Defenders' Guide 2025

より堅牢な防御の未来へ

新たな攻撃ベクトルに先手を打ちましょう。脅威アクターが古いターゲットを悪用する新たな手法に対処が必要です。まずは Defenders' Guide のハイライトからご紹介します。

多層的なセキュリティで防御の取り組みを構築

考慮すべき 3 点の重要事項

リスク管理 特定の脅威の発生見込みとその対応の可能性に基づいて対応に優先順位を付け、組織の脆弱性を軽減

ネットワークアーキテクチャ ファイアウォール、セグメンテーション、アクセス制御を通じてレイヤー型セキュリティを実装し、侵害から防御して阻止

ホストセキュリティ システムアップデート、ウイルス対策ソフトウェア、ファイアウォール、およびアクセス制御を通じて、個々のデバイスをマルウェアや不正アクセスから保護

マルウェアが潜んでいる可能性がある場所

2024 年にオープンポートのインシデントが発生した上位のプロトコル

58.0%
サーバー・メッセージ・ブロック（SMB）

14.5%
リモート・デスクトップ・プロトコル（RDP）

12.9%
Secure shell（SSH）

VPN 内に侵入した攻撃者が行うこと

- リモート認証サーバーを使用してユーザーを認証
- 正当な認証の悪用
- 不正な認証サーバーの利用
- 秘密の構成ファイルの抽出および復号

XSS の脆弱性を阻止

- すべてのユーザー制御パラメータに出力エンコーディングを追加
- コードレビューや Web アプリケーションファイアウォールで防御
- Cookie の窃取、Web サイトの改ざん、セッションライディング／クロスサイトリクエストの偽造など、脅威アクターによる実際の攻撃手口を阻止

攻撃者がコンテナを標的にしている理由

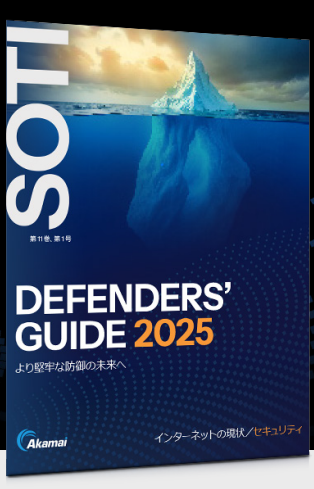
Akamai の研究者が Kubernetes に複数の脆弱性と戦術があることを発見。これが悪用されると、以下のような結果に発展：

- データ流出
- 権限昇格
- リモートコードの実行

事前対策と事後対応を組み合わせる

次の 4 つの基本原則を採りましょう

- サイバー衛生をあらゆる場所に導入
- セキュリティプラットフォームの背後に環境の一貫性を維持しながらレイヤー化
- ビジネスクリティカルなサービスを注視
- 信頼できる即応のインシデント対応チームやパートナーを持つ



Defenders' Guide 2025 をダウンロード