製品説明

EclecticIQプラットフォーム

脅威の現実を再びコントロールし、修復までの時間を数日から数分に短縮できるようにアナリストを支援。

政府と企業はサイバー脅威にさらされ、NCSC、CERT、SOC、IT部門、組織内の他の機能分野のサイバー防御を改善する必要に迫られてきました。

サイバー脅威インテリジェンス（CTI）は、セキュリティポートフォリオの望ましい機能から、基本必須機能へと変化しました。

はじめに

現実は厳しく、サイバー攻撃は今や日常茶飯事になっています。敵対者は賢く、高度に組織化されており、回避策を改ざんして使えないようにする術に長けています。セキュリティ専門家は、既存の脅威だけでなく、将来現われるかもしれない脅威に備えた計画を立て、準備することが求められています。これは非常に厄介なタスクです。結局のところ、個々の不具合や脅威ベクトルごとに備えをすることは、政府や企業にとって実行可能な対策ではないし、経済的に妥当なことでもありません。代わりに、リソースを効果的に配分し、発生する可能性が最も高い攻撃へのセキュリティ体制を強化することが肝要です。

政府と企業はサイバー脅威インテリジェンスの力を活用すれば、不要な情報をカットして、自組織との関連性が最も高い脅威を特定できます。脅威インテリジェンスプラットフォーム（TIP）を使用すると、アナリストは実用的なインテリジェンスを生成できます。一貫性の高い正確な脅威インテリジェンスを利用すれば、より的確な情報に基づいた戦略、戦術、運用の決定を推進して、最も効果的な改善策を確実に実施できます。その結果、組織への侵害による影響を最小限に抑えられます

。

EclecticIQプラットフォームは、アナリストを中心に考えられたTIPであり、オープンソース、商品サプライヤー、業界提携先からのインテリジェンスデータを1つの協働アナリストワークベンチに取り込みます。EclecticIQプラットフォームを使用すると、複数のインテリジェンスフィードの処理に伴う手動の繰り返し作業がなくなるため、アナリストは最も重大な脅威を特定し、タイムリーに対策を講じ、組織に対処方法をアドバイスし、同業他社と協働することができます。EclecticIQプラットフォームは、業界のベストプラクティスがベースになっており、CTIワークフローと産業スパイ活動などに関するノウハウを中心に据えて開発されています。

EclecticIQ

主なメリット

得意な作業に取り組めるようにすることでアナリストの生産性をアップ

EclecticIQ Platformでは、ワークフロー全体を迅速化するTIPの支援を利用できます。発見の自動化とデータエンリッチメントのおかげで、複数のフィードの処理やセキュリティ侵害インジケーター(IOC)によるソートなど、アナリストの役割に伴う繰り返し作業や日常作業をする必要がなくなります。代わりに、独自の知見を提供したり、脅威をより効果的に特定したりといった、得意とする作業に集中して取り組めます。

実用的なインテリジェンスを提供することで、対応をさらに迅速化

脅威データは、正確、タイムリーで、状況に即していなければ価値がありません。弊社の広範なデータ取得機能とエンティティエディターを使用することで、アナリストは人間と機械の両方が利用できる、STIXに適合した実用的なインテリジェンスを素早く作成できます。EclecticIQプラットフォームは、プラットフォーム自体の中で構造化インテリジェンスと非構造化インテリジェンスを作成できる唯一のTIPです。レポートとデータはITセキュリティコントロールにメールで、または直接送信されます。意思決定者は非構造化レポート内のリンクからEclecticIQプラットフォームのコンテキストを確認して、より的確な情報に基づくタイムリーな対応ができます。

脅威の現況全体に応じてセキュリティ対策を調整

EclecticIQプラットフォームを使用すると、組織は最も対処すべき攻撃ベクトルを特定できます。適切な実用的インテリジェンスで脅威に備えることで、最も必要とされる部分にリソースを割り当て、適切な対処方針に注力できます。脅威インテリジェンスをこのように効果的に利用することで、割り当てられた予算とリソースで多くの成果をあげ、既存の脅威と新たな脅威からビジネス資産を保護することができます。

