

報道関係各位

株式会社セキュアブレイン

セキュアブレインがエンドポイントへのサイバー攻撃を監視するSOCサービスを10月より販売開始

株式会社セキュアブレイン(本社:東京都千代田区、代表取締役社長 兼 CEO:新保 勲、以下「セキュアブレイン」)は、企業・組織のエンドポイントへのサイバー攻撃を監視するSOC(Security Operation Center)サービスを2017年10月より販売開始します。SOCサービスの第1弾として、米国Cisco Systems社のクラウドベースエンドポイント次世代マルウェア対策ソリューション「Cisco AMP for Endpoints(シスコ・アンプ・フォー・エンドポイント)」を使用し、セキュアブレインSOCにおいてリモート監視を行うエンドポイント監視サービスを提供します。

近年のサイバー攻撃は巧妙化しており、侵入を完全に防ぐことが難しいため、侵入されることを前提とした対策が必要になっています。しかし、特定の企業や組織を狙った標的型攻撃によって未知のマルウェアに感染した場合、社内ネットワークのPCからマルウェアの検体を特定することは非常に困難です。検体特定の調査に時間がかかると感染拡大や情報漏えいの恐れがあります。近年、重大事件の発生により、企業・組織は社内CSIRTを設置する動きが出てきていますが、セキュリティのスキルの高い人財の確保やコスト面など、自社ですべてのセキュリティ対策を講じるには多くの問題があります。

このような状況を受け、セキュアブレインは、従来のSOCサービスでは対応できなかったゲートウェイをすり抜けたマルウェアによる攻撃の分析を行うことが可能なSOCサービスの販売を開始します。エンドポイント監視に使用するCisco AMP for Endpointsは、マルウェア感染の経路を追跡し、感染したPCやマルウェアの検体を高速に特定することで企業・組織を防御するセキュリティソリューションです。Cisco AMPコネクタをインストールした端末の情報をクラウド上で解析した結果を基に、セキュアブレインSOCで攻撃の有無を判断します。攻撃を検知した場合には、メール・電話等で担当者に通知し、適切なインシデントの対応策を提供します。セキュアブレインは、Cisco AMP for Endpointsの販売・サポートを2012年から行っており、導入および運用の実績が豊富です。また、日本トップレベルのマルウェア解析チームを持つセキュアブレインの技術者が、検知したマルウェアを解析し、報告書を提供します。本サービスによりサイバー攻撃の状況把握と迅速な対策が可能になり、セキュリティ担当者の負担を軽減します。

SOC サービス概要

■監視サービスの主な内容

セキュアブレインSOCにおいてCisco AMP for Endpointsによるリモート監視を実施します。マルウェア検知をはじめとした脅威検知イベントの内容を確認し、検知イベントの原因となった問題や改善策をご提案します。未知のマルウェア感染時にはセキュアブレインの技術者が独自の検知ルールを作成しCisco AMP for Endpointsに登録することで感染拡大、再発を防止することが可能です。Basicサービス、Standardサービス、Advancedサービスの3種類のサービスを提供します。

1. Basic サービス(アラート監視サービス)

Cisco AMP for Endpointsから送信される検知アラートについてセキュアブレインの技術者が検知内容を確認し、検知内容の解説と顧客での対応の必要性などを連絡します。

2. Standard サービス(イベント分析サービス)

Basicサービスに加えてCisco AMP for Endpointsの脅威検知イベントについて、セキュアブレインの技術者が検知内容を分

析し、感染端末の感染経路や被害状況を確認し、対応方法について適切なアドバイスを提供します。

3. Advanced サービス(運用・インシデント対応サービス)

Basic、Standard サービスに加えて、検知したマルウェアの簡易解析を実施して、検知ルールの登録や除外設定などの運用を行います。脅威の分析を行い、拡散防止策、再発防止策を提供します。

