストと比較しました。

Anomali の経済性の概要

ESG の経済性分析によると、Anomali を導入した顧客は製品に非常に満足しており、セキュリティオペレーションの大幅な合理化、運用効率の向上、組織の保護に関する全体的な作業の改善を実感しています。ESG は、Anomali が以下の分野で大幅な節約効果とメリットを顧客にもたらしたことを確認しました。

- **SecOps 運用コストを低減**：Anomali の自動化およびオーケストレーション機能と、入念に設計された効率的なセキュリティツールと機能により、組織はセキュリティオペレーションを大幅に合理化し、セキュリティリソースの活用を強化できました。
- **セキュリティの効率を高め、組織に対するリスクを緩和**：顧客は、Anomali がセキュリティチームの能力向上とセキュリティプロセスのオペレーション化に貢献し、その結果、チームの効率が改善して、セキュリティ問題の特定と解消に要する時間を短縮できたと報告しています。
- **SecOps の生産性と満足度が向上**：Anomali は、繰り返し発生する作業や時間のかかる作業を自動化して、セキュリティ担当者を単純作業から開放し、より価値の高いセキュリティ業務に専念できるようにしたことで、生産性と満足度を高める効果があります。スキルを短期間で向上させ、コラボレーションと可視性を改善し、他のセキュリティ製品との相乗的な価値を高めることもできます。

セキュリティオペレーションの運用コストを削減

ESG は、Anomali 製品を導入したセキュリティチームが効率化、自動化、オーケストレーションによってセキュリティオペレーションが大幅に簡素化されたと報告していることを確認しました。ユーザーは、新しいテクノロジーの導入、脅威の調査、データの拡張、誤検知への対応、複数のソースから得た情報の関連付けなど多くのさまざまな領域で時間の大幅な節約または短縮を達成できたと報告しています。その結果、チームはすべてのセキュリティアナリストの生産性を向上して、ジュニアアナリストの能力を高め、短期間で新人研修を完了し、価値の低い作業に時間を浪費せずに問題の解決などの価値の高い活動に専念することができます。

- **管理の複雑さの軽減**：顧客は、ThreatStream により、複数のセキュリティ脅威のインテリジェンスストリームとポイントセキュリティ製品の管理に伴う複雑さが軽減されたと報告しています。管理すべきインターフェイスが減り、新しい有償フィードの AppStore 形式トライアルと導入が簡素化され、IOC の管理が統合されます。その結果、インターフェイスの異なる複数の製品の導入、管理、統合にかかる時間や労力を省くことができます。

- **迅速な価値創出**：ThreatStream は、組織にとって導入が迅速で容易なだけでなく、IOC との統合やプレミアムフィードの追加/削除もすばやく簡単に処理できます。強力なパートナーエコシステムとソフトウェア開発キット（SDK）により、組織はニーズに最適な内外の脅威インテリジェンスツールおよびフィードを短時間で取り入れることができます。さらに、顧客は「フリーミアム」オプションで有償インテリジェンスパートナーからのフィードを購読して脅威インテリジェンスプログラムの最適化を進めることができます。調達も簡素化され、組織は統合や問題のサポートに要する時間が短縮されたと感じています。つまり、組織はセキュリティ戦略およびツールを短時間でテストして統合することに成功しています。ある顧客は次のようにコメントしています。「Anomali のおかげで、ストリームの調達やインストールに要する時間と労力を節約できました。しかも、あらかじめセットアップされており、統合作業なしですぐに使用が可能なため、複雑度に応じて数時間から数日単位で作業時間が短縮されます」

「以前は調査とコンテキストの収集に数時間かかっていましたが、Anomali の導入後は、URL を入力したり Lens で切り替えたりするだけで、必要な防御方法を正確に把握できるようになりました」

- **合理化されたワークフロー**：Anomali は、SOC、CTI、インシデント対応チームを 1 つのプラットフォームにまとめることで、セキュリティワークフローの合理化を支援し、調査時間の短縮に貢献します。簡素化されたワークフロー、他のセキュリティフィード/ソリューションとの緊密な統合、脅威インテリジェンス/調査のエンリッチ化により、脅威検知、調査、対応のあらゆる側面でセキュリティチームメンバーの作業時間を最小限に留めます。

