Soliton

News Release

報道関係各位

2018 年 3 月 28 日
株式会社ソリトンシステムズ

国産 EDR/NGAV を活用したマネージドサービスを開始

- 専門アナリストが分析、インシデント対応負担を軽減 -

株式会社ソリトンシステムズ（本社：東京都新宿区、代表取締役社長：鎌田信夫　以下ソリトン）は、サイバーセキュリティ対策の EDR（Endpoint Detection and Response）と NGAV（Next Generation AntiVirus）のハイブリッド製品「InfoTrace Mark II for Cyber」の運用を支援するマネージドサービス「InfoTrace Mark II for Cyber Cloud」（以下 Mark II Cloud）の提供を、本日より開始します。

従来型のセキュリティ対策をすり抜ける脅威への対策として、EDR や NGAV への注目が高まっています。しかしその一方で、複雑化する脅威を理解した専任人材の確保や、継続的に EDR/NGAV を活用し、インシデント発生時に速やかな対応をすることに課題を抱えている組織も少なくありません。

Mark II Cloud では、「InfoTrace Mark II for Cyber」の EDR、NGAV 機能をクラウドサービスとして提供するとともに、お客様に代わって 24 時間 365 日で管理・運用を行うマネージドサービスを提供します。
マネージドサービスでは、「InfoTrace Mark II for Cyber」による検知アラートに対し、脅威を判定した速報レポートを提供、侵害の疑いのある端末のネットワークから隔離のほか、専門アナリストによる対応アドバイスや動的解析レポートなどにより、インシデントハンドリングを継続的に支援します。

また、今後 FireEye 社や Palo Alto Networks 社、Cylance 社等の他社脅威対策製品の検知イベントへの対応も予定しています。お客様が既に導入運用されている製品を最大限に活用したセキュリティ対策を支援してまいります。

【サービス特長】

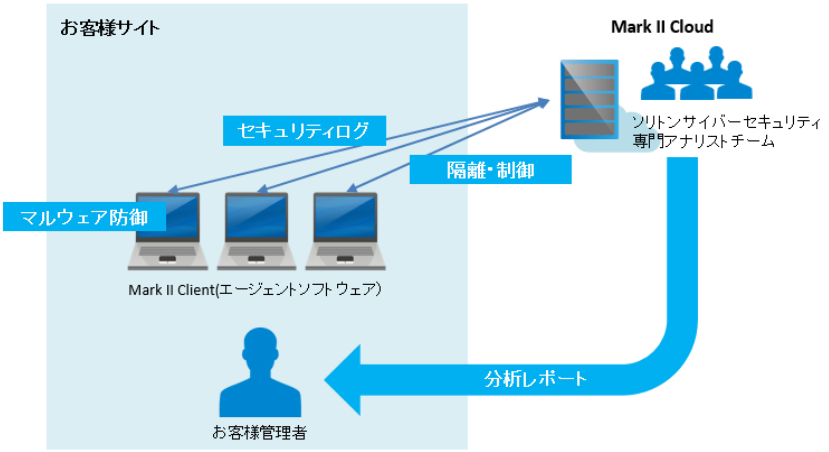
1. **インシデントの全容把握を可能にする EDR**
   カーネルレベルで取得する高精度セキュリティログが、インシデント発生の原因究明、影響範囲の特定を可能にします。EDR で取得するセキュリティログは、全て国内のデータセンターで安全にお預かりいたします。セキュリティログを長期間保管したいお客様へは、オプションでログ提供も行います。

2. **未知マルウェアだけでなく、ゼロデイ脆弱性攻撃も防ぐ NGAV**
   パターン非依存のマルウェア対策エンジンで、ゼロデイや未知マルウェアを防御します。

3. **専門アナリストが運用を支援**

News Release

ソリトンのセキュリティアナリストが、脅威対策やログ取得のチューニングから、インシデント発生時の対応までを支援します。



サービス概要図

アラート解説レポート（サンプル）

【株式会社ソリトンシステムズについて】

1979 年の設立以来、ソリトンシステムズは IT・エレクトロニクス業界にあって、常に新しい技術トレンドを見据え、いくつもの「日本で初めて」を実現してきました。近年は、認証を中心とした IT セキュリティからサイバー対策製品まで、また、携帯電話回線や Wi-Fi を利用した ハイビジョン・レベルの映像伝送システムなどに取り組んでおります。国産メーカーとして、オリジナルの「もの創り」、「独創」にこだわった製品とサービスを提供しております。

設立：1979 年、売上 165 億円/2017 年度　　https://www.soliton.co.jp/

Soliton

News Release

【 本件に関する問合せ先 】
株式会社ソリトンシステムズ　IT セキュリティ事業部
Tel: 03-5360-3811　netsales@soliton.co.jp

【 このリリースに関するマスコミからの問合せ先】
株式会社ソリトンシステムズ　広報　Tel: 03-5360-3814　press@soliton.co.jp