EclecticIQ

ホワイトペーパー

実用的なCTIに至る道

Chris O’ Brien著

どのような闘争や戦争においても、情報は価値ある商品となる。いかなる洞察や知識でも、攻撃者よりも防御側に有利に働けば、勝利と打破の違いを知らしめることになる。しかし、意味不明のメッセージや単純な誤解によって、コミュニケーション不足に陥り、不利に働くことが多すぎる。このことは、セキュリティチームがその完全なメリットの実現に苦労する、サイバー脅威インテリジェンス（CTI）の分野で特に顕著である。実のところ、実用的なCTIに至る道は、短くもなく容易でもない。しかし、それは非常に有意義で、CTI共有プロセスを大幅に強化できる重要なマイルストーンがいくつかあり、我々はそこを目指すことができる。

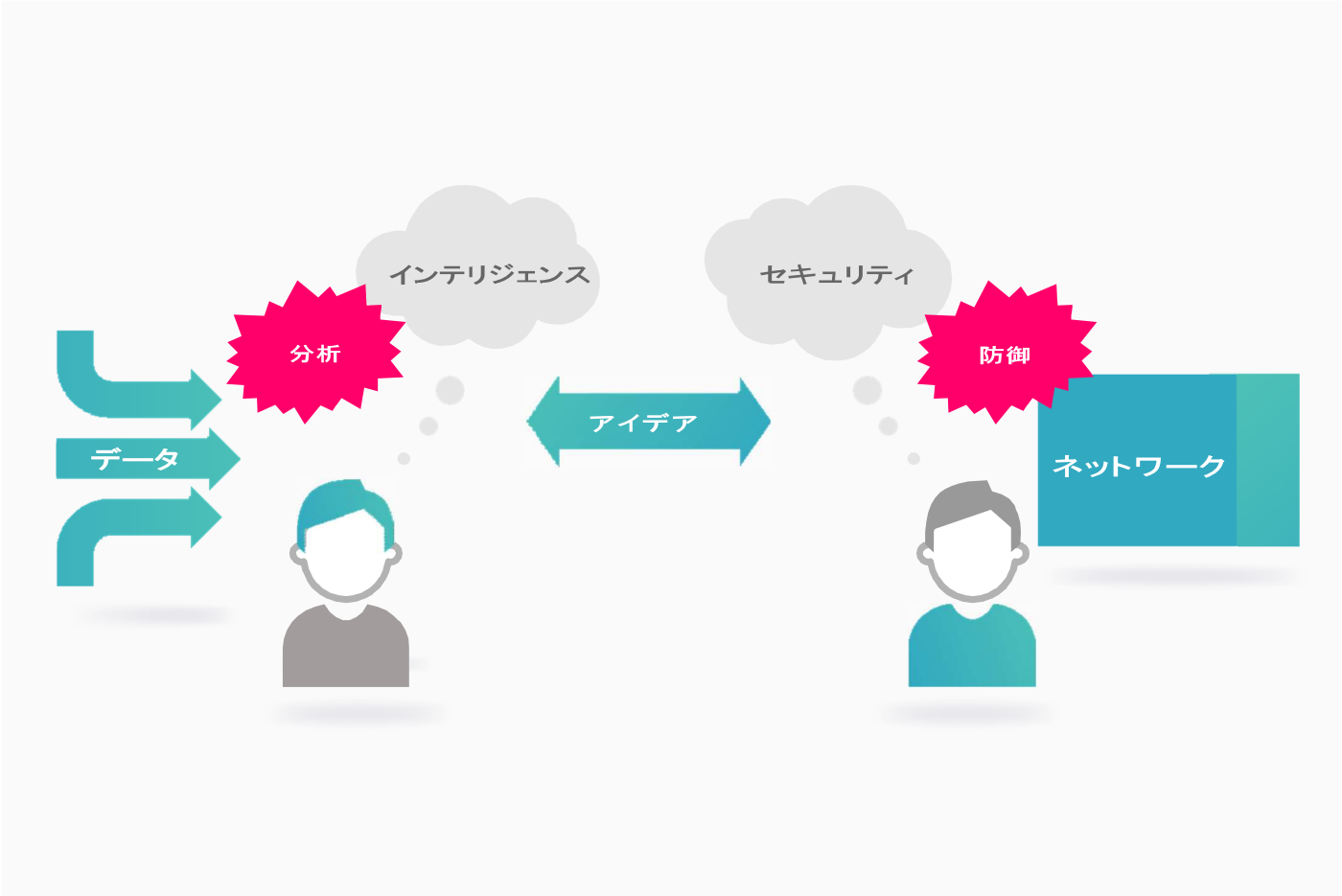
問題の本質は、インテリジェンスの専門家とセキュリティの専門家の間の解釈の違いから失われる見識もあるということである。セキュリティの専門家は、組織を保護する方法を知る必要があり、インテリジェンスの専門家（またはCTIアナリスト）は、防御に役立つ実用的な見識を備える。

