CROWDSTRIKE **FALCON**：エンドポイント**保護**の**新たな**スタンダード

次世代エンドポイント保護における5つの必須要素

市場の混乱を紐解く

次世代エンドポイント保護の真の姿とは

新旧を問わず、どのベンダーも自社こそが「次世代」の名にふさわしいと言い、市場は「ゲームチェンジャー」という謳い文句のエンドポイントセキュリティ製品で溢れ返っています。振る舞い検知機能を搭載しているものや、機械学習をある程度取り入れているものもあれば、クラウドベースの保護提供を宣伝しているものもあります。

しかし、これらの新しいソリューションの中身を覗いてみると、ほとんどが単純に初代のエンドポイント保護を強化した旧式のプラットフォームを反復しているに過ぎないことがわかります。新しい手法を 1 つや 2 つ取り入れているかもしれませんが、大部分は、いまだシグネチャベースの脅威検知などの古い技術や、オンプレミス配信向きの設計で陳腐化するばかりのアーキテクチャに大きく依存しています。そのため、クラウドソリューションとして販売されていても、内部では細かく分断されており、専用のクラウドソリューションの規模や効力には及びません。

最も大きな弊害は、エンドポイントソリューションの大半がいまだに、IOA（攻撃の痕跡）を探し出すことよりも、悪質な実行可能ファイルの阻止にこだわっていることです。IOA は、マルウェアファイルが存在しない場合であっても侵害の活動を示します。

CrowdStrike® は、真の意味で次世代エンドポイントセキュリティプラットフォームと言える、多数の新たな検知機能を備えています。本来の「次世代」ソリューションは、巧妙な攻撃に真っ向から対抗するために、より高度なテクノロジーと人力によるインテリジェンスをまとめたパッケージ一式を提供するものでなければなりません。エンドポイントセキュリティ製品が次世代ソリューションとして本格的に受け入れられるためには、諦めない攻撃者を何度も撃退できるほどの予測、防御、検知、可視化、インテリジェンスの機能を提供する必要があります。

これらの機能を備えた製品を見つけるために、意思決定者は次世代エンドポイントセキュリティソリューションで以下の 5 つの必須要素を探る必要があります。

要素1:
ITハイジーン

セキュリティはまず、どこが保護されていないかを把握することから始まります。そうすることで、セキュリティギャップを狭め、準備態勢がより整った状態で脅威に立ち向かうことができます。

環境内に誰がいて何が実行されているかを理解することが不可欠です。IT ハイジーン（IT の「衛生」）は、効率的なセキュリティプラクティスの基本要素であり、セキュリティチームと IT チームが先制措置を行い、今日の巧妙な脅威に立ち向かう準備をできるだけ整えるために必要な可視性と情報を提供するものです。

IT ハイジーンによって、少しの備えが大きな効果をもたらすようになります。たとえば、パッチ未適用の古いアプリケーションは、今も昔も、組織の IT 環境に侵入するための主な攻撃経路となっています。最近の調査によれば、組織の 75% がパッチ未適用の古いソフトウェアを最大のセキュリティリスクと見なしています。そのため、環境内で実行中の脆弱なアプリケーションを発見し、パッチを適用して、アップデートできる状態であれば、攻撃者に対して非常に有利になります。

これに加えて、どのようなシステムがネットワーク上で実行中であるかを把握することにより、セキュリティアーキテクチャ内の問題に対してプロアクティブに対応できます。IT ハイジーンによって、保護されていない BYOD（私有 IT 機器の業務利用）、サードパーティシステムなど、ネットワーク内にある未管理のシステムやリスクになりうるシステムを特定できるようになります。

認証情報の盗難も、攻撃者にとっての主要な攻撃手段であり続けています。環境全体にわたって、認証情報が使われている場所や管理者の認証情報が作成されている場所のすべてでログオンの傾向（活動内容 / 持続時間）を監視して可視化することにより、セキュリティチームが認証情報の不正利用や盗まれた認証情報を利用する攻撃を検知し、軽減できるようになります。

ヒント：IT ハイジーンは、組織のセキュリティ体制を改善するための確かな基盤になります。システム、アプリケーションの使用状況、ユーザーアカウントの活動をリアルタイムで監視して記録することで、セキュリティチームは、攻撃される前に問題を特定し、対処できるため、防御について最善の準備を行うことができます。

