CROWDSTRIKE

CROWDSTRIKE FALCON OVERWATCH
マネージド脅威ハンティング

情報漏洩を最後の砦として防止する強い味方

FALCON OVERWATCH：
大規模な情報漏洩事故を阻止

Falcon OverWatch サービスは、脅威を見逃さず、最終的に大規模な情報漏洩を防ぐために CrowdStrike が提供しているマネージド・ハンティング・サービスです。CrowdStrike が誇るセキュリティの精鋭チームが、お客様の環境内に起こる攻撃の挙動についてプロアクティブにハンティング、調査、助言を行うものです。脅威を見つけた場合、大規模な情報漏洩につながる前にインシデントに優先順位をつけ、調査して復旧するための支援を行います。

製品の主な機能

他にはないマネージド脅威ハンティングサービス

- **Falcon プラットフォームの上で提供** ― クラウド上に構築された Falcon プラットフォームには、1日あたり700億を超えるイベントが世界中からアップロードされます。この強力な Falcon プラットフォームの上で、OverWatch のサービスは提供されます。
- **24時間365日の対応** ― Falcon OverWatch™のチームは、日々、巧妙な攻撃者と「接近戦」で闘って得た専門技術を用いて、年間15,000以上の侵入を検知、阻止しています。OverWatch チームには、必要とあればわずか数秒でお客様に代わって対策を実施する体制があります。
- **“CROWD”の力** ― OverWatch は Crowd、すなわち大勢のお客様から提供される膨大な情報を武器として、新たに台頭する脅威を発見しています。世界のどこかのお客様の環境で攻撃が検出された場合、世界中全てのお客様の環境を即座に保護します。当社ではこれを「免疫コミュニティ」と呼んでいます。

主な特長

» **既脅威ハンティング** ― 環境内の脅威を24時間、365日体制でプロアクティブにハンティングし、False Negative も見逃しません。

» **アラートの優先順位付け** ― 独自の手法で、環境内の最も差し迫った脅威をピンポイントで検知し、誤検知の問題を解決します。

» **何をすれば良いかのガイダンス** ― OverWatch の脅威ハンターは、お客様に対して、攻撃の詳細を伝えるだけでなく、次に何をすべきかを指導します。

「1週間前、OverWatch から連絡があり、サーバーハイジャックで知られる組織を思わせる挙動が検出されたと言われました。連絡を受けたことによって、私たちはその問題に集中して対応し、対策を進めることができました。OverWatch の対応はとても素早く、『この問題について分かっている情報はこうだ』と教えてくれました。彼らの行動によって、当社のサーバの1台がブラックマーケットに売られてスパム発信者などの悪意ある人物に使用されるのを防ぐことができました」

― マーク・サウアー
TransPak 社　IT 部門ディレクター

- **膨大なアラートに振り回されない** — OverWatch は攻撃の兆候となる挙動を検知し、調査し、優先順位付けをします。これにより OverWatch は実際の攻撃のみを識別して通知することができ、膨大なアラート対応や誤検出の追跡に振り回されることがなくなります。

ワールドクラスのセキュリティ専門家による24時間体制の支援

- **お客様の SOC を大幅に強化** — Falcon OverWatch は24時間体制でお客様のためにプロアクティブに脅威ハンティングを行う専任のチームで、お客様の SOC の効率化と防御力の強化に貢献します。
- **専門家がどう対策するかを助言** — OverWatch は起きている事象に対してどう対応したら良いのかを助言を、アラートと共に提供しています。個々のお客様の状況に合わせてアラートを作成するため、対策の各ステップをすぐに実行することができ、解決までの時間を大幅に削減します。
- **攻撃者と互角に戦うために** — EDR ソリューションを導入するだけではなく、セキュリティのエキスパートを雇うことによって、高度なツールと知識を持った攻撃者に対して互角に戦うことができるようになります。

導入の早さとエンドポイントの軽さも魅力

- **時間、労力、費用を削減** — OverWatch は、クラウドネイティブの Falcon Insight™ や CrowdStrike Falcon® プラットフォームを活用するため、オンプレミスのサーバーなどは一切必要ありません。
- **短時間で稼働開始** — OverWatch は運用開始直後からマネージド脅威ハンティングを実行します。Falcon OverWatch はインストール後すぐにフル稼働してモニタリングを行ったり、記録を取ったりすることができます。リブートや細かい調整、ベースライン設定や複雑な設定は必要ありません。
- **エンドポイントが重くならない** — Falcon の軽量エージェントはわずか20MB のサイズ。検索などの処理は全てクラウド上の Falcon Threat Graph™ データベース上で行われるため、エンドポイントやネットワークへの影響はほとんどありません。

侵入を引き起こす前にインシデントを予防

ステルス技術を利用した最先端の標的型攻撃を見極めるためには、人間が調査しなければならないこともよくあります。そのため、Falcon OverWatch は、既存の防御システムでは見つからないインシデントをハンティングし、調査し、素早く対処します。

CROWDSTRIKE

CrowdStrike は、クラウドベースの次世代エンドポイントプロテクションの業界を牽引しています。 CrowdStrike は、次世代のアンチウィルス、EDR、および24時間体制のマネージド脅威ハンティングサービスを統合し、すべてを1つの軽量エージェントで提供する、業界初、かつ唯一の企業として、革新的なエンドポイントプロテクションを提供しています。

詳細は、**crowdstrike.com** をご覧ください。