CrowdStrike テクノロジーパートナー

servicenow

CROWDSTRIKE

ソリューション概要

CROWDSTRIKEとSERVICENOWのセキュリティ機能連携

セキュリティとITの機能連携により
脅威と脆弱性の優先順位付け、対応、修復を促進

課題

あらゆる業界において、進化を続ける脅威が問題になっています。企業は、脅威への対応、脆弱なアプリケーションの可視化、アラートの優先順位付けを迅速化するためのリソースが不足していると感じています。標的型攻撃が増加の一途をたどる中、セキュリティチームは大量のアラートに忙殺されるようになり、異種のソースからのデータを結合して、インシデント対応作業に優先順位をつけることに苦労しています。

ソリューション

CrowdStrikeとServiceNowの連携により、セキュリティオペレーションの効率化が図られ、脅威や脆弱性の特定、優先順位付け、修復が迅速化します。セキュリティチームは、インシデントが侵害に発展する前に、すばやく修復作業を行うことができます。

ビジネス上の価値

ユースケース	ソリューション	メリット
インシデント対応の迅速化	CrowdStrikeとServiceNowは、両ソリューションを利用中のお客様が、エンドポイントのイベントデータをFalconプラットフォームからServiceNow Security OperationsのSecurity Incident Responseアプリケーションに送ることにより、インシデント対応のワークフローを自動化して、重要なインシデントを即座に特定し、優先順位をつけることを可能にします。	セキュリティ・インシデントの作成と優先順位付けを簡素化し、重要なイベントへの迅速な対応、緩和、修復を実現します。
インシデントに脅威インテリジェンスを付加	両ソリューションのお客様は、CrowdStrikeが持つIOC（侵害の痕跡）情報をServiceNow Security Operationsの一部であるServiceNow Threat Intelligenceアプリケーションに自動的に送信して参照することができます。IOCがセキュリティ・インシデントに関連付けられると、コンテキスト情報の取得やデータエンリッチメントが可能になります。	セキュリティ・インシデント内でのIOCの検知と相関分析を自動化することにより、実用的な脅威インテリジェンスが得られ、アナリストは攻撃や脅威に迅速に対応できます。
アプリケーションの脆弱性に対応	CrowdStrike Falcon Spotlight™は、エンドポイントの脆弱性をほぼリアルタイムで、スキャンレスかつゼロインパクトで評価し、可視化と拡張レポート機能を提供します。ServiceNowのVulnerability Responseとの連携により、リスクスコアが提供され、クラスに基づいた優先順位付けが可能になります。	セキュリティ上のギャップを可視化し、攻撃の標的とされる領域を把握できるため、対応時間を短縮して、より適切な判断をより迅速に行い、攻撃をプロアクティブに防御することが可能になります。
デバイスの健全性とIT管理の向上	エンドポイントデバイスの詳細がServiceNow CMDBにインポートされるため、可視性とコンテキストが向上し、エンドポイントランキングとの相関を1つのビュー内で表示可能になります。	理解しやすい資産データにアクセスして、攻撃対象領域の全体像を把握し、認識されたセキュリティギャップに対処することで、セキュリティとIT運用の両方の成果を向上できます。

主な利点

CrowdStrike Falcon®プラットフォームが検知したエンドポイントでの悪質なイベントアクティビティ情報を利用して、ServiceNow®内でのセキュリティ・インシデントの作成を自動化

CrowdStrikeが収集したエンドポイントでのイベント・アクティビティ情報を利用することで、ServiceNow内での調査を加速

Falconプラットフォームからのデバイス情報をServiceNow®Configuration Management Database（CMDB）とIdentification and Reconciliation Engine（IRE）を使用し、インシデント対応プロセスに連携することにより、脅威の優先順位付けと対応を加速

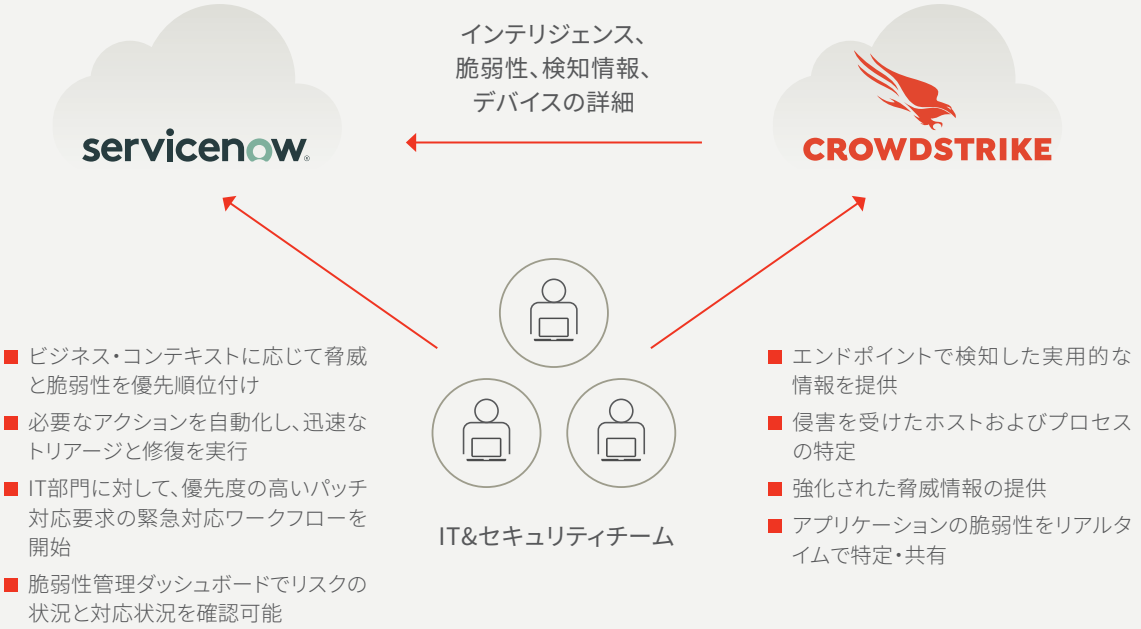
セキュリティチームによる迅速な修復を可能にし、侵害がもたらすダウンタイムと影響を最小限に抑える

