ATLAS® インテリジェンス・フィード（AIF）

セキュリティ脅威と可用性脅威への的確な対応

主な特長とメリット

精度の高い防御のための動的な更新

AIF は、最新の脅威情報によって常時更新することによって、Arbor Networks の全製品を通して検知ポリシーの精度を常に最大限に高めています。

キャンペーンベースの攻撃特定

マルウェアの特性に焦点をあて、各種の情報源からの攻撃データと組み合わせることよって、AIF は攻撃ポイントのみならず、キャンペーンの一部として仕掛けられる関連する攻撃を特定します。

攻撃への迅速な対応

AIF ポリシーは、攻撃に関する経緯などのコンテキスト情報を提供することで、的確な情報に基づいた迅速な対応を可能にしています。

脅威検証と優先度付け

脅威データの収集と分析に加えて、ASERT は、脅威の現状および実態にまで踏み込んで脅威の検証と優先度付けを行います。

セキュリティの脅威は、さまざまな形態を取って侵入してきます。ネットワークを停止に追い込むことから、ネットワークやデータの不正使用、さらにはデータの窃盗まで多岐にわたります。今日の企業にとって、ますます組織化し、巧妙化する高度な攻撃に対して万全の防御対策を施すことは最重要課題になっています。有効な脅威インテリジェンスは、攻撃者が仕掛ける巧妙さの進化のスピードに追随し、このリスクをミティゲーションするには、必須になってきています。有効な脅威インテリジェンスがあれば、セキュリティ担当者は発見した脅威に対して、自信を持って意思決定し、的確な行動を取ることできます。さらに、セキュリティ・チームを強化します。脅威に対する深度の深い考察を可能にし、リスクを迅速に特定することができます。これによって、セキュリティ・チームは企業にとっての貴重な人的資産として認識されるようになります。

高度な脅威への対処

ATLAS インテリジェンス・フォード（AIF）は、高度な脅威を構成する各種の攻撃にすばやく対処するためのポリシーと防御策を提供します。AIF は Arbor Security Engineering & Response Team (ASERT) のサービスの 1 つであり、Arbor の広範囲におよぶ深度の深いリサーチ力の恩恵を直接手に入れることを可能にします。

Arbor Networks は、エンタープライズおよびサービスプロバイダーの両ネットワークに対応する優れた製品ポートフォリオを提供しています。これらの全製品は、AIF のメリットを受けることができます。新たな攻撃の情報が入ると AIF がアップデートされ、変更内容はセキュアな SSL 接続を介してしてサブスクリプションにより Arbor 製品に自動的に配布されます。この最新の脅威インテリジェンスを活用することで、今発生している高度な脅威や攻撃を防止することができます。脅威から企業を守る最善の方法は、熟練したエキスパートによって精査された広範囲な視点からの最新の知見を持つことです。これが、ATLAS インテリジェンス・フォード（AIF）です。

効果的な脅威インテリジェンス・フィードの力

効果的な脅威インテリジェンスには、3 つの要件があります。

- 継続的収集されるネットワーク・トラフィックおよび脅威の実データ・ソース
- ネットワーク・トラフィックおよび脅威データを収集するための堅牢なインフラ
- 上記 2 つの運用管理と”ヒューマン・インテリジェンス”の脅威分析への追加を可能にする選任チーム

実際に使える脅威インテリジェンスは、単なる脅威データの収集と分析を超えるものでなければなりません。情報を行動に変え、有効化するには、自社のセキュリティ体制とのシームレスな統合が必要になります。これによって、個々の脅威からのリスクが特定され、実際に取るべく行動が明確に理解できるようになります。

