NRI グループからのお知らせ
Notification from NRI Group

Nomura Research Institute Group

2021 年 8 月 3 日
NRI セキュアテクノロジーズ株式会社

NRI セキュア、パロアルトネットワークスの「Cortex® XDR」を活用したセキュリティ管理サービスを提供開始

～ 端末、ネットワーク、クラウド環境等の一元管理を実現 ～

NRI セキュアテクノロジーズ株式会社（以下「NRI セキュア」）は、エンドポイント（端末）、企業のネットワーク、クラウド環境のデータを統合し、一元的な防御・検知・対処を実現する、パロアルトネットワークス株式会社 [1]の XDR[2]ソリューション「Cortex® XDR（コーテックス エックスディーアール）」を活用した「マネージド XDR サービス powered by Cortex XDR from Palo Alto Networks（以下「本サービス」）」の提供を、本日開始します。

サイバー攻撃の増加、テレワークやクラウドサービスの利用拡大に伴って、多くの企業で EDR[3]を用いたエンドポイント監視の導入が進んでいます。さらに、自社で管理する情報システム環境やネットワークと、外部のクラウドサービス等を含めた自社の情報システムの全体像を可視化しつつ、不正な動きに対する監視を強化し、有事の際に迅速な対処を行う「NDR」[4]と呼ばれる対策のニーズも高まりつつあります。

本サービスは、EDR と NDR の各種機能を兼ね備えた Cortex XDR の導入支援およびマネージドサービスを提供するもので、第 1 段階として、Cortex XDR の EDR 機能を活用したエンドポイントの運用監視サービスを提供開始します。第 2 段階として、NDR 機能の提供を 2021 年度内に開始する予定です。

■ Cortex XDR の特長

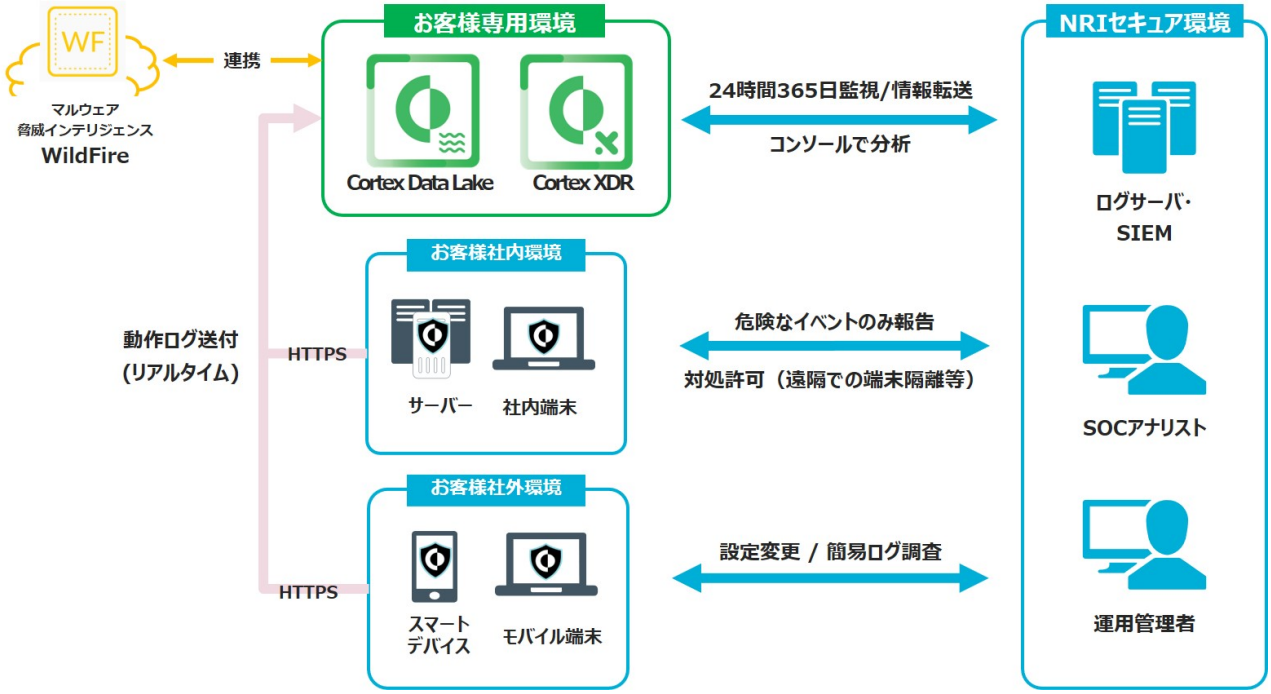
Cortex XDR は、エンドポイントから収集されるログ等の情報だけでなく、さまざまなセキュリティ製品から得られるログを収集・分析することが可能です。例えば、パロアルトネットワークスの次世代ファイアウォールで収集されるログや、その他サードパーティー製の各種クラウド対策ソリューション等に対応しています。