要素2：
次世代アンチウイルス

従来型のアンチウイルス（AV）は、97 ～ 99% の有効性を売り込むことで、この市場を生き長らえてきました。しかし、ほとんどのセキュリティ専門スタッフが身をもって知ったことは、一見すると小さな隙間（ギャップ）であるこの 1 ～ 3% が、既知、未知を問わずマルウェアを利用する敵にとっては大きな入口になるということです。さらに、古い AV のアプローチでは、ますます巧妙化するファイルレス手法に一切対処できません。実際、各種調査によれば、今日の侵害の多くはマルウェアがまったく使われておらず、むしろソーシャルエンジニアリングや第三者による認証情報の盗難などの手段によって実行されています。

とはいえ、従来型の AV は、このように欠点はあるものの、価値のないツールというわけではありません。AV の終焉が近づいていると推測するアナリストもいましたが、AV には依然として、明らかな脅威を除去するという点で大きな価値があります。ただし、AV はエンドポイントセキュリティへの唯一の解決策ではなくなっています。従来型の AV では、十分なレベルの保護をどうしても提供できないのです。

次世代 AV は、既知のマルウェアを特定して対処するだけのアプローチ、すなわち攻撃者によって悪用されうる脆弱性を残してしまうアプローチを超越しています。また、次世代 AV は、既知のシグネチャを識別して、脆弱性を利用するエクスプロイトをブロックするだけにとどまらず、より一層の防衛ラインを提供します。

さらに、次世代 AV は、振る舞い分析と機械学習を存分に活用して、未知の悪質なファイルを識別できる必要があります。マルウェアだけに着目する手法から一歩先を進み、事後ではなく、進行中に攻撃の兆候を探し出せることが必要です。このアプローチでは、攻撃後にのみ現れる IOC（侵害の痕跡）だけに頼るのではなく、必然的に IOA（攻撃の痕跡）を探すことになります。IOA を探すためには、環境全体から充分なエンドポイント活動データを収集し、その他の情報を使ってそれぞれの IOA のコンテキストを割り出し、最終的には、活動についてできるだけ詳細な全体像を描き出す必要があります。

ヒント：IT の意思決定者は、いわゆる「次世代」の AV 製品を評価する上において、振る舞い分析や機械学習を宣伝している製品については、注意して確認する必要があります。その判断材料は、分析されるデータの品質と関連性です。データが数秒間の実行データに限られている場合や、不審なファイルのみを見て情報を抽出する場合、進行中の活動が悪質なものかを判断するための十分なコンテキストが得られません。

次世代アンチウイルス（AV）ソリューションは、正規の活動と悪質な活動の両方を監視し、アナリストが誤検知によって疲弊しないようなアルゴリズムを利用すると同時に、攻撃を受けたことを示唆する一連の活動を検知できるものである必要があります。たとえば、実行されるファイルやコードだけを監視して、悪質であるかを判断すればよいわけではなく、IOA を表す以下のような振る舞いも探し出す必要があります。

- 攻撃者が自らの存在や活動を隠そうとしていないか
- 認証情報がメモリやディスクからダンプされていないか
- 権限がエスカレーションされていないか
- ネットワーク内でラテラルムーブメントが発生していないか

これらの振る舞いは、個別に見れば脅威を示唆するものでなくても、相互のコンテキストを考慮して調査した場合に、攻撃が進行中であることが明らかになります。

次世代 AV でこのような大量のデータを収集して迅速かつ正確に分析するためには、時代遅れのオンプレミス型アーキテクチャや従来型のデータベース手法を利用していては達成できないレベルの演算性能とスケーラビリティが必要になります。これらの成果は、グラフデータベースなどの最先端のデータモデリング技術をサポートできる、専用のクラウドプラットフォームによって初めて達成できます。そのために、CrowdStrike はクラウドベースの Falcon プラットフォームを構築しました。Falcon プラットフォームは、大量の離散したエンドポイントでの実行イベントを収集して保管し、それらを CrowdStrike Threat Graph™ データモデルを利用してリアルタイムで分析することができます。グラフデータベースを基盤として構築された CrowdStrike Threat Graph は、175 か国以上に位置するエンドポイントセンサーから収集されたデータを数秒で分析して関連付けることができ、その結果からパターンを特定して、攻撃が実行中であるかを判断します。