4. オプションサービス

- ・Cisco AMP for Endpoints 導入支援サービス
- ・マルウェアの詳細解析サービス
- ・半期・年次レポートサービス

■サービス提供方法

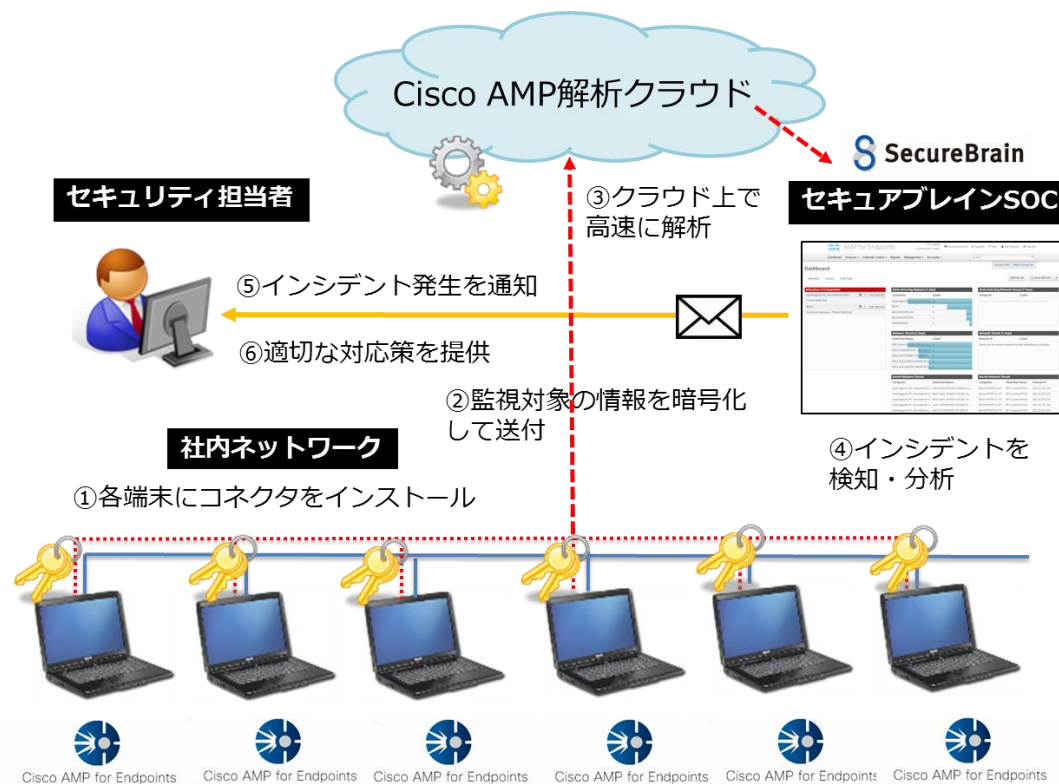
- ・メール・電話・ポータルサイト等による通知。
- ・顧客との取り決めに応じて、ビジネスアワー時間帯または 24 時間 365 日のいずれかで通知。

■価格

Basic サービス年間費 360,000 円(税別)より

(※Cisco AMP for Endpoints は、監視する PC の台数分のライセンスが必要になります。最小ライセンス数は 50 ライセンスです。価格はお問い合わせください。)

■SOC サービスのイメージ図



以上

セキュアブレインについて

株式会社セキュアブレインは、インターネット上の脅威が多様化する中、Web サービスを提供する事業者や企業にIT セキュリティを届ける、サイバーセキュリティ専門会社です。「より快適で安心できるネットワーク社会を実現するために、一歩進んだ技術で貢献する」というビジョンのもと、信頼性の高いセキュリティ情報と高品質なセキュリティ製品・サービスを提供する、日本発のセキュリティの専門企業です。詳細は、<http://www.securebrain.co.jp> をご覧ください。

◆ 本件に関する報道関係者さまからのお問い合わせ先 ◆

株式会社セキュアブレイン 広報担当:丸山 芳生(まるやま よしお)

e-mail: info@securebrain.co.jp 電話:03-3234-3001 FAX:03-3234-3002

〒102-0094 東京都千代田区紀尾井町 3-12 紀尾井町ビル 7F

※ 記載の会社名、製品名はそれぞれの会社の商標または登録商標です。