サイバー防衛支援共同体(CDAC)ケーススタディ：

脅威インテリジェンスの共有

2024年4月

このケーススタディは、CDAC、ThreatQuotient、Cyber Threat Alliance (CTA)、Mandiant（現在はGoogle Cloud傘下）による共同作業であり、本文内で言及しているテクノロジーの運用に基づいたものである。

背景

CRDFグローバル社のイニシアティブであるサイバー防衛支援共同体（CDAC）は、紛争中の同盟国に脅威情報、テクノロジー、訓練、助言、その他のサイバー防衛支援を提供することを目的とした サイバーセキュリティとテクノロジーのボランティア団体で、2022年2月にロシアによるウクライナへの侵攻を受け、ウクライナの公的機関や民間機関にサイバー防衛支援を提供する為に結成されました。ウクライナへの侵攻直後、米国の主要なサイバー専門家達は、ウクライナの重要インフラに対する深刻なサイバーリスクと世界的なサイバー脅威の状況を認識し、ウクライナに運用可能なサイバー防衛支援を提供するために米国の民間企業を集め、組織化するためにCDACを結成しました。

2022年3月にCDACが発足して以来、12社以上の企業がボランティアとして、ウクライナのサイバー防衛当局によるネットワークの安全確保、悪質なサイバー侵入者の追跡と対策、アタックサーフェスの監視の改善、重要インフラを保護するためのサイバー脅威インテリジェンスの提供などを支援してきました。CDACによる支援は、ウクライナがデジタル空間で活動する能力を維持するのに非常に効果的であることが証明されており、この取り組みが世界中の他の重要なパートナー国に支援を提供する可能性を示しています。以前から関係を築いていたサイバー専門家のネットワークよってCDACは結成され、ウクライナを支援するため、ロシアによる侵攻開始から数日以内に、有志を募り支援体制を整えました。

問題点

ロシアによるウクライナ侵攻の初期以降、CDACを通じて米国の信頼できる企業やボランティアからウクライナに対し、リアルタイムの脅威インテリジェンス情報、ソフトウェア、防御技術を提供する精力的な支援を行ってきました。ウクライナへの侵略当初、米国の大企業、非営利団体、政府組織は、ウクライナの窮地に陥った重要インフラや防衛組織に脅威インテリジェンスを提供し始めました。

ウクライナ全土のセキュリティ・オペレーション・センターが米国の協力者より脅威情報を受け取るようになると、情報の重複と量の多さに多方面からの情報のクロスチェックなどの処理が追い付かず、課題を悪化させてしまいました。この問題は、新たなボランティア組織、米国政府、その他の情報源が増えるたびに指数関数的に大きくなりました。CDACは、運営に政府および大規模な民間サイバー防衛チームの脅威インテリジェンス組織との深い経験を持つ人材が携わっていたことから、この問題を早い段階で認識していました。

脅威インテリジェンスは、商業、非営利、オープンソース、政府など、複数のソースから広く収集したものと、ブログ記事や評判の高い情報源など、信頼できるソースから収集された情報で形成される必要があります。そのうえで、重複排除・正規化したうえで、情報が必要とされる関係者の末端までいきわたるよう配信される必要があります。

解決策の模索

2023年1月、CDACはThreatQuotient社と協力し、ウクライナに提供されるすべてのインテリジェンスデータをより有用なものにするという課題に取り掛かりました。

ThreatQuotientは、欧州のThreatQuotientがホスティングするThreatQプラットフォームのSOC2認定インスタンスを寄贈し、さまざまなソースから脅威インテリジェンスを取り込み、ニーズに応じて重要インフラや政府機関にインテリジェンスを配信しました。ThreatQプラットフォームは、脅威インテリジェンスの集中型アグリゲーターおよびディストリビューターとして設定され、基本要件は以下のとおりでした：

- 複数のソースやフォーマットからインテリジェンスを取り込み、重複を排除
- 保存されたダイナミックサーチに基づいて、該当するターゲットに沿った情報を届ける（例として、信頼できる2つのソースからウクライナのエネルギー業界向けに情報が届いた場合、該当するターゲットに情報を届ける）
- 統合によって脅威インテリジェンスの充実を自動化し、その情報を指標とともに配信

他のCDAC参加者もこのプラットフォームに貢献している： Cyber Threat Alliance（CTA）は、ThreatQプラットフォームへのフィードをセットアップするためにThreatQuotientと協力して、APIを通じてCTAデータを取り込むための統合を開発しました。Recorded FutureとMandiant（現在はGoogle Cloudの一部）も、プラットフォームへ情報送信を開始し、ThreatQuotientとCDACはUS CISAと協力して、国土安全保障省（DHS）のAutomated Indicator Sharing（AIS）のフィードも取り込みました。