- **作業の自動化**：ユーザーは、ThreatStream の導入後に手作業が大幅に減ったと報告しています。セキュリティアナリストの日常の多くを占める繰り返し作業や時間のかかる作業（ソースの標準化、リスクプロファイルの調査と把握、脅威インテリジェンスのフォーマット化とリッチ化、レポートの作成など）を、Anomali で自動化したためです。また、設定、統合、セキュリティ関連の双方向の作業（SIEM、ファイアウォール、ネットワークデバイスなどのセキュリティソリューション間）の多くも、Anomali によりオーケストレーションされました。Anomali ユーザーの推定によると、Anomali

「アーカイブから SIEM ログを復元する作業には、本来なら 2 週間以上必要ですが、Anomali Match なら 1 時間足らずで完了します」

Match に匹敵する速度でログ情報の処理を行うには、最大 2.5 倍の人員が必要です。「本来なら 10 人必要な作業を、4 人で完了できます」

- **無駄な時間の削減**：Anomali を導入した組織は、誤検知への対応回数が減り、「アラートによる疲労」がはるかに軽減されたと報告しています。ユーザーは、より重要な作業に多くの時間を使えるようになったと感じています。脅威インテリジェンスの調査とリッチ化を自動化することで、状況把握に要する時間が短縮され、繰り返しの作業を強いられるリスクが減り、人的エラーが原因のトラブルシューティングが減少しました。あるユーザーは次のように述べています。「インジケータを取得して意味を解析したり、そのインジケータが悪性である理由を突き止めたりする必要がなくなりました。以前はこのような作業に 90% ほど取られていたのです」

組織のセキュリティの効率性を高めてリスクを緩和

Anomali は、他のセキュリティ製品と連携することで、合理化されたソリューションを提供し、IOC の特定、誤検知の削減、脅威を理解および修正するためのコンテキストと知見の提供に効果を発揮します。調査に回答した顧客は、Anomali によってセキュリティオペレーション全体の効率が大幅に向上したと考えています。一部の顧客は、Anomali によって脅威の特定および修正効率が最大 90% 向上したと報告しています。

「Anomali がなければ、多くの脅威を見逃したり、特定と修正にはるかに長い時間がかかったりすでしょう。もはやセキュリティモニタリングに不可欠なツールと言えます」

- **知見の取得のスピードアップ**：エンドユーザーは、Anomali を他のツールと併用した場合にインサイト取得までの時間が大幅に改善されたと感じています。顧客は、フィードがスピードアップし、可視性が向上し、IOC でリッチ化されたデータによって認知と脅威検知の時間が短縮され、最終的に平均対応時間（MTTR）と修正が改善されたと報告しています。ある顧客は、9 日以上かかっていた IOC の検証作業が Anomali Match によってわずか 10 分で完了するようになり、MTTR が改善されたと報告しています。顧客は、Anomali のおかげで膨大な量の多種多様な脅威や IOC を短時間で検知、調査、修正できるようになったと感じています。

- **機械学習を活用したインテリジェンス**：Anomali では、機械学習アルゴリズムを使用して、脅威コンテキストのリッチ化を提供し、脅威の優先度設定を支援し、イベントの履歴評価を実行します。これにより、組織は数時間に及ぶ手動の作業で得られる成果よりも包括的かつ効果的なインテリジェンスをタイムリーに獲得できます。セキュリティオペレーションチームは、脅威の特定、調査、対応が迅速になったと報告し、かつてないほどチームが効率的になったと感じています。あるユーザーは次のようにコメントしています。「Anomali により、私たちは初めて飛躍的な成長を遂げ、インターネットから情報を収集して組み込む能力を管理して、人間の能力を超えるレベルまで到達できました」

