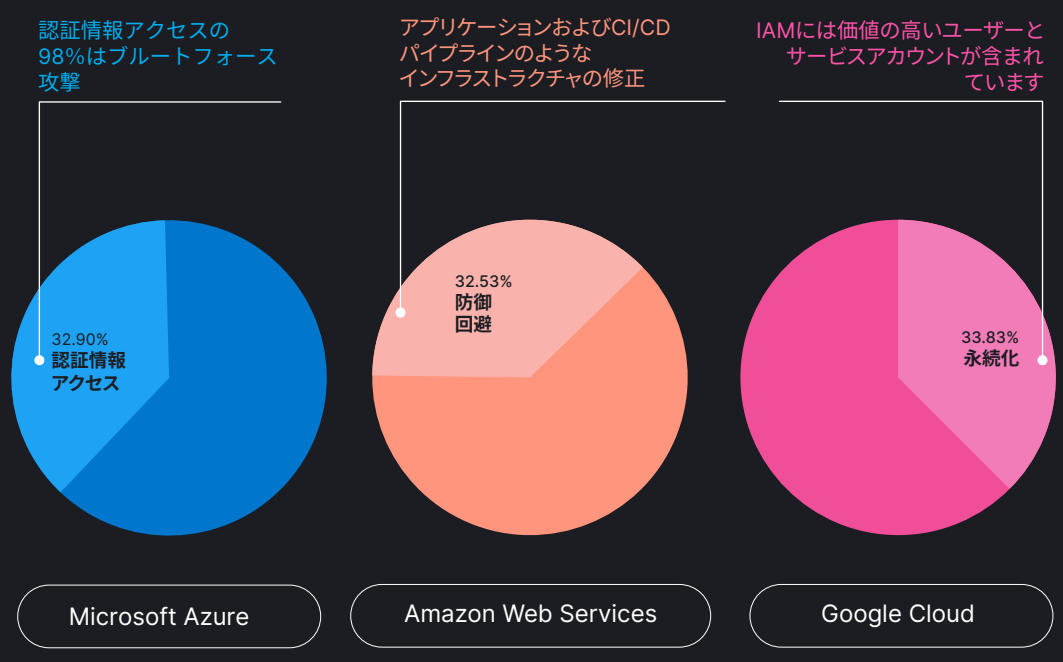
elastic security labs

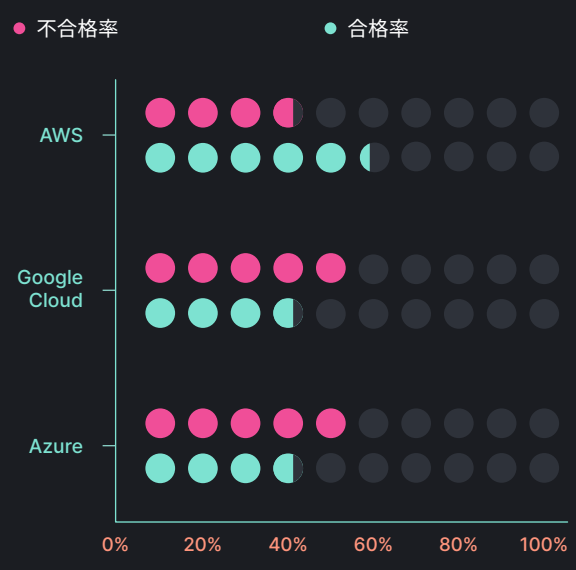
2024年版Elasticグローバル脅威レポートに見る攻撃者の手法

認証情報アクセス、防御回避、クラウド環境の永続化を確認しています。



クラウド環境はCISベンチマークで保護できます

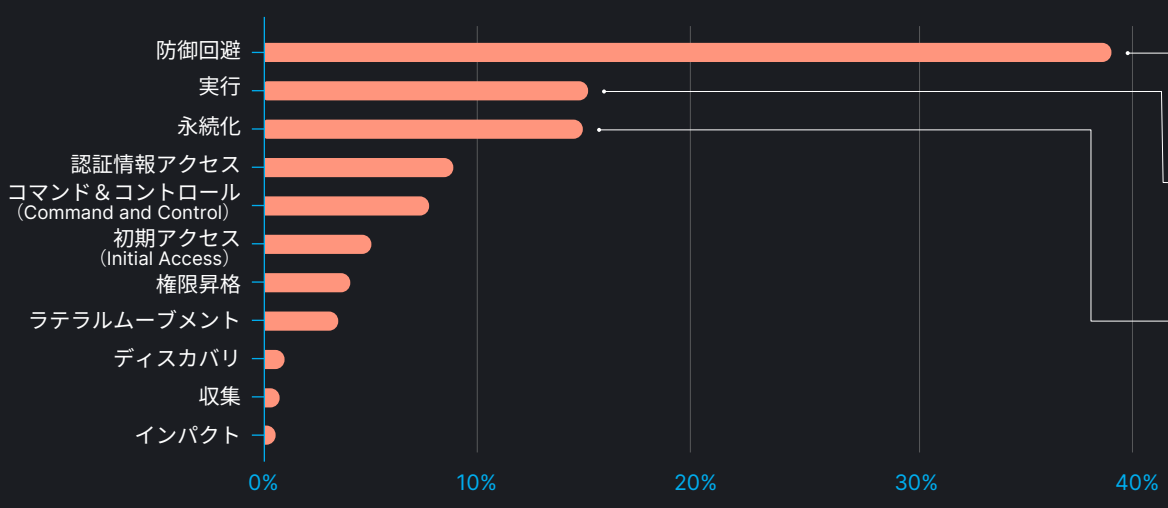
Elastic Security Labsは、すべての主要なCSPでチェックに失敗したことを確認しました。クラウド環境で構成ミスがないかをご確認ください。



昨年から何が変わったか

- 認証情報アクセス技術が**3%増加**、特にセキュリティ保護されていない認証情報は**31%増加**
- 防御回避技術が**6%減少**
- 永続化技術は**8%増加**

エンドポイント内の攻撃は以下のとおりです。



