VECTRA
SECURITY THAT THINKS.®

ケーススタディ

DZ BANK、AI を活用したサイバー攻撃の検知でプライバシーを侵害せずにセキュリティ保護を実現

「ファイアウォールや侵入検知防御システムなどの従来のシステムでは、標的型諜報攻撃やネットワーク内の異常な振る舞いをカバーしきれません」そう語るのは、ドイツで900カ所以上の協同組合銀行の中央機関として機能するDZ BANKのITセキュリティ担当シニアサービスマネージャー、Matthias Tauber氏です。

「シグネチャーベースのシステムでは、見落とした脅威は発見できず、既知の脅威しか検知できません。そこで我々は、新しい技術への移行を検討していました」同氏とそのチームは、隠れたサイバー攻撃を検知し、脅威をより早く阻止するために、AIを活用した新しいネットワークトラフィック分析に注目していました。

セキュリティとプライバシーの両立

2017年時点で5,060億ユーロの資産を持つDZ BANKは、ドイツにおいて資産規模で第2位の銀行です。

協同組合銀行は、ドイツの多くの中小企業にサービスを提供。DZ BANKは、中央信用機関として、これら協同組合銀行のビジネスを強化し、資本市場へのアクセスを提供しています。同行は、個人、法人、機関投資家向けの銀行サービスを提供しており、ヨーロッパ、アジア、米国で30,000人の従業員を擁しています。

「シグネチャーベースのシステムでは、見落とした脅威は発見できず、既知の脅威しか検知できません」

Matthias Tauber氏
DZ BANK、ITセキュリティ担当シニアサービスマネージャー

DZ BANK

組織

DZ BANK

業種

金融サービス

課題

- 従来のシグネチャベースのファイアウォール、IDS、IPSでは見落とされていたような高度な脅威を検知する
- 異常だが問題ではない振る舞いと攻撃者による高リスクな振る舞いを区別する

選定基準

脅威の検知にかかる時間を短縮、アラートを自動的に優先順位付け、インシデント対応を迅速化する、使いやすいネットワークトラフィック解析プラットフォームであること

結果

- 厳しいデータプライバシー法を遵守しながら、データセンターやユーザーおよびIoTデバイスに潜む攻撃者を検知することが可能になった
- 内部脅威やIT管理者によるポリシー違反のリスクを軽減
- AIによる脅威検知と迅速なインシデント対応により、セキュリティオペレーションの作業負荷を軽減

「Cognitoを使うことで、最もリスクの高い脅威に集中できます。他のソリューションでは、何百から何千規模の偽陽性を取り除くためにフィルターが必要です」

銀行の資産、業務、および機密情報を保護するというTauber氏が担当する業務は、データプライバシーと金融に関する幅広い規制によって大変複雑になっています。ドイツでは、従業員および通信に対して、偵察したり電子的に監視したりすることがほぼ禁止されています。

「Betriebsrat」と呼ばれる、地域や企業レベルで労働者を代表するドイツの経営協議会も、DZ BANKのサイバーセキュリティとデータ保護に影響を与える存在です。加えて、EU一般データ保護規則（GDPR）とドイツの金融商品市場指令（MiFID II）が2018年に法制化されました。

セキュリティの穴を特定

サイバーセキュリティを継続的に強化するための取り組みの一環として、Tauber氏のチームは、NISTサイバーセキュリティフレームワークに対して金融機関のセキュリティ体制基準を制定しました。「その結果、標的型諜報攻撃とネットワークの異常を検知する能力に問題があることがわかりました」と同氏は言います。

この穴を埋めるために、DZ BANKはVectra® AIのAI駆動型のサイバー攻撃の検知と脅威ハンティングプラットフォームであるCognito®を採用しました。Cognitoは、データセンターのワークロードやユーザーおよびIoTデバイスに潜む脅威を、リアルタイムに検知し、アラートを自動的に優先順位付けするので、迅速に対応することができるようになりました。