CTIプラクティスの有効性の向上

組織はCTIプラクティスによって配布されるインテリジェンスを活用して、防御を受動的ではなく臨機応変に改善できます。動的な協働ワークスペース、直感的なグラフ、検索およびピボットツールを利用することで、アナリストは大量のデータを解読して、関係性、パターン、傾向を特定できます。検証される仮説が増えるにつれ、組織内でインテリジェンスへの要求にタイムリーに対応できるようになります。

CTIの投資回収率の向上

EclecticIQプラットフォームは、自社セキュリティチームの手足となります。その自動化機能とエンリッチメント機能で、手動作業でかかる諸経費をなくして投資回収率を向上させます。アナリストは手動作業から解放され、より効果的に脅威を特定して、生産性を強化できます。ITの視点で見ると、EclecticIQプラットフォームは様々な構成設定が可能であり、既存のセキュリティインフラと容易に統合します。
SIEM、エンドポイントソリューション、ファイアウォールなど様々なセキュリティシステムに統合する既存の統合オプションのカタログはさらに増え続けています。さらに、ソフトウェア開発キット(SDK)を使えば、特注システムを速やかに追加できます。

製品概要

協働ワークスペース内で一連の主要なワークフローとプロセスを使用することで、アナリストは適切な実用的インテリジェンスを速やかに特定できます。EclecticIQプラットフォームでは、脅威コンテンツが統合、標準化、強化されるので、アナリストはインテリジェンスの選別、分析、協働、作成に注力できます。

EclecticIQプラットフォームは、SOC、CERT、情報リソース、脆弱性管理、ITアーキテクト、ビジネスや組織のリーダーなどの利害関係者に情報を伝えられるよう、脅威インテリジェンスアナリストを効率的にサポートします。