- **その他の脅威インテリジェンス処理**：ThreatStream により、チームはこれまで以上に多様な脅威インテリジェンスを大量に処理できるようになりました。より多くの外部フィードをテストして管理し、ほぼリアルタイムの脅威情報と組織内で培った脅威インテリジェンスを組み合わせることができます。脅威アクターのプロファイリングを行い、アクターを長期にわたって追跡する能力についても、非常に高い価値が認められています。ある顧客は次のように述べています。「フィードを取り込んで相関を取る機能などは他の TIP にもありますが、Anomali は自社のデータを取り込む機能も提供するため、真の価値をもたらしてくれます」

- **より効率的なセキュリティ対応**：調査に応じたすべてのユーザーは、Anomali によってセキュリティ脅威への対応効率が飛躍的に向上したと回答しました。ThreatStream は、膨大な量のインテリジェンスを処理して脅威を迅速に特定するだけでなく、アナリストが強いられていた煩雑な作業を大幅に減らすことができるように、フィードの更新、インジケータの関連付け、セキュリティ侵害分析による関連インシデントの把握を自動化し、先行調査および修正アクションを提案します。ある顧客は次のように述べています。「単にどの IP が悪化していると通知するだけでなく、IP が悪化している理由とともに、実行されたアクティビティや必要なステップも把握できます」

「膨大なメールや IP を 1 つずつチェックするのではなく全体像を把握できます。それらの 90% は、1 つの侵害、1 つのインジケータ種別、または 1 つのタグから発生しているということを確認できるのです」

この機能が重要な理由

どの組織も、ビジネスにとってより効果的なセキュリティを提供したいと考えています。

Anomali の顧客は、Anomali によって脅威の特定および修正効率が最大 90% 向上したと感じています。ある組織は、Anomali のおかげで、前もってセキュリティ侵害を特定し、部門の枠を越えた対策を講じて、ユーザーアカウントを侵害行為から保護したことで、ユーザークレジットの盗難による 40 万ドル以上の被害を回避できたと報告しています。

- **より多くの情報に基づくセキュリティ関連意思決定**：ユーザーは、Anomali が提供するシンプルながら効果的な多くのダッシュボードにより、脅威を視覚化し、意思決定の優先度を設定し、他のチームと有効に情報共有できるようになったと報告しています。また、内蔵のサンドボックス機能、Anomali の専門脅威インテリジェンスサポートチームの利用、同業他社との情報共有により、組織内部の判断に役立つ追加情報を得られます。ユーザーは、Anomali がより多くの情報に基づくタイムリーな意思決定を支援して組織に対するリスクの緩和に貢献したという意見で一致しています。

SecOps の生産性と満足度を向上

調査に応じたすべての組織が、所有するリソースを最大限に活用するための組織変革に Anomali が貢献したと感じています。チームの生産性が大幅に向上しただけでなく、役割に関するチームの満足度も高くなり、事業部門や同業他社とのコミュニケーションが改善されたと報告されています。

- **セキュリティプログラムの生産性の向上**：ThreatStream は、すべてのスタッフの生産性を高め、最も価値をもたらす領域に集中できるようにします。経験の浅いメンバーも、短期間で研修を完了してチームに貢献できるようになり、習得も早く、迅速に経験を積んで、さらに価値の高い役割をこなせるようになると報告されています。これは、組織にとっても個人のキャリアにとってもメリットになります。

「Anomali を導入したことで、非常に大規模なチームに担当させるような作業を 2 人の人員でこなせるようになったため、高い成果が上がっています」

- **セキュリティチームの満足度の向上**：エンドユーザーは、Anomali によって仕事の質が向上したため、安心して帰宅できるようになり、会社を守るために大いに貢献できたと感じています。全体として、自分の仕事をよりポジティブな体験として捉えられるようになったと報告しています。組織は、Anomali によって強力なチームを編成できるようになり、人材の開拓と維持が困難な分野でスタッフを容易に確保できる環境が構築されたと感じています。