ウクライナの組織はさまざまな方法で脅威インテリジェンスを取り入れ始めました。政府機関やエネルギーセクターの利用者の一部は、すでにSOCでThreatQを使用していたため、自前のThreatQインスタンスからCDACでホスティングされたインスタンスへ直接接続することができました。

定常アーキテクチャ

上述したように、脅威インテリジェンス共有機能の基本アーキテクチャは、データの取り込み、重複排除、正規化から始まります。 下にあります図 1 は、構造化・非構造化されたさまざまなタイプの脅威データを表しています。データは提供元のタイムスタンプに基づいて重複排除され、受信者が消化しアクションを起こせるように1つのレコードとして表示されます。このアーキテクチャには、ACEと呼ばれるThreatQの自然言語処理（NLP）機能が組み込まれており、レポートを自動的に解析し、利用者に送信される脅威ライブラリにデータを追加します。

一般的に、敵対勢力と地域に基づいてすべての利用者に送信されるデータのベースラインがあります。第二のユニークな情報群は、様々な要件に基づいてその情報が必要となる異なる利用者に送られます： CDACはさまざまな民間および公的機関と協力し、インテリジェンス・スコアリングとTLPコントロールを使用して、どのスマート・

コレクションをどの利用者に送るかを決定します。 利用者はまた、エクスポートのタイミングだけでなく、希望するデータの種類を表明することもできます。また、このアーキテクチャでは、CDAC ThreatQインスタンスの直接の利用者が、別のThreatQプラットフォームやMISPを使用して、配下組織などにインテリジェンスを配布することもできます。

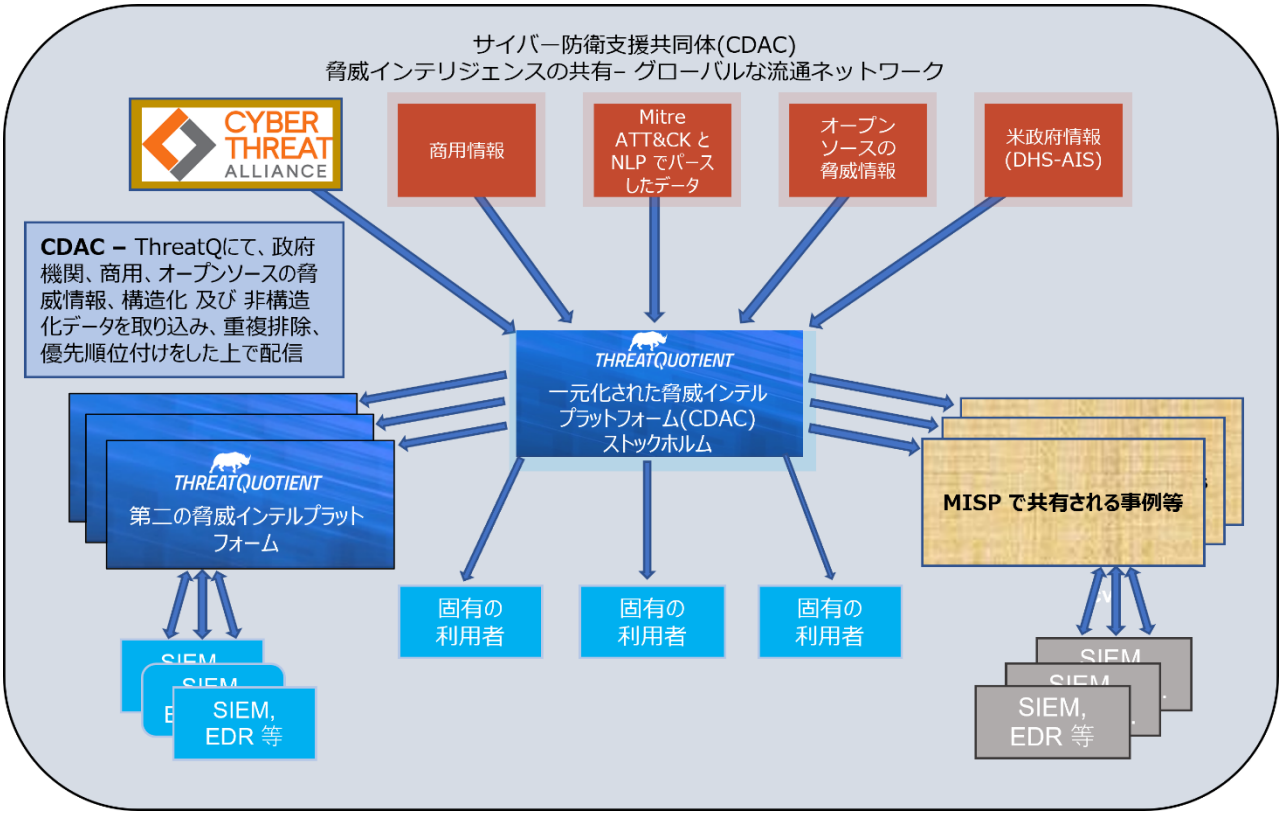

図*1*：脅威インテリジェンス共有アーキテクチャ

このプラットフォームでは、エアギャップ（隔絶された）環境でのデプロイメントも可能で、インターネットに面した1つのプラットフォームが、データダイオードを介して2つ目のプラットフォームにデータを渡すことができます。