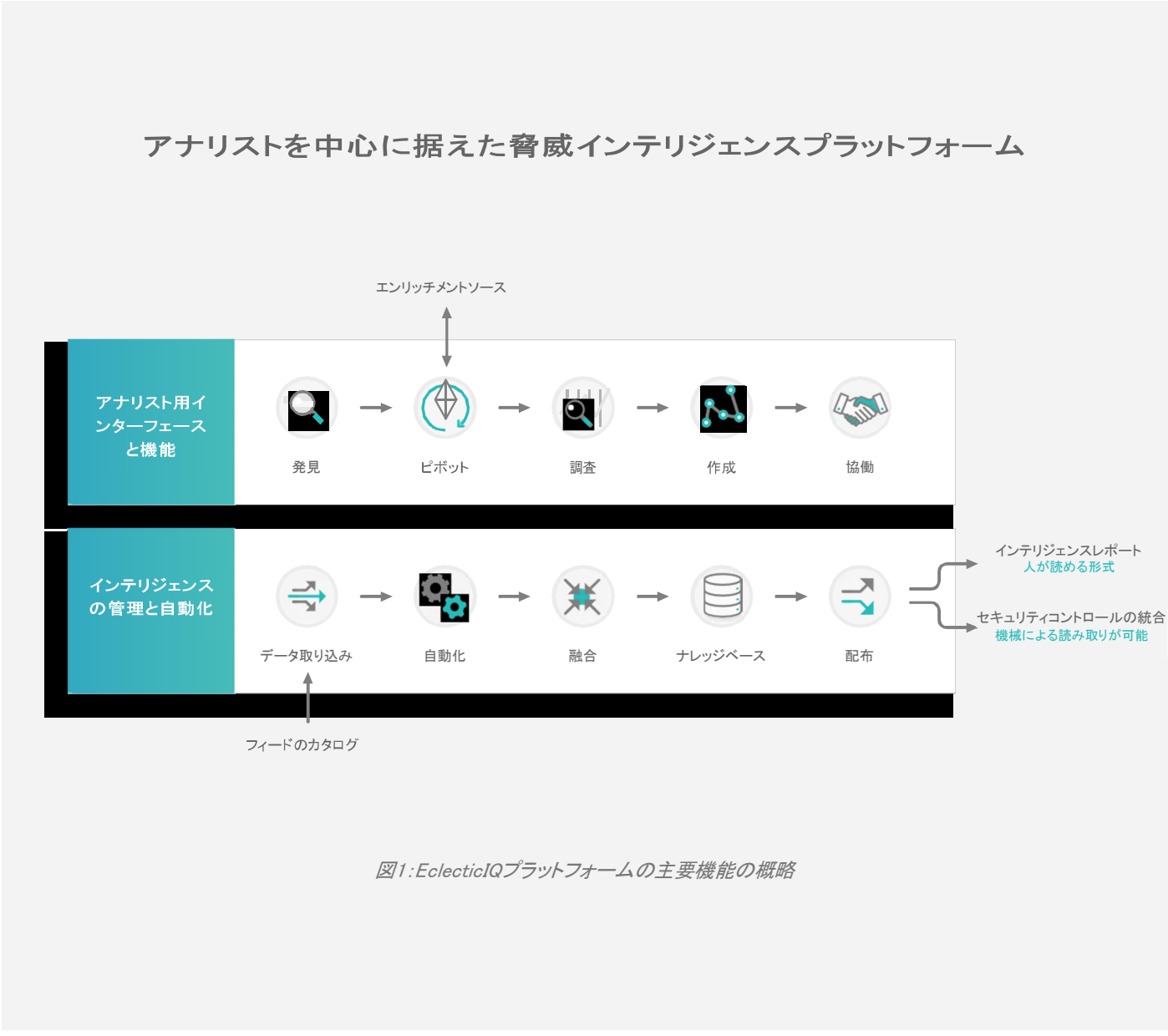

図1:EclecticIQプラットフォームの主要機能の概略

収集および相関付け

EclecticIQプラットフォームは、オープンソース、商品サプライヤー、内部ソース、業界提携先など複数のソースからのインテリジェンスデータを収集します。新しいフィードソースが定期的に追加されるため、最新の情報が利用可能になります。データを自動的に取り込んだ後は、エンティティエディターを使ってプラットフォーム内でインテリジェンスを作成することができます。エンティティエディターを使用すれば、EclecticIQプラットフォームから出ずに、STIXに適合した構造化/非構造化インテリジェンスを作成できるため、アナリストの時間が節約されます。

EclecticIQプラットフォームのデータ取り込み機能によって、業界で最も幅広い種類のデータ形式の作業が可能になります。取り込み機能では、pdf、csv、独自仕様の形式、STIXなど複数の形式がサポートされるため、生成されたインテリジェンスは、使用されるソースが幅広いため、忠実度と精度がより高い情報となっています。

その結果、より徹底して脅威の現実を把握でき、関連する脅威が予測しやすくなります。

データ融合機能によって選別プロセスが強化されるため、データ内のつながりと関係性を即座に捉えることができます。EclecticIQプラットフォームは重複排除、関連情報の抽出、エンジンルールの使用による強化、タグ付け、グループ化、操作の自動化の諸機能を搭載しています。
データ融合によって、多大な労力を要するプロセスの部分が除去されるため、アナリストは脅威の状況について包括的な視点を速やかに得ることができます。また、自動化により、大量のデータを処理する際の人による見落としのリスクが最小限に抑えられます。