両専門家の動機は異なるため、異なる視点から問題に取り組む。

ネットワークを防御するセキュリティ専門家は、「何が？」を気にする。つまり、こう尋ねる。「何が私のネットワークを攻撃しているのか？そして、それに対して防御するために私に何ができるか？」

一方、CTIアナリストは「なぜ？」に焦点を当てる。つまり、こう尋ねる。「なぜ私たちのネットワークが標的にされているのか、そしてなぜ気にする必要があるのか？」

2つの職業で重なるのは「どのように？」の質問、つまり「攻撃はどのように行われているか？」などである。この関心の合流点は、戦術、技術、手順（TTP）の規律が作用する場所である。



この2つの役割を、同じ組織で働くさまざまな人々と考え、彼らの間のコミュニケーションを、脅威インテリジェンス共有機能と考えてみよう。最終目標は、一見無関係に見えるデータポイントの複数の糸口をつかみ、そこから価値ある結論を引き出すことである。当然、この分析の目的は、ネットワークの防御を成功させることである。

これを前提とする次のような問題がすぐに特定できる。

1. **インテリジェンス対セキュリティ。**インテリジェンスとセキュリティの間には強い相関関係があるが、2つの仕事の基本的な目的は正反対であることが多いようである。もしも敵対者がネットワークの攻撃を

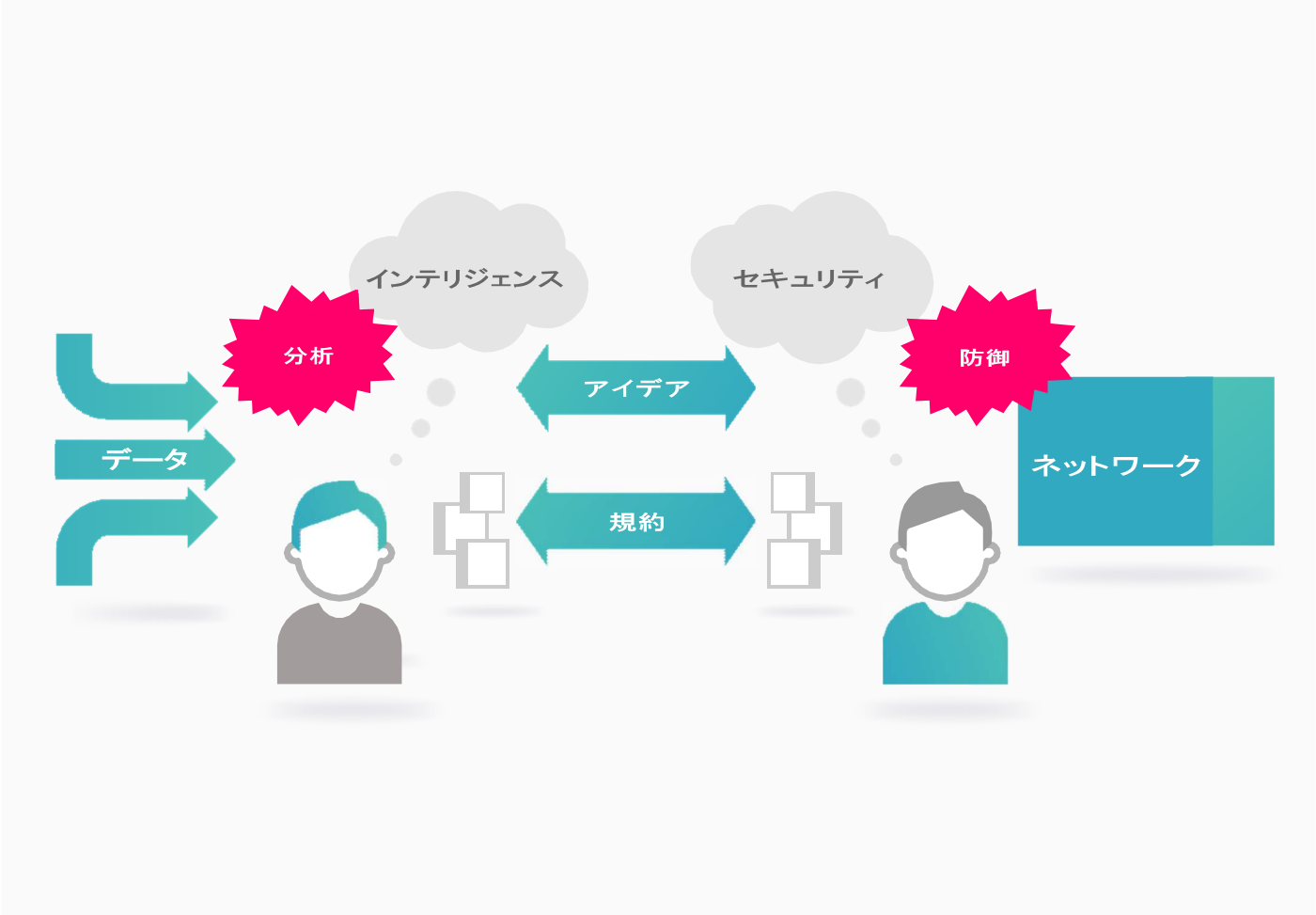
試みても、きわめて安全に保護されているために足がかりさえ得られないとしたら、これは明らかにセキュリティの「勝ち」である。しかし、敵対者がすぐに失敗したという事は、私たちが彼らの動機や能力について何も学ばなかったことになるため、それはインテリジェンスの「負け」である。この種のインシデントにあるのは常にバランスであり、ケースバイケースで判断する必要がある。しかし、これによって示されるのは、一見相反する2つのアプローチ間でアイデアを直接共有すると、論争につながりやすいということである。