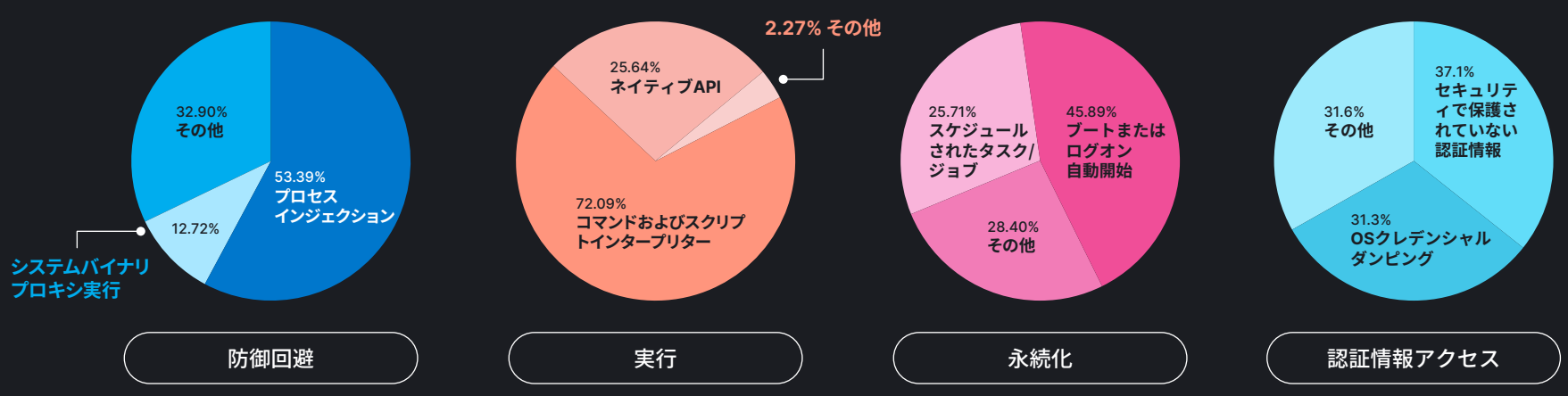
攻撃者は脆弱性を悪用しコードを注入して実行します

攻撃者の目的は1つではありません。当社はデータ収集、難読化、DLLローディングを観測しています

攻撃者は自動的に発生する効率的なアクションを求めています

約70%の観測された行動は、防御回避、実行、永続化です

Windowsエンドポイントで観測された手法 (OSテレメトリの92.7%)



2025

年が近づいています。以下を行うことを検討してください。

- CISベンチマークのスコアを計算して向上させる方法を計画します
- X で @ElasticSecLabs をフォローしてください
- 全文をダウンロード Elasticグローバル脅威レポート
- Elastic Security Labsの検出エンジニアリング動作成熟度モデルで保護ライブラリを監査しましょう。

次のアドレス指定に重点を置きます。

- 防御回避
- 実行
- 永続化
- 認証情報アクセス