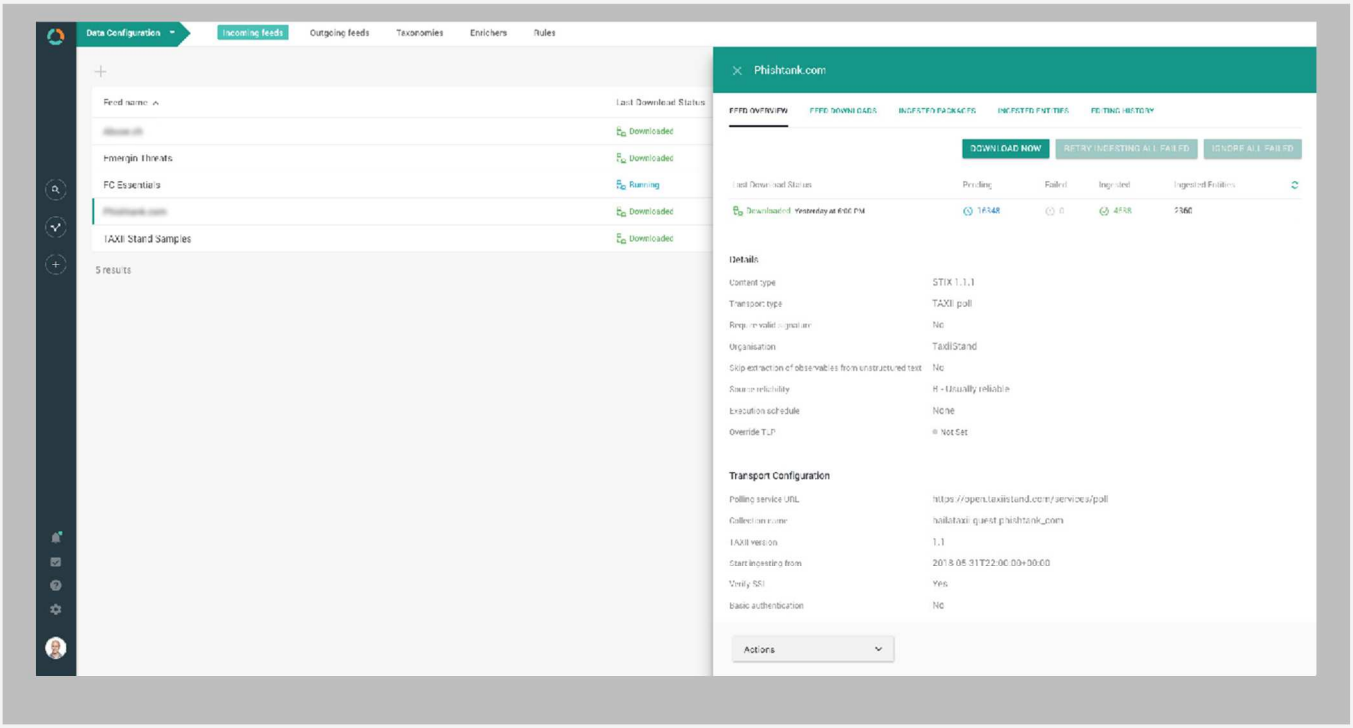

図2: 受け取ったフィードの概要を明確に把握

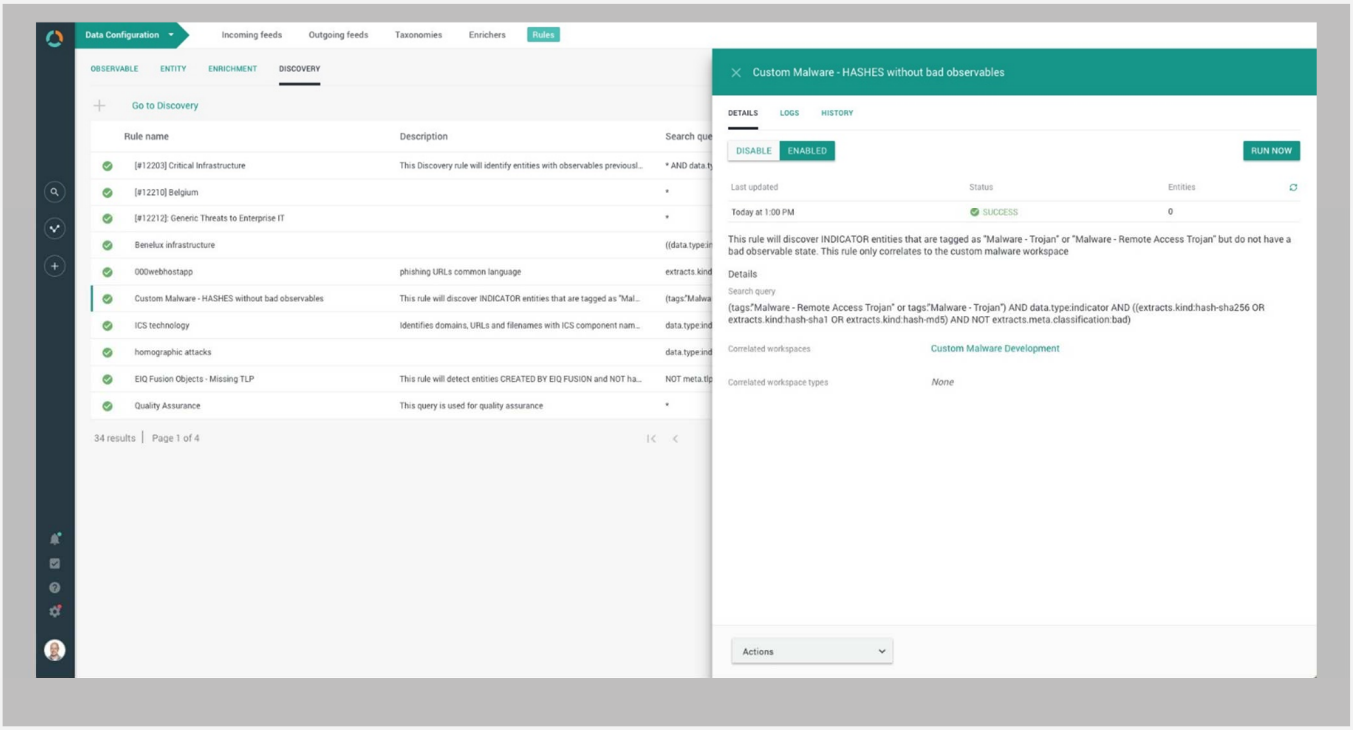

図3：直感的なルールエンジン

分析および協働

EclecticIQプラットフォームでは、認定、選別、発見のプロセスの自動化により、アナリストは大量の脅威インテリジェンスを日々処理することができます。たとえば、発見機能では、ほぼリアルタイムのフィードとアラートを設定できます。さらに、自分自身または同僚に対して、アクションのフォローアップ作業をプラットフォーム内で設定できます。その結果、プロセスの合理化、共同作業の促進、アナリストによる作業の拡大が実現して、CTIプラクティス内に効率化がもたらされます。

また、ナレッジベースのワークフロー重視の視点を取り入れた動的なワークスペースによって、共同作業がさらに強化されます。動的なワークスペースにより、アナリストはデータを脈絡なくまとめるのではなく、ビジネスプロセス（インテリジェンス要件やチーム設計など）を基にインテリジェンスをまとめて分類することができます。

CTIクリップボードアドオンの導入によって、データをよりシンプルにEclecticIQプラットフォームに追加できるようになりました。そのため、アナリストはブラウザから離れることなくウェブサイトから直接データをキャプチャできます。こうした効率的な方法で、プラットフォームに直接データを保存、入力できます。