2. **解釈とバイアス。**アイデアを伝え合うことはCTIの中核となる。伝えようとする内容が、
脅威の重大度、細部の重要性、誤解を招くデータソースの不適切性のどれであっても、アイデアの提示方法と解釈のされ方は複雑であり、いろいろに解釈される。

3. **実現に要する時間。**コミュニケーションが主観的であることを十分に理解していても、相手に自分の考えを確実に理解してもらうには時間と労力を要する。

これが、CTIの分野における我々の現在地である。アナリストとセキュリティの専門家はいまだに、効果的ではない手段でアイデアを交換している。
受信者に思考プロセスを説明するために、何行ものテキストが必要な場合がある。そのテキストが終わるまでに書き手が理解されていれば良いのだが、このコミュニケーションプロセスは非効率的であり、誤解されやすい。

明らかに、この種の相互作用は、アイデア共有のための共通フレームワークの作成に役立つ規約から恩恵を受けるだろう。



ステージ0：インテリジェンスレポート

規約の目的は次のように単純である。ある種の情報は本質的に目標地点となる場合があり、そうあるべきであり、迅速に伝達するべきということに、同意すること。

そのために、論文には要約があり、新聞には大見出しがある。詳細をすべて知りたくない場合は、一定の提供ルールのもとで、できるだけ多くの客観的に役立つデータを入れておくということに賛同しよう。

時間の経過とともに、そのルールを改良して、適切なデータが抽出され、最終的にはそのルールがコミュニケーションの唯一の手段になり得る、という状態となる。

このアプローチには、次のような具体的なメリットがある。

1. **時間とリソースを節約。**レポートの主題が脅威アクターなのかマルウェアファミリーなのかを理解しようとするよりも、専門家には他にもっとすることがあると、我々は考えるべきである。事前に定義されたオントロジを使用すると、アナリストが作成者の言語をリバースエンジニアリングする時間が不要となる。

