

News Release

2018年12月5日
NRIセキュアテクノロジーズ株式会社

NRIセキュア、情報セキュリティの監視やインシデント 対応の自動化・高度化を支援するサービスを提供開始

NRIセキュアテクノロジーズ株式会社（本社：東京都千代田区、社長：小田島 潤、以下「NRIセキュア」）は、企業における情報セキュリティの監視業務やインシデント（事故・事件）発生時の対応業務を自動化および高度化するための、「SOAR（ソアー）^{*1} 導入・運用支援」サービスを提供開始します。

情報システムやコンピュータのセキュリティインシデントに関する通知を受け取り、適切な対応を実施するチームまたは組織を指す「CSIRT（シーサート）^{*2}」を設置する企業が増える一方、セキュリティを専門とする人材の不足により、CSIRTや監視業務を担う組織（SOC^{*3}）に高度な人材を安定的に確保することが難しくなっています。また、業務手順が属人的になっている場合、担当がいなくなると、業務が継続できなくなるリスクもあります。

そのため、セキュリティインシデントの調査から対処に至るまでの業務プロセスを自動化・高度化するSOARツールが登場し、注目されています。SOARツールは、(1) 自動化による対応速度と対応品質の向上、(2) インシデント対応業務の集約、(3) インシデント検知の高精度化、(4) インシデント対応状況の可視化と経営層への迅速な報告、などの効果を期待できます。

しかしながら導入にあたり、他システムとの接続設定など、自社の監視・運用に合わせたカスタマイズが必要となります。これがボトルネックとなり、自社で導入したものの、ツールを効果的に活用できなかったり、導入を見送ったりするケースも見られます。

NRIセキュアは、上記の問題点を解決し、SOARツールを最大限に活用するために、ツールの導入と運用それぞれの場面で支援するサービスを提供します。

各サービスの主なポイントは、以下の通りです。

■SOAR 導入支援

・各種SOARツールの導入コンサルティング

お客様の業務環境に適したSOARツールの選定や導入に向けた社内への提言を実施し、ツールを活用した監視運用業務の設計と、自動化する業務領域の定義を行います。

・SOAR ツールの導入、環境構築

すでに導入されている SIEM^{※4} 製品およびセキュリティ機器との接続を設定し、監視・インシデント対応業務の自動化手順書（プレイブック）を作成します。

■SOAR 運用支援

・SOAR ツールに関する教育・運用支援

導入した SOAR ツールの利用方法について、担当者へのレクチャーを実施し、運用業務フローの定期的な見直しを支援します。

・SOAR ツールの構成変更とカスタマイズ

新たなイベントログへの対処方法やセキュリティ機器の追加設定のほか、導入後に発生した脅威や業務フローに対応するためのプレイブックの作成、見直しを支援します。

本サービスについての詳細は、以下の Web サイトをご参照ください。

<https://www.nri-secure.co.jp/service/consulting/soar.html>

NRI セキュアは、今後も、企業におけるサイバー攻撃対応能力の向上に向けた支援および関連サービスの拡充を通じて、安全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 SOAR (Security Orchestration and Automation Response) :

セキュリティインシデント対応業務の品質向上および生産性を高めることを目的に、企業の情報システムに導入されている様々なツールと連携しながら、インシデントの調査から対処にかかわる業務プロセスを自動化すること。

※2 CSIRT に関する、NRI セキュアの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/consulting/csirt.html>

※3 SOC (Security Operation Center) :

企業などにおける情報システムへの脅威を 24 時間 365 日監視し、脅威情報の分析などを行い、対応策を示す専門組織。

※4 SIEM (Security Information and Event Management) :

日本では「セキュリティ情報イベント管理」と訳され、サーバやネットワーク機器などの各種アプリケーションから集められたログ情報を一元的に蓄積・管理し、異常があった場合にいち早く検知・分析をする仕組み。

【ニュースリリースに関するお問い合わせ】

NRI セキュアテクノロジー株式会社 広報担当

TEL : 03-6706-0622 E-mail : info@nri-secure.co.jp

【ご参考】

●NRI セキュアが提供する、CSIRT および SOC 関連のサービスマップ

