elastic security labs

2024年版

Elasticグローバル脅威レポート

脅威動向SOCリーダーが知っておくべきこと

2024年版Elasticグローバル脅威レポートは、セキュリティチームやCISOの皆様に実用的な洞察を提供するために作成されました。本レポートは、パブリックテレメトリとElastic固有のテレメトリの両方を利用して、10億を超えるデータポイントを数か月にわたって分析した結果から得られた主要な発見事項を明らかにしています。これらの要点は、データからのインサイトと組織向けの推奨アクションにまとめられています。

トップインサイト

01 企業によるクラウド環境の誤った構成

クラウドセキュリティポスチャ管理（CSPM）に関する新しいセクションでは、環境をCIS（Center for Internet Security）のベンチマークと比較したところ、クラウドサービスプロバイダー（CSP）に関係なく、平均して環境の約50%がチェックに失敗していることがわかりました。

02 防御回避は依然として最も頻繁に見られるエンドポイント戦術

防御回避はエンドポイントの行動の38%を占めており、攻撃者はセキュリティシステムの操作に慣れていることがわかります。特に、この数字は昨年から6%減少しています。これは、ディフェンダーツールが効果的に機能していることを浮き彫りにしています。

03 資格情報アクセスアラートは、特にクラウド内で増加し続けています。

クラウド環境内では、資格情報アクセスがアクティビティの23%を占めました。さらに、エンドポイント環境では、これらの手法が前年比で3%増加していることが明らかになりました。これらは、情報窃盗犯やクレデンシャルブローカーの蔓延や、セキュリティツールの認知度が高まっていることが原因と考えられます。

04 敵はディフェンダーツールを悪用して効率的にシステムに侵入しています。

観測された悪意のあるファイルの53%は、企業が弱点を発見するために活用し、敵対者がその弱点を悪用する、攻撃的なセキュリティツール（OST）であることが確認されました。これらのOSTは、プロセスインジェクション（今年のWindowsアラートイベントの53%を占めた防御回避の一形態）のような新しい機能を作成するための大規模なR&Dチームを持っています。

05 生成AIによる攻撃の量や影響の増加は観察されず

セキュリティチームは、今後GenAI攻撃が急増することを懸念しています。脅威の量はわずかに増加しましたが、GenAIはアラートの要約やタスクの自動化などの機能によって防御側のテクノロジーを大幅に強化しました。

 |

主な提案

01 環境を頻繁に監査する

攻撃者は、環境に侵入する際、許容範囲が広い、または誤って設定されたセキュリティ制御に頼っています。いったん侵入すると、センサーやデータを改ざんすることに集中します。ベンチマークとリスク評価は、企業内のアクセスを効果的に管理するためにベストプラクティスや業界標準を利用しているかどうかを特定するのに役立ちます。

02 セキュリティ制御を調整することで、生成AIに備えることができます。

GenAIの増加は、ソーシャルエンジニアリングの企ての増加につながります。これらの企てなどを識別できるようにユーザーベースをトレーニングすることは常に良い考えですが、セキュリティチームは、フィッシングの企てが成功しても長期にわたる被害を引き起こさないように、制御と権限を確認する必要もあります。

03 防御回避攻撃を無効化するためのインタラクティブなエンドポイントエージェントを実装する

防御回避攻撃はここ数年間、主な戦術となっています。減少傾向にあるとはいえ、攻撃者は依然としてこれらの方法を利用して環境に侵入し、操作しています。Elastic Agentなどのエンドポイントテクノロジーは、必要なツールの数を減らしながら可視性と機能を提供します。

04 漏洩した資格情報に対する堅牢な対応計画を作成する

ブルートフォースや不審なメモリからのブラウザ認証情報へのアクセスなどの手法が定期的に使用されているのを観察しました。漏洩した資格情報をローテーションし、侵害対応のための迅速なワークフローを編成することは大きな違いを生みます。セキュリティチームは、まだ多要素認証を義務付けていない場合は、義務付ける必要があります。

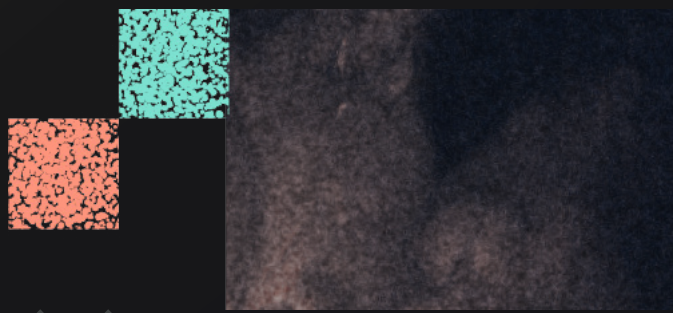
05 クラウド環境とCISベンチマークの比較

CISベンチマークは業界標準であり、注意が必要な領域を迅速に特定するのに役立ちます。チームはスコアを監視して向上させる計画を立てる必要があります。これにより、長期的には脅威の検出が向上し、リスクが軽減されます。

脅威の展望を知る

こうした脅威の進化に備えましょう。Elasticの提案をすべて把握し、2024年版Elasticグローバル脅威レポートで今日の脅威の詳細な状況を確認してください。また、Elasticの専門家を @ElasticSecLabs でフォローすることもできます。

Elastic Security がセキュリティ運用を最新化する方法をご覧ください。



elastic security labs