- **ビジネスプロセスの改善**：顧客は、ThreatStream を導入したことで、セキュリティ組織間で効果的に情報共有できるようになり、セキュリティチーム、事業単位、エンドユーザー間で非常に有意義な話し合いが可能になったとコメントしています。ある組織は次のように述べています。「Anomali を活用することで、非常に優れたプロセスを構築できました。不正対策チーム、レッドチーム（検証）、脅威インテリジェンスチーム、さらにコンプライアンスチームと連携することで、私たちが何を目指して全力で取り組んでいるのかを明らかにできます」 顧客は、監視対象の脅威をわかりやすく示せるため、ユーザーを効率的に教育できたと感じています。さらに、Anomali の導入前は、数時間かけて詳細な説明を文書化する以外に、事業部門とコミュニケーションを取る方法がなかったと述べています。

「Anomali は、すでにあるプロセスを改善するだけでなく、新たな道も切り拓いてくれます。より効率的な方法でコミュニケーションできるようになりました」

- **同業他社とのコラボレーションの改善**：顧客は、Anomali によって、組織内で収集された脅威インテリジェンスと修正案を同業他社グループと信頼できる方法で共有する手段を獲得したと感じています。これにより、組織は、同業他社に貢献したり、リーダーとして認知されたりするようになります。同業他社グループはより効率的に脅威を特定して修正できるようになるため、他社がすでに行った調査を繰り返す無駄を省くことで貴重な時間を節約できます。ある顧客は次のように述べています。「インテリジェンスを他のグループと共有できるようになったので、非常に助かっています。インテリジェンスを共有することで、同じような深さまで掘り下げたり、同じような苦労を経験したりする必要がなくなりました」

ESG の分析

ESG は、ベンダー提供の資料、経済とテクノロジーに関する一般および業界の知識、お客様とのヒアリング調査の結果から得た情報を活用し、3 年間の ROI モデルを作成しました。このモデルを使用して、Anomali ThreatStream、Match、Lens を導入した場合と脅威分析および検知プラットフォームなしで運営を継続した場合のコストとメリットを比較します。ESG が実施した Anomali の顧客へのヒアリング調査では、経済のモデル化における経験と専門知識に基づいて、Anomali 製品の技術的な検証を行い、モデルシナリオの基盤を構築しました。

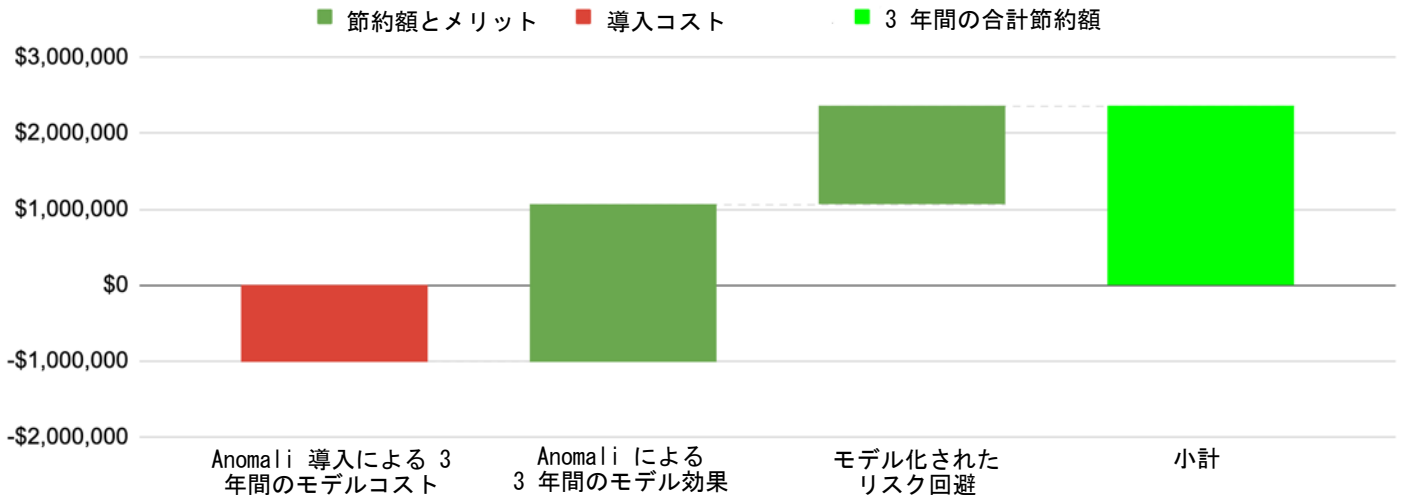
ESG がモデリングした組織は、経験度が異なる 10 人の脅威インテリジェンスアナリストで構成され、従業員 1,500 人の組織にセキュリティサービスを提供します。ESG は、3 年間の年間サブスクリプションコスト、ハードウェアノード、インフラストラクチャコスト、サポートおよびメンテナンスとともに、予想されるコストを、Anomali プラットフォームのインストール、導入、従業員トレーニングに分割しました。