ARBOR® NETWORKS
The Security Division of NETSCOUT

DDoS やボットネットから企業を防御するAIFの特長

AIF は、Arbor Networks の顧客によってその有効性が実証されています。大規模化・巧妙化する標的型・複合型の高度な脅威を防御しています。

さらに正確に脅威を検出するために、AIFは次のことを可能にします。

- 攻撃のボリュームを問わず、ボリュームしきい値に達する前に、脅威を特定。
- 信頼性に応じてさまざまなレベルの防御を適用。
- 数百万ものマルウェア・サンプルを使って制御下で試された検証に基づいて、攻撃インテリジェンスを適用。
- ボットネット関連のすべてのマルウェアにほか、特定のマルウェアのリバース・エンジニアリングに対応。
- Arbor のグローバルなセンサー・ネットワークを活用して、インターネット上の脅威を 24 時間体制で監視。
- 継続的に、ボットネット、そのロケーションおよび攻撃方法を時系列に追跡管理。
- ATLAS は 、匿名のトラフィック・データを Arbor Networks と共有することに同意していただいた 300 社を超えるお客様との共同プロジェクトであり、全インターネット・トラフィックの約 3 分の 1 に相当するデータを収集しています。

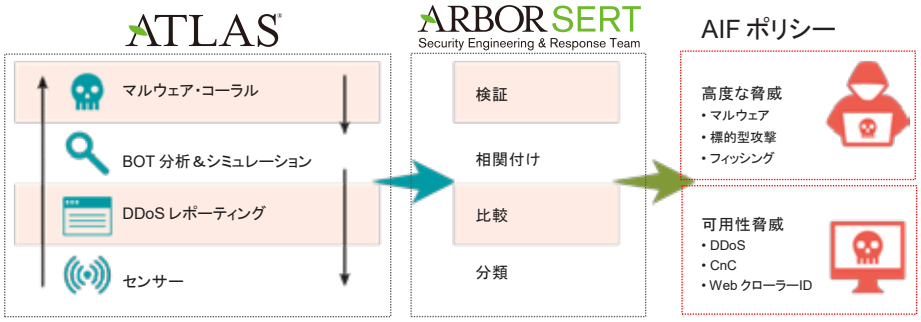

図 1ATLAS は、さまざまなツールやプロセスを使って、脅威データを収集・解析しています。ASERTは、攻撃の能力および潜在性に焦点を絞り、攻撃キャンペーンの複数の兆候を見つけ出します。これらの兆候のインジケータが、ATLASインテリジェンス・フィードを介してすべての Arbor 製品へ提供されています。

Arbor が誇るワールドクラスのセキュリティリサーチ・チームは、新たに発生するイン ターネット上の脅威の分析および発見に加えて、ターゲットを絞った防御策の開発を専門的に行っています。Arbor は、高度な脅威の検知だけでなく、的確な情報に基づいたミティゲーションの判断に必要な、攻撃に関する経緯などのコンテキスト情報を提供するために、攻撃データの収集やパートナー情報連携・分析といった各種ツールを組み合わせて AIF ポリシーを作成しています。

AIF をサポートする主要テクノロジーの 1 つに、Arbor の動的なレピュテーション・インテリジェンスがあります。レピュテーション・インテリジェンスは、AIF ポリシーを形成する脅威インジケータの検証となります。ASERT はトラフィックおよび脅威データを収集する一方で、マルウェアの攻撃手法を含む、攻撃のさまざまな要素を一元化することを可能にしています。しかしながら、まだ表面化していない脅威を未然に防御するためには、レピュテーション・インテリジェンスには、特定の IP、DNS または URL がいつ、どれくらいの期間、攻撃されたのかを明確に実証することが求められます。的確な AIF ポリシーは、信頼性評価スコアを通して、攻撃検証が追加されています。Arbor 製品に提供されるそれぞれの AIF フィードにはこのタイプの攻撃検証が信頼性評価スコアとして提供されているため、ユーザーは Arbor 製品によって特定される脅威の重大度と可能性を明確に判断することができます。