全てのログはパロアルトネットワークスのクラウドデータストア「Cortex Data Lake」[5]に常時収集され、セキュリティデータを一元管理することで、インシデント（事故・事案）の迅速な対応を実現します。

■ 本サービスの概要

NRI セキュアでは、PC やサーバ等のエンドポイントにインストールした Cortex XDR の専用エージェント[6]の設定情報管理とアラート監視を企業に代わって行い、マルウェア[7]感染をはじめとするインシデントの予防や早期検知から、インシデント発生時の対処までを一気通貫で提供します。NRI セキュアが提供する「セキュリティログ監視サービス（NeoSOC）」の専門アナリストやパロアルトネットワークスのソリューションに精通した担当者が運用にあたることで、インシデント発生時における対応の迅速化や影響範囲の適切な把握につながり、セキュリティリスクの低減が期待できます。

図：「マネージド XDR サービス powered by Cortex XDR from Palo Alto Networks」の全体像



本サービスの詳細については、次の Web サイトをご参照ください。

https://www.nri-secure.co.jp/service/mss/cortex-xdr

NRI セキュアは今後も、企業・組織の情報セキュリティ対策を支援するさまざまな製品・サービスを提供し、グローバルな規模で安全・安心な情報システム環境と社会の実現に貢献していきます。

---

[1] パロアルトネットワークス株式会社：
世界的なサイバーセキュリティのリーダー企業として、各組織や従業員の業務を変革する技術により、クラウド中心の未来を創造しています。統合プラットフォームを提供し、パートナーとのエコシステムを強化することで、クラウドやネットワーク、デバイスを越えて数万の組織を最前線で防衛しています。詳細は、次の Web サイトをご覧ください。
https://www.paloaltonetworks.jp

[2] XDR：
Extended Detection and Response の略称。XDR とは、エンドポイント、ネットワーク、クラウド等から適切なデータを取得し、それらすべてのデータの分析を集中管理して行うソリューションを指します。

[3] EDR：
Endpoint Detection and Response の略称。主にエンドポイントにおけるインシデント発生後の対応を、明確化・迅速化する機能を持つセキュリティ対策製品を指します。

[4] NDR：
Network Detection and Response の略称。機械学習やその他の分析手法を用いて、企業ネットワーク上の疑わしいトラフィックを検出します。

[5] クラウドデータストア「Cortex Data Lake」：
次世代ファイアウォール、Prisma Access、Cortex XDR 等のセキュリティ製品のログをクラウド上に保存・記録する機能を提供します。

[6] エージェントをインストールしないサービス提供形態にも対応可能です。エージェントを入れにくい工場等の環境にも適しています。

[7] マルウェア：
不正かつ有害な動作を行う意図で作成されたソフトウェアや悪質なコードの総称で、ウイルス、トロイの木馬等を含みます。

【お知らせに関するお問い合わせ】
NRI セキュアテクノロジーズ株式会社　広報担当
TEL：03-6706-0622　E-mail：info@nri-secure.co.jp