メリット面に関して、ESG は、セキュリティチーム全体の生産性向上で予想されるコスト削減やメリットをモデル化しました。このモデルでは、フィードの管理とキュレーション、調査を実施と結果の報告、他のセキュリティシステムとの統合、コラボレーション組織との脅威インテリジェンスの共有、組織全体での内部的なインテリジェンスの共有と報告に関連するタスクで予想される 20%～70% の改善をベースとしています。ESG は、控えめな予想として、セキュリティチームがこうした作業を遂行するために合計マンアワーの 35% しか使用しないと想定しています。ESG のモデルでは、これらの作業の遂行時に生産性が 58% 改善され、3 年間の合計節約額は 96 万 9,000 ドルと算出されました。この節約によって削減された工数は、Anomali 導入以前は不可能だったセキュリティ関連の追加作業に回すことができます。

ESG のモデルでは、誤検知の 40% 削減（60 万 8,000 ドル）、Anomali が提供するセキュリティ製品に関連する価値（サンドボックス、フリーミアム、プレミアム脅威インテリジェンスフィード、応答性の高い Anomali サポート、Anomali University によるトレーニング）の合計が 45 万 2,000 ドル、プロフェッショナルサービスの廃止、トレーニング、認定、簡素化された調達および統合に関連する他のコスト節約（5 万 3,000 ドル）となっています。

ESG は、早期検知の可能性が高まったことによるデータ侵害の減少、全体的な効率の改善、問題修正の迅速化、データ侵害で発生するコストの削減、検知能力とより迅速で効果的な自動アクションで得られるリスク回避もモデル化しています。データ侵害の可能性と想定コストは、Ponemon Institute が公開している一般に入手可能なデータに基づいています。ESG は、Anomali は組織に対するリスクを緩和し、3 年間でデータ侵害のコストを最大 129 万 2,000 ドル回避できると算出しました。ESG モデルによる費用対効果分析を図 3 に示します。

図 3.ESG による Anomali 脅威インテリジェンスプラットフォームにおける 3 年間の費用対効果分析



出典：Enterprise Strategy Group

数字が意味する事実

ESG のモデル分析によると、モデル組織での大幅な節約とメリットが予測されます。あらゆる導入の背後にある経済性を正確に表現できるモデルシナリオは存在しないため、ESG は各組織が独自の分析を行って節約額を予想することを推奨します。ESG では、当社の分析に含まれている以下のコストを考慮することをお勧めします。

- **Anomali ソリューションの導入コスト**：Anomali サブスクリプション、FTE とソリューションの導入、テスト、トレーニングに要するプロフェッショナルサービスのマンアワー、Anomali を実行するためのアプライアンス、電力/冷却/フロアスペースのコスト、ハードウェアのサポートおよびメンテナンスコストが含まれます。

- **脅威インテリジェンス製品の価値**：サンドボックス、TIP Intel、付属のフリーミアムとプレミアム脅威インテリジェンスフィード、Anomali University によるトレーニング、エキスパートサポートなどと同等のソリューションへの投資額。

