インシデント対応を自動化する SOAR

SOAR (Security Orchestration, Automation and Response)

・複数のシステムやセキュリティシステムなどから収集された情報を分析し、
インシデントへの対応において、優先順位付けや運用の自動化により効率化

- Threat and vulnerability management
- Security incident response
- Security operations automation

SIEM に
オーケストレーション
と自動化を増強

セキュリティ管理者の
人材不足を解消

SOAR (Security Orchestration, Automation and Response) は、SIEM（Security Information and Event Management）と同様 Gartner 社によって提唱された言葉で、セキュリティインシデントに対応するためのソリューションスタックです。SOAR のスタックは、標準化されたインシデント対応のアクティビティを定義し、プライオリティ付けや自動化によって、セキュリティ対応の効率化を実現します。

SOAR の最も重要な機能は次の 3 つです。

- 脅威と脆弱性の管理･･･脆弱性の修復をサポートし、ワークフローやレポートなどを提供
- セキュリティインシデント対応･･･セキュリティインシデントへの対応を計画し、管理、追跡、調整方法をサポート
- セキュリティ運用自動化･･･ワークフロー、プロセス、ポリシーの実行などの自動化とオーケストレーション

近年、RPA も盛んになりセキュリティの運用に携わる部門では、セキュリティオーケストレーションと自動化の SOA (security orchestration and automation）への関心が高まり、その恩恵を得たいという気運が盛り上がってきております。よって、多くの企業が SOAR のサービスを活用して、社内のセキュリティとイベント管理で使用してきた SIEM ソフトウェアを増強しようという動きがあります。SIEM と SOAR スタックの両方が、あらゆる機器やシステムからログなどのセキュリティ関連データを集約する一方で、ベンダが提供する SOAR サービスはより広範な内部および外部アプリケーションとの統合を実現してくれるようです。
SIEM では、インシデント情報やログのデータが一元管理でき、ツールを使用すれば 1 つのダッシュボードで見ることができましたが、インシデントに関連する対応のアクションは人間が行うことが基本でした。それに加え、SOAR では、インシデントについての優先順位付けや、対応プロセスやレポーティングなどをフローに従って自動化するところまで踏み込んでいます。
今後、RPA によって事務系にまでソフトウェアロボットが活躍しだすと、運用管理すべきシステムが数多くなります。そのためのセキュリティ対策に携わる運用担当者不足の問題に対応するためには、圧倒的な運用効率化が必要で、どれだけセキュリティインシデントの対応を自動化できるかがカギとなります。

© CEC Customer Service Ltd.