Zscaler Breach Predictor

現在の攻撃を特定し将来の攻撃を予測する
予防型の検知と対応ソリューション

© 2024 Zscaler, Inc. All rights reserved.

ソリューションの概要

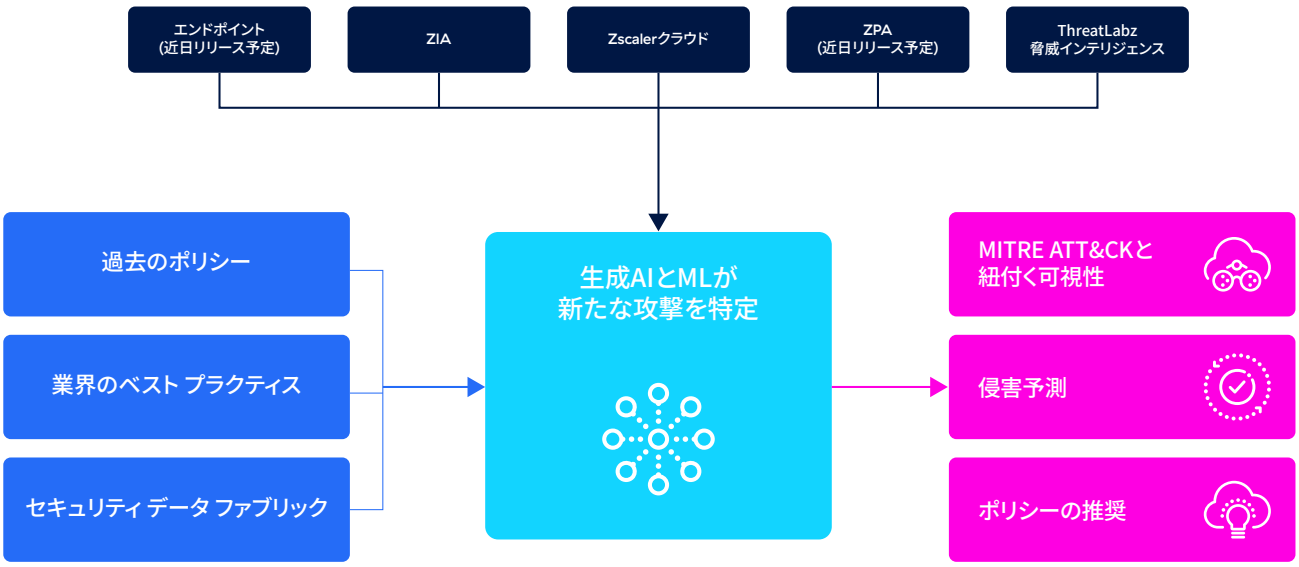
組織はランサムウェアやマルウェアなどの脅威に絶えず悩まされている一方、こうした脅威の存在によって EDR、XDR、SOAR といったツールの進歩が促され、多くの場合、対応の自動化を改善することにつながっています。しかし、攻撃の発生ペースは依然として憂慮すべきものです。攻撃者は生成 AI を武器に、脆弱性の悪用、攻撃対象領域の探索、防御を突破するためのユーザー行動の操作を、よりすばやく効率的に行えるようになっています。

攻撃は絶え間なく発生しており、このような脅威の増大によって、SIEM を中心としたトリアージの課題はその深刻さを増しています。誤検知や担当部門の業務過多につながることは言うまでもありません。そこで今、組織にとって非常に重要なのが、より予防に重きを置いたセキュリティの検討です。

Zscaler Breach Predictor は、進行中の攻撃を特定して今後の潜在的な攻撃を予測する、初の予防型の検知と対応 (PreDR) ソリューションです。MITRE ATT&CK の戦術、技術、手順 (TTP) にマッピングされた攻撃者のアクティビティーを可視化し、影響を受けるユーザーに関するリアルタイムのインサイトを提供することで、進行中の攻撃を把握して阻止します。高度な AI/ML を活用することで、セキュリティ侵害を予測して、脆弱性の悪用が起こる前に予防的にセキュリティを強化し、最終的にセキュリティ運用を簡素化できるよう組織を支援します。

Breach Predictor のメリット

- **脅威に関する可視性の向上：**攻撃経路を可視化し、MITRE TTP にマッピングされた攻撃者のアクティビティーに関するリアルタイムのインサイトを取得します。
- **侵害の予測と防止：**AI を活用した侵害確率スコアリングとポリシーの推奨を活用することで、悪用される可能性の高い攻撃経路を予防的に排除し、組織の全体的なリスクを低減します。
- **SOC の効率向上：**セキュリティ イベントの総数を減らしながら、攻撃の調査能力を強化することで、SOC のワークフローの負担を軽減します。



© 2024 Zscaler, Inc. All rights reserved.

