CYFIRMA
DECODING THREATS

国際的金融グループ、CYFIRMAが提供する脅威ディスカバリー＆サイバーインテリジェンスプラットフォームによりM&A取引関連の損失を事前に回避

企業
グローバル金融サービス企業グループ

業種
銀行、金融サービス

本部
アジア

ソリューション
DeCYFIR –Threat Visibility & Cyber Intelligenceモジュール

お客様のチャレンジ

- M&Aに対する現状調査により企業スパイ行為が判明
- 不法行為による損失を軽減する必要

お客様のベネフィット

12倍
スレットハンティングのスピード

16倍
対応策の実行スピード

4億米ドル
コストを抑制

M＆A失敗、株価暴落の回避成功

企業概要

国際的金融グループ（以下"同社"と表記）はアジア有数のバンキングサービス企業の一社です。その資本金は2021年時点で約104億米ドルに上り、大規模な金融コングロマリットの中枢企業の一社です。事業の一環としてビジネス優位性の実現に向け戦略的にM＆Aを展開しています。

お客様のチャレンジ

M＆Aは企業の戦略的価値の創出に大きな役割を果たしますが、巨大資本が関与することでサイバー攻撃者や国家支援型脅威アクターなどに市場誘導の恰好のターゲットとして狙われる可能性があります。

企業スパイ行為に従事するハッカーは、交渉中の競合他社の動きを弱めるために秘密裡かつ慎重に選別した対象として、攻撃の標的を定めます。ダークウェブ上でM＆Aに関する非公開データを売買、もしくは搾取的投機などにより不当に利益を得ようする脅威アクターらによって、M＆A取引自体も標的とされることがあります。

同社は事業ポートフォリオ拡充に向け買収検討中のアフリカの石炭事業会社を評価している最中でした。正確な状況理解に向けて

"デジタルリスク検出機能は攻撃対象領域の迅速な検知に大きな役割を果たしました。対処すべきセキュリティギャップを認識できました"

同金融グループ,SOCチームリーダー

“DeCYFIRのおかげで企業スパイにより発生した被害を最小限に抑え、その手順を明確かつ迅速に行うことができました。結果、企業ブランドに多大な損失を与え株価暴落を発生させる恐れのあるM＆Aの失敗を無事に回避できました。また許容範囲を超える買収取引を白紙にし4億USドルの資金を節約しました”

同グループ会社,情報セキュリティ責任者

M＆Aプロセスを考慮にいれデューデリジェンスチームとの協業を狙いとし同社はCYFIRMAを採用しました。

CYFIRMAをどのように活用したか

同社は買収検討中の石炭事業会社のセキュリティ態勢とリスクプロファイルを分析し、M＆Aプロセスの早期段階でサイバーセキュリティ脅威を判別、全プロセス上のリスク低減を図りたいという狙いを持っていました。

DeCYFIR™が誇る予見的脅威インテリジェンスにより企業スパイ活動を即座に検知しました。

こうして同社は世界初の予見的サイバーインテリジェンスプラットフォーム”DeCYFIR™”の採用を決め短時間で導入を実行しました。運用開始後、DeCYFIR™は同社の入札詳細情報のSNSへの漏洩を即座に検知しました。

リーク情報には同社による石炭事業会社の評価情報ならびに買収提示価格、株価、入札、従業員の残留や新組織図、統合計画といった詳細情報までもが含まれていました。

DeCYFIR™の高度な予見的インテリジェンスエンジンにより、仮想ドローンをディープウェブ、ダークウェブ上のフォーラムや地下マーケットに設置して継続監視し、同様に石炭事業会社取得に名乗りを挙げた他社四社の入札情報をも明らかにしました。

驚くべきことにM&Aの仲介ブローカーがこれら四社の入札者に対し全て同一であったこともDeCYFIR™により明らかになりました。

重要な点は、DeCYFIR™は瞬時にデータ漏洩のフラグを立て損害や被害を最小限化するための対応策を迅速に実行します。

DeCYFIR™によって、買収競合他社四社が石炭事業会社に持つ関心事項を明らかにしM＆Aブローカーにそれらを関連づける ことで、同社は脅威アクターがさらに敏感に反応するであろう動機事項についてもより詳しく理解することができました。

DeCYFIRは攻撃対象領域と攻撃ベクトルを迅速に明らかにしました。

独自の知見に基づき、お客様はDeCYFIRのデジタルリスク検知機能を速やかに活用し、同社のデジタルフットプリントと攻撃対象領域を特定することに成功しました。これは同社セキュリティチームが正確に対策を実行するための必須事項でした。