2. **真意を伝える。**レポートの言語をリバースエンジニアリングするプロセスでは、色々な解釈の余地が残るため、受け取る側の一方的な意見に負けてしまう。そのため、元のレポートの本来の意図が変わってしまう可能性がある。規約は、そのようなあいまいさを減らすために効果的である。

3. **ヒューマンエラーを減らす。**これらのプロセス全体を通じて、タイプミス、コピーアンドペーストのエラー、および完全に回避できる同様の問題が発生する機会は何度もある。規約はこれらの問題を減らし、メッセージングの一貫性と信頼性を維持して、偶発的な誤解を避けることに役立つ。

それでは次に、規約を定義しなければならない。これはインテリジェンスコミュニティにとって新しい論理ではない。「スタイルガイド」の中でインテリジェンスレポートを書くという実践は、伝えるべきメッセージを伝えるために、非常に具体的な表現を使うことであり、場合によっては情報機関の専門職自体と同じくらい古いことなのかもしれない。

あらゆる点で、最高品質の最終成果レポートを作成することは、それ自体が情報運用の特徴を表している。

セキュリティの専門家（そのようなレポートの読者）については、その規約の発展を我々の目の前で確認することができる。

ステージ1：指標の監視リスト

インテリジェンス：「私はAPT5632の最近の悪意のある活動すべてについてのレポートを書いています。そこには、セキュリティに役立つはずの膨大な量の情報があります。」

セキュリティ：「ありがとう。でもレポートを全部読む時間はありません。セキュリティセンサーに展開するべき指標だけ送ってもらえますか？」

インテリジェンス：「いいですが、それだと前後関係がわかりませんよ。」

セキュリティ：「前後関係はまったく不要です。その指標に確信があるなら、私に必要なのはそれだけです。」

読者が受け取ることが特に重要だと著者が信じている指標のリストを含めることは、規約の定義への大きな第一歩である。
セキュリティチームは多くの場合、インテリジェンス側よりも速いテンポで作業しているため、すばやく簡単に取り込めてセキュリティコントロールに展開できる指標を欲しがる。

両当事者がその指標監視リストに何を入れるかについて合意すれば、規約が形成され始める。
NATOアドミラルティコードのようなベストプラクティスを採用して標準化された指標レベルを使えば、脅威に関する情報の伝達に役立つ。

この規約は、逐次のエンティティ分類規約から生じる問題に対処するためにも必要である（つまり、「この指標は信頼できるレベルです」と言われても、それはセキュリティチームが有効な決定を下せるほど明確ではない）。

ステージ2：TTPクラスタリング

セキュリティ：「私に送ってもらった指標は、特にあるドメイン名で多くの誤検知を引き起こしています。あのURLは本当に悪意のあるものですか？」

インテリジェンス：「もちろんです。このウェブサイトは、既知の組織犯罪グループによる最近の攻撃によって侵害されており、閲覧者にマルウェアを配信しているところです。残りの指標は、配信するマルウェアを検出する方法です。」

セキュリティ：「それでは、これらの指標のコンテキストはまったく別物ですね。つまり、そのコンテキストに応じて別の処置が取られなければなりません。指標に関係する処置はどうしたらわかりますか？できる限り自動化したいと考えています。」

インテリジェンス：「わかりました。関連のある各手法に分けて指標をグループ化します。」

サイバー脅威インテリジェンスを分類する手段として事業がTTPの背後に集結しているのを見るのはすばらしいことであり、これは対処行動の背景導出を自動化するための大きな一歩である。書面によるレポートから詳細を抽出して規約に含めるようにすればするほど、アナリストの「アイデア」にともなうデータ量を減らすことができ、より多くの自動対処で詳細を利用できる。

社内で合意済みの規約を使用する場合でも、あるいはMitre ATT&CK Frameworkなど全般的に合意済みの「ライブラリ」を使用する場合でも、すべての裏付け情報を読むことなくコンテキストをすばやく理解できることは、成熟の大きな一歩である。データの意味がわかれば、セキュリティの専門家はデータを正しいコンテキストで使用できる。その結果、誤検知を大幅に減らし、さらにリソースの負担も減らすことができる。

ステージ3：構造化インテリジェンス

ただし、このアプローチの問題は、いまだに2次元ということである。指標があり、前後関係もあるが、他にも考慮すべき可変のものがある。

セキュリティ：「そのデータはすばらしいですが、そのマルウェアのExfiltrationステージとCommand and Controlステージの両方に同じIPアドレスが含まれていることに気づきました。これはタイプミスですか？」

