SOMPOリスクマネジメント
安心・安全・健康のテーマパーク

NEWS RELEASE

2021年9月15日

脅威インテリジェンスサービス「Kryptos Logic Platform」の提供開始
～マルウェア感染等に特化したアクショナブルな脅威インテリジェンスの提供～

ＳＯＭＰＯリスクマネジメント株式会社（本社：東京都新宿区、代表取締役社長：桜井淳一、以下「ＳＯＭＰＯリスク」）は、本年9月15日に組織全体のマルウェア感染状況の可視化を支援するアクショナブル脅威インテリジェンス(*1)サービス「Kryptos Logic Platform」の提供を開始します。

*1 脅威インテリジェンス：
攻撃者の意図、目的、ターゲット、能力、攻撃パターン等に関する情報を収集・分析し、脅威の検知、防止、対処等に活用できる有益な知識として生成された情報。

1. 背景

近年、複雑化・巧妙化するサイバー攻撃に対応するため、脅威インテリジェンスを活用することにより、攻撃の予兆を早期に把握し、必要な対策を迅速に講じようとする企業が増えています。

一方、こうした企業の多くは、様々な情報源から入手した一貫性のない膨大な情報の選別・精査に多くの時間とリソースを費やさざるを得ず、またダークウェブ(*2)上での漏洩情報の調査結果に対して有効な対応手段を見出すことができないなど、本来の脅威インテリジェンスの利点や有効性を十分に享受できずに投資対効果が向上しないといった課題を抱えています。

このような背景を踏まえ、ＳＯＭＰＯリスクは、脅威情報の中から企業に直接関係する情報のみを検出し、サイバーセキュリティの侵害を予測、準備、検知することで効果的な洞察かつ迅速な対策の実施を可能とするアクショナブルな脅威インテリジェンスサービス「Kryptos Logic Platform」の提供を開始します。

*2 ダークウェブ：
匿名性の高い特別なネットワーク上に構築されたウェブサイト。通常の方法ではアクセスできないため、違法性の高い情報やマルウェア、物品等の取引が行われている。

2. 「Kryptos Logic Platform」の概要

（1）内容

ソフトウェア・アズ・ア・サービス（SaaS）として顧客アセット（IPアドレスとドメイン）に関する情報を24時間365日監視・分析し、企業に直接関係するアラートを発報します。これにより、迅速かつ有効なマルウェア対策の実施を可能とします。

（2）特長

特長１： 攻撃者の通信を傍受する独自の検知技術

【1】ボットネット(*3)エミュレーターを構築することで不正なネットワークの通信を傍受。IP アドレスやドメイン名から疑わしい通信を検出し被害者の特定を可能とします。また、この技術により漏洩した認証情報や E メールによるフィッシング、窃取されたパスワードなどを検出することができます。

【2】使用されていない IP アドレスに通信する端末は、攻撃者からの指示でインターネット上をスキャンしている可能性があるため、センサーで通信を監視することにより、このような疑わしい通信を検知することが可能です。

【3】Kryptos Logic のカスタムセンサーでネットワークトラフィックを監視し、攻撃者のコマンド＆コントロール(C2)アドレスに接続しようとする感染 IP の特定を可能とします。

【4】Netflow(*4)データを Kryptos マルウェア・インテリジェンス(*5)(Kryptos データ・ウェアハウス)に照会することで感染 IP を特定。顧客アセットに該当する侵害の痕跡を検出することが可能です。

特長２： 導入の容易さ

IP アドレスとドメインを登録するだけで即座に利用することが可能です。エージェントやアプライアンスなどの導入は不要で、システムへ負荷や影響を与えずに調査を実施します。

*3 ボットネット：
インターネット上でマルウェア等に侵害された端末の集合体であり、攻撃者は感染したシステムやネットワーク上にランサムウェアをインストールするなど悪意のある目的のため、P2P 通信またはセントラルコマンド機能を使って数千から数百万に及ぶデバイスを制御することが可能。

*4 Netflow：
通信事業者がネットワークのトラフィックを監視・分析するための技術。ネットワーク接続の分析を目的としており、送信元、送信先の IP やポート番号などの限定された情報を含む。

*5 Kryptos マルウェア・インテリジェンス：
マルウェアサンプル日々収集し、1 日に数万件の新しいマルウェアサンプルを高度なサンドボックス技術を用いて解析を行うデータウェアハウス。

3. 今後の展開

「Kryptos Logic Platform」は、潜在的なサイバーリスクに関連する実用的な情報を提供し、ソフトウェア等のインストールを必要としないシームレスな導入が可能です。お客様の資産をサイバー脅威から守り、顕在化されていない脅威を先取りするため、この次世代プラットフォームを大企業だけでなく中堅企業に対しても積極的に提案していきます。

