News Release

2025 年 5 月 22 日
SCSK セキュリティ株式会社

SIEM の導入効果を最大化し、サイバー攻撃検知能力を高めるソリューション「CardinalOps（カージナルオプス）」の提供開始

SCSKセキュリティ株式会社（本社：東京都江東区、代表取締役社長：小峰　正樹、以下 SCSKセキュリティ）は、イスラエルのサイバーセキュリティサービスプロバイダである CardinalOps Ltd.（本社：テルアビブ、CEO：Michael Mumcuoglu、以下 CardinalOps）と代理店契約を締結し、同社が開発するサイバーセキュリティに関するクラウドサービスの国内での提供を開始します。

1. 背景

多くの企業では、加速するサイバー攻撃の脅威に対してEDRやSASEの導入といった IT 環境をゼロトラストモデルに移行するなどのセキュリティ対策を実施していますが、近年のサイバー攻撃の攻撃手法はますます高度化・巧妙化しています。次のセキュリティ強化策としてSIEM（Security Information and Event Management）を活用したインシデント検知能力の向上が挙げられていますが、SIEMの活用にあたり、活用方法や改善指標の客観的な基準がないため、多くの企業では「どこから手を付ければ良いのか」「何をもって改善したと判断できるのか」といったニーズがあります。
また、高度なセキュリティ対策を行っている企業の中には、MITRE ATT&CK フレームワーク※1 を活用してインシデント検知能力の可視化に取り組んでいますが、複雑なフレームワークを理解し、自社が実装しているセキュリティ対策状況と照らし合わせ、現状のインシデント検知能力を可視化できる高いレベルの専門知識が必要となっており、セキュリティ人材が不足している状況下で、企業はセキュリティ対策に課題を抱えています。

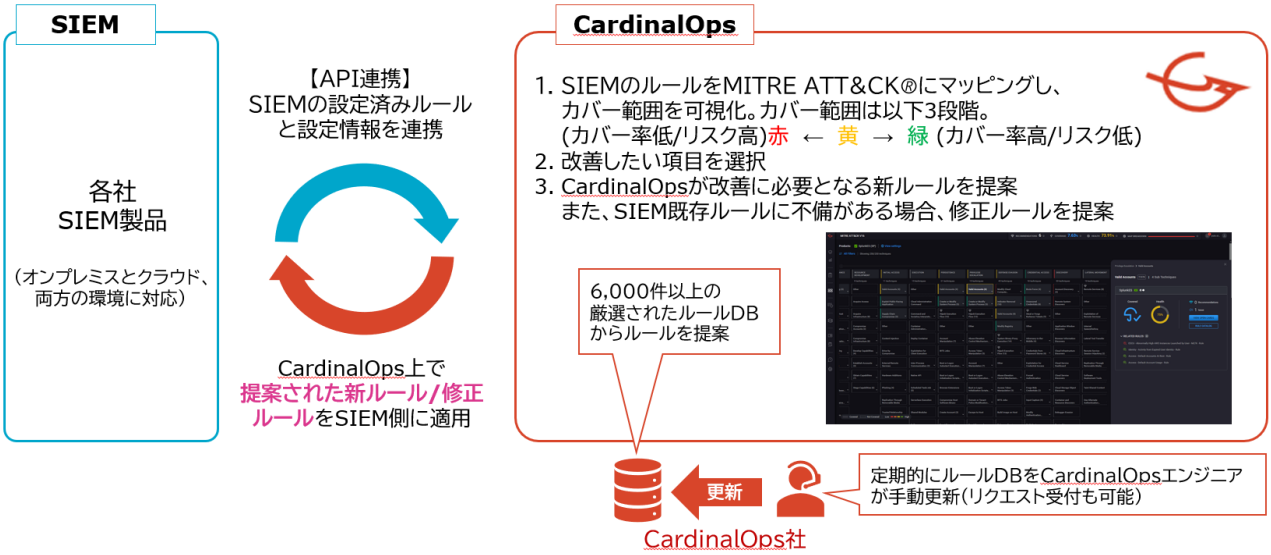
※1
米国の非営利組織である MITRE Corporation が公開する、サイバー攻撃の戦術（Tactics）、攻撃手法（Techniques）、攻撃手順（Procedures）を分類してまとめたフレームワーク。それぞれの頭文字を取った TTP は攻撃シナリオを表し、サイバー攻撃のプロセスを可視化することに役立つ。

2. サービスの概要

CardinalOps は、企業が導入している SIEM が、MITRE ATT&CK をどの程度カバーできているか可視化し、カバー範囲を広げるために必要な SIEM のルールを自動生成・提案します。企業のセキュリティ担当者は CardinalOps が提案してくる SIEM のルールを適用させるかどうかを判断するだけで、サイバー攻撃検知能力を向上させることができます。CardinalOps からの提案と適用するルールの選択を繰り返すことで、高度化・巧妙化し続ける脅威を検知するための最適な SIEM 環境を実現することができます。

詳細は下記 URL をご参照ください。

- SCSK セキュリティの CardinalOps 紹介ページ：
  https://scsksecurity.co.jp/services/cardinalops/
- CardinalOps 社の Web サイト(英語のみ)：https://cardinalops.com



3.サービスの特長

(1) 多くの SIEM 製品をサポート

CardinalOps は稼働しているSIEMと API で連携することによって動作し、数多くの SIEM 製品を公式にサポートしています。また、クラウド SIEM とオンプレミス SIEM の両方に活用することができます。