Zscaler Breach Predictor の特長

1 日あたり 500 兆のシグナルに基づく AI を活用
Zscaler では、世界最大のセキュリティ クラウドとセキュリティ データ ファブリックを運用しており、Zscaler の AI/ML エンジンは、Zero Trust Exchange を流れる 1 日あたり 500 兆を超えるシグネチャーから得られる脅威インテリジェンスとインサイトによってトレーニングされています。

Breach Predictor は、AI/ML モデルを活用して、さまざまなソースから取得したデータを分析します。このソースには、過去のポリシー、ベスト プラクティス、セキュリティ データ ファブリックのコンテキスト、IoC と脅威インテリジェンス、ZIA、ZPA、Cloud Sandbox、エンドポイントで収集したデータなどが含まれます。こうしたデータを総合的に分析することで、侵害確率をモデル化し、起こり得る攻撃に対する予防型のポリシーを提案します。

結果として、悪用される可能性の高い攻撃経路を排除して攻撃者に先手を取り、侵害リスクを徐々に減らすことができます。

予防型セキュリティ

AI を活用した侵害確率スコアリング：侵害確率スコアを利用することで、侵害を受ける可能性を評価し、プロアクティブなリスク軽減を実現するとともに、SOC の対応の負担を軽減できます。

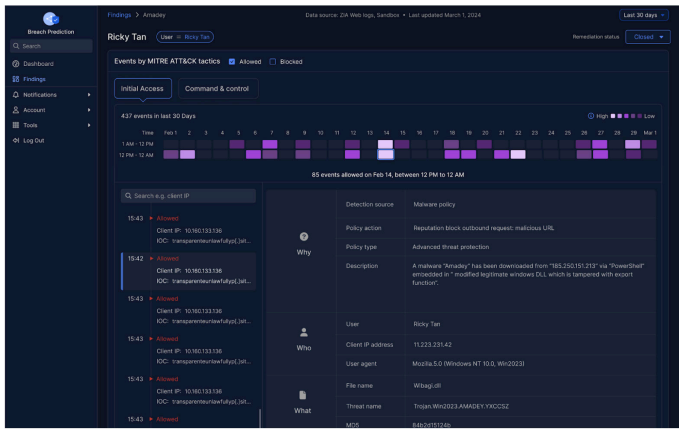
各攻撃段階にマッピングされた攻撃経路の可視化：攻撃の 4 つの段階にマッピングされた潜在的な攻撃経路を可視化し、悪用される可能性の高いものを攻撃の発生前に把握できます。

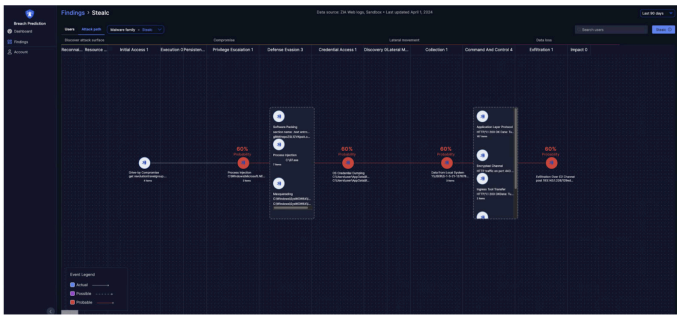
攻撃者が取り得る行動の分析：攻撃者の一般的な行動を詳しく把握することで、最も差し迫った脅威に対するセキュリティをプロアクティブに整備、強化できます。

予防型のポリシー推奨とアラート：リアルタイムの正確なアラートとカスタマイズされたポリシー推奨を通じ、攻撃経路を予防的に封じ込め、セキュリティ イベントと SOC の対応の負担を軽減できます。

近日リリース予定

© 2024 Zscaler, Inc. All rights reserved.





主な機能

攻撃の完全な可視化

- **攻撃アクティビティーの追跡：**最も一般的なマルウェア ファミリーおよびマルウェア カテゴリーに関連付けられたアクティビティーを、攻撃のすべての段階にわたって特定、追跡することで、的を絞った脅威の軽減および防止対策を可能にします。
- **マルウェアの IoC の MITRE TTP へのマッピング：**確認された侵害の痕跡 (IoC) を MITRE ATT&CK フレームワークの TTP と関連付けることで、脅威の理解と対応戦略を強化します。
- **侵害されたユーザーに関する詳細な情報把握：**攻撃パターンを可視化し、ユーザーへの影響を確認して修復を迅速化します。
- **攻撃経路の詳細に関するダッシュボード：**攻撃の詳細を簡単に確認し、より具体的な発見内容を関連するマルウェアのアクティビティーおよび TTP とあわせて把握できます。ダッシュボードには、将来の攻撃の予測発生確率も含まれます。

zscaler™ | Experience your world, secured.™

Zscaler について
Zscaler (NASDAQ: ZS) は、より効率的で、俊敏性や回復性に優れたセキュアなデジタル トランスフォーメーションを加速しています。Zscaler Zero Trust Exchange は、ユーザー、デバイス、アプリケーションをどこからでも安全に接続させることで、数多くのお客様をサイバー攻撃や情報漏洩から保護しています。世界 150 拠点以上のデータ センターに分散された SSE ベースの Zero Trust Exchange は、世界最大のインライン型クラウド セキュリティ プラットフォームです。詳細は、**zscaler.jp** をご覧いただくか、Twitter で **@zscaler** をフォローしてください。

© 2024 Zscaler, Inc. All rights reserved. Zscaler™、Zero Trust Exchange™、Zscaler Internet Access™、ZIA™、Zscaler Private Access™、ZPA™、**zscaler.jp/legal/trademarks** に記載されたその他の商標は、米国および / または各国の Zscaler, Inc. における (i) 登録商標またはサービス マーク、(ii) 商標またはサービス マークです。その他の商標はすべて、それぞれの所有者に帰属します。

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.jp