報道関係各位

2014 年 3 月 19 日
アーバーネットワークス株式会社

Arbor Networks、高度な脅威検知、インシデント対応、セキュリティ検証の機能を備えた Pravail® Security Analytics を発表

30 日間の無料トライアルを実施

米国マサチューセッツ州バーリントン、2014 年 3 月 19 日－エンタープライズやサービス・プロバイダーのネットワーク向けに分散型サービス拒否（DDoS）攻撃や高度な脅威の対策ソリューションを提供するリーディング・プロバイダ Arbor Networks, Inc.（以下「Arbor Networks」）は、本日、高度な脅威検知、インシデント対応、およびセキュリティ検証の機能を備えた Pravail Security Analytics を発表しました。このソリューションを実現させた技術は、Arbor Networks が 2013 年 9 月に買収したオーストラリア・シドニーを拠点とするビッグデータ・セキュリティ分析の分野のイノベーター企業、Packetloop 社が開発したものです。

Arbor Networks プレジデントのマシュー・モイナハン（Matt Moynahan）は、「Arbor は企業のセキュリティ・チームに、自社ネットワークで起こっている活動に関する最も詳細なデータを提供します。Pravail Security Analytics は、お客様が自社のグローバル・ネットワークへの攻撃をかつてなく早くかつ詳細に把握することを可能にする、強力なソリューションです。私達は大量のデータに意味のある前後関係を与えることで、セキュリティ・チームがごく一部の重要なデータに的を絞ってより素早く対応し、自社ネットワーク環境内にはびこる脅威が業務に影響を与える前に、その脅威を特定できるようにすることを重視しています」と述べています。

グローバルな攻撃インテリジェンスによるローカルな保護

Pravail Security Analytics を常にネットワーク・セキュリティの最先端に維持している攻撃インテリジェンスは、Arbor Networks の ATLAS®（アクティブ・スレット・レベル・アナリシス・システム）を基盤としています。ATLAS はグローバルなインターネット・トラフィック上で Arbor Networks と最大 70TB/秒の匿名データを共有する、全世界 300 社近くのサービス・プロバイダーとの協力関係により実現されたシステムです。この包括的な視点により、攻撃の状況に関するグローバル規模での見識が得られるのです。このデータセットを Arbor Networks のセキュリティ研究チームが分析し、そこから検知方法を開発して、企業内で発生する脅威や悪意ある活動を識別するためのフィンガープリントを作成しています。

企業のグローバル・ネットワークに潜む攻撃を発見する

昨今の攻撃者は、短期的な目に見える邪魔者となることを目指してはいません。代わりに陰湿な洗練された手法を用いて組織を周辺から蝕んでくるため、障害の兆候は状況が手遅れになるまで発見できない場合が多いのです。微妙かつ高度な標的型攻撃を真に理解するためには、企業がすべてのネットワーク・トラフィックの完全な記録を保持する必要があります。データを非常に高速に分析できる Pravail Security Analytics は、リアルタイムな攻撃への対応決定に利用できるほか、データを将来の確認のため保存することで、最新の脅威インテリジェンスを使用して以前は検出されなかった攻撃を特定できるようにします。

IDC のセキュリティ製品担当リサーチ・マネージャであるジョン・グレイディ氏は、「各組織は自社ネットワーク内に潜む高度な脅威の問題への対処に役立つソリューションを求めています。Arbor Networks の Pravail Security Analytics はセキュリティ・アナリスト向けの強力なプラットフォームで

あり、膨大な量のデータを処理して、リアルタイムと履歴の両方のデータセットに潜む脅威を暴く直感的な視覚化機能により、実施可能なインテリジェンスを提供してくれます。Arbor Networks は現在、NetFlow、パケット・キャプチャ、および ATLAS インフラストラクチャによるグローバルな脅威インテリジェンスをユニークに組み合わせたソリューションを提供しており、シグニチャベースのソリューションをくぐり抜ける昨今のダイナミックな脅威に対処しています」と語っています。

オンプレミスまたはクラウド内での迅速な展開

Pravail Security Analytics はビッグデータ技術を活用しているため、世界一流のセキュリティ分析ソリューションを展開し運用したいと考えている組織にとっては、導入の敷居が低くなっています。組織ではパケット・キャプチャをクラウド内の Pravail Security Analytics に安全にアップロードして、脅威が特定されてから数分のうちにデータの分析を開始できます。法令順守関連の問題でパケット・キャプチャをアップロードできない組織の場合は、コレクター・アプライアンスを使用して Pravail Security Analytics をオンプレミス・ソリューションとして展開することも可能です。コレクター・アプライアンスを利用すれば、ストレージや高速キャプチャ・ポイントの処理機能をスケールアウトしたり、複数の場所に展開して分散カバレッジを実現したりもできます。

- クラウドのみ – キャプチャをクラウド内の Pravail Security Analytics にアップロードして、ストレージ、処理、分析を行うことができます。
- オンプレミス – すべてのキャプチャ、ストレージ、処理、および分析は、Pravail Security Analytics コレクター内に保管されます。
- クラウド/オンプレミス – Pravail Security Analytics コレクターはキャプチャ、ストレージ、および処理のため組織のネットワークに展開され、分析データは分析と可視化のためクラウド内の Pravail Security Analytics に送信されるという構造のハイブリッド・モデルです。

既存のデータセットを活用したクラウド・ソリューションの製品デモンストレーションが用意されています。ユーザーはこれを利用してソリューションを試用し、その強力な機能を実際に体感してみることができます。

クラウド・ソリューションの無料トライアルも用意されているため、自社のネットワーク・パケット・キャプチャを脅威、異常、誤用などについて素早く分析できます。無料トライアルでは、30 日間で最大 1GB のデータをアップロードできます。

Pravail Security Analytics オンプレミス・ソリューションの一般公開は 2014 年 4 月 30 日を予定しています。

Arbor Networks について

Arbor Networks は DDoS 攻撃や高度化する脅威から世界の大手企業および大手サービス・プロバイダーのネットワークを安全に守ることを支援しています。Arbor Networks は全世界のエンタープライズ、キャリア、モバイルの市場において DDoS 保護ソリューションを提供する世界をリードする主要ソリューションプロバイダーです（Infonetics Research 社調べ）。高度化する脅威に対する Arbor Networks のソリューションは、パケットキャプチャと NetFlow 技術を組み合わせることで、ネットワーク全体を可視性し、マルウェアや悪意のあるインサイダーの脅威を迅速に検出し、削除することを可能にします。Arbor Networks はまた、動的なインシデント対応、履歴分析、視認性、フォレンジクスについても市場をリードする分析機能を提供しています。Arbor Networks は、企業のネットワークやセキュリティの担当者がセキュリティのエキスパートになり、企業のセキュリティ強化を実現することを目指しています。Arbor Networks の目標は、お客様がセキュリティ問題を迅速に解決し、事業リスクを低減できるよう、ネットワーク上の脅威の視認性とセキュリティ・インテリジェンスの提供を可能することです。

Arbor Networks の製品およびサービスについて詳しく知りたい方は、Arbor Networks の日本語サイト www.arbornetworks.com/jp/ を参照してください。また、業界唯一の革新的なインターネット監視システム ATLAS®のデータに基づく調査、分析および知見については、ATLAS セキュリティポータル（英文）をご覧ください。