CASE STUDY : CRIMINAL IP THREAT INTELLIGENCE

デジタルアイデンティティサービスにおける不審アクセス分析と脅威インテリジェンス

ユースケース
脅威調査およびリスク検証

業界
デジタルアイデンティティおよび
トラストサービス

地域
インドネシア

ソリューション
Criminal IP Threat Intelligence

主なポイント
・インフラベースの脅威検証
・デジタルサービス向けの外部脅威コンテキスト
・不審なIPアドレスおよびドメインの調査

概要

インドネシアのデジタルアイデンティティおよびトラストサービス企業は、自社のデジタルサービスに関連する不審な外部インフラを調査するために、**Criminal IP Threat Intelligence(TI)**を活用しています。

本人確認、認証、デジタル取引サービスを運用する環境では、個別のログインやアクセスイベントだけで脅威の有無を判断することは困難です。モニタリングの過程で未知のIPアドレスやドメインが確認された場合、分析担当者には、その活動の背後にあるインフラを把握し、追加確認が必要かどうかを判断するための外部コンテキストが必要になります。

Criminal IPは、外部脅威およびインフラインテリジェンスを提供することで、
不審な指標に対する調査を支援し、より正確なリスクベースのセキュリティ判断を可能にします。

導入前の課題

Criminal IP TI の導入以前は、デジタルサービスの活動に関連する
不審なインフラを評価する際に、より豊富な外部コンテキストが必要でした。

1 不審なIPに関する情報の制限

IPアドレスだけでは、その活動の背後にあるインフラ、サービス、脅威特性を十分に把握することが困難でした。

2 インフラリスク判断の難しさ

不審なアクセスは、ホスティング事業者、VPN、プロキシ、スキャナーなど、さまざまなインフラから発生する可能性があるため、正確な判断には追加のコンテキストが必要でした。

3 外部情報の検証にかかる時間

未知のインフラのリスクや特性を把握するために、複数の外部情報ソースを個別に確認しなければならないケースが多くありました。

4 個別活動を超えた可視性の不足

1つのアクセスイベントや指標だけでは、不審活動に関連する周辺インフラを十分に把握することが困難でした。

導入方法

Criminal IP TI は、既存のセキュリティおよびアイデンティティ保護プロセスに、
外部インフラの観点から得られる脅威情報を追加します。

不審な活動が確認された場合、分析担当者は個別のイベントだけに依存するのではなく、ネットワーク特性、露出サービス、ホスティング 環境、既知の脅威シグナルなど、その活動の背後にあるインフラをあわせて確認できます。

このような追加コンテキストにより、セキュリティチームは該当する活動が一般的なインフラ、匿名化サービス、または潜在的に悪性のシステムに関連しているかどうかを、より正確に判断できます。

Criminal IP を活用した調査プロセス

Identify | 識別
不審活動に関連するIPアドレス
またはドメインを確認します。

Assess | 評価
リスクレベル、ホスティング情報、サービス、インフラ特性を確認します。

Investigate | 詳細調査
追加分析が必要な場合は、VPN、プロキシ、スキャナー、マルウェア、C2活動などの脅威指標を確認します。

運用連携

不審なログインのコンテキスト確認
不審なアクセス活動が検出された場合、
分析担当者は Criminal IPを活用して、
アクセス元IPの外部インフラを
確認し、関連するリスク要素や匿名化サービスに関する シグナルを分析します。

ドメインおよびインフラの検証
調査過程で不審なドメインや関連インフラが確認された場合、ホスティング、証明書、ネットワーク、脅威情報をあわせて 確認し、当該インフラとの関連性をより正確に判断します。

高リスクインフラの確認
ホスティングサービス、VPN、プロキシ、スキャナー、または既知の悪性活動に関連するIPアドレスを、追加の脅威コンテキストとあわせて確認し、追加調査が必要なインフラを識別します。

導入効果

Criminal IP TIを活用することで、該当企業はデジタルセキュリティ運用に
関連する不審な外部インフラを、より効果的に評価できるようになりました。

不審アクセスに関する豊富なコンテキスト
個別のアクセスイベントだけでなく、不審なアクセスの背後にあるインフラまで把握できます。

リスクの高いインフラの識別能力向上
ホスティング、VPN、プロキシ、スキャナー、悪性活動に関する追加インテリジェンスを活用し、より詳細な確認が必要なインフラを識別できます。

一貫した脅威検証
さまざまなインフラ情報と脅威シグナルをあわせて確認することで、不審活動をより一貫した基準で評価できます。

調査効率の向上
IPアドレス、ドメイン、ネットワーク、脅威情報を1つの環境で確認できるため、外部コンテキストの収集に必要な作業を削減できます。

デジタルトラスト運用の支援
外部脅威インテリジェンスにより、信頼性の高いデジタルアイデンティティおよび取引サービスを保護するための
セキュリティ運用に、追加のコンテキストを提供します。

WHY CRIMINAL IP?

デジタルアイデンティティサービス環境では、正常な活動と不審なインフラを区別するために、個別のアクセスイベントを超えた追加コンテキストが必要でした。

Criminal IP TIは、IPアドレスおよびドメインのリスク情報に加え、ネットワーク、サービス、ホスティング情報、脅威指標を提供し、セキュリティチームが不審活動の背後にあるインフラをより正確に把握できるよう支援します。

また、広範なインターネット可視性とOSINTベースのインテリジェンスにより、デジタルサービスを保護するセキュリティチームの迅速な脅威検証と、詳細なインフラ分析を支援します。

Criminal IP で脅威コンテキストを活用し、より信頼性の高いデジタルサービス運用へ。

デモを申し込む