このアーキテクチャでは負荷の高い処理がクラウド内で実行されるため、エンドポイントの安全性と最適なパフォーマンスを維持しながら、エンドポイントへの影響をほぼゼロに抑えつつ最大限の保護を提供することができます。Falcon の次世代 AV 機能は、未知の脅威が侵害につながる前にその脅威を発見してブロックするために必要な可視性とスピードを実現するように、独自に設計されています。

IOAの仕組み：現実世界の犯罪にたとえると

IOA の仕組みを解説するために、現実世界での銀行強盗の計画と実行について考えましょう。賢い泥棒はまず、標的となる場所の「事前調査」を行い、偵察に行って潜在的に脆弱な場所を特定し、把握します。犯罪を成功させるための最善の日時と作戦を決定したら、犯行を開始します。監視の目をかいくぐれそうな時間を選んで銀行に侵入し、セキュリティシステムを停止させて金庫を探し、暗証番号の解除を試みます。成功した場合、お金を掴んで、そっと出口に向かってミッションを終わらせます。

この例では、銀行強盗が、強盗に入ってそこから逃げるという目標に向かう中で見せた一連の振る舞いが、IOA となります。一連の振る舞いには、銀行周辺を走行（標的の特定）、駐車、建物への侵入、セキュリティシステムの停止などが含まれるでしょう。言うまでもなく、これらの行動のいずれも、個々では必ずしも攻撃が差し迫っていることを示唆するものではありません。これらの個々の出来事が組み合わさり、その特定の組み合わせが観測された場合にのみ、潜在的な脅威を識別して排除できるのです。

要素3：エンドポイントでの検知と対応

フルに機能する EDR（エンドポイントでの検知と対応）システムであるためには、エンドポイント上での関連するすべての活動を記録できる必要があります。この記録は、リアルタイムおよび事後の詳細調査のために利用されます。

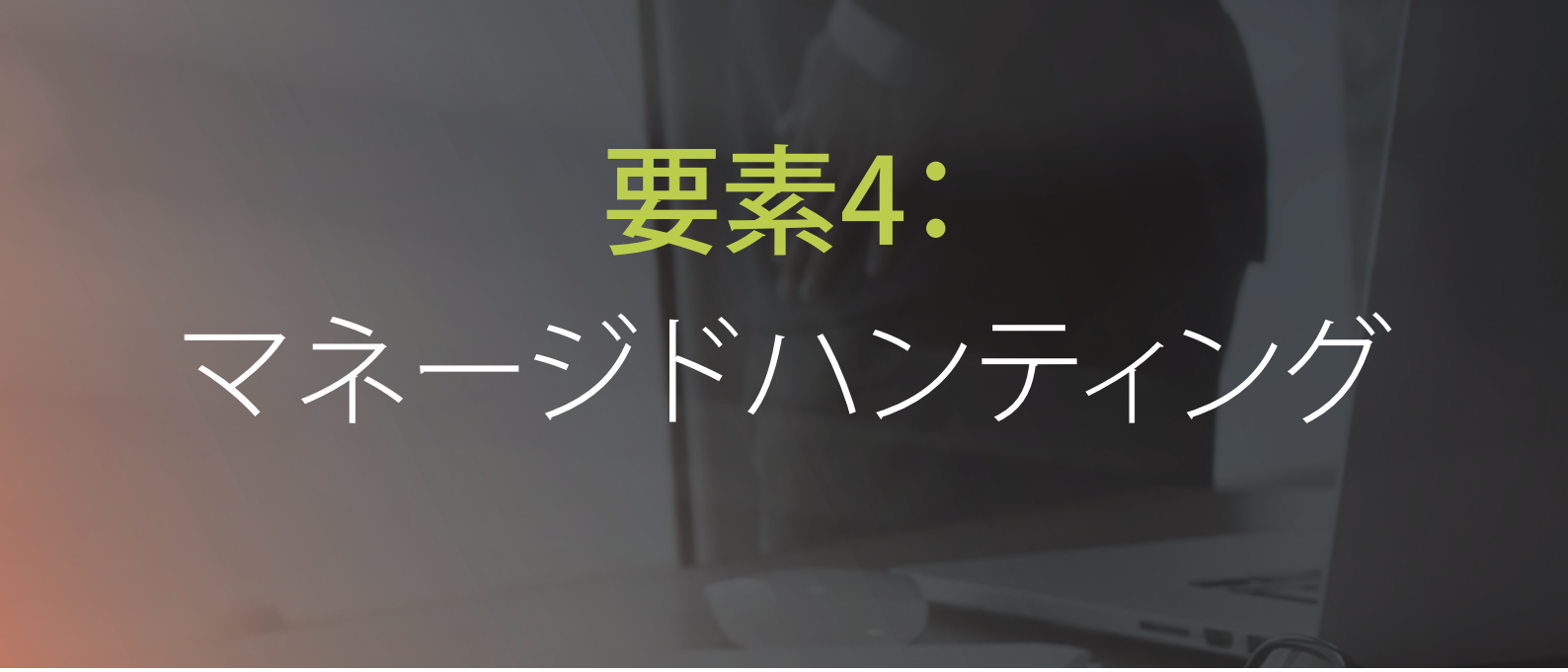
このようなソリューションは、動きを検知したときに録画を開始する監視カメラと比較できます。EDR 製品はすべての活動を記録する必要があり、その記録は、以下のような攻撃の始まりを示唆するシステム動作によって始まります。

