Press Release

2017 年 10 月 3 日
丸紅 IT ソリューションズ株式会社

事前対策型 サイバー攻撃分析・復旧ソリューション、販売開始

業界初、企業内全サーバー・全 PC の精細かつリアルタイムな挙動の把握を実現
高度な知識不要で標的型攻撃・ランサムウェアの迅速な対処が可能に

丸紅 IT ソリューションズ株式会社（本社：東京都墨田区、代表取締役社長：三浦 邦嗣 以下、丸紅 IT ソリューションズ）は、サイバーセキュリティに関する企業向けソフトウェアとサービスを提供する Cyber Secdo Ltd.（本社：イスラエル、ラアナナ市 CEO：Shai Morag）と国内独占販売代理店契約を締結し、同社の提供する事前対策型サイバー攻撃分析・復旧ソリューション「SECDO」の販売を本日より開始します。

今日、企業のシステム担当者のほとんどは、次世代ファイアウォール、ウイルス対策ソフト、SIEM（Security Information and Event Management、セキュリティ情報/イベント管理システム）などの多くのセキュリティ製品から膨大な量のアラート通知を受けており、日々どのアラートから原因調査すべきか優先順位を付けるトリアージに追われています。このような状況では本来対応すべきサイバー攻撃の兆候を示す重要なアラートを見逃してしまうリスクを抱えています。
SECDO は、様々なセキュリティ製品のアラート通知を、人手による調査が必要な危険度の高いものかどうかを自動で判別し、危険度の高いアラートに対してはその根本原因を自動で特定します。加えて、企業が管理する全てのサーバーやクライアント端末の被害状況、感染経路を容易に把握できる情報を提供します。これにより、システム担当者がアラートを受けてから最短数分で被害の全貌を特定し、的確な対策を策定することが可能です。また被害に遭ったサーバーやクライアント端末のサービスを止めることなく、悪意のあるプログラムの活動をリモートからピンポイントに停止することができ、事業への影響を最小限に抑えながら、迅速に被害からの復旧を進めることが可能です。

SECDO は、サイバー攻撃対策の段階に応じた、監視機能“Observer”、分析機能“Analyser”、対応機能“Responder”の 3 つの機能で構成されています。

監視機能“Observer”は、業界初(*)のスレッドレベル(プログラムの最小実行単位)で、企業が管理するサーバーやクライアント端末の全ての動作をリアルタイムに記録する機能を提供します。この機能により、サイバー攻撃の起点から、侵入・感染経路、被害に遭ったサーバーやクライアント端末に至るまで、攻撃者や悪意のあるプログラムの活動を間断なく連続して記録することが可能です。たとえ攻撃者がサーバーやクライアント端末内の侵入・攻撃の痕跡を削除した場合でも、痕跡および削除の操作は“Observer”に記録されています。

分析機能“Analyser”は Cyber Secdo 社の特許技術である Causality Analysis Engine™により、“Observer”の記録と様々なセキュリティ製品のアラート通知内容とそれらの因果関係をリアルタイムに分析します。多数のアラートの中から危険度の高いものを自動で選別した上で、アラートの原因となった攻撃者や悪意のあるプログラムのすべての活動を、理解しやすいグラフィカルなインタフェースで時系列に表示します。加えて、攻撃者や悪意のあるプログラムの活動の痕跡を基に、企業が管理する全てのサーバーやクライアント端末を調査し、感染の拡大有無等、被害状況を迅速かつ的確に特定することが可能です。

対応機能“Responder”は、“Observer”や“Analyser”の情報を基に、リモートでサーバーやクライアント端末の被害調査・復旧対応を実施する機能を提供します。復旧対応においては、Cyber Secdo 社の独自技術である IceBlock™によりメモリ内の特定スレッドの動作のみを停止することが可能です。また、サーバーやクライアント端末のスクリーンショットを常時記録しておくことや、“Responder”との通信を保持したまま被害に遭ったサーバー・クライアント端末をネットワークから隔離することも可能です。

標的型攻撃、不正侵入、マルウェアをはじめとするサイバー攻撃の高度化・巧妙化が進んでおり、いまや被害を完全に防ぐことは大変困難な状況です。そこで平常時から企業が管理するサーバーやクライアント端末の挙動を記録し、被害が発覚した際の調査や分析に活用することで、被害からの復旧時間の短縮化を図る事前対策型のセキュリティソリューションの利用が始まっています。しかしこれまでの製品は、企業が管理する全てのサーバーや全てのクライアント端末で動く、全てのプログラムの活動を間断なく連続して記録することが不可能でした。そのため攻撃者や悪意のあるプログラムの活動情報の不足を、後追いで補うことのできる極めて高度な専門性をもつ技術者を必要としていました。今回、販売開始する事前対策型サイバー攻撃分析・復旧ソリューション SECDO の登場によって、一般的なシステム担当者でも的確かつ迅速にサイバー攻撃に対応できるようになります。

事前対策型サイバー攻撃・分析復旧ソリューション SECDO は、クラウドサービス版とサーバーソフトウェア版（オンプレミス向け）の二種類の提供形態を用意しています。
丸紅 IT ソリューションズでは、SECDO を活用した、サイバー攻撃被害に関する監視・検知・分析・復旧のアウトソーシングサービスも提供する予定です。

■本サービスに関する詳しい情報は、事前対策型サイバー攻撃分析・復旧ソリューション SECDO の紹介サイトをご覧ください。
http://www.marubeni-itsol.com/solution/secdo/

※Cyber Secdo 社調べ

以上

【丸紅 IT ソリューションズ株式会社について】
丸紅 IT ソリューションズは、丸紅グループ向けならびにエンタープライズ向けに、IT コンサルティング、業務システムやセキュリティ基盤の構築、システムの運用設計、各種クラウドサービスなどの事業を展開しています。確実なプロジェクト管理力と IT 基盤構築力、運用設計力で、開発プロジェクトを成功に導き、お客様のビジネス革新を実現します。
丸紅 IT ソリューションズ ホームページ: https://www.marubeni-itsol.com/

【Cyber Secdo Ltd.について】
Cyber Secdo は、イスラエルのサイバーセキュリティ対策専業ベンダーです。イスラエルに本社と研究開発センターを、ニューヨークに営業拠点を設け、セキュリティインシデント自動分析・対応システムの開発・販売、およびインシデントレスポンスサービスの提供を行っています。
Cyber Secdo ホームページ:https://secdo.com/

＜報道関係の方のお問い合わせ先＞
丸紅 IT ソリューションズ株式会社
経営管理部企画課
電話:03-6658-1290 ファックス:03-6658-1520

＜お客様のお問い合わせ先＞
丸紅 IT ソリューションズ株式会社
IT 基盤本部 基盤営業部
電話:03-6658-1790 メール:secdo_sales＠marubeni-itsol.com