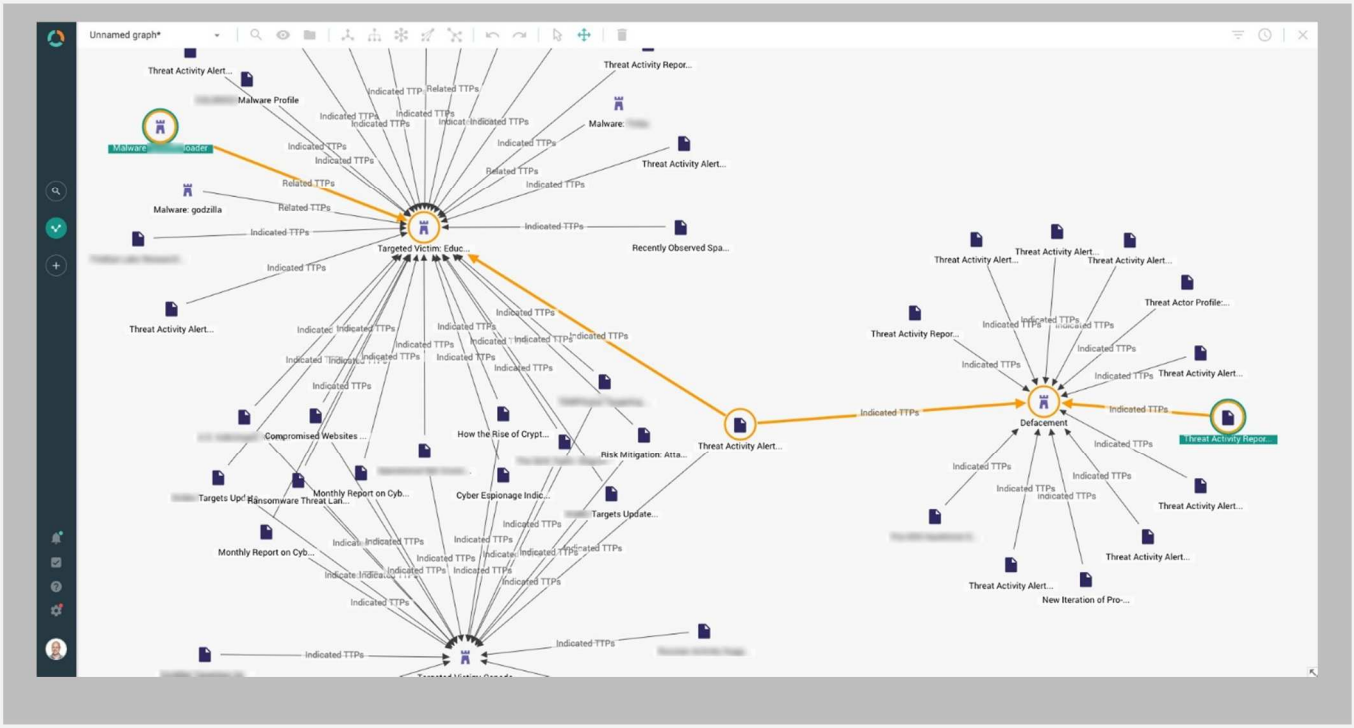

図4:関係を容易に分析

作成および配布

EclecticIQプラットフォームの場合、アナリストは同じデータソースに基づく、人と機械の両方が読めるレポートを作成できるため、一貫性と正確性が確保されます。

プラットフォーム内でのレポート作成は、速やかにかつシンプルに行うことができます。
ワークスペースと動的なデータセットのおかげで、複数のツールや場所から情報を集めたり、コピー＆ペーストする作業は不要です。プラットフォーム内ですべての作業を処理できるため、レポート作成にかかる時間が大幅に短縮されます。

機械読み取り用のレポートは、ITセキュリティコントロールに自動的に送信されます。人間が読めるレポートの場合、アナリストは日々のダイジェスト版と詳細なインテリジェンスレポートの両方を提供できます。

EclecticIQプラットフォームでは、レポート内にリンクが埋め込まれているため、意思決定者はプラットフォーム内で直接インテリジェンスのコンテキストにアクセスできます。さらに、EclecticIQプラットフォームは、人間に解読可能なレポートをメールで配布する唯一のTIPであり、このサポートにより、組織の他の人々は重要な脅威インテリジェンスを容易に利用できます。