- アプリケーションの実行
- ネットワークへの接続
- Web サイトへのアクセス
- ファイルのディスクへの書き込み

EDR システムはこれら大量のデータをプロアクティブに捜索して、ほかの方法では検知できないような悪質な活動パターンを発見できます。

さらに重要なことに、EDR システムは、発見された侵害を軽減するための容易な手段を提供する必要もあります。たとえば、無防備なエンドポイントを封じ込めて侵害の進行を防ぎ、ダメージが発生する前に修復を行えるようにします。

このようなソリューションが、必要となるすべてのデータを収集して維持できるのは、クラウドによるスケーラビリティを利用できる場合に限られます。また、クラウドデプロイメントは、ネットワークの外部や VPN の外部にあるリモートシステムを保護するためにも不可欠です。さらに、クラウドの機能があるからこそ、多数の組織に渡りこの種の振る舞いを分析し、匿名の脅威インテリジェンスが蓄積されるクラウドソースコミュニティの集合知を利用できるのです。



要素4:
マネージドハンティング

結局のところ、攻撃者は人間であり、人間には適応力と創造力があります。防御する側が技術だけに頼って攻撃に対抗していては、極めて不利な状況に置かれます。

ヒント:効果的な次世代エンドポイントソリューションは、入手したデータを活用して脅威をプロアクティブに探し出すというハンティングを行う、セキュリティエキスパートチームによって支えられる必要があります。

優秀なハンティングチームは、自動化された対応システムが見過ごした可能性のある事柄を発見するだけでなく、過去に起こったインシデントから学習し、蓄積されたクラウドソースデータを活用して、そのデータを徹底的に分析し、顧客に対して、悪質な活動が検知されたときの対応ガイドラインを提供することができます。

このようなマネージドハンティングが、次世代エンドポイントセキュリティの要です。これがなければ、顧客は人員不足の社内チームだけで、不審な活動を 24 時間 365 日監視しなければならず、極めて巧妙な攻撃への対応方法についてのガイダンスもない状態になります。マネージドハンティングは、諦めない敵の創意工夫に対抗するため、エキスパートによる防御チームの知力を結集したものです。

CrowdStrike Falcon® プラットフォームは、ほかに例を見ないような脅威ハンティング専門チームを結成しており、このチームの存在と、Falcon によって収集された堅牢なデータを合わせることで、他のシステムやテクノロジーでは検知もできないような攻撃を阻止できます。

要素5：
脅威インテリジェンス

侵害を単独で阻止できる製品やサービスは存在しません。侵害の阻止には、人、プロセス、テクノロジー、インテリジェンスが必要であり、かつ、それらが連携する必要があります。

