よりスマートな防御：AIによるサイバーセキュリティ強化の現状

大手B2Bソフトウェア企業における セキュリティ強化へのAI活用の実態

人工知能（AI）は、今やセキュリティチームにとって欠かせないツールとなっており、脆弱性の予測と修正、脅威検出の迅速化、インシデント対応の自動化に役立っています。このように、サイバーセキュリティ向けAIはすでに企業に価値をもたらしています。

厳しい環境

世界的にデジタル化が進展する中、サイバーセキュリティの重要性は高まっています。同時に、悪意のある行為者は、AIの悪用などによって戦術、手法、手順を高度化させ、違法行為の頻度と影響を拡大させています。しかし、AIは悪意のある行為者により効果的に対抗できるツールを提供しており、優位性を防御側へと引き戻しつつあります。こうしたAI強化型ツールは、SFでもなければ、大手B2Bソフトウェア企業で研究開発段階のものでもありません。むしろ、すでに導入され、悪意のある行為者への対抗や企業の情報の保護に貢献しています。

すでに導入が進むサイバーセキュリティ向けAI

政策立案者は、大手B2Bソフトウェア企業においてAI強化型サイバーセキュリティツールの導入がすでに進んでいることを踏まえるべきです。その上で、高リスクAIの管理に関する政策を検討する際、サイバーセキュリティ向けAIの導入を意図せず遅らせることは、結果としてセキュリティの意図せぬ低下を招きかねないということに留意すべきです。

cisco

AI強化型のフィッシング防御

ある金融機関では、行員を狙った高度なフィッシング攻撃が急増しており、機密性の高い顧客データや金融システムが危険にさらされる恐れがありました。そこで、エージェント型AIを活用して脅威を検証し、個別の調査計画を実行しながら、AI主導の優先順位付けによってセキュリティオペレーションチームの業務効率化を支援するCisco XDRを導入することで、ネットワーク、エンドポイント、メール、クラウド環境全体にわたる統合セキュリティを構築し、包括的な可視化と自動対応機能を実現しました。この導入により、フィッシングなどのサイバー脅威に対するセキュリティ体制が改善され、コンプライアンスプロセスの効率化が促進された結果、同行は金融サイバーセキュリティの最前線に躍り出ました。

elastic

オープンソースのAI駆動型セキュリティ

米国のある州政府機関は、コロナ禍の期間中、サイバー脅威とデータ量の異例の急増に直面しました。その結果、既存のオンプレミス情報技術インフラは処理能力の限界を迎え、公的資金が危険にさらされました。そこで、Elastic Securityへの移行によってセキュリティオペレーションをクラウドに

一元化し、Elasticのセキュリティ機能とAI機能を活用して異常なログインアクティビティをリアルタイムで分析することで、不正なアカウント乗っ取りを検知できるようになりました。この移行により詐欺計画に対する可視性が向上し、インシデント対応時間の短縮と5,000万ドルの税金の節約につながりました。

IBM

AI強化型の脆弱性管理

ある電子商取引企業は、広大なデジタルインフラ全体の脆弱性の特定と優先順位付けに苦労していました。そこで、IBMのAIベースのセキュリティソリューションを採用し、機械学習を活用して脆弱性を継続的にスキャンし、事業への潜在的な影響を評価するようにしました。これにより、セキュリティチームは最も重要な問題の修正に迅速に集中できるようになり、その結果、悪用のリスクが低減し、システム全体のレジリエンスが向上しました。

Microsoft

セキュリティチーム向けAIエージェント

ある医療機関は、セキュリティインシデントの件数や複雑さへの対処に課題を抱えており、その結果、対応の遅れやリスクの増大につながっていました。同機関のセキュリティチームは、脅威防御、デバイス管理、脅威インテリジェンスなどのアクティビティにSecurity Copilotエージェントを活用するMicrosoft Security Copilotを統合することで、インシデント発生時にリアルタイムのガイダンスと自動分析結果が提示されるようにしました。その結果、対応プロセスの効率化、解決時間の短縮、機密性の高い患者データの保護能力の強化につながりました。

okta

AIを活用したリスクベースの多要素認証（MFA）

あるSaaS企業は、生産性を低下させることなく情報システムへのアクセスを管理するという難題に直面していました。同社は、Okta Adaptive MFAの導入により、リスクに基づいて認証要件を調整できるようになりました。典型的なユーザー行動が示す低リスクのログインの場合、ユーザーは簡単な認証を利用できますが、高リスクのログイン試行の場合には、Oktaは生体認証やワンタイムパスコードなどの追加ステップを要求することで企業を保護します。AI対応の適応型認証は、追加の製品や不必要に面倒な手順なしでリスクを管理するのに役立っています。

paloalto NETWORKS

AI主導型のセキュリティオペレーションセンター（SOC）

米国のある州は、34機関3万5,000ユーザーをサポートしながら、州内30万エンドポイントでインシデントの検出と防止を行っていました。同州は、Palo Alto NetworksのAI強化型SOCを利用することで、平均解決時間を24時間以上から2分未満に短縮すると同時に、インシデントの86%を自動的に解決しました。このプロアクティブなアプローチにより、管理業務に追われていたセキュリティスタッフを、脅威ハンティングやインシデント対応といった高度な業務に再び集中させることができました。

SAP

AI駆動型のData Privacy Integration匿名化

ある製造業の顧客は、機密性の高い内部人事監査を実施する必要がありました。そこで、AI対応のSAP Data Privacy Integration（DPI）匿名化サービスを利用することで、仮名を生成し、それを使用して当該監査を実施した後、監査情報を実際の個人に関連付けることができるようにしました。このAI駆動型のサービスにより、同顧客は監査のセキュリティとプライバシーを確保することができました。

servicenow

AI支援型のセキュリティオペレーション

フォーチュン500に名を連ねる、あるSaaS企業は、厳しいサイバー脅威環境に直面していました。そこで、20種類以上のServiceNow AIエージェントを利用して、トリアージ、調査、監査対応のインシデント後レポートの作成など、幅広いセキュリティオペレーションやセキュリティタスクを支援することにより、アナリストがわずかな時間で作業を完了できるようにし、防御アクションを迅速化することで、生産性の大幅な向上を実現しました。統合、自動化、AIの組み合わせにより業務が効率化され、より迅速で効果的な検知・対応ソリューションを通じて、会社のセキュリティ体制強化に役立っています。

今後も前進

これらのユースケースは、サイバーセキュリティにおけるAIの応用が机上の空論ではなく、すでに企業を保護していることを示しています。企業や政府機関は、AIで強化されたサイバーセキュリティソリューションに投資することで、サイバーセキュリティリスクを効果的に管理し、国民や顧客により良いサービスを提供することが可能になります。