Falcon Spotlightがゲームチェンジャーに：常に進化するAIによる脆弱性管理

October 12, 2021 | Khanh Tran | Endpoint & Cloud Security | Executive Viewpoint

本件は、10月12日～14日に開催、Fal.Con 2021 CrowdStrikeサイバーセキュリティカンファレンスの発表に関連しています。

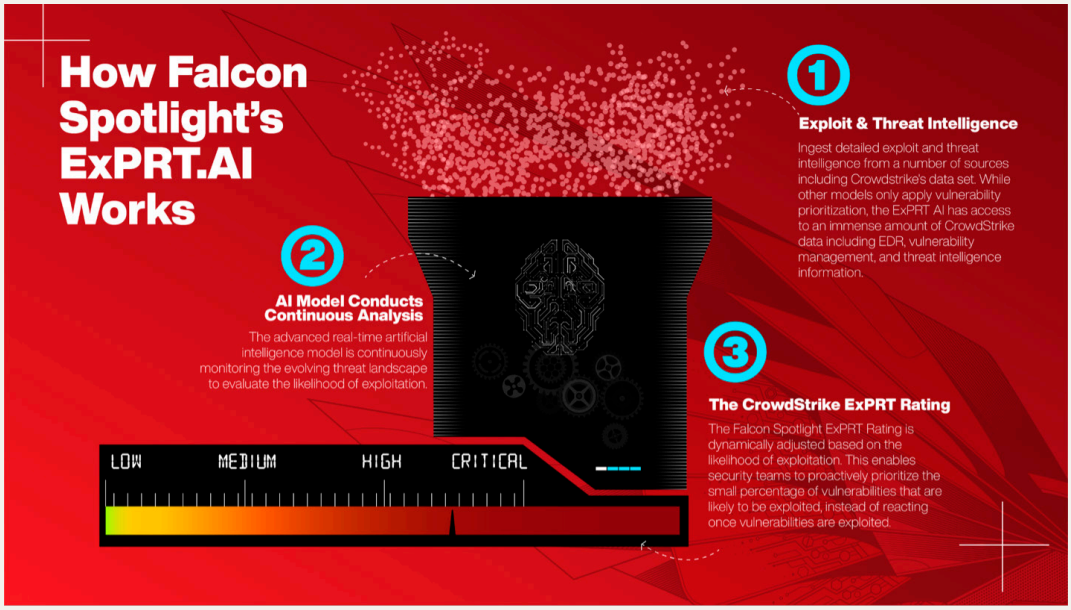
組織を弱体化させ、悪影響をもたらす脆弱性を適切に監視するために、SecOps が利用できる時間は限られています。また、重要度の高い脆弱性が数多く存在するなか、組織の環境を守るために、一つ一つの脆弱性の緩和と対応に時間を割くことは不可能ではないにしろ、非常に困難です。時間には限りがあり、深刻な脆弱性は溢れかえっています。では、すべての必要なパッチを常に更新し、セキュリティホールをふさぐためには、どのように厳しい管理を行えばよいのでしょうか。

最近までは、SecOps のスタッフが全力を尽くすことが最善策とされており、脆弱性管理ソリューションを購入し、限られた時間の中で、できる限りの対応を行っていました。担当者は、重大な脆弱性のうち、どれが組織に最悪の影響を及ぼすかを判断するのに、ダッシュボードを見ながら手動で判断する必要がありました。しかし、脅威や攻撃者グループの数は急増しており、過去 5 年間では、**脆弱性の数が前年比で倍以上**のペースで増えています。

共通脆弱性評価システム（CVSS）と呼ばれる業界標準の脆弱性スコアリングでは、深刻度の高い脆弱性が増加していると評価しており、SecOps の担当者は、それぞれの脆弱性に対する緩和策や対応策を講じることを求められています。しかし、そうするための能力やリソースが不十分である場合もあるでしょう。その結果、組織にとって本当に危険な脆弱性にパッチの適用や緩和が行われなかったり、リスクの低い脆弱性の優先度を下げられなかったりするケースも多くあります。