巧妙な敵は相手に気付かれずにすばやく動くことができるため、侵害を阻止し、その影響を最小限に抑え、最大の保護効果を得るためには、セキュリティチームがすべての防御機構を自動的かつ正確に企業全体に配備するために必要になるインテリジェンスを受け取る必要があります。

次世代のエンドポイント保護のアプローチを完全にサポートするためには、脅威インテリジェンスが、インシデントをより早く理解し、それに対応して解決するという戦術的優位性以上のものを提供する必要があります。また、セキュリティエキスパートが運用レベルでリソースの優先順位を付けるために必要となるプロアクティブなアラートやレポートも提供する必要があります。真の意味でインサイトに富んだ脅威インテリジェンスはそれだけにとどまらず、さらに、セキュリティリーダーが正しい意思決定を行い、固有のリスクに適応させたセキュリティ戦略を定義するために役立つ情報を提供しなければなりません。

ヒント：脅威インテリジェンスの価値は、組織を侵害からプロアクティブに保護するために必要となる、極めて正確でアクショナブルな最新情報を提供できることにあります。このような情報を提供するためには、脅威や敵に関すること、およびそれらを阻止するために必要となることを深く理解している必要があります。

だからこそ、次世代エンドポイント保護を探し求めるセキュリティ専門スタッフは、製品がセキュリティインフラストラクチャだけに特化しているのではなく、総合ソリューションの一部に脅威インテリジェンスも含まれていることを確認する必要があります。

必須要素を実現するために：
クラウドの力

次世代エンドポイント保護を構成するこれら 5 つの必須要素を効果的に実現する唯一の方法は、専門のクラウドアーキテクチャを利用することです。オンプレミスモデルは、複雑なデータセットをリアルタイムで収集して長期間保管し、その大量のデータを適切なタイミングで詳細分析して侵害を防止するといった極めて困難なタスクには不向きです。クラウドを利用すれば、ペタバイト規模のデータを数か月続けて保管し、実行されているあらゆる活動についての履歴情報を得ることが可能です。CrowdStrike Threat Graph を利用することで、これらの大量のデータストアを数秒で分析でき、IOA が検知されたときには進行中の攻撃を即座にブロックし、任意の時点でこれらの活動が組織環境内で発生したかどうかを遡って確認することができます。また、クラウドにより、複数の環境にわたってデータを蓄積し、多数の利用者の知識とインテリジェンスを存分に活用できます。

現時点で、多くのエンドポイントセキュリティ製品はクラウド対応だと主張していますが、実際には主にオンプレミスシステム向けに開発されたアーキテクチャをベースとしています。この「載せただけ」なクラウドモデルが専用のクラウドネイティブシステムのパフォーマンスに勝ることはありません。クラウド経由で接続されていても、ベンダーのデータセンター内に設置され、それぞれ隔離されたアプライアンスでは、クラウドソースの基本的なメリットを活用できません。「クラウドの力」を活用できるためには、多数の顧客のデータストリームを関連付けられる、真のクラウドモデルが必要になります。

次世代エンドポイントセキュリティを導入初日から提供

次世代エンドポイントセキュリティにおけるこれら 5 つの各基本要素は、多数のベンダーによって、ばらばらの状態でテストされ展開されています。防御だけに特化している企業もあれば、機械学習に力を入れている企業もあります。多くの企業は、1 ～ 2 つの限定的な検知技術に固執しており、次世代エンドポイントセキュリティに必要とされるすべての要素を 1 つの統合ソリューションとして提供できる企業は、CrowdStrike を除いて存在しません。

CrowdStrike のホリスティックデザイン（包括的設計）という考え方は、5 つの各要素がそろったときにのみ次世代エンドポイントセキュリティの効力が発揮されることを示しています。これらすべての要素が連携していなければ、次世代エンドポイント保護と呼ぶにふさわしくありません。

ほかのセキュリティベンダーによる、内部で分断された付加的なアプローチとは異なり、CrowdStrike の専用クラウドアーキテクチャは、IT ハイジーン、次世代 AV、EDR、24 時間 365 日のマネージドハンティングサービス、脅威インテリジェンスによる 1 つの統合プラットフォームによって、隠された攻撃をプロアクティブに探し出します。