ATLAS インテリジェンスの適用

Arbor Networks のポートフォリオに含まれる製品は、AIF を活用するように設計されていますが、各製品は、その用途に合わせて、AIF の異なる部分を活用しています。NetFlow を分析する製品もあれば、ネットワーク・パケットに注目する製品もあります。AIF 内のポリシーには、それぞれの製品に対して的確な情報が含まれます。

Arbor Networks® APS

APS は、帯域幅のしきい値に基づいて可用性の脅威をブロックするだけでなく、AIF ポリシーを使用して、アプリケーション層を狙った「ロー・アンド・スロー（低帯域幅、低速度）」の攻撃を含む各種 DDoS 攻撃を特定します。これに加えて、AIF は、APS が特定のタイプのボットネットを検知し、ネットワークの侵害を防止するのにも役立ちます。このような可用性の脅威やボットネットの脅威がネットワークに侵入するのを阻止することで、これまで必要であったセキュリティ・デバイスを不要にします。

Arbor Networks® Spectrum

Spectrum 内の ATLAS セキュリティ・インテリジェンスによって、フォレンジクス分析のために攻撃イベントに対する深度の深い考察を可能にします。リスクを迅速に特定することができます。AIF で提供される攻撃インジケータによって、どの攻撃がネットワーク内で発生または発生する可能であるかに加えて、どこに拡がっているかを特定することができます。さらに、企業内の最も重要な資産に対するトラフィックをこの脅威情報にオーバーレイすることができます。また、コンテキストやその他の情報も提供されるため、詳細な調査に向けたイベントのエスカレーションに役立てることができます。

Arbor Networks® SP

AIF からのセキュリティ・インテリジェンスによって、SP の顧客は社内または顧客へのサービスに影響が出る前に大規模 DDoS 攻撃を迅速に検知することが可能になります。

Arbor Networks® TMS

TMS で使用する AIF ポリシーは、DDoS 攻撃をすばやく確実にブロックするための詳細情報を提供します。悪意ある攻撃は多大なコストを伴うダウンタイムを発生させる可能性があり、これをブロックするにはこの正確さが不可欠です。この AIF は、Cisco ASR 9000 DDoS 防御製品にも同一レベルの防御を提供しています。

ATLAS インテリジェンス・フォード（AIF）の詳細

AIF には 2 つのサブスクリプション（スタンダードとアドバンスド）が用意されています。この 2 つのサブスクリプションによって、自社のニーズに合った攻撃検知/防御レベルを選択することができます。

AIF スタンダード

スタンダード・フィードによって、マルウェアやボットネット、サービス拒否（DoS）など、企業を標的とする今日の最も一般的な攻撃を検知し、これに対処できます。ポリシーと防御策は常時アップデートされ、新しい攻撃の情報を入手できるため、広範囲の正確な検知が可能になります。このフィードに含まれるポリシーおよび防御策の例は以下のとおりです。

脅威ポリシーのタイプ			APS	Spectrum	SP	TMS**
コマンド &コントロール	• ピアツーピア • HTTP • IRC		○	○	○	
DDoS レピュテーション脅威	• 攻撃者 • 標的		○	○	○	
マルウェア	• Webshell • ランサムウェア • RAT • 偽装アンチウイルス • バンキング • 仮想通貨 • スパイウェア • ドライブ・バイ • ソーシャルネットワーク	• DDoS ボット • ドロッパ • 詐欺広告 • ワーム • 認証情報窃盗 • バックドア • エクスプロイトキット • POS • その他	○	○	○	
IP地理ロケーション	• インバウンドのソースに対して国別にロケーションを特定 • アウトバウンドトラフィックのデスティネーションに対して国別にロケーションを特定		○	○	○*	○
DDoS RegEx	• ATLASから入手したIPアドレスに基づいてDDoS 攻撃者を特定 • ATLAS HTTP Flooder から入手した兆候に基づいて DDoS 攻撃者を特定		○			○
Web クローラーの特定	既知の検索エンジンからの Web サービスへのインバウンド接続を特定		○			
ET Pro SA導入時の標準	• IDS シグニチャ			○		

