SOLUTION BRIEF

FortiRecon ACI で、差し迫った脅威や現在の脅威のコンテキストに基づく実行可能なインテリジェンスを獲得

概要

脅威インテリジェンスは、すべてのセキュリティオペレーションセンター（SOC）にとって重要な要件です。しかし多くの場合、組織のセキュリティチームは精選されたインテリジェンスを得ることなく、時間のかかる分析を自力で行うことで、実用的かつ意味のある情報を抽出しているのが現状です。

フォーティネットの DRP（Digital Risk Protection：デジタルリスク保護）ソリューションの一部である FortiRecon ACI（Adversary Centric Intelligence：アドバーサリーセントリックインテリジェンス）は、ダークウェブ、サイバー犯罪者のアンダーグラウンド、およびオープンソースインテリジェンス（OSINT）ソースを監視し、評価する FortiGuard の脅威エキスパートが提供するインテリジェンスであり、お客様の組織の代わりに、差し迫った脅威と不正に取得されたデータに関する情報を収集します。

「攻撃者について知れば知るほど、彼らの行動に的確に対応できるようになります。」[1]

鍵となる精選された脅威インテリジェンス

脅威インテリジェンスと見なされる情報量は近年飛躍的に増大しており、セキュリティチームはその量に圧倒されています。カスタマイズされた真に実行可能な情報を入手し、すばやく効果的な保護を実現することは、（不可能ではないとしても）非常に困難になっています。この増大し続ける問題を解決する鍵は、外部のソースから精選されたインテリジェンスを取得することです。このソースは、セキュリティチームが注目すべき重要情報を発見し、配信できるだけの処理能力と専門知識を備えている必要があります。このようなソースを利用することより、チームが処理する分量を削減できるだけでなく、組織を差し迫った脅威から守る対策をより迅速に実行できるようになります。

FortiRecon ACI で待望の実行可能なインテリジェンスを配信

FortiRecon ACI は、差し迫った脅威に関するコンテキストに基づいた実行可能なインテリジェンスを組織に提供します。これにより、迅速なインシデントレスポンスが可能になるとともに、攻撃者をより理解できるようになり、資産を守る能力が向上します。

ACI がカバーする対象は以下のとおりです。

- ダークウェブと他のアンダーグラウンドや招待制フォーラム
- オープンソースのインテリジェンスソース
- 代表的な脅威から新たな脅威に関する技術的な脅威指標
- 10 ヵ国語以上の多言語ソース

攻撃者に関する実行可能なインテリジェンスを活用することで、リスクをプロアクティブに評価し、既存のオンプレミス、クラウド、およびリモート環境の脆弱性を特定し、セキュリティ担当者の意識を向上させることができます。

ACI には、リサーチャーが外部非公開の招待制フォーラム、ダークウェブ、オープンソースなどに直接関わって入手したヒューマンインテリジェンス（HUMINT）も含まれます。ヒューマンインテリジェンスに取り組んでいる当社のアナリストは、特定のお客様に合わせたインテリジェンスの評価と精選も行い、ソースの信頼性と情報内の信頼性の評価レベルについて、アドミラルティ / NATO システムに従った信頼度の格付けを行います。

組織に提供されるインテリジェンスは、収集後に以下の条件に基づいてフィルタリングすることができます。

- 金融サービス組織の VPN や RDP へのアクセスを標的にする攻撃といった業界固有の脅威
- 地理的地域に固有の脅威
- 特定の組織に対する脅威（この種の脅威については即座にアラートが送信されます）