Kryptos Logic の脅威インテリジェンスは、新たな調査方法や脅威検知ロジックなど、様々な独自機能・サービスを有しています。ＳＯＭＰＯリスクは、企業のセキュリティ強化に向けたプロアクティブな取り組みにおいて脅威インテリジェンスの活用を推進しており、お客さまのニーズに合ったサービスを提供するべく、ラインナップを拡充していく予定です。

（1）「Kryptos Logic Platform」活用例

【1】インターネット上の新たな保護レイヤーとして

「Kryptos Logic Platform」は、インターネット上のモニタリングにより、従来のゲートウェイやエンドポイントの対策をすり抜ける悪性通信や侵害をリアルタイムで検出することで、迅速なインシデントレスポンスを実現します。

【2】海外を含む拠点数の多い企業向けのマルウェア感染対策として

「Kryptos Logic Platform」は、組織全体のマルウェア感染状況をモニタリングし、かつ企業が保有するアセットに対して重大な脆弱性を過去のものも含めて可視化することが可能です。思うようにセキュリティ対策が進まない海外拠点やインターネットの出入口を複数保有する企業において、効率的・効果的なマルウェア感染対策としての活用が可能です。

【3】マルウェア感染によるインシデント時のモニタリングとして

「Kryptos Logic Platform」は導入が容易であることから、インシデント対応時の事業再開における「クリーンアップ宣言」に向けたモニタリングとしても有効活用でき、かつインシデント対応が不完全であったため再度の攻撃を受けるという事態を防ぐことも可能です。

（2）オンラインセミナー開催（無料調査サービスキャンペーン）

「Kryptos Logic Platform」の提供開始にあたり、2021 年 10 月 7 日（木）14:00 からオンラインセミナーを開催します。なお、オンラインセミナー視聴特典として、希望する企業に対し「Kryptos Logic Platform」による無料調査サービスを提供します（先着 30 社限定）。詳細は、当社ウェブサイト(*6)をご参照ください。

*6 https://www.sompocybersecurity.com/information/view/412

ＳＯＭＰＯリスクマネジメントについて

ＳＯＭＰＯリスクマネジメント株式会社は、損害保険ジャパン株式会社を中核とするＳＯＭＰＯホールディングスのグループ会社です。「リスクマネジメント事業」「サイバーセキュリティ事業」を展開し、全社的リスクマネジメント（ERM）、事業継続（BCM・BCP）、サイバー攻撃対策などのソリューション・サービスを提供しています。

内容に関するお問い合わせ先

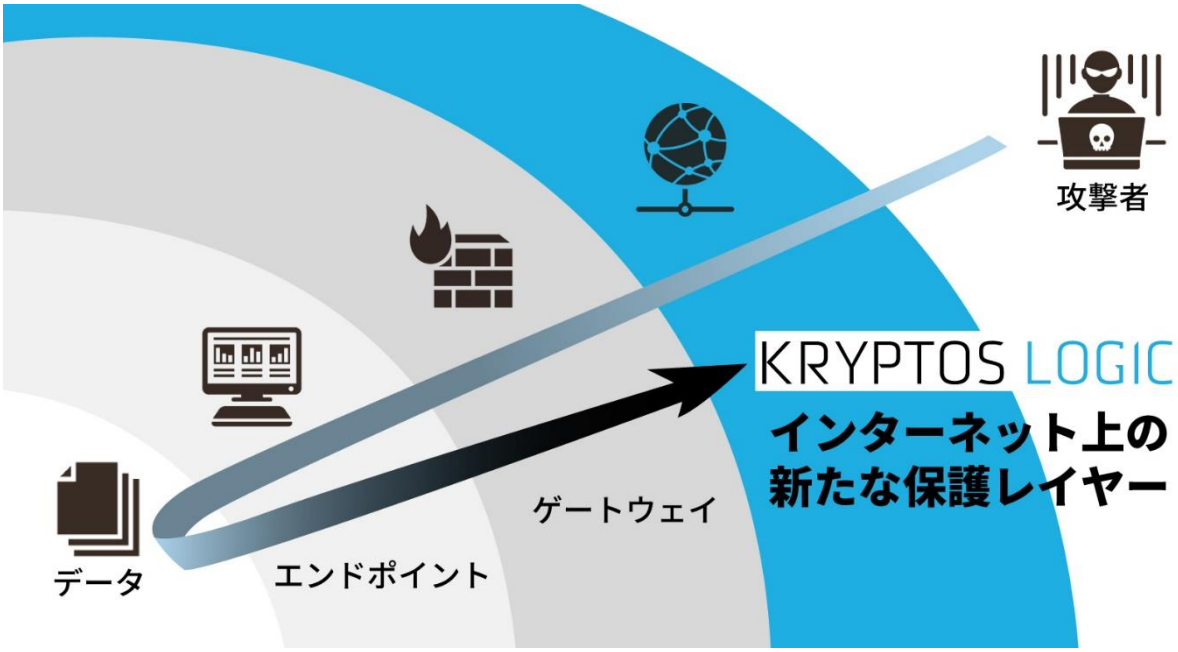
ＳＯＭＰＯリスクマネジメント株式会社 サイバーセキュリティ事業本部
プロダクト戦略部［担当：田嶋］
〒160-0023 東京都新宿区西新宿 1-24-1 エステック情報ビル
TEL：03-6630-4122（直通）

