ソリューション概要

「コンテキスチャル」警告メールバナー

ジャストインタイムで、メール受信時にメール攻撃の可能性があることを的確に知らせる

どんなに優れたメールセキュリティソリューションを実装したとしても、テクノロジーには限界があります。「人」を狙う攻撃は、最終的には「人」による防御が不可欠です。フィッシング攻撃に立ち向かうための最終防衛ラインは、エンドユーザー一人ひとりなのです。ジャストインタイムの的確な警告バナーを不審なメールに表示することで注意を喚起することは、巧妙化し続ける悪意のある攻撃からあなたの会社や組織を守るためには不可欠になっているのです。

この課題を解決するIRONSCALESの「コンテキスチャル」警告バナーは、次のコンテンツの内容に対して警告を発します。

- これまでメールを受信したことがない始めての送信元
- ビジネスメール詐欺（BEC）防御で使われる文言
- 送信元アドレス偽装
- 正確な送信者名を使うなりすまし
- 正確な送信者名を使うなりすまし
- 本物そっくりなメールドメイン
- 表示名に企業名の表示
- 表示名に既知アドレスの表示

このような状況を打破するためには、最新の脅威インテリジェンスとユーザー行動分析に基づいて、的確にエンドユーザーに潜在的な攻撃を警告するソリューションが今必要とされています。

課題

高度なフィッシング攻撃は常に進化しており、マシンラーニング/AIを搭載した先進のメールセキュリティソリューションでさえ、すべてを検知することはできません。これまでのメールテクノロジーでは、社外から送信されるすべてのメールに手当たり次第に「迷惑メール」バナーを入れることが一般的です。この結果、エンドユーザーはこのようなバナー警告を無視してしまうことという危険な行動に引き起こしてしまいます。このような状況を打破するためには、最新の脅威インテリジェンスとユーザー行動分析に基づいて、的確にエンドユーザーに潜在的な攻撃を警告するソリューションが今必要とされています。

ソリューション

IRONSCALESでは、マシンラーニング（ML）モデルによってメールの内容を自動解析しています。その結果、疑わしいと判断されたメールに自動的にコンテキスチャル警告バナーを表示します。

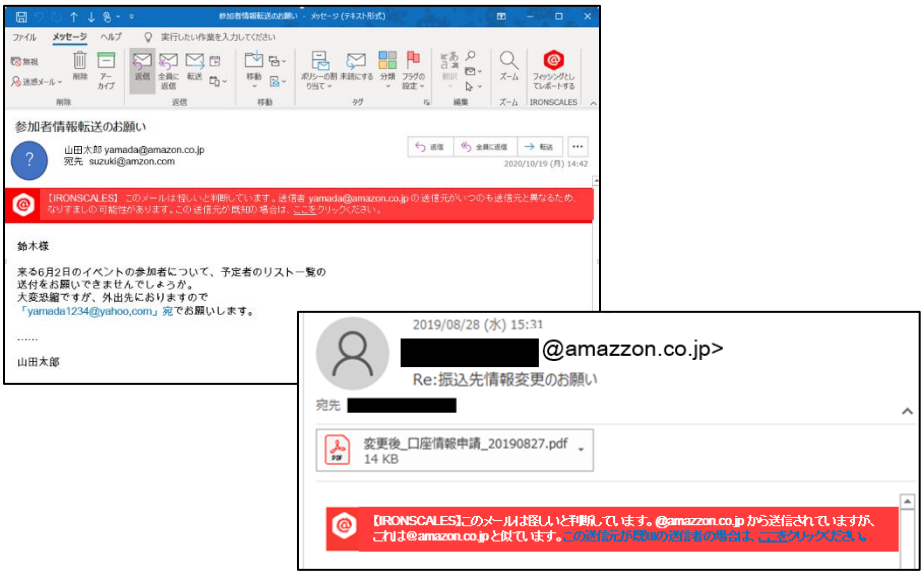
各バナーには、IRONSCALESのMLモデルがなぜ不審メールと判断したのか、具体的な理由が記載されています。

警告バナーは、会社ロゴ、緊急サポート先、担当窓口など、自由にカスタマイズできます。

導入時に行われる90日間のメールボックスのスキャン分析は 各エンドユーザーが定期的にやり取りしている外部送信者をベースラインデータとして特定します。これによって、繰り返しメールをやり取りしている外部送信元を判定します。

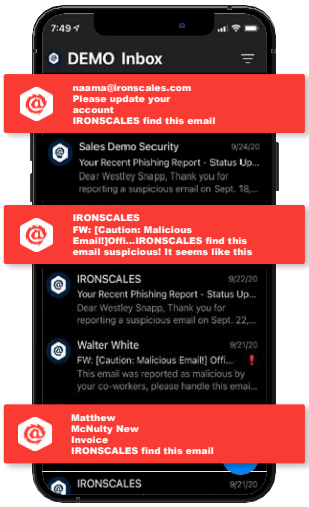
警告バナーは、どのデバイスでも、どのメールクライアントでも、判定結果をシームレスに表示します。

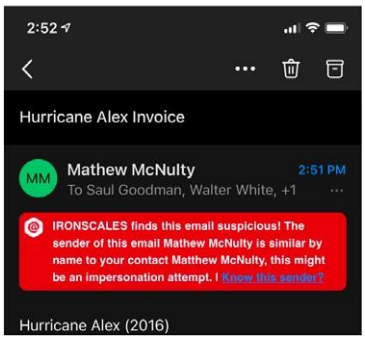
デスクトップパソコンの表示例



> 警告バナー表示と直感的な自己管理は素晴らしい。これは、IRONSCALESが弊社を水際で防衛してくれている証しです。そして、もう1つ大切なことは、弊社のメールセキュリティシステムが安全であることを簡単に示すことができることです。IRONSCALESが提供する視覚的なツールは、取締役会への現状報告には必須です。
>
> OrthoCarolina社テクノロジーサービス統括バイスプレジデントNeil Stein氏

スマートフォンの表示例





なぜIRONSCALESなのか？

1. まず、第一に、IRONSCALESが選択されるのは、導入の早さと運用の容易さです。そして、BECやアカウント乗っ取りなどの高度な攻撃など、あらゆる種類のメール脅威を阻止する能力において、他に類を見ないサービスを提供していることです。
2. IRONSCALESは、メールボックスレベルで、攻撃のターゲットとなる可能性が最も高い部署から導入といったスモールスタートが可能。
3. IRONSCALESが「メールセキュリティ」と「ユーザーアウェアネス」を組み合わせた包括的なメールセキュリティプラットフォームであることも、IRONSCALESが選択される理由の1つです。

IRONSCALESをさらに知りたい方は、
www.ironscales.jp をアクセスしてください。

あらゆるタイプのフィッシング攻撃の予見、検知・防御から隔離・削除までの迅速かつシンプルなソリューションを今すぐ手に入れることができます。

IRONSCALES
SAFER TOGETHER

販売代理店