またリスクの軽減に向け、侵害や攻撃の再発を防止することができます。同社の企業ブランド、評判、財務状況への潜在的な被害の抑制に貢献しました。

DeCYFIRはSNS上で漏洩、発見された高機密性のその他のM＆A情報を速やかに検知しました。買収競合企業がM＆A交渉で不利益を被るよう機密情報取得を目的として雇用された複数サイバーハッカーグループにより取得されたであろう電子メールアカウントを検出しました。

これらの攻撃者達は企業上層部を標的としたフィッシングメールを送信していました。電子メールは個別の標的に合わせ巧妙にカスタマイズされており、M＆Aに関連する"おとり"を巧みに利用して被害者を誘導、添付ファイルを展開させたり、高性能なデータ漏洩マルウェアを埋め込んだリンクをクリックさせたりしました。

またVBAマクロも実行され重要人物のユーザー名やパスワードを盗み出していました。これら資格情報を取得後、M＆A関連の取引がどのように展開、進捗しているかについて取得済電子メールを通じ リアルタイムに情報閲覧ができた可能性がありました。

DeCYFIRはさらに侵害を受けたドメイン、サブドメイン、IPアドレスなどの各種デジタル資産を公開しました。こうした資産情報は、ハッカーフォーラム、ダークウェブ、複数ビンサイト上で検知され、悪意のある攻撃者が同社の防御をかいくぐり機密データを盗み出した事実を示していました。

重要な点：顕在化したデジタルリスクを発見するまでのスピードが、ブランド、レピュテーション、財務へのダメージの大きさを左右します。

DeCYFIRによって攻撃対象領域の全貌を迅速に検知し同社セキュリティオペレーションセンター（SOC）チームが、システム強化を実行することで当該対象領域を迅速に減少させることができました。このような対策には盗用電子メールアカウントの回復や不要なサービス、ユーザーアカウント、ポートの無効化といった対応が含まれています。

DeCYFIRはなりすましや侵害の試みを検知しました。

DeCYFIRは、同社の経営陣を装った虚偽のものも含めフィッシング上で従業員を誘導、悪意ある電子メールをクリックさせるため使用された関連虚偽電子メールIDを公開しました。

さらにDeCYFIRは同社になりすましてユーザーから個人情報を盗み出そうとした複数オンライン事業者によるブランド侵害の試みを発見しました。

重要点：DeCYFIRがなりすましや侵害に関する背景、詳細、影響度を提供し、同社SOCチームがこうしたリスクを即座に対応、改善策を実行することでエクスポージャーの追加拡大を防ぐことができました。同様にこうした領域の防御態勢を強化し以後同社ネットワークにAPTグループーが侵入することを防ぐことがきました。

DeCYFIRが提供するリスクレーティングと推奨対策に基づき、サイバーセキュリティのリソースに優先付けを実行できます。

データ漏えいの検知時点から同社は被害の抑制に向けサイバーセキュリティの関連リソースを早急かつ同期的に最適化させる必要性を認識しました。

リスクレーティングと推奨対策で分類したDeCYFIRのアラート機能により効果的な修復オプションとエクスポージャーの重大性を瞬時に両方示すことで、経営陣とSOCチームがトリアージに向けリスクに応じたアプローチを実行するのに大きく役立ちました。

重要点：脅威が常に進化する状況下では貴重なサイバーセキュリティのリソースを適切な箇所に配置することこそ影響の抑制に非常に重要です。

DeCYFIRのアラートとダッシュボード上でリスクとハッカビリティススコアと推奨対策を確認し、同社チームはセキュリティトリアージの"場所"と"方法"を正確に把握することができました。

DeCYFIRのトレンドインディケーターにより同社経営陣がリスクとエクスポージャーを可視化することができました。

DeCYFIRにより攻撃対象領域、なりすましと侵害、データ侵害モニタリング、SNSや公開インターネットにおけるエクスポージャー、ダークウェブ上のエクスポージャー、脆弱性エクスポージャーの六つの主要ドメインにおける傾向分析を確認、同社のシニア経営陣が現行リスクを監視、先手を打つことができました。

重要点：同社の経営陣は侵害行為を懸念しており、攻撃者により社内の他領域への攻撃経緯を確認したいと希望していました。DeCYFIRのトレンドインディケーターにより新出リスクへのエクスポージャーならびに現行セキュリティ防御の進捗状況を単一ダッシュボード上で容易に追跡することができました。

CYFIRMAは石炭事業会社の買収における同社の方針再評価を支援し、結果として4億米ドルに上る資金の節約、M＆A失敗の回避に貢献しました。

競合入札者の四社全てではないにせよ、その一部が入札情報にアクセスし優位的な情報の取得方法を理解していた事実に基づき、またデータ漏洩の発生を受けて同社は石炭事業会社の買収決定を再検討することにしました。

