News Release

2020年10月19日
株式会社アイネス

アイネス、三菱総合研究所と連携し「CyCraft AIR」を用いた AI 主導型セキュリティオペレーションサービスを提供開始

―顧客のサイバーセキュリティ対応をワンストップで支援―

株式会社アイネス（本社：東京都中央区、代表取締役社長：吉村 晃一、以下 アイネス）は、株式会社三菱総合研究所（本社：東京都千代田区、代表取締役社長：森崎 孝、以下 MRI）と連携し、株式会社 CyCraft Japan（本社：東京都千代田区、代表取締役社長 兼 CEO：Benson Wu、以下 CyCraft）が独自開発した「CyCraft AIR」を用いた AI 主導型セキュリティオペレーションサービスを、2020 年 10 月 19 日に提供開始します。

1. 背景

世界中でデジタル化が進展する現在、企業・組織において、サイバーセキュリティの確保は極めて重要な経営課題となっています。企業等には CSIRT※1 や SOC※2 などのサイバー攻撃対応組織を設置して、サイバー攻撃を検知し対応する体制の構築が求められています。しかしながら、個々の企業等にとっては、日々進化するサイバー攻撃に対し技術的なキャッチアップを行い、十分な体制を構築することは、技術・資金・人材等の点から非常に困難です。

2. サービスの概要

アイネスは MRI と連携し、台湾に本社を置く CyCraft が独自開発した CyCraft AIR を活用してセキュリティオペレーションの支援サービスを拡充し、マネージドセキュリティサービス※3 の提供を開始します。本サービスによって、お客さまのサイバーセキュリティに関するコンサルティングから日々のセキュリティオペレーションまでを一貫して支援することが可能となりました。

従来のセキュリティオペレーションは、人手に依存するため運用コストが高く、また、インシデント発生時の原因分析に多くの時間を要するなどの課題がありました。このような状況に対し、CyCraft AIR を使うことでセキュリティオペレーションの多くを AI により自動化でき、貴重な人材をインシデント対応業務に集中させられる効果が期待できます。

アイネスは MRI と連携して、セキュリティオペレーションの業務設計から、CyCraft AIR の導入、SOC/CSIRT の運用支援、インシデント対応支援等をワンストップで実施するサービスを提供し、お客さまのサイバーセキュリティ対策強化と業務効率化の同時達成に貢献します。

3. CyCraft AIR の特長

CyCraft AIR は数万台規模のサイバーセキュリティ状況を一元的に管理でき、即時アラート通知、相関性解析、攻撃手法と経路調査および調査後の修復まで、ワンストップで対応することができます。さらに、オンプレミス型※4 やクラウド型、常駐監視型や単発サービスなど、お客さまのさまざまなニーズに柔軟に対応することができます。

CyCraft AIR で収集されたデータは CyCraft の分析センターへ送られ、マルウェアのサンプルやメモリ内のコマンド、その他シグネチャベース※5 のウイルス対策では分類できない疑わしい振る舞いを、AI を用いて調査します。その環境として、内部データソースに加え複数の外部データソースを統合することで脅威データベースを拡充し、有効なビジネスインテリジェンスを提供します。

CyCraft AIR は米 MITRE 社の MITRE ATT&CK® フレームワーク評価を受け、業界トップクラス

の不審行為検知能力を持つとの評価結果が 2020 年 4月に発表されました。また国内最大級のインターネットテクノロジーイベントである Interop Tokyo 2020 においては、セキュリティ部門の Best of Show Award グランプリを受賞しました。

4. 導入効果

CyCraft AIR を導入することで、従来数日から数週間かかっていたインシデント調査を短時間で実施できます。一連のプロセスが AI により自動化されることにより、遅くとも 12 時間以内にネットワーク全体の分析レポートが届けられ、効率的なトリアージ※6 と脅威ハンティングを可能にします。また、感染端末をネットワークから遮断してファイル削除やプロセス停止等を行うと同時に、リモートで復旧を行うことで、組織のレジリエンスを高めることが可能です。

5. 今後の展開

アイネスは MRI と連携し、大規模なセキュリティ専門部署を置くことが困難な中堅企業や、自治体・大学などを主な対象として、この CyCraft AIR を用いた AI 主導型セキュリティオペレーションサービスの導入運用の支援を行います。さらに、MRI をはじめ、パートナー企業と共に、お客さまの複雑化し変化し続けるサイバーセキュリティの課題に対して、グループの総合力でお応えできるよう、サービスの高度化を継続的に図っていきます。

※1 CSIRT: Computer Security Incident Response Team の略で、企業などに設置され、サイバー攻撃に関する情報を SOC から受け取り、調査・対応を行う組織
※2 SOC: Security Operation Center の略で、サイバー攻撃に関するサーバーやネットワーク機器が生成するログを監視し分析を行い、サイバー攻撃を検知する組織
※3 マネージドセキュリティサービス: 外部のセキュリティ専門家が、端末やネットワークを監視することで、SOC の機能（一部は CSIRT の機能）を代行するサービス
※4 オンプレミス型: 自社内でサーバー等の情報システムを構築・運用する形態
※5 シグネチャベース: コンピュータウイルスの特徴的なパターンや一部分をパターンファイルに保存しておき、ウイルスの疑いのあるファイル等を検査する際にそのパターンファイルと照合することでウイルスを検出する手法
※6 トリアージ: セキュリティインシデントが発生したときに、その重要性や緊急性に基づき対処の優先順位を定めること

■株式会社 CyCraft Japan について

株式会社 CyCraft Japan は台湾に本社を置く AI サイバーセキュリティ業界のリーダーです。最先端の CyCraft AI 技術でサイバーセキュリティ自動化サービスを提供しています。CyCraft AIR ソリューションには次世代アンチウイルスソフト、EDR、及び CTI が搭載されています。SIEM との連携も可能です。アジアの政府機関、フォーチュン・グローバル 500 企業、主要銀行および金融機関、台湾・シンガポール・日本・ベトナム・タイをはじめとする APAC 諸国の主要インフラ・航空・通信・ハイテック企業と中小企業に、サイバーセキュリティサービスを提供しています。日本、シンガポールに拠点を設けており、積極的にグローバルビジネスを展開しています。

URL：https://www.cycraft.com/ja-jp/

≪CyCraft AIR を活用した AI 主導型セキュリティオペレーションサービスの紹介ページ≫

https://www.ines.co.jp/service/CyCraft.html

＜本件に関するお問い合わせ先＞

株式会社アイネス
〒104－0053　東京都中央区晴海三丁目 10 番 1 号

【サービスに関するお問い合わせ】
株式会社アイネス　ＩＴソリューション本部　ＩＴ営業部　丹羽、武田
E-mail ： itsales@ines.co.jp

【報道関係者からのお問い合わせ】
株式会社アイネス 経営企画部　広報担当　内藤、鍬田
E-mail ： koho@ines.co.jp