The Defender's Advantage

エグゼクティブサマリー

Mandiant

Google Cloud Security

昨今のデジタル時代においては、どの組織もサイバー脅威の影響を免れることはできません。セキュリティ侵害によるデータの盗難、経済的損失、社会的信用の失墜といった潜在的な影響は、強力なサイバー防御の重要性を浮き彫りにしています。このガイドでは、予防的かつインテリジェンス主導のサイバー防御プログラムを実現するための主要な戦略について説明します。

サイバー防御について

サイバー防御とは、受け身の保護対策にとどまることなく、積極的に抵抗し、侵害の影響を軽減することです。効果的なサイバー防御には、インテリジェンス、検出、対応、検証、追跡、管制の 6 つの重要な機能における協調的な取り組みが必要です。各機能は組織のデジタル アセットの保護のために、それぞれ異なるものの相互に関連した役割を担います。

インテリジェンス: 指針の提供

脅威インテリジェンスは強力なサイバー防御プログラムの基盤です。脅威アクターとその戦術、手法、手順（TTP）に関する情報の収集、分析、伝達を行います。攻撃者の行動を理解することで、組織は予防的に防御戦略を実行でき、情報に基づいたリスク管理の意思決定をすることができます。

計画、指示、収集、分析、作成、伝達、フィードバックから成る脅威インテリジェンスのライフサイクルにより、インテリジェンスの運用に構造化されたアプローチが適用されます。組織内のさまざまな関係者に合わせた主なインテリジェンス サービスが、セキュリティ関連の各役割に貴重な分析情報を提供します。

悪意のあるアクティビティの検出と調査

悪意のあるアクティビティの効果的な検出は TTP の把握と、それに合わせた検出メカニズムの調整にかかっています。分析と適応の継続的サイクルである検出エンジニアリングが、TTP に基づくロギング、信頼性の高いアラートの追求、継続的な最適化を行います。検出のスケーリング、アラート疲れの軽減、対応時間の短縮には自動化が重要な役割を果たします。

明確に定義された検出ツール導入戦略を立て、人材育成に重点を置くことで、効果的に脅威を特定し対応するために必要な適切なツールと専門知識を確保できます。

セキュリティ侵害への対応

インシデント対応は、サイバー防御の重要な要素です。初期トリアージのプロセスには、セキュリティ侵害の範囲と性質を把握するための迅速な評価とデータの収集が含まれます。判断ポイントと後続の手順で対応プロセスを導き、ハンドブックで効果的な修復のための構造化された手順を提供します。

調査ライフサイクルの主要な活動と循環的な性質が、綿密な分析と証拠収集を可能にします。調査加速ツールやマイクロサービスなどの最新の機能強化により、対応プロセスが効率化されます。

封じ込めと駆除の目的は、侵害の速度を抑え、不正な内容を削除することです。セキュリティの強化と各インシデントから得られた教訓が、継続的な改善に役立ちます。テストと対応計画の検証により、将来のインシデントに対する準備体制が整います。

セキュリティ対策とオペレーションのターゲットを絞ったテストと検証

攻撃対象領域を予防的に管理し、セキュリティ検証の構成要素を包括的に理解することがは、復元力の高い防御体制にとって不可欠です。インテリジェンス主導の検証は、最も関連性の高い脅威に絞ってセキュリティ対策とオペレーションの効果を評価することに重点を置いています。検出エンジニアリングのライフサイクルを継続的に検証して強化し、効果的な脆弱性管理を行うことで、強力なセキュリティ ポスチャーを確立することができます。

アクティブな脅威ハンティング

脅威ハンティングでは、既存の検出メカニズムを回避した可能性がある隠れた脅威をプロアクティブに探索します。インテリジェンスの分析情報と脅威モデリングに裏付けられ、適切に構造化された脅威ハンティング プログラムにより、未知であった脅威の特定が可能になります。脅威ハンティングのパイプラインが、仮説の作成から追跡の実行、検出のユースケースの作成まで、ハンティングのプロセスを推進します。

管制センターによるサイバー防御の連携

管制センターはサイバー防御の中枢神経系であり、組織全体の整合性、復元力、権限移譲、説明責任を推進します。効果的なリソース管理、スタッフ配置、プロセスと手順の作成が、強力なセキュリティ ポスチャーに寄与します。指標とトレンドにより、サイバー防御プログラムの効果についての分析情報が得られます。

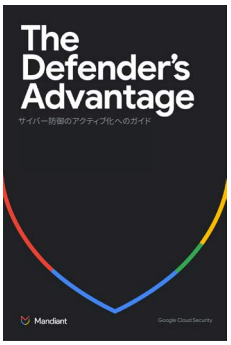
重大インシデント発生時は、優れたリーダーシップと効果的なクライシス コミュニケーションが特に重要になります。準備を整え連携することで、迅速で効果的な対応が可能になり、セキュリティ侵害の影響を最小限に抑えることができます。

サイバー防御のアクティブ化

サイバー防御のアクティブ化を成功させるには、ステークホルダーの賛同、人員配置の慎重な検討、そして自動化やマネージド サービスなど、取り組みを加速させるための推進力が必要です。柔軟な利用モデルが、組織固有のニーズに対応するカスタマイズされたソリューションを提供します。

まとめ

The Defender's Advantage（防御側の優位性）では、サイバー防御への予防的かつインテリジェンス主導のアプローチが強調されています。脅威状況の把握、攻撃者の TTP に対する防御の適応、セキュリティ対策とオペレーションの継続的な評価と改善により、組織はデジタル アセットを効果的に保護し、進化するサイバー脅威に直面してもオペレーショナル レジリエンスを維持することができるのです。



The Defender's Advantage（防御側の優位性）について詳しくは、以下をご覧ください。
https://cloud.google.com/security/resources/defenders-advantage