2021年8月6日
NTTアドバンステクノロジ株式会社

SKYSEA Client View『EDRプラスパック』に対応したSOC連携サービス「EDR端末監視ソリューション（SKYSEA & yarai SOC）」を提供開始

NTTアドバンステクノロジ株式会社（以下：NTT-AT、本社：東京都新宿区、代表取締役社長：木村丈治）は、高度化・巧妙化するサイバー攻撃に対応して端末の監視を強化する「EDR端末監視ソリューション（SKYSEA & yarai SOC）」（以下：本サービス）の提供を8月6日から開始します。

本サービスは、Ｓｋｙ株式会社（以下：Ｓｋｙ社、東京本社：東京都港区、大阪本社：大阪市淀川区、代表取締役：大浦淳司）が提供するクライアント運用管理ソフトウェア「SKYSEA Client View*1」のオプションである『EDRプラスパック』をご利用のお客様を対象としたSOC（Security Operation Center）サービスで、高度化・巧妙化するサイバー攻撃からリモート環境の端末を含めマルウェアへの感染などを防御します。

NTT-ATは、すでにICT-24セキュリティオペレーションセンター（ICT-24SOC）にてEDR（Endpoint Detection and Response）による端末監視サービスを提供しており、本サービスの提供開始により、コロナ禍での業務環境セキュリティ強化でお困りのお客様の「端末セキュリティ強化」に貢献します。

■提供開始の背景

従来からデータを暗号化して暗号通貨の支払いを要求するランサムウェアは存在しており、これに対してはバックアップを確実に実施することで対策されていました。さらには、昨今、それらの対策を回避するため、データを盗み出した上で暗号通貨の支払いを要求し、要求に従わない場合には、盗み出したデータをインターネットに公開するという悪質なサイバー攻撃が大幅に増加しています。

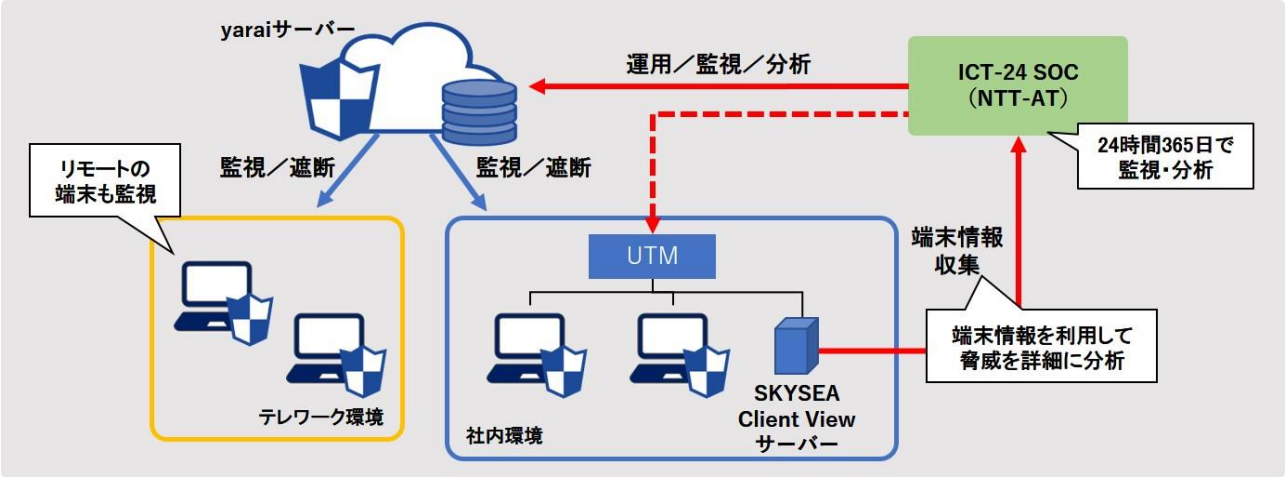
このようにサイバー攻撃者が攻撃手法を進化させている中で、防御する側の防御策の強化が求められています。そのため、これまでのセキュリティ対策パッチの適用とEPP（Endpoint Protection Platform）の組み合わせに加え、EDRの導入を検討されている企業・組織が増加してきています。

