

「IJ C-SOC サービス」の監視対象を拡大し

正規アカウントの悪用を検知する「アイデンティティ保護機能」を提供

ー EDR・ネットワーク監視と連携した分析で、脅威の早期発見とセキュリティ運用負荷の軽減を実現ー

当社は、セキュリティオペレーションセンター(SOC)でお客様システムのセキュリティログを 24 時間 365 日監視し、インシデント対応を行う「IJ C-SOC サービス」において、既存の「EDR(※)運用オプション」に、CrowdStrike 社の「CrowdStrike Falcon® Identity Threat Protection (ITP)」を活用したアイデンティティ保護機能を追加し、本日より提供開始します。

本機能は、ユーザの認証活動や権限変更などを継続的に監視し、認証情報の窃取や正規アカウントの悪用を起点とする攻撃の兆候を検知します。アイデンティティ情報だけでなく、ネットワーク、エンドポイントに関する監視情報も横断的に分析することで、単一の製品やログでは把握しにくい脅威を可視化し、脅威の早期発見を支援するとともにセキュリティ運用の負荷を軽減します。

(※)EDR(Endpoint Detection and Response): エンドポイント(PC やサーバなど)における不審な挙動を検知し、対応を支援するセキュリティ技術。

背景

近年のサイバー攻撃では、マルウェア感染や脆弱性の悪用だけでなく、窃取した認証情報や正規アカウントを悪用して組織内部へ侵入する手法が増加しています。攻撃者が正規ユーザとして振る舞うことで、従来のネットワーク監視やエンドポイント監視をすり抜け、管理者権限を奪う「権限昇格」や他の端末・サーバへ侵害範囲を広げる「横展開」にいたるケースが少なくありません。

このような攻撃への対策として、認証情報の利用状況やユーザの振る舞い、権限変更などを継続的に監視し、侵害されたアカウントの検知・対応を行う「ITDR (Identity Threat Detection and Response)」が注目されています。一方で、ITDR を有効に活用するためには、アイデンティティ情報に関するアラートを 24 時間 365 日体制で監視し、脅威を調査して対応を判断できる専門知識と運用体制が求められます。当社は、これまで「IJ C-SOC サービス」の「EDR 運用オプション」で、CrowdStrike Falcon によるエンドポイント監視を提供してきました。今回、ITP が検知するアイデンティティ脅威情報を新たに監視対象として追加し、ネットワークやエンドポイントの監視情報と相関分析することで、認証情報を悪用した攻撃への対策を強化し、お客様のセキュリティ運用負荷を軽減します。

アイデンティティ保護機能の特徴

1. 正規アカウントを悪用した攻撃を早期に発見

従来のマルウェア対策やネットワーク監視では検知が難しい、認証情報の窃取やアカウントの乗っ取りによる攻撃を監視します。Active Directory などの認証基盤の利用状況を継続的に分析し、不審な権限昇格や横展開などの攻撃兆候の早期に検知します。

2. ネットワーク監視・EDR と連携し、脅威を横断的に分析

IJ C-SOC サービスで取得するネットワークや CrowdStrike EDR の監視情報に、新たにアイデンティティ情報を追加します。複数の情報を組み合わせて相関分析することで、単一のログでは判断が難しい脅威を可視化します。

3. 専門アナリストが 24 時間 365 日監視し、迅速な対応を支援

検知したイベントは IJ C-SOC のアナリストが確認し、調査・通知・一次対応を実施します。お客様は

ITDR の専門人材や運用体制を自社で抱えることなく、高度なアイデンティティ監視を活用でき、本来の業務に注力しやすい環境を整えられます。

参考価格(税別)

300 ユーザの場合

費用区分	EDR 運用オプション(既存オプション)	アイデンティティ保護機能(今回追加分)
初期費用	1,183,600 円	769,340 円
月額費用	377,300 円	245,245 円

※上記価格にライセンス費用は含まれていません。

当社は今後、Active Directory に加え、Microsoft Entra ID や Okta など複数の認証システムへの対応を進め、製品を横断してアイデンティティ情報を統合的に分析できる SOC 機能を提供していきます。さらに、脅威インテリジェンスや AI 技術の活用、各種セキュリティ製品との連携強化を進め、ネットワーク、エンドポイント、アイデンティティ、クラウドなどの情報を統合的に分析する次世代 SOC に向けて、監視・分析・対応機能を拡充してまいります。

エンドースメント

株式会社インターネットイニシアティブによる「CrowdStrike Falcon(R) Identity Threat Protection (ITP)」を活用したアイデンティティ保護機能の提供開始を心より歓迎いたします。

サイバー攻撃は日々高度化・複雑化しており、企業はこれまで以上に迅速な検知と対応が求められる中、インターネットイニシアティブが既に提供されている IIJ C-SOC サービス EDR 運用オプションに加え、新たに提供されるアイデンティティ保護機能により、お客様のセキュリティ体制全体の強化に貢献されるものと確信しています。

クラウドストライク合同会社
代表執行役員社長 尾羽沢 功

報道関係お問い合わせ先

株式会社インターネットイニシアティブ 広報部 太田、増田

TEL : 03-5205-6310 FAX : 03-5205-6377

E-mail : press@ij.ad.jp URL: <https://www.ij.ad.jp/>

※本プレスリリースに記載されている社名、サービス名などは、各社の商標あるいは登録商標です。

※本プレスリリースに記載されているサービスの価格、仕様、内容などは発表日現在のものです。その後予告なしに変更されることがあります。