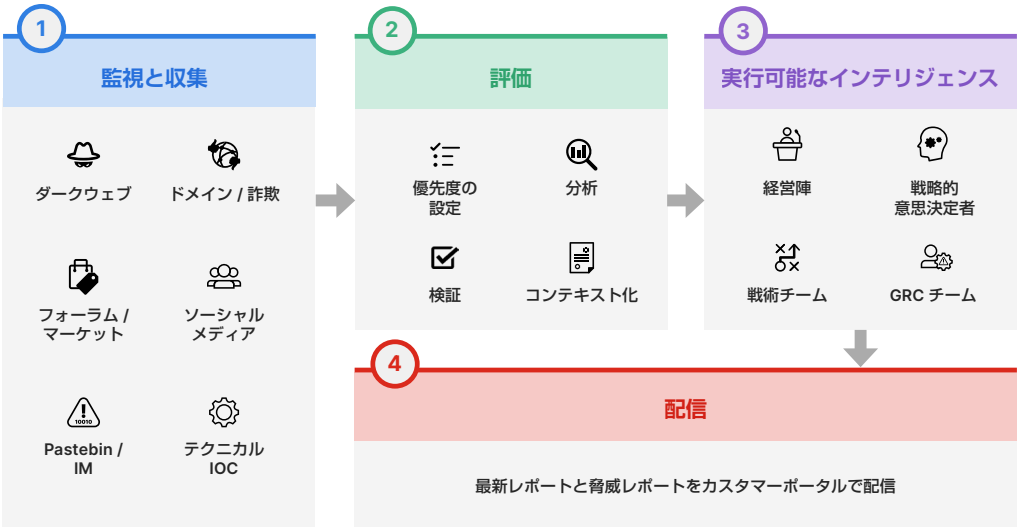
組織に対する脅威には以下のものが含まれますが、これらに限定されません。

- 認証情報の流出
- その他のデータ漏洩
- 現在よく利用されている脆弱性のエクスプロイト
- 新たな攻撃ベクトル
- 新たな TTP（戦術、手法、手順）

これらの脅威の例としては、以下のものがあります。

- 公開された S3 バケット
- ダークウェブで従業員のシステムへのアクセスを販売する攻撃者

金融サービス業界の場合、ACI にはクレジットカードの BIN の監視と、クレジットカード番号流出の最初の兆候が見られた際のアラート送信も含まれます。



FortiRecon ACI の特長

このように高度な技能を持つ熟練した脅威インテリジェンスチームによる支援は、以下の実現に役立ちます。

- 緊急の差し迫った脅威にすばやく直接対処
- 攻撃者の TTP に関する知識を活かして全体的リスクを軽減
- 脅威インテリジェンスの負担を軽減
- 限られたリソースを最も重要なことに集中
- 会社の SOC チームが通常行わないアンダーグラウンドへのアクセスと関与を外部委託

インテリジェンスは以下の内容で配信されます。

- 脅威を評価した詳細情報を提供する脅威レポートと、高度な脅威に対して防御するプロアクティブなアプローチを実装するための推奨事項
- FortiRecon のソースによって発見されたセキュリティの問題、脆弱性、エクスプロイト、そしてダークウェブへの広告の投稿に関するタイムリーな情報と調査速報を提供する脅威アラート

FortiRecon によるデジタルリスクからの保護

FortiRecon ACI は、FortiRecon BP（Brand Protection：ブランド保護）と FortiRecon EASM（External Attack Surface Management：外部攻撃対象領域管理）の両方とともにライセンス契約できます。FortiRecon BP、EASM、ACI が付属する FortiRecon の総合ソリューションには、以下の機能が含まれます。

- デジタル資産の検出、アンダーグラウンドや公開フォーラムでの情報漏洩の検知、ブランド攻撃などへの迅速なアクション
- アカウント、Web サイト、不正モバイルアプリケーションのテイクダウンサービス
- 必要に応じて「外部から内部の」可視化を可能にする柔軟なライセンス
- 直感的 GUI（グラフィカルユーザーインタフェース）によるエグゼクティブレベルからテクニカルレベルまでのビュー
- 脅威とインシデントに関する専門知識の提供（FortiRecon アナリストによる追加の解析からインシデントレスポンス / 評価サービスまで）

FortiRecon ACI の利点

- 精選されたインテリジェンスによって、分析から対応までの時間を短縮
- 組織、その業界、地域に固有の脅威に関するインテリジェンス
- OSINT と非公開ソースの両方から幅広くインテリジェンスを収集
- 脅威の戦術、アクター、およびエクスプロイトと流出データに関する知識の向上

フォーティネットによる包括的なセキュリティとサービスの提供

フォーティネット セキュリティ ファブリックは、FortiGuard 脅威インテリジェンスによる最新の保護を活用することで、攻撃ライフサイクルのあらゆる段階でエンドツーエンドのセキュリティを実現します。FortiGuard Labs 脅威リサーチチームは、オンデマンドの分析、評価、対策サービス、訓練も提供しており、豊富な知識と経験を活用して、世界中の数十億の脅威イベントを収集して分析し、関連性を特定します。これらの豊富な専門知識、経験豊富なダークウェブの研究者、多言語のインテリジェンス収集、HUMINT（ヒューマンインテリジェンス）のスペシャリストが協力してサービスを提供することにより、限定フォーラムや招待制フォーラムを含む最新の脅威活動に関する脅威インテリジェンスやデータへの比類ないアクセスが可能になります。生成される FortiRecon レポートのほぼ 4 分の 1 は、このサービスで収集されたヒューマンインテリジェンスのみに基づくものであり、リスクの最も現実的なビューを提供します。

終わりに

FortiRecon ACI は、精選された実行可能かつタイムリーなインテリジェンスを提供し、組織のセキュリティの確保、迅速な行動、そして最も重要かつ重大なリスクへの集中を可能にします。FortiRecon の詳細については、当社の Web サイトをご覧ください。

[1]「Intelligence-Driven Incident Response: Outwitting the Adversary」、Scott J. Roberts および Rebekah Brown著、O'Reilly Media, Inc.、British Assessment Bureau、2021年11月29日（英語）

フォーティネットジャパン合同会社

〒106-0032
東京都港区六本木 7-7-7　Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ

SB-FortiRecon-ACI-202211-R1