KELA
チートシート

サイバー攻撃から組織を守る 7つのポイント

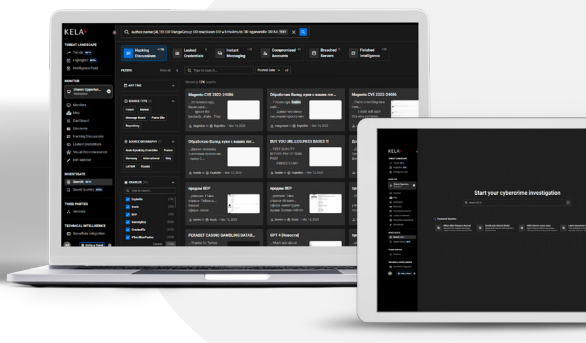
EMPOWERED BY KELA

監視・分析・学習・行動
サイバーセキュリティの未来は不透明です。しかしその一方で、「組織が今後直面しうる様々な課題に対処するためには、常に進化するサイバー脅威情勢にあわせた対応が重要となる」ことは明白です。その最善策として、組織のサイバー脅威インテリジェンスにプロアクティブなアプローチを導入することが挙げられます。このチートシートでは、脅威に対して真にレジリエントな組織へ変化するために必要な7つのポイントをご紹介します。

組織の目となり耳となる

× 01 アンダーグラウンドに広がるサイバー犯罪社会の仕組みを理解する

サイバー犯罪者は、潜在的な標的に関する情報共有や攻撃ツールの開発、戦略の策定など様々な場面で協力体制をとり、違法マーケットプレイスで窃取データを売買しています。そのような**アンダーグラウンドに広がるサイバー犯罪社会の仕組み**を理解することで、攻撃が発生する前にその予兆を読み取って事前に阻止することが可能となり、今後起こりうる攻撃から自社を保護できる可能性を高めることができます。



◈ 02 サイバー犯罪ソースを監視して自社のエクスポージャーをチェックする

セキュリティ業務にプロアクティブなアプローチを採用して監視活動を行い、組織の資産が秘密裏に窃取されたり、公開されていないかチェックしましょう。また、セキュリティチームのサイバー犯罪調査スキル育成を目的としたトレーニングへの投資も重要です。彼らが組織のネットワークに影響を及ぼすことなく調査を遂行できるよう、隔離したネットワークと専用のワークステーションも準備しましょう。

03 敵を知る

自社を狙いそうな攻撃者の思考や習性を学び、理解します。彼らの行動パターンや好みの攻撃手法、興味を持っている分野、その他可能であれば個人的な情報も分析しましょう。敵を理解することで彼らの次の手を読み、組織を守るために適切な行動を起こすことが可能となります。

↻ 04 過去のインシデントから学ぶ

過去に発生した攻撃がどのように行われたのかを理解することで、自社に対する侵害で悪用されうる脆弱性の種類を知ることができます。また攻撃のプロセスについて理解を深める中で、サイバー犯罪者が使用する様々なマルウエアやハッキングツールについても学ぶことができるでしょう。例えば、他社で発生したインシデントの原因が、適切にセキュリティ保護されていないAPIにあったとします。その場合、攻撃で悪用された脆弱性についてできる限り多くの情報を入手し、自社が使用しているAPIに類似の脆弱性がないかをチェックして、対策につなげることが可能となります。
また被害を受けた組織の多くは、セキュリティ企業が将来のインシデントを阻止できるよう、攻撃の詳細を公開することに前向きです。インシデント情報の共有を支援するコミュニティを構築することも、組織がともに脅威を打破し、攻撃を阻止するために有用です。

05 アタックサーフェスを縮小する

アタックサーフェスを縮小する基本的な方法には、技術的な取り組みと組織的な取り組みの2つがあります。技術的な取り組みとしては、ファイヤーウォールの適切な設定、アクセス権限の最小化、アプリケーションのホワイトリスト作成、組織的な取り組みとしては、職務分掌による過度なアクセス権限の集中防止、従業員のセキュリティ研修、詳細かつ正確な脅威インテリジェンスデータを活用したセキュリティ計画の策定などが挙げられます。アタックサーフェスを縮小するには技術的・組織的取り組みの両方を実行することが理想的ですが、現状として大半の組織はいずれか一方に重点を置いており、また技術的な取り組みを重視している傾向にあります。しかし組織的な対策を適切に導入するほうが難しいとはいえ、この傾向は改善する必要があります。組織の中にいる人々と彼らの持つ知識が、組織のセキュリティ体制において本質的な差を生み出すのです。

06 最新のテクノロジーで組織を保護する

優れた脅威インテリジェンスプロバイダーを活用することは、サイバー犯罪との闘いにおいて貴重な財産となります。選ぶべきプロバイダーの条件として、組織が被害を受けることのないよう最新のツールとテクノロジーを提供してくれること、またさらに重要な点として、信頼できる実用的な知見をタイムリーに提供してくれることが挙げられます。

⊕ 07 目標を定め、サイバー脅威インテリジェンスを今年の重要事項に設定する

アンダーグラウンドのサイバー犯罪社会は進化と拡大を続けており、脅威アクターは攻撃に悪用できる脆弱性を常に探しています。組織が彼らのサイバー攻撃を未然に阻止するための秘訣は、**プロアクティブ**であることです。具体的には、サイバー犯罪脅威インテリジェンスを組織の重点事項としてとらえ、目標を設定し、継続的な学習や従業員のトレーニングを実施することが挙げられます。また適切なツールを活用し、自社のデータと資産を侵害や窃取、その他様々な不正行為から保護することもその一環といえるでしょう。

もっと詳しく学ぶには?

KELAのサイバーインテリジェンス調査の最新情報はこちらからご覧いただけます。

KELAサイバー脅威インテリジェンスプラットフォームの無料トライアルをぜひご利用ください。