* 製品パッチを介して SP、TMS および Cisco ASR 9000 DDoS 防御製品にアップデートされる IP 地理ロケーション。
** TMS 内で使用される AIF ポリシーは、Cisco ASR 9000 DDoS 防御のためのものと同一です。

図 2：AIF スタンダード・フィードを使って特定された脅威の例すべての防御策およびポリシーは常時アップデートされるため、上記のリストは随時変更されます。

高度な脅威への取り組みにおける Arbor 独自のポジショニング

Arbor は、長年にわたり、ボットネットに関する調査研究や DDoS ミティゲーションに取り組んできました。

DDoS は日々進化しています。サイバー犯罪や APT 攻撃に用いられるマルウェアやボットネットのいわば分派から主力の攻撃となっています。この中、Arbor は ASERT チームとそのリサーチカを拡張し、新たに生まれる脅威を特定し、分析してきました。ASERT の脅威インテリジェンスへのアプローチには、脅威の特定を支援するだけではなく、その蔓延度や重大度を確認するなどの、次のような各種の要素が含まれています。

- Red Sky Alliance などの有用なパートナーシップ。これを通じて、2,300 万台以上の PC にアクセスし、その徹底解析よって集積された脅威インテリジェンスを活用。
- Red Sky Alliance から入手した実環境でのインジケータに基づいて攻撃キャンペーンを追跡するとともにレピュテーション監視を実施。
- 外部パートナーのテクノロジーと自社構築のる分析/プロセスの両方から構成される高度なマルウェア分析バックエンド・システムを活用。

これらの脅威データと分析を活用して、ASERT が AIF を作成します。Arbor のお客様はこれを使用して、自社のネットワークやその周辺で発生するイベントを検知することがかのうです。ネットワークに関するミクロな視点と、ATLAS ポータルを介して提供されるグローバルなインターネット・トラフィックに関するマクロな視点を組み合わせ活用することにより、高度な脅威への対処における優位性を手にすることができます。

AIF アドバンスド

アドバンスト AIF は、検知が困難なステルス型の攻撃が懸念される場合に最適です。このフィードのサブスクリプションを利用すれば、スタンダード・フィードに含まれるすべての防御策およびポリシーのほか、キャンペーン型の持続的な攻撃などの攻撃パターン（特定の企業を標的とする高度にカスタマイズされている上、正規のアクセスに見えるために検知が困難）を発見するための追加ポリシーをご活用いただけます。このサブスクリプションに含まれる防御策とポリシーの例は以下のとおりです。

	脅威ポリシーのタイプ	APS	Spectrum	SP	TMS
ロケーションに基づく脅威	• トラフィック匿名化サービス • TOR • プロキシー • シンクホール • スキャナー • その他	○	○		
メール脅威	• スパム • フィッシング	○	○		
標的型攻撃	• APT • ハクティヒズム • RAT • ウォータリング・ホール • ルートキット	○	○		
モバイル	• モバイル C&C • スパイウェア • 悪意あるアプリ	○	○		

図 3AIF アドバンスド・フィードを使って特定された脅威の例すべての防御策およびポリシーは常時アップデートされるため、上記のリストは随時変更されます。アドバンスド・サブスクリプション内のポリシーは、SP、TMS または Cisco ASR 9000 DDoS 防御では現在、利用することができません。

ARBOR NETWORKS

The Security Division of NETSCOUT

本社
76 Blanchard Road
Burlington, MA 01803 USA
米国内通話料無料：+1 866 212 7267
TEL：+1 781 362 4300

北米
米国内通話料無料：+1 855 773 9200

ヨーロッパ
TEL：+44 207 127 8147

アジア・パシフィック
TEL：+65 6664 3140

日本
〒101-0063
東京都千代田区神田淡路町 2-105
ワテラス アネックス 13 階
TEL：03 3525 8040
お問い合わせ japan@arbor.net

www.arbornetworks.com