攻撃のブロックと検知、および未発見の脅威の解明において極めて優れた性能を備えるほかにも、クラウドベースの Falcon プラットフォームは、軽量で迅速なデプロイメントも可能にします。ハードウェアや追加のソフトウェアを購入、設定、管理、アップデートする必要がなく、エンドポイントセキュリティの展開は簡単ですぐに完了します。オンプレミスシステムは展開の終了までに 1 年かかることもありますが、CrowdStrike はこれまで、数十万のエンドポイントで構成される環境の場合でも、わずか数時間で導入展開されています。CrowdStrike はクラウドアーキテクチャという性質上、既存のセキュリティソリューションと並行して容易に導入できるため、シームレスな移行が可能です。

CrowdStrike は、お客様の時間、労力、ビジネスプロセスへの影響を最小限に抑えながら侵害を即座に阻止するという最終目標を掲げています。究極的にはそれが次世代エンドポイント保護の定義になります。

侵害からの保護は継続的な戦いである。

次世代エンドポイント保護ソリューションが真の意味で効果を発揮するには、継続的に侵害からの保護を行う必要があります。これはつまり、防御、検知、可視化、インテリジェンスを常に提供して、侵害の発生前、発生中、そして発生後も保護するということです。

CrowdStrike の次世代エンドポイント保護は、これらすべての要素を 1 つの小さなエージェント内に統合し、クラウドによってサポートします。このエージェントは、エンドポイントやユーザーに影響を及ぼさずに数時間で導入展開することが可能です。CrowdStrike は、侵害を継続的に阻止できるからこそ、確固たる真の次世代エンドポイント保護ソリューションであると言えます。

次世代エンドポイントの評価基準

複数のソリューションの評価と比較に、以下の基準をご活用いただけます。
これらの基準は、CrowdStrike のセキュリティエキスパートが、
効果的な次世代エンドポイント保護ソリューションにとって不可欠だと考えるものです。

（当てはまるものすべてをチェックしてください）

次世代エンドポイント保護の評価基準

防御セキュリティとITハイジーン	CROWDSTRIKE FALCON ENDPOINT PROTECTION	ソリューション2	ソリューション3
ネットワーク上にいる人を常に表示	X		
ユーザーが実行しているアプリケーションのリアルタイム情報と履歴情報を表示	X		
ユーザーアカウントが使われている場所とその方法を表示	X		
保護と防御			
エンドポイント上で機械学習（ML）によって既知およびゼロデイのマルウェアから保護	X		
ランサムウェアから保護	X		
マルウェアだけでなくファイルレス攻撃（移動可能な*実行可能ファイルやその他のファイルを使わない攻撃*）からも保護	X		
既知および未知のエクスプロイトから保護	X		
進行中の攻撃を動的に阻止（*攻撃者が連鎖的攻撃の前段階を実行している場合に、権限のエスカレーション、ラテラルムーブメント、認証情報の盗難などの攻撃者の活動を阻止*）	X		
オンライン/オフライン、オンプレミス/オフプレミスでの保護	X		
検知と対応			
カーネルモードでの動作により完全な可視化に対応	X		
侵害を受けたシステムのネットワーク封じ込めを実行	X		
24時間365日の監視とプロアクティブハンティングを提供	X		
クイック検索機能を提供（*検索結果は5秒以内に表示*）	X		
フォレンジック			
効率的かつ迅速なフォレンジック分析を行うために必要なデータを記録	X		
どのデータが盗み出されたかを究明可能	X		
長期的なデータ保持機能を提供	X		
侵害を受けたシステムがアクセス不可の状態または破損した状態でもフォレンジックデータを提供	X		

