Press Release

2015 年 4 月 15 日

本リリースは、米国 Blue Coat Systems, Inc.が米国時間 2015 年 3 月 24 日に配信したリリースの抄訳です。当資料の正式言語は英語であり、その内容および解釈については英語が優先されます。米国で発表されたリリース（英文）につきましては、該当のプレスリース【https://www.bluecoat.com/company/press-releases/blue-coat-global-intelligence-network-enables-customers-more-effectively】をご参照ください。

ブルーコート、Global Intelligence Network の統合を発表
高度な脅威に対し、これまで以上に効果的な防御、検出、対応を実現

製品ポートフォリオとリサーチラボの統一で、インターネット／マルウェアの脅威に対するインテリジェンスが 1 つに ー かつてない強固な保護環境とセキュリティ総費用の削減を実現

ビジネス・アシュアランス・テクノロジーのマーケットリーダーであるブルーコートシステムズ合同会社（本社：東京都港区、以下ブルーコート）は本日、クラウドベースの Global Intelligence Network を同社の全製品ポートフォリオに組み込まれ統合されたことを発表しました。これには、先頃同社が買収した Norman Shark 社のサンドボックステクノロジーと Solera Networks 社のフォレンジックおよびインシデントレスポンス製品も含まれています。これで、同社の全ての製品が脅威に関する情報を継続的に送受信できるようになり、セキュリティ担当者はリアルタイムに情報を入手することで、これまで以上に効果的に脅威を防御することが可能になります。また、この統合によって攻撃を減少させ、より効果的な高度な脅威防御（Advanced Threat Defense）を実現します。

Global Intelligence Network が収集した蓄積型インテリジェンスによって、ブルーコートの導入企業は先回り的に脅威をブロックし、誤警報（フォールスアラーム）につながるサンプルを減らし（99.9%の減少）、潜在的に最も破壊的な影響をもたらす恐れがある脅威をピンポイントに識別して対応しながら、様々なコストを削減することが可能になります。

先頃 Ponemon Institute が実施したリサーチには次のように述べられています。「セキュリティスタッフがマルウェアのアラートへの対応に費やしている時間の 3 分の 2 が、誤った情報への対応です。このようにマルウェアの誤警報や不正確なアラートへの対応に費やされている時間に伴うコストは、年平均で 127 万米ドルに上ります。」ブルーコートは既知の脅威と未知の脅威の両方に対して最高レベルの精度で防御し、企業は誤警報とその対応に要するコストを削減することが可能になります。

ブルーコートの社長兼 COO（最高執行責任者）、マイケル・フェイ（Michael Fey）は次のように述べています。「積極的な製品開発と企業買収によって、ブルーコートの製品群は個々の製品がそれぞれ互いに補完し合いシナジーをもたらして、製品全体のポートフォリオが強化されました。これは、買収と R&D の成果を最高レベルにまで高めたと言えるでしょう。これによって、企業は可視性と高度な脅威防御の両方において、ネットワーク全体を網羅した業界で最もパワフルなソリューションを手にすることができます。より明瞭な可視性、また未知の脅威からもほぼリアルタイムに防御できる環境など、これほど高いレベルの保護環境を 1 社で提供できるベンダーは、ブルーコート以外に存在しません。」

製品の統合に加え、ブルーコートは情報セキュリティの主要な分野で世界クラスの経験とノウハウを有する複数のリサーチャーを迎え、脅威に対するリサーチ能力をさらに強化しました。この Blue Coat Labs では、世界 15,000 社を超える企業からの蓄積型ユーザーエクスペリエンスを活用するブルーコートの WebPulse リサーチに、Norman Shark 社からはマルウェア分析、また Solera Networks 社からはセキュリティアナリティクスについての新しい経験とノウハウ、テクノロジーを統合します。これによって、急速に変化しつつある脅威に対し、リアルタイムの保護を実現する他に類を見ない環境が実現されました。この環境は、既知の脅威と新しい脅威の 99%以上を防御する能力を保持しています。このような高精度の防御を可能にすることで、高度な脅威

のペイロードは劇的に減少し、サンドボックスソリューションでのマルウェア検出に必要な容量を少なくすることができ設備投資の削減が可能になります。

ブルーコートならではの脅威を可視化するアプローチは、ユーザー保護と業界への周知を図るための新しい脅威のリサーチに貢献してきました。たとえば Blue Coat Labs は、軍や外交官、企業役員などをターゲットにした非常に高度な多層化マルウェア攻撃「The Inception Framework」を発見しました。

ブルーコートシステムズについて
ブルーコートは、セキュリティを確保することにより、あらゆるアプリケーションや、サービス、デバイスを安全に活用して、生産性を向上することを可能にし、お客様の創造性、コミュニケーション、コラボレーション、イノベーション、実行力、競争力を強化して、ビジネスを活性化するためのソリューションを提供します。
詳細は www.bluecoat.co.jp をご覧ください。

本件に関する報道関係者問い合わせ先
ブルーコートシステムズ　広報代理
株式会社旭エージェンシー
担当：笠羽・高木
Tel: 03-5574-7890
Fax: 03-5574-7887
E メール：bluecoat@asahi-ag.co.jp