Japan Nexus Intelligence Inc.

INTERCEPT
Cyber intelligence

危機的状況における オンラインレピュテーションの追跡と保護

“ネガティブなナラティブ”を用いた攻撃と
敵対的影響力工作への対策

敵対的影響力工作とは?

政府・企業・いかなる個人も、選挙への影響、社会的不安の煽動、社会的評価の損害、復讐などを目的とした敵対的影響力工作の影響を受ける可能性があります。

**当社は、これらの脅威を確実に特定し、
迅速かつ効果的に対処し、発生した影響を最小限に抑える
プロフェッショナルな対応力を備えています。**

現代社会における課題

現代社会では、敵対的影響力工作が企業や政府機関にとって重大な脅威となり、選挙や公共のナラティブ操作、企業の評判やM&A、重要な顧客関係にまで悪影響を及ぼす可能性があります。

このような課題に対応するため、企業の評判を守ることを目的に、IRチームとPR活動を連携させ、最先端の防御サービスを提供します。これにより、ブランドを保護し、進化する脅威に対する回復力を維持します。

選ばれる理由

当社は、サイバー空間における脅威者の特定・分析やリスク軽減、敵対的影響力工作への対応に関する豊富な経験を有しています。

当社のソリューションは、インターネット上における虚偽情報や根拠のない非難、過剰請求や顧客情報の不正利用、社員への不適切対応、環境問題に関する誤解など、さまざまなリスクへの対応が可能となっています。さらに、経営者に対する虚偽のスキャンダルの生成・拡散や、影響力の拡大を狙ったサイバー攻撃にも対処可能です。

基本方針

独自の方針に基づき、調査および対応チームがお客様の特定のニーズとリスクに合わせて対応を行います。攻撃者が使用する戦術・技術・手順(TTPs)の詳細な特定と分析を経て、各脅威に対処するための包括的かつ統合的な戦略を提供し、脅威の無力化とレピュテーションの回復プロセスを実行します。

政府機関をはじめ、主要金融機関、上場企業、先進的なテクノロジー企業など、多様な組織への導入実績を有しています。

サイバー攻撃と同様に、敵対的影響力工作に対しても事前の備えが求められます。

概要と特長

Japan Nexus Intelligence及びそのパートナーである9500 Groupは、独自のアプローチと最先端テクノロジーを融合させ、敵対的影響力工作に対する効果的な防御策を提供しています。

潜在的な影響力工作を早期に察知し、事前に対策を講じるとともに、発生時には迅速な対応で被害の拡大を防ぎます。

脅威の全体像を把握し、攻撃者の特定、抑止策の立案、影響力工作の排除、そして被害からの回復支援まで、実効性の高いインテリジェンスを一括でご提供します。

ソリューション概要

- 常時監視と初動対応の強化
- 敵対的影響力工作の要素分析
- 攻撃者の戦術・技術・手法（TTPs）の解析
- 攻撃排除を支援する実行可能なインテリジェンス
- PRチームと連携したレピュテーションの回復支援

独自ソリューション

- 最新技術の活用
- 攻撃者視点に立った分析
- サイバー空間における影響力工作の検出
- 敵対的影響力工作に対する積極的な抵抗
- 独自メソッドに基づいた分析アプローチ

INTERCEPT
Cyber intelligence

+81-3-5579-2597

info@j-ni.com

j-ni.com