次世代エンドポイント保護の評価基準

	CROWDSTRIKE FALCON ENDPOINT PROTECTION	ソリューション2	ソリューション3
製品の完全性			
攻撃前、攻撃中、攻撃後も保護	X		
セキュリティエキスパートによる24時間365日のマネージドハンティングと対処方法を含むアラートを提供	X		
自己完結型である *(完全な次世代機能を実現するための追加の製品、エージェント、モジュールは不要)*	X		
Windows、Mac、Linuxをサポート	X		
展開、管理の容易さ、ユーザビリティ			
完全なクラウドベースの管理と展開のオプションを提供	X		
インストールやアップデートでの再起動が不要	X		
数週間、数か月ではなく数日での完全な導入展開と運用開始が可能	X		
エンドポイント上では極めて小さいフットプリント *(検索の実行中を含め、常にCPU使用率が1%未満)*	X		
チューニングやエキスパートレベルの設定は不要	X		
INTELLIGENCEとINTEGRATION			
サードパーティのSIEMとの統合による自動IOC取り込み	X		
独自のインテリジェンスを提供(インテリジェンスが他のソースに依存していない)、更に他者との統合、拡張用のAPIを提供	X		
戦術的、運用的、戦略的な脅威インテリジェンスを提供	X		
アトリビューション(攻撃の特性、属性)を提供	X		

確認すべき事項

次世代エンドポイント保護
ソリューションの仕組みについて情報を得る
ための質問集です。これらの質問によって、
そのソリューションがどのようなタイプで
何を期待できるかを評価できます。

1. 製品は攻撃前、攻撃中、攻撃後の支援ができるか？
2. すでに侵害を受けていて、その侵害の後に製品を導入展開した場合に、製品は何ができるか？
3. 製品は、攻撃者がどのように環境にアクセスしているかを示せるか？どのような仕組みでそれを行っているか？
4. 製品は誰が攻撃しているかを示せるか？どのような仕組みでそれを行っているか？
5. 製品は将来の侵害について、保護、検知、管理をどのように行うか？
6. 製品の完全運用までにどれほどの期間がかかるか？
7. 社内チームが重要な事象を見逃した場合に、アラートや助言を受けることができるか？
8. 製品は、盗み出されたファイルの情報を示せるか？
9. マルウェアを使わない攻撃についてはどのように検知するか？
10. マルウェアを検知するためのテクノロジーはいくつ使われているか？
11. 製品は、盗難された認証情報の使用や権限の不正使用を検知できるか？
12. 防御、検知、対応のニーズすべてを満たすために、個別の製品 / モジュール / エージェント / アプライアンスはいくつ必要になるか？
13. 製品を導入するために、どのような追加のハードウェアやソフトウェア（サーバー、アプライアンス、データベースライセンス、エンドポイント上のコンポーネント）が必要か？それらは次世代エンドポイント保護ソリューションに含まれるのか、それとも追加費用がかかるのか？
14. ソリューションはエンドポイントのパフォーマンスにどのように影響するか？ディスク、メモリ、CPU のフットプリントはどの程度か？
15. ソリューションが自らを保護するために使っているセキュリティコントロールはどのようなものか？
16. ソリューションはほかのセキュリティツールやエンタープライズツールと統合するか？

CROWDSTRIKEについて

CrowdStrike® は、クラウドベースのエンドポイント保護のリーダー企業です。
CrowdStrike Falcon プラットフォームは企業全体のエンドポイントの状況を即座に
可視化し、ネットワークに繋がっているものだけでなく、繋がっていない
エンドポイントまでも保護します。

CrowdStrike Falcon は数分で展開でき、導入初日から対処方法を含むアラートや、
リアルタイムでの保護を実現します。
その中には次世代アンチウイルス、EDR、ならびに 24 時間 365 日体制の
マネージドハンティングサービスがシームレスに統合されています。
クラウドインフとシングルエージェントによるアーキテクチャは、複雑さを排除し、
拡張性、管理性、および速度を向上させます。

CrowdStrike Falcon は、シグネチャを用いない洗練された AI や IOA
（Indicator of Attack）による最先端の振る舞い検知技術を利用し、
既知の脅威と未知の脅威をリアルタイムで阻止し、あらゆる種類のサイバー攻撃
からお客様の環境を保護します。クラウド上に構築されたグラフデータベース、
CrowdStrike Threat Graph ™によって、世界各地からクラウドにアップロードされる
1 日たり 1,000 億件以上のセキュリティイベントを即座に相関分析し、
脅威を検知・防御します。


CROWDSTRIKE

CROWDSTRIKE

www.crowdstrike.com

詳細は、crowdstrike.com/sites/jp/ をご覧ください。
CrowdStrike Japan 株式会社
〒 100-0005
東京都千代田区丸の内 1 丁目 6-5