■提供開始のねらい

サイバー攻撃対策の取り組みの基本は『計画・検知・隔離・調査・封じ込め・修復・インシデント対応』ですが、これらの多くは端末の動作に関するログ情報をもつSKYSEA Client Viewと、ファイルの特徴や実行プロセスの振る舞いを監視し検知・防御する機能を持つ次世代エンドポイントセキュリティ「FFRI yarai*2」を組み合わせたSKYSEA Client View『EDRプラスパック』の導入により、実現可能となります。一方で、その導入効果を最大限に引き出すためには専門的なノウハウも必要となることから、お客様からSOCサービスを求められるようになりました。

こうしたニーズにお応えするため、これまでNTT-ATが代理店として長期間にわたって提供してきた「FFRI yarai」の販売とマネージドサービスの提供ノウハウをもとに、今回、SKYSEA Client View『EDRプラスパック』に対応したSOC連携サービスを提供することといたしました。

NTT-ATは、ICT-24セキュリティオペレーションセンター（ICT-24SOC）で、お客様に代わって端末のセキュリティを監視します。



【提供するソリューションのイメージ】

■本サービスの概要

（1）概要

本サービスは、お客様が導入された　SKYSEA Client View『EDR プラスパック』を代行監視するものです。24 時間 365 日お客様システムの運用・監視を行う NTT-AT の ICT-24SOC が、お客様に代わって社内環境だけでなく、リモート勤務環境もまとめて端末を監視することで、テレワークが進む中でお客様の監視負担を軽減できます。

（2）主な特長

「FFRI yarai」によるふるまい検知に加え、端末の異常を検知した際、CISSP 資格保有者等の経験豊富なセキュリティアナリストが SKYSEA Client View から得られる過去のプログラムの動作や利用者の操作など過去の端末の動作情報も使用して状況を分析し、推奨する対策を提示することができます。

（3）提供形態

SKYSEA Client View『EDR プラスパック』を利用中のお客様の拠点と、NTT-AT の ICT-24SOC との間を VPN により接続し、ICT-24SOC から SKYSEA Client View および「FFRI yarai」を 24 時間 365 日、監視いたします。

「FFRI yarai」で攻撃検出のアラートがあがると、SKYSEA Client View の端末のログを用いた分析などにより端末を調査し、必要があれば端末隔離等の対応を実施します。

■提供開始

8 月 6 日

■提供価格

ご利用や価格などに関する詳細につきましては、下記「お問い合わせ先」までお問い合わせください。

■今後の展望

コロナ禍でテレワークが進む中、これまでのファイアウォールなどでオフィスネットワークの入口を守るセキュリティから、リモートワーク環境も守り、そしてクラウド利用も守る時代への移行が進んでまいります。このような中、NTT-AT はゼロトラストの実現に向け、クラウド PROXY、CASB*3 等も拡大サポートしていく予定です。また、クラウド型 UTM*4 の提供をはじめ、さまざまなソリューションを組み合わせたセキュリティサービスを展開してまいります。

*1：SKYSEA Client View
⇒ Sky社が開発した 端末の資産管理・ログ管理・セキュリティ管理を提供するソリューションです。

*2：FFRI yarai
⇒ FFRI セキュリティ社が開発した パターンファイルに依存しないふるまい検知機能をもったエンドポイントセキュリティです。 標的型攻撃のトリガーとなる未知の脆弱性攻撃や、未知のマルウェア攻撃からシステムを保護します。

*3：CASB（Cloud Access Security Broker：キャスビー）
⇒ ガートナー社が提唱した用語で、企業が利用するクラウド・アプリケーションについて可視化、データ・プロテクション、ガバナンスを実現するサービス／製品を指します。

*4：UTM（Unified Threat Management）
⇒ 「統合脅威管理」の意味で、複数のセキュリティ機能を 1 つに集約して運用するネットワークセキュリティ対策のことです。

本件に関するお問い合わせ先

【商品に関するお問い合わせ先】
NTTアドバンステクノロジ株式会社
セキュリティ事業本部
セキュリティサービス&ソリューションビジネスユニット
SOC担当
https://www.ntt-at.co.jp/inquiry/product/skysea-yarai-soc/

【報道関係のお問い合わせ先】
NTTアドバンステクノロジ株式会社
ビジネス推進部コーポレート・コミュニケーション部門
増田・加藤
E-mail: inquiry@ml.ntt-at.co.jp