CrowdStrike テクノロジーパートナー

CROWDSTRIKEとSERVICENOWのセキュリティ機能連携

テクニカルソリューション

CrowdStrike Falcon on ServiceNowでは、ServiceNow Security Incident Responseのインシデントを自動作成することにより、Falconプラットフォームからのアラートおよび検知データをセキュリティ・インシデント対応プロセスに連携する機能を提供します。CrowdStrikeが検知したエンドポイントでのセキュリティイベントは、ServiceNowに送信され、集中的な分析、ワークフローの自動化、対応の効率化の推進に活用されます。CrowdStrikeの脅威インテリジェンスが追加情報としてインシデントの範囲、攻撃者の属性に関するインサイトを提供し、ServiceNowのセキュリティ・インシデントを強化します。CrowdStrikeが収集したエンドポイントのイベントアクティビティを連携することで、ServiceNow内での調査と修復を加速します。



ソリューションの主な機能

1. Falcon Intelligence™は、重要な脅威アクター、攻撃ベクターおよび脅威インテリジェンスのトレンドに関する実用的な知見をServiceNow® Security Operationsに提供します。
2. CrowdStrike Falconは、次世代アンチウイルス、EDR、マネージド脅威ハンティングを組み合わせて、攻撃を検知・防御します。また、実用的なリアルタイムのイベントデータをServiceNowに提供して、さらなる分析と自動対応を可能にします。
3. Falcon Spotlightは、スキャンを実施することなくエンドポイントの脆弱性、さらに脆弱性対応でパッチ適用した状況の確認をほぼリアルタイムに特定し、可視化、拡張レポートを提供します。
4. ServiceGraph Connector for CrowdStrike on ServiceNowは、Falconプラットフォームから送信されるデバイスデータをインシデント対応プロセスに連携する機能を提供します。
5. ServiceNow® Security Operationsは、CrowdStrikeからほぼリアルタイムで特定される脅威インテリジェンスとエンドポイントのイベントアクティビティを利用し、ServiceNow Security Incident Response内で自動的にセキュリティ・インシデントを作成します。さらに、ServiceNow Vulnerability Responseのワークフロー、自動化機能、およびITとの緊密な連携とハイジーン機能が組み合わされ、重大な脆弱性への対応と修復を迅速化します。

CrowdStrike テクノロジーパートナー

CROWDSTRIKEとSERVICENOWのセキュリティ機能連携

SERVICENOWについて

ServiceNow（NYSE：NOW）は、人にしか出来ない、付加価値の高い新しい仕事を創造します。当社のクラウド型プラットフォームとソリューションは、従業員と企業双方に優れたエクスペリエンスを生み出し、生産性を高めるデジタルワークフローを提供します。

ServiceNowの製品であるServiceNow Security Operationsでは、Security Incident ResponseとVulnerability Responseの2つのソリューションが提供されています。これらはセキュリティチームとITチームが、インシデントや脆弱性により迅速かつ効率的に対応できるように設計されています。

詳細については、**https://www.servicenow.co.jp/** をご参照ください。

CROWDSTRIKEについて

CrowdStrike® Inc.（Nasdaq：CRWD）は、サイバーセキュリティのグローバルリーダーであり、セキュリティ侵害を阻止するためにゼロから構築したエンドポイント・ワークロード保護プラットフォームにより、クラウド時代のセキュリティを再定義しています。CrowdStrike Falcon®プラットフォームは、軽量なシングルエージェントによるアーキテクチャで、クラウドスケールの人工知能（AI）を活用し、リアルタイムで組織全体の保護・可視化を提供するとともに、ネットワーク内外でエンドポイントに対する攻撃を防止します。独自のCrowdStrike Threat Graph®を採用したCrowdStrike Falconは、世界で最も高度なセキュリティデータプラットフォームのひとつとして、世界中から取得した週5兆件超のエンドポイント関連イベントをリアルタイムで相関分析しています。

CrowdStrikeについて覚えておいていただきたいことはただ1つです。**「We Stop Breaches」**

次世代アンチウイルス
無料トライアルにアクセス

Crowdstrike.jp で詳細をご覧ください