PRESS RELEASE

2019 年 10 月 1 日

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、Cisco Umbrella に SOC サービスを付加したサービスを販売開始

Cisco Umbrella に Cisco AMP for Endpoints を連携させた SOC サービスも提供

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:青山健一、以下「セキュアブレイン」)は、米国 Cisco Systems 社のクラウドセキュリティサービス「Cisco Umbrella(アンブレラ)」を新規導入または既に導入済の企業・組織に対し、高リスクなイベントを検知した場合に管理者にリアルタイムで通知を行う SOC(Security Operation Center)サービスを本日より販売開始します。また、Cisco Umbrella に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・エンドポインツ)」を連携させ、セキュアブレイン SOC においてリモートでエンドポイントを監視する SOC サービスも提供します。

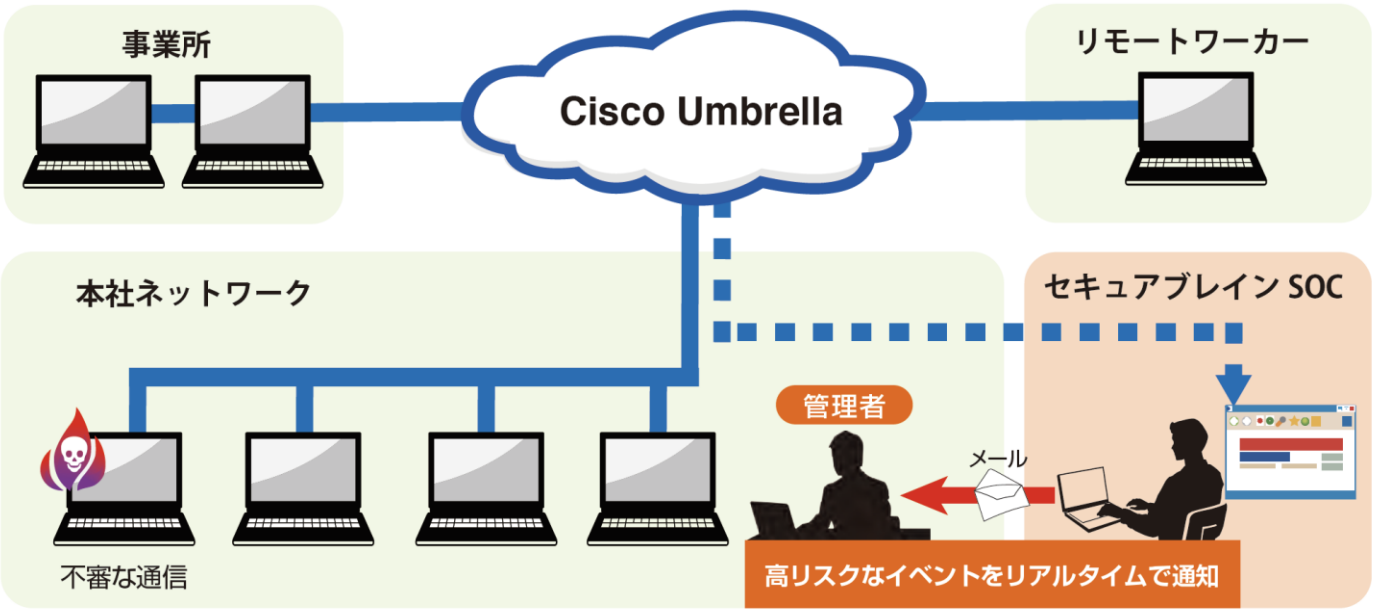
Cisco Umbrella は、DNS(Domain Name System)が行う「名前解決」の仕組みを利用したクラウドセキュリティサービスです。ハードウェアの導入は不要で、DHCP サーバーやルーター、ファイアウォールの DNS 設定を変更するだけで導入できます。従来のセキュア Web ゲートウェイとは異なり、Web やメールだけでなく、すべてのポート/プロトコルでトラフィックを検閲します。また、ドメイン名を IP アドレスに変換する際に Cisco Talos(※1)などの脅威インテリジェンスと連携し、危険な IP アドレスへの変換をしないことで、マルウェア、標的型攻撃メール、フィッシングサイトなど危険なサイトへのアクセスをブロックすることが可能です。社内、社外、VPN 接続の ON/OFF を問わず、あらゆる場所、ユーザー、デバイスを保護します。

近年、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。セキュアブレインは、Cisco Umbrella から上がってくる高リスクなイベントを検知した場合、管理者にリアルタイムで通知するサービスを、「Cisco Umbrella SOC サービス」として提供します。通知はメールで行われ、コンソールやレポートファイルを開かなくてもメールで内容の確認が可能です。また統計情報から不審なアクセスを繰り返す端末も通知します。セキュアブレイン SOC を利用することで、クリティカルなセキュリティイベントをリアルタイムに把握することが可能になり、セキュリティ担当者の負担を軽減します。

Cisco Umbrella と Cisco AMP for Endpoints を連携させることで、より強固なセキュリティ対策が可能になります。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 Umbrella の検知イベントを元に感染端末の詳細な情報を得ることができます。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、メールで管理者に通知し、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、報告するサービスをオプションで提供します。

(※1)Talos は、ネットワーク脅威の専門家集団です。Talos が提供する脅威インテリジェンスの情報は、既知および未知の脅威からお客さまのネットワークを保護するためにシスコのセキュリティ製品によって活用されています。

Cisco Umbrella SOC サービスのイメージ



Cisco Umbrella SOC サービス概要

■高リスクなイベントをリアルタイムで通知

通常スケジュール設定した時間でしか通知されない内容をリアルタイムに通知

コンソール、レポートファイルを開かなくてもメールで内容の確認が可能

■統計情報から不審なアクセスを繰り返す端末を通知

セキュリティカテゴリで短期間に何度もブロックされている端末を通知

■定期レポート

Cisco Umbrella で生成可能な月次レポートの送付

■オプションサービス

Cisco Umbrella 導入支援サービス

Cisco Umbrella＋Cisco AMP for Endpoints SOC サービス概要

■Basic サービス(アラート監視サービス)

Cisco Umbrella と 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。

■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 Umbrella と 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。

■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。

■オプションサービス

・Cisco Umbrella および 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

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、https://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