脆弱性管理の世界では、CVSS スコアが今も重要な位置を占めていますが、SecOps チームは、自社の環境に現実的かつ直接的なリスクをもたらす脆弱性に優先順位を付けることができる、よりダイナミックで直感的な評価方法を求めています。CrowdStrike の Falcon Spotlight™ チームは、世界中の SecOps チームが直面しているこの非常に重要かつ差し迫った課題を認識していました。そこで登場したのが、CrowdStrike の新しい ExPRT.AI ソリューションです。

Falcon Spotlight の ExPRT.AI（Expert Prediction Rating Artificial Intelligence）モデルは、さまざまな脆弱性および脅威ベースのテレメトリー情報を活用しています。これらの情報には、CrowdStrike 独自の脅威インテリジェンスも含まれ、Falcon Spotlight のコンソール内で、動的かつ俊敏な、定期的に更新される ExPRT レーティングを提供します。ExPRT レーティングは、SecOps が必要とする答えを提供し、どの脆弱性が組織を本当に危険にさらすのかという有益な知見を与え、組織環境にとって本当に重要な脆弱性を優先的に特定するための可視性と機能を提供します。



Falcon Spotlight の ExPRT AI：強力な脆弱性予測モデル

Falcon Spotlight を利用するお客様は、ExPRT.AI モデルの価値をすぐに実感できます。このモデルは、既存のデータでの対応ではなく、組織がどの脆弱性を優先すべきかを予測します。 ExPRT.AI モデルは、次の 2 つの重要な要素に基づいています。

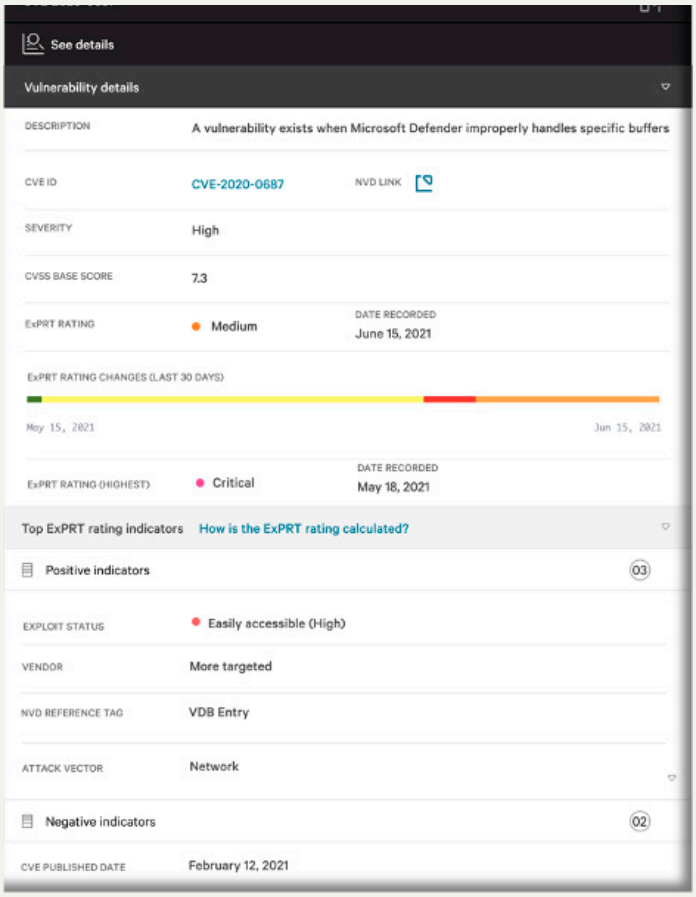
- **データ**：ExPRT.AIは、脅威/エクスプロイト・インテリジェンスの優れたデータベースを活用しています。このデータは、CrowdStrikeの脅威インテリジェンスを含む多くのソースから取得されます。ExPRT.AIを実現しているのは、CrowdStrikeのデータセットです。他のベンダーのソリューションでも、データサイエンスを脆弱性の優先順位付けに適用することはできますが、CrowdStrikeがEDR、脆弱性管理、インテリジェンス、脅威ハンティングの各サービスから得ているようなデータがありません。
- **モデル**：状況に常に順応するこのモデルは、過去のデータと新しいデータを使用して、脆弱性の悪用の可能性を予測します。ExPRT.AIモデルでは、AIが入力データを使用して可能性の予測を調整し、時間とともに動的に変化するスコアを提供できる利点があります。これにより、Falcon Spotlightのお客様は、問題が発生する前に脆弱性に対しプロアクティブに対応することができます。常時学習を続けるExPRT.AIは、最新の情報に反応するだけでなく、将来起こりうることも予測します。そのため、パッチ適用担当者はリスクに事前対処することが可能になります。