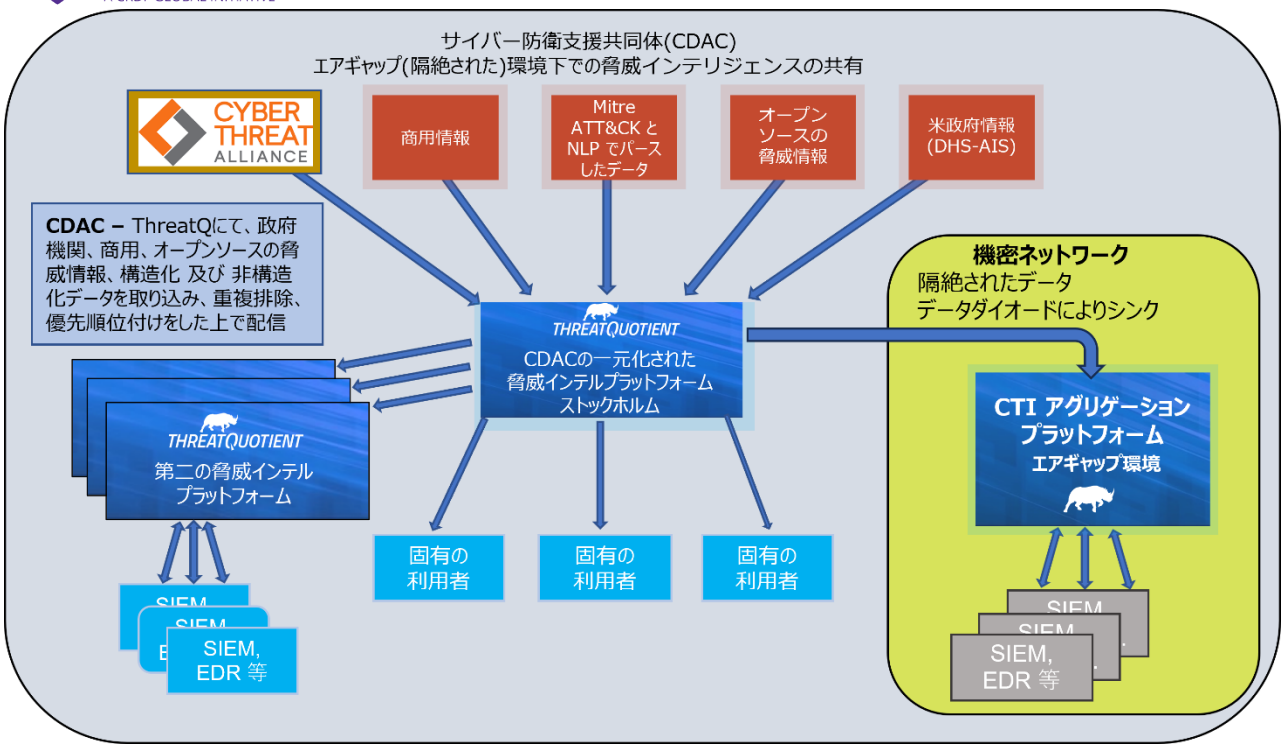

図2：エアギャップ環境下での脅威インテリジェンス共有プラットフォーム

今後について

CDACは、非営利、商業、政府機関の集合体によって構築された、世界中で迅速に展開し利用することができる複製可能なモデルです。CDACで構築したプラットフォームは、現在そして将来のサイバー危機を変える可能性を秘めています。CDACの脅威情報共有の集団的アプローチに用いられた手法は、質の高い情報を活用し統合する官民の協力的パートナーシップによって実現されたものであり、画期的なものであります。情報を受信した組織は、限られたサイバー防御のリソースを、リスクの高い脅威に集中させ、敵対者の攻撃目標に基づき、防御を自動的に割り当てることが可能になります。このアーキテクチャと協力体制は、地理的、政策的、あるいは安全保障上の懸念に応じて、入力と出力のフィードを調整することで、他の状況にも対応できる既製の構造を提供することができます。また、このアーキテクチャには拡張性があり、状況が必要とする他のソースからのフィードを必要に応じて追加することができます。

※本資料はCDACのウェブサイトに2024年4月1日に掲載された「Case Study: Threat Intelligence Sharing」を翻訳したものとなります：https://crdfglobal-cdac.org/case-study-threat-intelligence-sharing/