DATA SHEET

FortiWeb 脅威分析サービス

提供形態：

AI を活用した脅威分析で最も重要な脅威の特定を支援

セキュリティアナリストは、大量のセキュリティアラートが発生する、急速に進化する脅威環境に直面しています。脅威アクターは、新たな攻撃フレームワーク、巨大なボットネット、新しい脆弱性を悪用して高度化した攻撃キャンペーンを次々と仕掛けるようになっています。組織が多くのアプリケーションをクラウドに移行し、それらのアプリケーションでビジネスの重要な機能が提供されるようになっていることが、セキュリティアナリストが直面する状況をさらに困難なものにしています。アプリケーションの攻撃対象領域の急速の進化と拡大が続く今、セキュリティアナリストは、セキュリティツールで生成される膨大なアラートの処理を可能にする優れたツールを必要としています。

優れたツールを持たないセキュリティチームは、その多くが単独では価値が低いように見える大量のイベントに圧倒されるだけでなく、詳しい調査を経た後にようやく誤検知であることに気づくという事態に陥ります。このような大量に発生するアラートにより、重要なセキュリティイベントを見逃したり見落としたりする恐れがあります。

FortiWeb 脅威分析サービスは、機械学習アルゴリズムを活用してアプリケーションの攻撃対象領域全体の攻撃パターンを特定し、包括的なセキュリティインシデントに集約します。パターンを特定して深刻度を割り当てることで、重大な脅威を重要度の低いアラートや誤検知から切り分け、セキュリティチームが重大な脅威に集中できるようにします。

セキュリティアラートの調査にあたっては、コンテキストに加えて、複数のイベントを時系列に結び付ける機能が必要になります。FortiWeb 脅威分析サービスは、数千ものアラートを評価し、特定されたパターンに基づいてそれらのアラートをインシデントに分類することで、手動でのアラートの評価に伴う複雑さを解消します。この合理化されたビューにより、SOC アナリストが重大な脅威への対応に集中できるようになります。

主な機能と特長

- AI ベースの脅威分析
- 共通する特性やパターンを識別して、意味あるセキュリティインシデントに分類
- インシデントリスクの優先度の設定
- ワークフローの統合

主なメリット

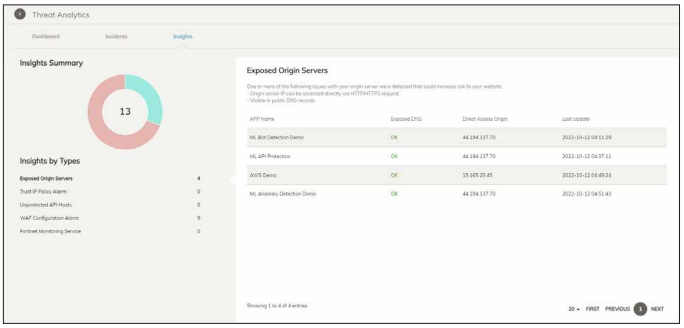
- 脅威の検知とレスポンスを簡素化
- WAF アラートのセキュリティ調査を高速化
- アナリストを最も重要な脅威に集中できるように支援
- 実用的インテリジェンスにより、調査結果に基づいてセキュリティを強化するための推奨事項を提示
- ハイブリッドクラウド環境全体からイベントを取得
- 過剰なアラート対応を軽減

ハイライト

脅威分析の実用的インテリジェンスとインシデントの補強

脅威分析サービスは、Web 資産に対する攻撃を監視し、WAF 構成を評価することで、セキュリティポスチャを継続的に評価します。攻撃データとフォーティネットの顧客ベース全体の相互参照により、不審なトラフィックや異常なトラフィックを相関付けることで、お客様の構成に基づいて攻撃の可能性が高い場合にアラートを通知します。

脅威分析の実用的なインテリジェンスにより、WAF 構成の強化、将来の攻撃のブロック、誤検知の軽減を可能にする推奨アクションを提示します。



SaaS、クラウド、オンプレミスのアプリケーションの可視性

FortiWeb 脅威分析サービスは、すべての FortiWeb アプライアンス、FortiWeb VM、FortiWeb Cloud からイベントを取得し、SOC アナリストに必要な Web アプリケーションの攻撃対象領域全体の実用的インテリジェンスを提供します。このソリューションでは、アプリケーションを導入する場所や利用する FortiWeb フォームファクターに関係なく、アプリケーション攻撃対象領域の脅威を一元的に表示できます。脅威分析で企業全体のイベントが集約されるため、複数の場所や Web 資産を含む企業規模の攻撃キャンペーンをアナリストが特定できるようになります。

オーダー情報

製品	個別	バンドル	
	アラカルト	アドバンスト	スタンダード
脅威分析サービス	✓	✓	

FortiWeb-2000F の例を以下の表に示します。

製品	説明
バンドル	アドバンストバンドル（FortiCare Premium + AV、FortiWeb セキュリティサービス、IP レピュテーション、FortiSandbox クラウドサービス、クレデンシャルスタッフィングディフェンス、および脅威分析）
アラカルト	脅威分析サービス

脅威分析サービスは、FortiWeb Cloud に含まれています。また、FortiWeb アプライアンスおよび VM の保護対象であるアプリケーションで、アドバンストバンドルの一部として、またはアラカルトとして利用することもできます。

フォーティネットジャパン合同会社

〒106-0032
東京都港区六本木 7-7-7　Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