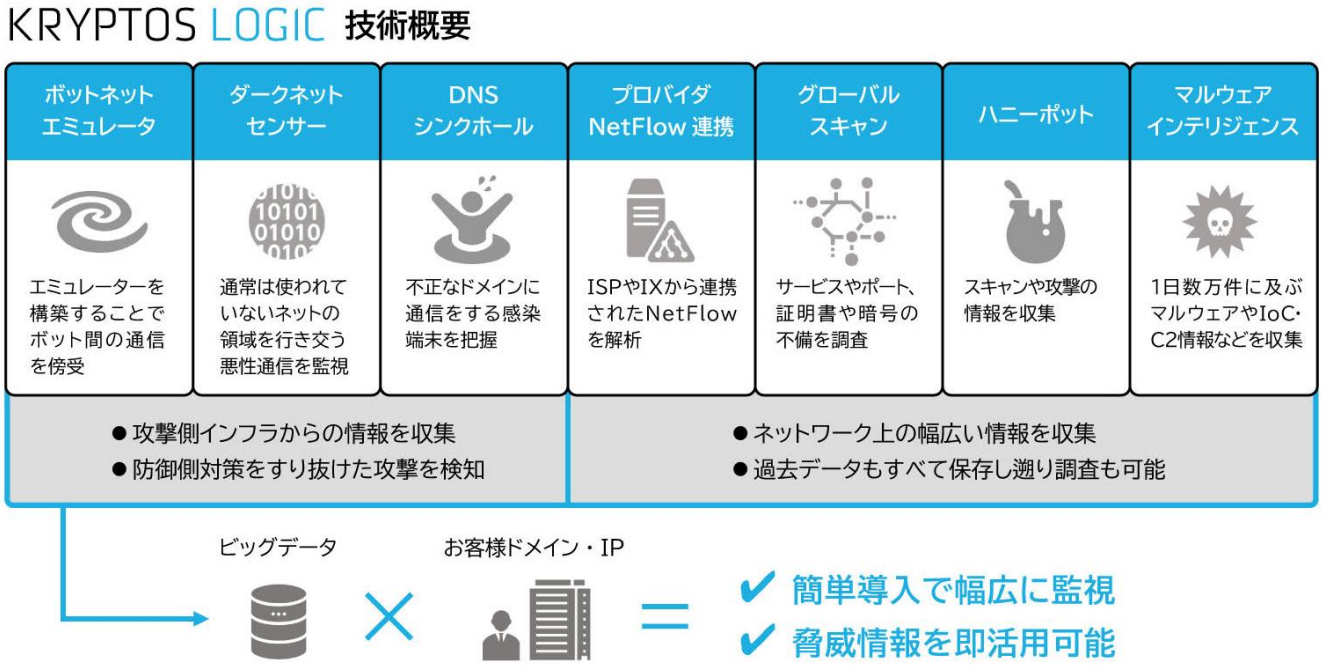
報道機関の方からのお問い合わせ先

ＳＯＭＰＯリスクマネジメント株式会社
総合企画部［担当：野本］
〒160-0023 東京都新宿区西新宿 1-24-1 エステック情報ビル
TEL：03-3349-5102（直通）

別紙

■「Kryptos Logic Platform」の概要





※「Kryptos Logic Platform」は Kryptos Logic 社のサービスをベースとしたプラットフォームです。

Kryptos Logic（本社：米国 ロサンゼルス　https://www.kryptoslogic.com/）

最先端の脅威インテリジェンスサービスを専門とするグローバルサイバーセキュリティ企業であり、WannaCry、Emotet、Mirai など、これまでの大規模なサイバー攻撃に対する取組が世界的に認められています。