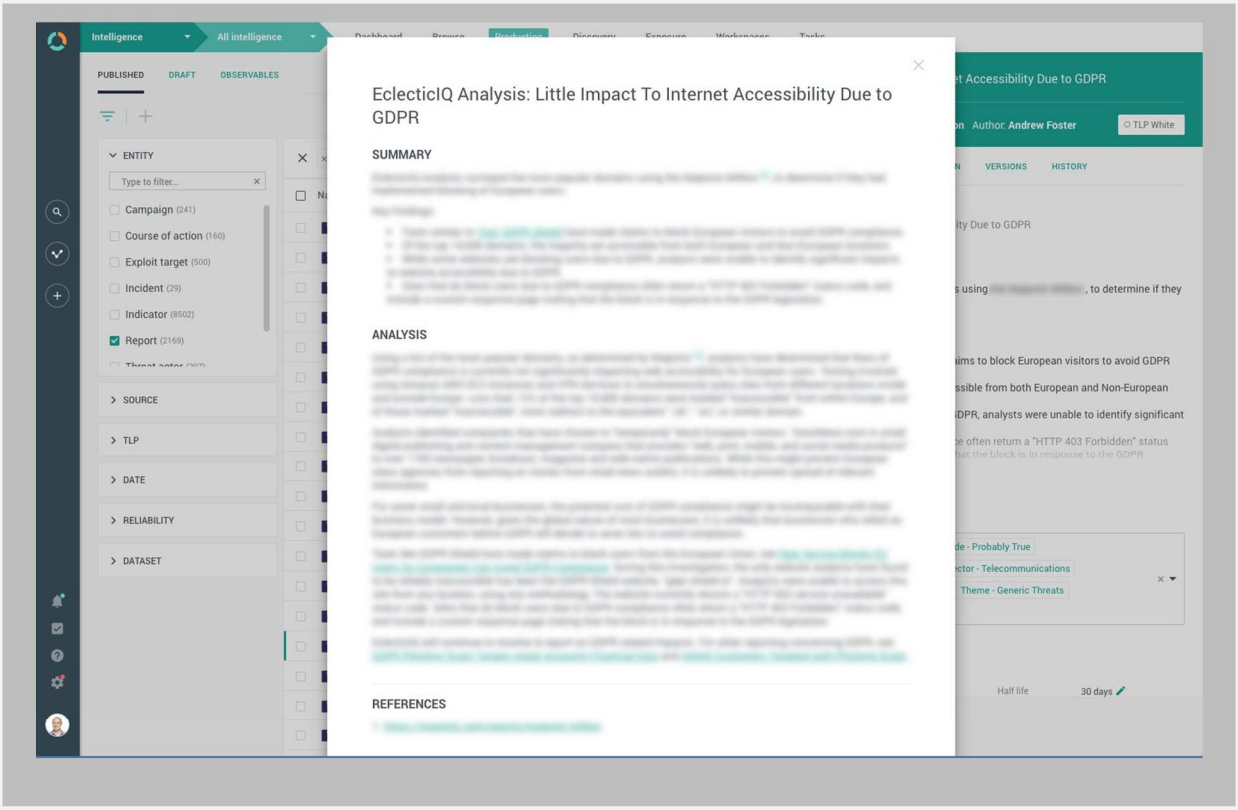

図5：機械と人間の両方の可読要件に対応する、短時間で済むレポート作成

企業の要件に対応

複数の組織からなる行政機関か、成長中の企業かを問わず、EclecticIQプラットフォームでは、仮想マシン上または物理的ハードウェア上で単一インスタンスから多層インスタンスに展開するための柔軟な、複数の方法を利用できます。
本製品は、様々な導入トポロジを選択できる、オンプレミスで提供されています。導入の形式としては、1つのインスタンスから、プラットフォーム間のインテリジェンスのやり取りに応じて各種アクセスレベルがある複数のノードまで対応します。

マネージドソリューションを好む組織の場合は、EclecticIQがプラットフォームをホストするという選択肢があります。

EclecticIQプラットフォームはRHEL、CentOS、およびUbuntuオペレーティングシステムをサポートすることで、既存のITインフラに容易に統合できる柔軟なソリューションをIT管理者に提供しています。

INTELLIGENCE POWERED DEFENSE

www.eclecticiq.com