(2) SIEM ルールの高い品質

SIEMのルール提案は、CardinalOps の独自技術によって自動生成されたものに対して、本番環境に適用させて問題ないかの検証をエンジニアが行います。高度な知見を持ち、経験豊富なエンジニアによるマニュアル作業を活用することで高い品質を担保しています。

(3) 継続的な SIEM 高度化を支援

CardinalOpsは一週間に5つの新しいルールを提案します。企業のセキュリティ担当者は提案されたルールを適用させる活動を継続することで自社SIEMのサイバー攻撃検知能力向上を継続的に、着実に実現して行くことができます。

4.CardinalOps の効果

SCSK セキュリティはお客様環境の改善に CardinalOps を活用し、お客様のセキュリティレベル向上とともにセキュリティ運用現場の負荷を軽減し、セキュリティ人材不足の解消を実現する「SOC/CSIRT モダナイゼーション」を推進します。

(1) SIEM 活用の高度化

CardinalOps を活用した SIEM の高度化には MITRE ATT&CK を詳細に理解する必要も、SIEM 製品について技術的に習熟する必要もありません。CardinalOps が提案してくるルールとともに MITRE ATT&CK 該当箇所を分かりやすく解説してくれます。検知したいイベントを選択、提案されたルールを適用させるだけで SIEM 活用の高度化を実現することができます。

（2）SIEM 構築時の品質向上

SIEM は検知したい事象を具体的に定義しないとルールを書くことができないため、SIEM の運用をアウトソースしている場合でも、企業のセキュリティ管理者は導入している SIEM製品の特性を理解する必要があります。CardinalOps を活用すれば特定製品に依存した知識は必要無く、MITRE ATT&CK という基準に照らし合わせたスムーズなルール作成を実現することができます。

（3）SIEM マイグレーション時のクオリティアシュアランスツールとして活用

SIEM 製品の移行時に、旧製品で動作していたルールを一つずつ新製品に書き換えるという進め方をすると、製品の特性を吸収するために作業工数が増大します。CardinalOps を活用し、MITRE ATT&CK のカバー範囲を合わせるというアプローチを取ることによりシンプルで分かりやすく、品質の高い SIEM マイグレーションを実現することができます。

（4）SIEM エンジニア/SOC 担当者の工数削減

従来は高いレベルの専門知識を持つ SIEM エンジニア/SOC 担当者が膨大な工数をかけて手動で SIEM ルールを作成していました。CardinalOps のルール自動生成・提案により、SIEM エンジニア/SOC 担当者はルールの質を担保しつつ、同時に所用する作業工数の削減を実現することができます。

5. 開発元からのエンドースメント

We are honored to partner with SCSK Security, a renowned cybersecurity firm in Japan. This alliance presents a promising opportunity for CardinalOps to extend our solutions to the burgeoning Japanese market. Together with SCSK Security, we will help organizations maximize the effectiveness of their detection tools and operationalize advanced adversary intelligence to decrease exposure and defend against modern threats.

（日本語訳）日本を代表するサイバーセキュリティ企業であるSCSKセキュリティと提携できることを光栄に思います。この提携は、CardinalOps にとって、急成長を遂げる日本市場へソリューションを展開する有望な機会となります。SCSKセキュリティと共に、組織が検知ツールの有効性を最大限に高め、高度な攻撃者インテリジェンスを運用することで、リスクを軽減し、最新の脅威から防御できるよう支援します。

Michael Mumcuoglu, Co-Founder and CEO at CardinalOps

6.SCSKセキュリティについて

SCSKセキュリティは、サイバーセキュリティ対策に特化したSCSKグループの専門事業会社です。SI事業で培ったコンサルティング・基盤構築・運用サービスと、最新技術を活用した高品質なプロダクトを組み合せることで、顧客企業のサイバーセキュリティリスクを低減するとともに、セキュリティ領域における投資対効果を最大化させ、安心・安全な社会の実現に貢献いたします。

商号	:SCSKセキュリティ株式会社
代表者	:代表取締役社長 小峰 正樹
本社所在地	:東京都江東区豊洲 3-2-20
出資比率	:SCSK株式会社 100%

SCSK
SCSKセキュリティ

事業内容	:セキュリティサービス開発・販売(コンサルティング、脆弱性診断/評価、トレーニング等)、セキュリティ製品販売
URL	:https://scsksecurity.co.jp/

7.SCSKグループのマテリアリティ

SCSKグループは、経営理念「夢ある未来を、共に創る」の実現に向けて、社会と共に持続的な成長を目指す「サステナビリティ経営」を推進しています。
社会が抱えるさまざまな課題を事業視点で評価し、社会とともに成長するために、特に重要と捉え、優先的に取り組む課題を7つのマテリアリティとして策定しています。
本取り組みは、「安心・安全な社会の提供」に資するものです。

－最新かつ高度な知見の提供により、セキュリティ品質の向上と運用現場の負荷を軽減
－高度化・巧妙化するサイバー攻撃への対策強化による、サイバーセキュリティリスクの低減

8.本件に関するお問い合わせ先

【製品・サービスに関するお問い合わせ先】
SCSKセキュリティ株式会社
ビジネス開発本部　ビジネス開発部　CardinalOps 担当
E-mail:sys-info@scsksecurity.co.jp

【報道関係お問い合わせ先】
SCSKセキュリティ株式会社
管理本部 コーポレートマネジメント部　広報担当
E-mail　:Yasuyuki.Morita@scsksecurity.co.jp
　　:Sayaka.Ohta@scsksecurity.co.jp