DeCYFIR搭載の予見的インテリジェンスプラットフォームの独自のインサイトは、石炭事業会社のセキュリティ態勢が同社基準に準拠していない可能性やM＆A成立後に同社ネットワーク環境を危険にさらす可能性をも示唆しました。

最終的に同社は石炭事業会社の買収中止を決定、4億米ドルに及ぶ買収提示資金を節約する結果となりました。同社はこうして企業評価や株価の急落をもたらす恐れのあるM＆A被害を回避することができました。

重要点：万が一同社が買収を進めていたとしたら石炭事業会社取得について過重な支払いをする結果を生んでいた恐れがあります。

アナリストに買収が過大評価に基づき計画されていることが判明すれば、同社株価は大きく下落、企業ブランドは大幅な損失を被る状況が想定され、企業ブランドのロイヤルティや収益の大幅な減少へとつながる恐れもありました。

DeCYFIR™で脅威に先手を投じる

現在、同社ではDeCYFIR™を日々活用し脅威を予測して潜在的な攻撃に対応しています。

複合的なサイバーインテリジェンスにより組織内の利害関係者各自が必要なインサイトを取得できます。

組織内の各レイヤー（具体的に戦略部門、経営部門、運用部門など）に合わせそれぞれカスタマイズされたDeCYFIR™の複合的なインテリジェンスにより、同社の各組織レベル関係者はリスクのエクスポージャーと攻撃対象領域に関して各自適切な判断を下すことができました。

戦略部門：潜在的な脅威アクターに関し、"どの攻撃者が"、"どういった動機で"、"何を攻撃してくるのか"といった疑問を解明し、経営陣が脅威インテリジェンスに基づき戦略、ガバナンスならびに方針を随時更新できる状態にある必要があります。

経営部門：CISOやCIOといった同社責任者がプロセスや手順を改善するにあたり必須となる、"どの資産を"、"いつ"、"どのように攻撃しようとしているのか"についてのインサイトを提供します。

運用部門：セキュリティコントロールやデバイス更新に必要な重要情報をSoCチームに提供、"どのように攻撃しようとしているのか"そして"何に対して攻撃しようとしているのか"についてのインサイトを提供します。

コンテキストに基づくインサイトは、進行中のサイバー攻撃に対し無二の知見を提供します。

DeCYFIR™に搭載されているリスクドシエ機能によって悪意あるスレットアクター、彼らのキャンペーンならびに攻撃手法をあぶり出し、同社は直面するサイバー攻撃を阻止するための新たな方針や制御の更新に必要となる貴重なインサイトを獲得しました。これには現在計画中の攻撃のみならず進行中の攻撃も含んでいます。

アウトサイドイン（ハッカー視点）の予見的スレットインテリジェンスにより、既知未知を問わず脅威に先手を打ちます。

既知および未知の脅威主体とベクターの双方について、アウトサイドインの視点で脅威を事前に特定することで、金融グループが魅力的なターゲットである理由と、悪用される可能性のある脆弱性についての洞察が得られました。

同社がサイバー攻撃を予測、全セキュリティ態勢を強化するのに大きく役立ちました。

緊急的な対応を要するサイバー攻撃に対して正確なアラートを提供することにより適応的なサイバーセキュリティを実現することが可能となります。

DeCYFIR™は同社SOCチームに優先度と関連性に基づく戦術的な改善策も提供しています。これらは金融サービス業、同業界の活用テクノロジーや地理条件に的を絞った脆弱性、脅威存在痕跡（IoC）に対して効果的に作用することが可能です。

こうして同社SOCチームはシステムにパッチ対応を実行しつづけ早急な改善措置が必要な弱点を修正することができました。以後のサイバー攻撃を阻止できるよう、同社がセキュリティ防御を継続的に進化させることができた点は注目に値します。

CYFIRMA について

DeCYFIRは脅威ディスカバリー＆サイバーインテリジェンスプラットフォーム企業ですサイバーインテリジェンスを攻撃対象領域ディスカバリーおよびデジタルリスク保護と組み合わせることにより、予見的でパーソナライズされた、また必要なコンテキストを含む、アウトサイドインおよびマルチレイヤーのインサイトを提供します。CYFIRMAはクラウドベースのAIとMLを活用した脅威インテリジェンス分析プラットフォームを提供し、組織がサイバー攻撃の計画段階で潜在的な脅威をプロアクティブに特定できるように支援しています。ハッカーの視点と外部の脅威情勢に対する深い洞察を提供するという独自のアプローチによりお客様が迫りくるサイバー攻撃に適切に備えることをサポートしています。

CYFIRMAは数多くのFortune 500企業と連携しており、米国、日本、シンガポール、インドにオフィスを構えています。

CYFIRMAの詳細についてはhttps://www.cyfirma.jp/ を御覧ください。

CYFIRMA

DECODING THREATS