- **誤検知処理のためのコストの回避**：ESG では、アナリスト 1 人当たり 1 日 50 件の誤検知が発生し、誤検知 1 件当たり 2 分の時間を浪費し、Anomali で誤検知が 40% 削減すると想定しています。

- **セキュリティオペレーションの生産性向上**：ESG の控えめな詳細モデルでは、Anomali 導入前の工数と比較して、フィード収集（70% 改善）、フィード管理およびキュレーション（70% 改善）、調査と報告（60% 改善）、運用中セキュリティシステムとの統合（20% 改善）、外部コラボレーション（50% 改善）、内部での共有とオペレーション（60% 改善）といった改善を予想しています。

- **リスク低減の定量化**：ESG は、業界の平均比率と比較して検知と対応が 70% 改善した場合のデータ侵害のリスクと、システムの自動化によるデータ侵害コストの削減期待額（いずれも Ponemon Institute により報告された数値）を算出しました。

より大きな真実

サイバーセキュリティの強化は、ESG 調査回答者の複数年にわたるテクノロジー支出のビジネスドライバーリストで常に上位を占めています。組織が、チームの拡大、チームの整理、新しいソリューションへの投資を続けた場合、明らかなことが 1 つあります。問題となるのは、セキュリティツールや脅威インテリジェンスの不足ではなく、インテリジェンスとアラートに基づいて情報を効率的に管理し、解釈し、適切な行動を取ることができる人材の不足です。現代のセキュリティ組織は、セキュリティプロセスを合理化し、繰り返し作業を自動化し、AI 駆動型のインテリジェンスを提供し、人員による効率的なオペレーションを可能にする脅威インテリジェンスプラットフォームを必要としています。

ESG は、Anomali ThreatStream、Match、Lens が顧客のセキュリティ投資を最大限に活用するためのプラットフォームを提供していることを検証しました。セキュリティチームの能力は向上し、生産性が高まり、最も重要な作業に専念できます。また、SIEM などセキュリティ製品に対する投資を容易に統合して強化することで、さらなる価値を引き出し、脅威インテリジェンスフィードを直ちに評価、購入、統合できるようになります。顧客は、可視性が大幅に改善され、内部的には組織内の他の部門、外部的には同業他社やセキュリティ組織と脅威インテリジェンスを共有する能力が飛躍的に高まったと報告しています。

ESG のモデル化したコストメリット分析では、Anomali を導入した組織がセキュリティチームの生産性の改善、付属の脅威インテリジェンス製品による付加価値、リスクの緩和からどの程度の節約を期待できるかを評価しています。モデルでの主な前提は、ESG による Anomali 顧客の検証に基づいています。ESG のモデルでは、毎月の節約額は最大 9 万 3,000 ドルと算出されており、予想される投資収益率（ROI）は 233% です。

Anomali は、組織の既存のセキュリティ製品とは競合せず、チームの運営の機能面の変化も必要としません。Anomali は、脅威インテリジェンス、ツール、ソリューションを強化して活用し、セキュリティチームの効率を高め、セキュリティに関するコミュニケーションをビジネスの他の領域に拡大することを可能にします。ESG のヒアリング調査に応じたすべての組織は、より小規模なチームでより多くの成果を達成し、マンパワーだけで現実に達成できる範囲をはるかに超えたオペレーションを実現できたと感じています。新しい役職で Anomali を導入した顧客もいます。「前の役職で Anomali を使用していました。新しい役職についたとき、Anomali なしではチームの目標を達成できないと感じたのです」アナリストの皆さんは、こうした告白こそ、変革的なテクノロジーの証だとすぐに気付かれるでしょう。セキュリティオペレーションの変革と合理化を模索し、脅威インテリジェンスを最大限に活用することを望んでいるなら、Anomali にコンタクトを取り、自分のチームに適した脅威インテリジェンスプラットフォームかどうかを確認することをお勧めします。

Enterprise Strategy Group は、IT アナリスト、調査、検証、戦略企業として、市場インテリジェンスと実践的な知見を世界中の IT コミュニティに提供しています。