インテリジェンス：「いいえ、間違いではありません。マルウェアは実際に、そのインフラストラクチャを「ラウンドロビン」し、時にはCommand and Controlに、また別の時にはExfiltrationに、同じIPアドレスを使うことがあります。」

セキュリティ：「使用方法にパターンはありますか？」

インテリジェンス：「はい。タイムスタンプの回転に基づいていて、アルゴリズムがわかれば実際にはすぐに予測できます。」

セキュリティ：「すばらしい、大いに使えますね。」

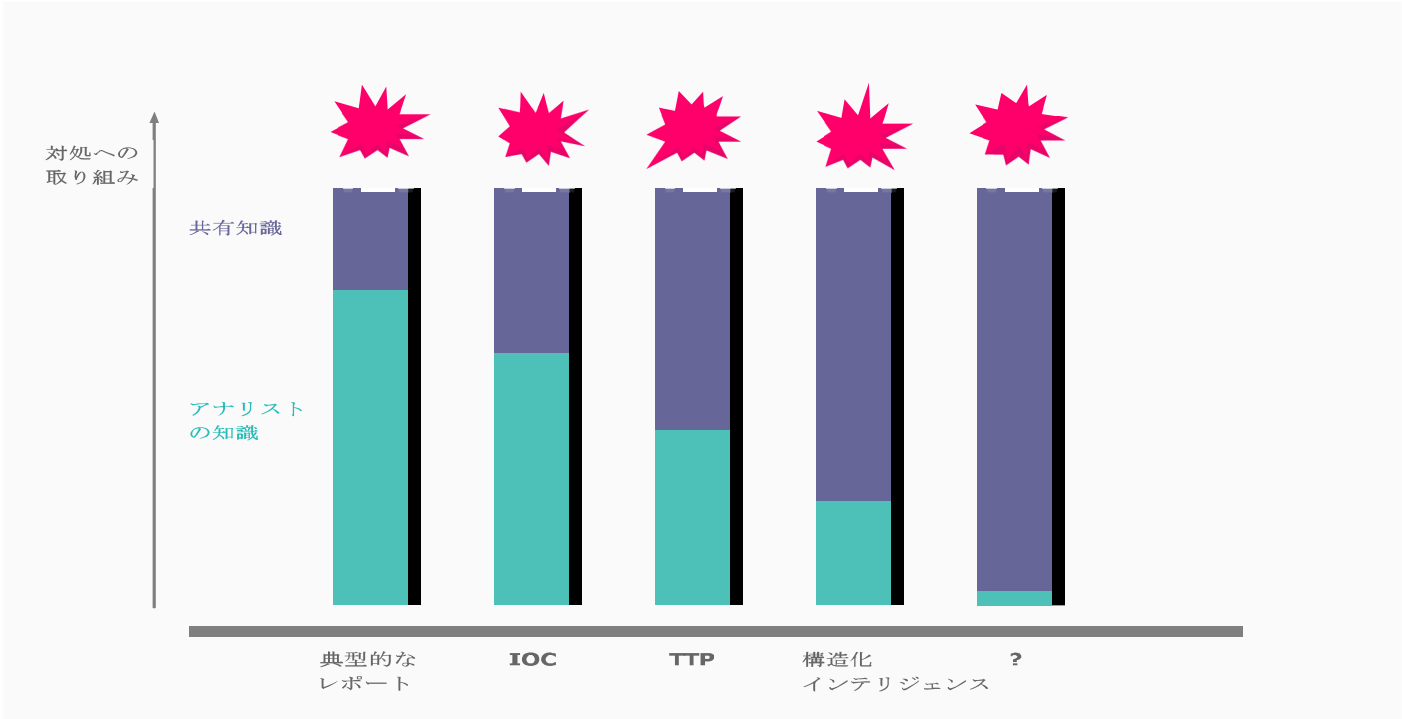
TTPの使用に同意すると、データの分類方法について共通の理解を受け入れることになる。しかし、これがうまくいくのは、必要な内容を2次元で表現できるうちに限られる。これは、データが非常に急速に複雑になるサイバーセキュリティドメインでは特に問題である。

