次世代セキュリティ対策

リアルタイム脅威検出からインテリジェント防御まで

CrowdStrikeで実現する

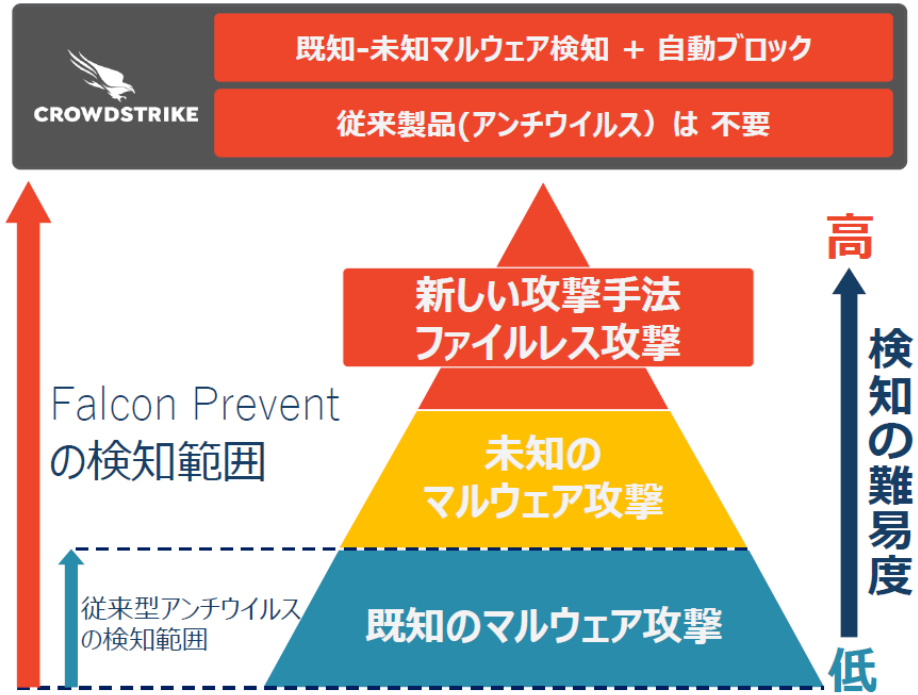
高レベルのセキュリティ対策

TECHVAN

第3章　CrowdStrike Falcon Platform の機能（1） NGAV

次世代アンチウイルス NGAV(Next Generation Anti-Virus)とは

次世代アンチウイルスといえば、未知の部分とファイルレス攻撃などに対する振る舞い検知の部分がフォーカスされがちですが、それら機能も備えながら、従来型のパターンマッチングベースによる検知は、機械学習の検知ロジックで対応しています。このため、従来のパターンマッチングベースと組み合わせなければ検知漏れしてしまう、ということもありません。



EDR （ Endpoint Detection and Response ）とは

EDRで求められる機能は、イベントを取得し、状況に応じて、端末隔離などのレスポンス機能があること、そしてイベントの詳細を可視化することが必須です。CrowdStrikeでは、高速なインシデントの対応を提唱しており、検知１分、調査10分、復旧まで60分で対応することを目標にしています。

そこで「アンチウイルスがいい」「EDRも早く対応できる」機能を備えると、どのようなメリットがあるのか、そもそも検知はどういう仕組みなのか、次ページから解説します。