DATA SHEET

FortiResponder MDR（Managed Detection and Response）サービス

はじめに

フォーティネットは、業界でも最大規模の研究者とアナリストで組織されたチームのひとつで、200 名以上もの研究および分析のエキスパートが世界中から集まっています。フォーティネットの専任エキスパート集団は、長年にわたって破壊的な脅威と攻撃者の新たな戦術、手法、手順に目を光らせ続け、マルウェア、ボットネット、モバイル、ゼロデイ脆弱性をはじめとする脅威の重要領域をくまなく研究しています。その幅広い経験と専門知識を活用し、フォーティネットはお客様に MDR サービスを提供しています。24 時間 365 日体制のこのサービスは、フォーティネットの経験豊富なアナリストチームと FortiEDR プラットフォームによる継続的な監視、アラートのトリアージ、脅威の追跡、インシデント処理を実現します。

FortiEDR のアドオンサービスである FortiResponder MDR サービスは、FortiEDR によって検知されたアラートと疑わしい脅威の監視に重点を置いています。このサービスは、お客様が受け取るすべてのアラートが確実に認知され、適切に対処されることを目的としています。この脅威エキスパートのチームが、お客様に代わってすべてのアラートのレビュー / 分析、脅威のプロアクティブな追跡、そしてアクションを実行することで、リスクプロファイルに沿った確実な保護を提供します。さらに、FortiResponder チームはインシデントレスポンス担当者および IT 管理者にガイダンスと次に採るべきステップを提示します。MDR サービスでは、その一環として以下のアクティビティが提供されます。

サービスの機能と成果物

継続的な脅威検知 / 分析

フォーティネットのエキスパートチームは、FortiEDR プラットフォームから送られるアラートを活用し、24 時間体制で脅威を監視 / 追跡し、環境に侵入した可能性のあるイベントを分析します。代表的なアクティビティの一部を以下に紹介します。

- マルウェアの静的 / 動的両方の分析
- メモリ分析による不正なプロセスの検知
- 潜在的脅威および不要なプログラムの特定
- 環境のチューニング：安全なアプリケーション向けの詳細な例外の設定
- 追加のフォレンジック情報の取得と分析：
  - Windows イベントログの記録
  - AmCache ファイル
  - ホストファイル
  - スケジュールされたタスクのログファイル
  - ブラウザ情報

脅威の封じ込めと修復

ホストの侵害が特定された場合、FortiResponder チームはビジネスオペレーションに影響を与えずに脅威を隔離することを目的とした、最初の戦術的封じ込めオプションを提供します。FortiEDR テクノロジーを活用するこれらのオプションには、次の機能が含まれます。

- ディスクへの書き込みプロセスを阻止
- 別のデバイスへの通信をブロック

これらの封じ込めオプションの一部は、フォーティネットのプレイブック・テクノロジーを通じて既に自動化されている場合があります。自動化されていない場合は、フォーティネットのチームがプレイブックやグループ / セキュリティポリシーを使用して追加の構成を支援します。

主な利点

SOC の進化を加速する必要がある組織は、FortiEDR と FortiResponder サービスを通じて提供される高度なエンドポイントセキュリティの組み合わせにより、24 時間 365 日体制での対応と既存 SOC リソースの拡張というメリットを享受できます。これにより、検知もれの懸念を解消しながら脅威へのレスポンスを向上し、インシデントへのレスポンスプロセスをオペレーション化し、アラート対応の負荷を軽減できます。これらのサービスによって、SOC チームの層に厚みが増し、経験の浅い SOC 担当者がより高度なタスクを担うことができるようになります。その結果、組織は既存の人材の活用効率を高め、脅威や犯罪者に対処できるようになります。さらに、外部プロバイダーからの日々のサポートが、過剰な責務を担うセキュリティチームにとって欠かせないバックアップとなり、チームの対応力を拡張可能になると同時に、検知とレスポンスに要する平均所要時間を短縮できるようになります。

- SOC の進化を加速
- 既存の SOC を拡張
- アナリストの過労を防止

さらに、フォーティネットの脅威分析に基づいて戦術 / 戦略の両面で修復ステップのガイダンスを提供します。次の戦術オプションは手作業 / 自動のどちらでも実行可能です。

- プロセスを終了
- ファイルを削除
- レジストリから永続性を排除

レポートとアラート

フォーティネットのチームは、発見したセキュリティの課題に対してお客様が知識に基づく決定を行うことができるように、適切な情報を確実に提供します。FortiEDR テクノロジーによって実行されるすべてのセキュリティイベントは 24 時間以内に処理され、重大な問題に対しても適切なレスポンスが実行されます。イベントが分析されると、チームは脅威の情報と推奨されるレビュー / 修復ステップを含むインシデント通知を E メールで送信します。

お客様は、インシデントまたはイベントに関する詳細情報やガイダンスのリクエストを E メールでエスカレーションすることもできます。フォーティネットのエキスパートチームは、これらのリクエストに 24 時間 365 日体制で対応します。問題の深刻度に応じて、電話または Web 会議でのコミュニケーションが可能です。

エンゲージメントの進展に伴い、プラットフォームの状態や特定の脅威 / トレンドといった環境に関する詳細情報が必要になることがあります。フォーティネットのコンサルティングソリューションアーキテクトや FortiResponder チームは、定期的に環境の評価を提供します。この評価では、以下のような情報が提供されます。

- デバイス対象範囲と FortiEDR ライセンスの使用状況
- FortiEDR プラットフォームの状態
- 検知されたマルウェア、脆弱 / 不要なプログラム
- 全体的な脅威のトレンドと推奨事項
- 質問と問題の処理
- 修復に関する問題への対応（必要に応じて）
- トレーニングの必要性への対応（必要に応じて）

トレーニング

サービスの導入初期プロセスの一環として、フォーティネットのエキスパートチームは FortiEDR プラットフォームでのイベントのレビュー / 分析方法に焦点を当てた初期トレーニングを実施します。

購入単位

本サービスは、FortiEDR バンドルの一環として、または FortiEDR におけるスタンドアロンのアドオンとして購入できます。本サービスは、FortiEDR の保護対象となることが想定されるエンドポイント総数に対して、エンドポイント毎の料金が適用されます。

サービスユニット	説明
Managed Detection and Response	MDR サービス、1 年間：24 時間 365 日の脅威の監視およびインシデントトリアージのメール通知、オンデマンドのレポート、ガイダンス付のリモート修復、レスポンスのオーケストレーションに関するプレイブックのセットアップ

フォーティネットジャパン株式会社

〒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