フィッシングの報告メールからノイズを除去する.

COFENSE TRIAGE™

お客様が抱えている問題.

本物のフィッシングメールを見つけるためのノイズカットに時間がかかりすぎる. 担当アナリストが報告された大量のスパムメールを抱えてしまうと、御社は貴重な時間を失い、脅威は拡散を始めて、やがて脅威はネットワークに数日、数週間、さらには数か月も留まることになる可能性もあります。アナリストに、誤検知を迅速に特定して、「最初にどこに焦点を当てるべきか」という重大な質問に答える権限を与えます。

Cofense のソリューション.

Cofense Triage では、フィッシングの脅威に より速く優先順位を付けて修復できます。従業員が報告する文化はフィッシング攻撃を阻止するための鍵ですが、仕事をうんと抱えたSOCチームは報告内容に優先順位を付ける必要があります。時間を食う手動プロセス（脅威の実際の指標を見つけて理解するために必要な多数の手順）によって作業を遅らせてしまうのではなく、Cofense Triage を使用して分析を自動化し、意思決定に焦点を当てて問題の修復を迅速化します。

Cofense Triage を使用すれば、ユーザーから報告されたメールの分析を高速化し、本物のフィッシングメールをすばやく見つけて、より効果的に対応することができます.

レスポンスを改善する.

従業員から不審なメールを報告された場合、フィッシングの脅威に関連する指標を検索する必要があります。Cofense Triage の継続的に更新される数千のルールのライブラリは、アナリストに攻撃者の戦術に関する指標と洞察を迅速に提供し、リスクの高いメッセージを分離してレスポンスタイムを大幅に改善します。

脅威を見つける.

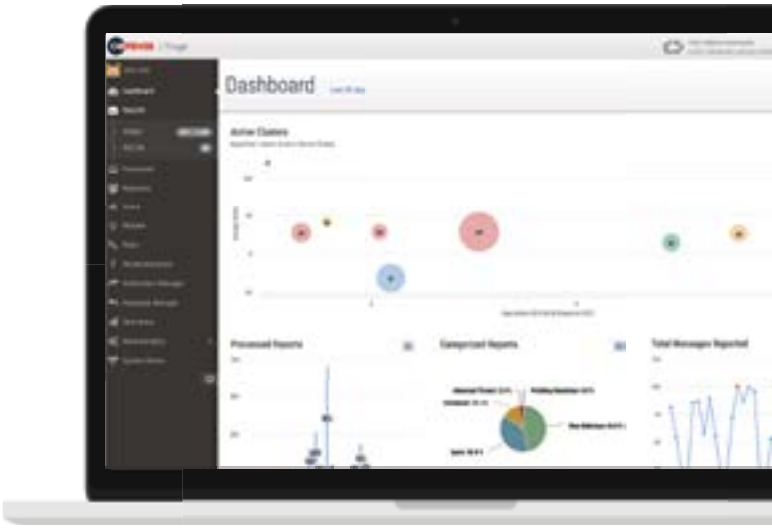
Cofense Triage は、報告されたメールを集めてペイロードに基づいてクラスターにし、キャンペーンの識別を支援します。業界トップのスパムエンジンがメールを分類して、誤検知と既知の不正なメールを識別します。Cofense Intelligence 専有のルールは、既知の脅威を識別し、貴重なアナリストコンテキストを提供しま

防御を強化する.

Cofense Reporter™ を使用する信頼できる従業員はフィッシング脅威インテリジェンスの貴重な情報源となり、本物の脅威を表面化します。メッセージに悪意のあるコンテンツが含まれているかどうかを報告者に知らせて、フィッシング防御を強化する SOC チームとのパートナーシップを構築します。

COFENSE TRIAGE の仕組み.

Cofense Triage は、脅威の識別と調査を自動化することによって、インシデントの対応者がすべてのアラートに迅速に対応できるようにします。SOC チームは、結果の解釈とフィッシングの脅威への効果的な対応に集中できます。



開始.

組織の規模に関係なく、つぎの導入オプションがあります: 御社のチームが完全に管理する仮想アプライアンスとしてオンプレミス版。Cofense セキュアクラウドインフラストラクチャでホストされるクラウド専用インスタンス。または、Cofense Phishing Defense Center™ によってホストされ、完全に管理されるマネージドサービス。

データを SIEM へエクスポートする.

Cofense Triage は、報告データを LogRhythm などの SIEM ソリューションにエクスポートして、分析の追加レイヤーを提供し、組織が既に使用している他の資産を活用できます。また、Cofense Triage を使用すると、syslog や API を介してアラートとイベントをインシデント管理システム、チケットシステム、またはその他のログシステムにインポートして、アラートとイベントを監視、管理し、応答することができます。

VIRUSTOTAL 付きで出荷.

Cofense Triage には VirusTotal のプライベートサブスクリプションが付属しており、脅威分析をサポートしています。または、御社独自の VirusTotal API キーを使用できます。Cofense Triage は、分析のためにファイルハッシュまたは URL を VirusTotal に自動送信して、AV エンジンおよび ウェブサイトスキャナーを使用した、悪意のあるコンテンツの検出を可能にします。

COFENSE VISION™との統合.

従業員が報告したメールは、豊かな情報源です。しかし、フィッシングメールを報告しないユーザーはどうでしょうか？Cofense Vision は、かれらを識別し、脅威を迅速に封じ込めるのに役立ちます。Cofense Vision が Cofense Triage と連携して設定されている場合、適切な権限を持つスーパーユーザーとオペレーターは、報告されたメール中のドメインと添付ファイルを検索し、従業員が報告し損なったメッセージを、すべての受信トレイから、Triage から直接、1回クリックするだけで隔離することができます。

ウェブサイト: cofense.com/contact **電話:** 703.652.0717
住所: 1602 Village Market Blvd, SE #400
Leesburg, VA 20175