人の持つ専門知識に加え、データサイエンス、機械学習、振る舞い分析を融合したCognitoは、手動では時間のかかる脅威ハンティングと対応を、自動化します。それによって、数日から数週間かかる脅威ハンティングを数分に短縮し、セキュリティ運用の作業負荷を36分の1に軽減できます。

脅威をより早く発見

Cognitoの常時学習型の振る舞い監視モデルは、攻撃者をリアルタイムで検知し、迅速で断固とした対応と論理的な調査開始点を設定します。

「Cognitoを使うことで、最もリスクの高い脅威に集中できます。他のソリューションでは、何百から何千規模の偽陽性を取り除くためにフィルターが必要です」とTauber氏は言います。

Cognitoでは、直感的なVectra Threat Certainty Index™に表示される、脅威と確実性のスコアからアラートを自動的に優先順位付けします。その結果、DZ BANKは、攻撃指標を持つどのホストデバイスが最大のリスクをもたらすのか、自信を持って即座に知ることができます。

Cognitoは、ペイロードや通信内容ではなく、豊富なネットワークメタデータ、関連するログ、クラウドイベントを分析するため、厳格なプライバシー法を遵守しながらも、高度な脅威をリアルタイムで自動的に検知できます。

協調した取り組み

「Cognitoはスキルの差を解消するのに役立ちます。Cognitoは使いやすく、分かりやすいので、セキュリティ運用チームが従うべきランブックを簡単に書くことができます」とTauber氏は語ります。

フロントラインのオペレーションは、マネージドセキュリティサービスプロバイダーが担当しています。Tier 1とTier 2のベンダーがCognitoを使用してサイバー攻撃を検知し、最もリスクの高い脅威をDZ BANKのセキュリティチームにエスカレーション、そしてDZ BANKのセキュリティチームもCognitoを使用して詳細な調査を行います。

「Cognitoでは、グレーゾーンでの振る舞いを確認することができ、疑わしい振る舞いがあれば、クライアントPCに何が起こっているかを確認することもできます」

内部不正のリスクを低減

DZ BANK が Cognitoを選択した目的は、高度な脅威を検知し、グローバルネットワーク上から検知した攻撃者の振る舞いが問題あるものか否かを見分けるためでした。しかし、導入してからすぐに、内部からの脅威リスクを低減するための不可欠なツールとなりました。

IT管理者のアカウントは、攻撃者にとって特に把握したい情報です。同行ではセキュリティ対策の一環として、IT管理者は、特別に保護された指定のクライアントPCからのみ業務を行うこととしています。しかし、急いでいたり、うっかり忘れてしまうなど、この予防措置を怠ってしまうことがあります。

「すべての管理者は特定の管理用クライアントPCを使用するというガイドラインを設けています。管理者がこのガイドを遵守しているのか、Cognitoを使うことで確認できます」

例えば、Cognitoがリモートでのコマンド&コントロールの動作を検知した場合、それは誰が不正使用をしているという指標となります。規定以外のクライアントPCから作業している、もしくはアカウントが侵害されている可能性もあります。

Cognitoを使うことで、セキュリティ運営チームは、リスクの高い脅威であるかどうかを迅速に判断できます。また、内部の問題であれば、IT管理者がポリシーガイドラインになぜ従わなかったかを突き止めることが可能です。

自動化を実現する

Tauber氏とそのチームは、AI駆動型であるCognitoの活用を進めています。そして、リアルタイムでの脅威の検知を自動化し、インシデント対応を迅速化するとともに、社内外のセキュリティ運営にかかる作業負荷を軽減しています。

Cognitoは、DZ BANKの連携されたセキュリティエコシステムの一部でもあります。Cognitoのイベントは、同行のSplunkセキュリティ情報およびイベント管理（SIEM）システムにも公開されています。そして現在、Cognitoプラットフォームの機能を拡張して、より迅速で決定的なインシデント調査を行うことや、攻撃をさかのぼって調査することを検討しています。

詳細については、info-japan@vectra.aiまでお問い合わせください。