ExPRT.AI は、リスクがゼロあるいはほぼないと思われる脆弱性の優先順位を下げながら、SecOps が本当に重要な作業に集中できるようにします。

継続的にアップデートされ透明性のある ExPRT レーティング

ExPRT.AI によって生成されるのが ExPRT レーティングです。このレーティングでは、業界標準の CVSS スコアリングとは異なる方法を利用しています。CVSS は、特定の脆弱性に対する評価を数値化したスコアを提供し、National Vulnerability Database（NVD）では深刻度の評価が追加されています。このようなスコアリングは有用ですが、限界もあります。状況が変化したり、別のエクスプロイトが発見されると、新たなデータによって脆弱性の深刻度の評価が変わってくる可能性があります。CVSS や NVD のスコアは静的なものであり、あくまである時点でのものです。その後の要因によって脆弱性のリスク評価が変わるかどうかは、IT スタッフが自分で判断しなければなりません。

一方、ExPRT レーティングは、動的で透明性の高いものです（下図参照）。最初にレーティングが提示され、その脆弱性に関連する新しいデータが取得されると、それに基づいて深刻度が変化することもあります。また、レーティングのすぐ下にポジティブな指標とネガティブな指標が表示されるため、SecOps は変化の要因を明確に把握できます。



Falcon Spotlight コンソールには、CVSS ベースのスコアリングも引き続き表示されますが、ExPRT レーティングによって、スタッフが必要とするコンテキストと可視性が得られるため、最終的に脆弱性管理のライフサイクルを合理化および簡素化できます。

Falcon Spotlight で SecOps の態勢を直ちに強化

御社の SecOps チームが、**脆弱性管理**とパッチ適用のプロセスに Falcon Spotlight を使用していないのであれば、今が始めるチャンスです。脆弱性の予測と、透明性のある動的なレーティングを提供できる最先端の AI モデルにより、SecOps チームは組織全体におけるセキュリティ態勢を劇的に改善することができます。鍵をしっかりとかけておけば、犯罪者に侵入される可能性を低減できるでしょう。

Falcon Spotlight に関する詳細な情報については、営業担当者にお問い合わせいただくか、**製品紹介ページ**をご覧ください。

追加情報：

Falcon Spotlight™ による脆弱性管理を紹介するビデオ（英語）を是非ご覧ください。御社のシステムやアプリケーション内の脆弱性を迅速に監視し、優先順位をつける方法をご覧いただけます。

CVSS スコアとは

共通脆弱性評価システム（CVSS）は、CrowdStrike をはじめとする多くのサイバーセキュリティ企業がソフトウェアの脆弱性の深刻度や特徴を評価・伝達するために使用している、オープンかつ独立した業界標準です。CVSS ベーススコアは 0.0 から 10.0 の範囲で算出され、CVSS スコアに対し **National Vulnerability Database（NVD）**による深刻度評価が付加されます。脆弱性スコアリングの詳細については、**こちらの記事（英語）**を参照してください。

その他のリソース

- Falcon Spotlightをお試しいただき、御社の環境内の脆弱性の発見と管理にお役立てください。
- 脆弱性を簡単かつ効率的に優先順位付け。Falcon Spotlightのカスタムフィルターやチームダッシュボードを活用して、可視性を向上させる様子をご覧ください。（英語）
- 企業が優先すべき重要な脆弱性については、毎月更新されるPatch Tuesdayブログシリーズ（英語）をご覧ください。
- CrowdStrikeの次世代型AVをお試しください。Falcon Prevent™の無料トライアル版

原文：Falcon Spotlight Is Changing the Game: Vulnerability Management With Ever-Adapting AI
https://www.crowdstrike.com/blog/introducing-falcon-spotlight-exprt-ai/