書面によるレポートをいまだにコミュニケーションで使う理由の一部は、多層で時系列の非対称攻撃ベクトルの微妙さとニュアンスを伝えることはスプレッドシートでは難しいためである。

そのため、ますます複雑で多次元のパターンでデータをモデル化しなければならなくなる。これは単に、きれいにグラフ化するということではない。データを構造化された形式で記録することで、インテリジェンスの事実を照会可能な形式で詳述する。

事実上、セキュリティの専門家が必要なものについてデータを照会できる場合（たとえば、「マルウェアインフラストラクチャのタイムスタンプローテーションをすべて表示する」）、インテリジェンスアナリストの仕事は、事実を最も明確に、そしてできるだけ客観的に正しく記録することである。

簡単？いや、もちろんそうではない。実際、このプロセスで破綻することが多い。CTIプラクティスが成熟するにつれて、指標を通り越し、いまやコンテキストを提供できるTTPの威力の把握を急速に進めている。しかし、構造化インテリジェンスの強固な基盤の上に構築された場合にのみ、CTIプラクティスは、こうした基本的な会話を超えて、真に革新的なインテリジェンス–セキュリティ間のデータ共有への移行が期待できる。



結論

異なる3つの規約ステージを進むにつれて、インテリジェンスアナリストが知識を頭の中から共有の企業理解へと徐々に移行できるようにしていく。

私たちは、「APT8563685」について知るべきことをすべて知っている対象分野の専門家だけを抱えるような、サイバーセキュリティ業者から離れようとしている。真のメリットは、その知識を共有知識として記述し、さまざまなユースケースや自動パスで簡単に照会できることである。

特別なアナリストの知識が少なければ少ないほど、共通の形式によってより広いコミュニティと共有することができる。その結果、インシデントに迅速に対応し、チームリソースとチームが防御するネットワークの両方への影響を減らすことができる。

これをさらに一歩進める、構造化インテリジェンスを超えたドメインがほぼ確実に存在する。人工知能と機械学習の分野での動向によって、すばらしく有望なアプリケーションも現れている。

だからといって、将来アナリストの居場所がなくなるわけではない。単に、報告とコミュニケーションの手法を拡張して、より簡単に実行できるようにする必要があるということだ。広く共有できる優れた見識を備えた「開発アナリスト」が出現し続けていることを考えると、分析とツール開発の両方のスキルを持つ人々がこの分野で繁栄することになるだろう。その始まりはインジケーターからTTPへの移行であるが、これは構造化インテリジェンスの基盤に組み込まれている。

実用的なCTIに至る道

本書の著者

Chris O' Brien
EclecticIQのインテリジェンスシニアディレクター

公共部門と民間部門の両方で、サイバーセキュリティとインテリジェンス分野のチームを率いてきた。Chrisは、インシデントの追跡と対応を行うイントルージョンアナリストとしてスタートし、NCSCUKの設立を支援した最初のテクニカルアナリストの1人だった。EclecticIQ社に入る前、Chrisはサイバーインシデントへの迅速な対応をサポートするための技術ナレッジ管理を専門とするNCSCのサブテクニカルディレクターを務めていた。現在はフュージョンセンターのインテリジェンス運用ディレクターを務めている。

EclecticIQ

EclecticIQは、行政機関と一般企業を対象に、インテリジェンスで強化したサイバーセキュリティを実現します。お客様のサイバーセキュリティを脅威の現実に重点的に合わせる、アナリストを中心に据えた製品とサービスを開発しています。その結果、インテリジェンス主導型セキュリティ、検出と予防の向上、コスト効率に優れたセキュリティ投資が実現します。

弊社のソリューションは、脅威の調査、脅威ハンティング、インシデント対応作業など、あらゆるインテリジェンス主導型のセキュリティプラクティスに携わるアナリストに特化して開発されています。
また、お客様のITセキュリティコントロールやシステムと緊密に統合させます。

EclecticIQは欧州、英国、北米のオフィス、および付加価値を提供する認定パートナーを通じてグローバルに事業を運営しています。

EclecticIQの詳細については、www.eclecticiq.comをご覧ください。

Twitterは@eclecticiqをフォローしてください。

EclecticIQ
INTELLIGENCE POWERED DEFENSE