【プレスリリース】

マカフィー株式会社
2021 年 2 月 3 日

※当資料は、米国時間 2021 年 1 月 28 日に米国で発表されたプレスリリースの抄訳です。

マカフィー、セキュリティ運用を変革する
エンドポイント、ネットワーク、Web 向けの業界初のプロアクティブな XDR を発表

クラウドネイティブの MVISION XDR は、
エンドポイント、ネットワーク、サードパーティのテレメトリを活用し、
攻撃前後の攻撃ライフサイクルを管理する前例のない先進的で実用的なインテリジェンスを提供

デバイスからクラウドまでを保護するサイバーセキュリティ企業である米国マカフィー（McAfee Corp、本社：米国カリフォルニア州、Nasdaq：MCFE）は、MVISION Extended Detection and Response（XDR）の一般提供を発表しました。Web およびネットワークテレメトリを加え、エンドポイントに留まることなく脅威の検出や対策を統合し最適化することで、より迅速で積極的な調査サイクル、自動化による対応の簡素化、セキュリティ オペレーション センター（SOC）の継続的な最新化などを実現します。

マカフィーのエンタープライズ戦略グループ[1]の調査によると、80%以上の組織が、脅威にあふれた今日の状況に危機感を抱き、脅威の検出・対策のためのソリューションへの投資を増やすことを計画をしています。具体的には、調査対象の組織の 3 分の 2 以上が半年から一年以内に XDR に対する投資を予定しており、半数近く（48%）は個別に管理しているソリューションを統合型 XDR ソリューションに置き換えることを検討しています。

エンタープライズ戦略グループ シニアプリンシパルアナリストのジョン・オルシック（Jon Oltsik）は、次のように述べています。「組織にはもはや、効果のない脅威対策ツールとコンテキストを導入する余裕はありません。XDR の活用は、SOC の現レベルを向上させるチャンスにつながると考えています。既存ツールを使った、時間と労力のかかる受け身の運用方法ではなく、悪意ある行為を事前に予測し、自動化によって対策の決定を迅速に行うことができる、包括的な統合型 XDR ソリューションの活用に移行するよい機会です。」

マカフィーの最高製品責任者であるシシル・シン（Shishir Singh）は次のように述べています。「セキュリティチームは、手動で時間のかかる受け身の調査プロセスから、全体的な管理のコストと複雑性を軽減しつつ、より高度で頻繁な攻撃に対抗するために悪戦苦闘しています。MVISION XDR は、主な攻撃経路に関する積極的で実用的なコンテキストを提供します。企業全体で脅威の検証と対応を簡素化、迅速化、自動化することで、SOC リソースを最大限に活用し、事業への影響を軽減します。」

ガートナーの XDR ソリューションのリスクと利点に関するレポート[2]（英語）では、次のように述べられています。「XDR 製品は Endpoint Detection and Response（EDR）プラットフォームが自然に進化したものであり、セキュリティチームにとって主要なインシデント対応ツールとなっています。XDR

製品の主な価値提案は、より多くのセキュリティコンポーネントをひとまとめにすることで、セキュリティ運用の生産性を向上させ、脅威の検出および対応機能を強化することです。それらを統合することで、複数のテレメトリストリームを提供し、さまざまな検出形式の選択肢を提示し、同時に複数の対応が可能になります。」

MVISION XDR の一般公開により、マカフィーは SOC エクスペリエンスを向上させます。アナリストがエンドポイントだけに留まらず、脅威のコンテキストをより包括的に把握できるようにすることで、無駄な時間を省き、脅威が発生したり被害を受ける前に、脅威をよりよく理解した上で慎重に行動できるようになります。MVISION XDR は、次の機能を備えています。

- **積極的で実用的なインテリジェンス:** MVISION Insights は、先を見越した脅威の優先順位付け、対応、適切な行動の指示に役立ちます。
- **AI ガイド付き調査:** AI ガイド付き調査、MITRE ATT&CK との紐づけ、リアルタイムハンティングにより、高度な脅威キャンペーンの調査を簡素化します。
- **クラウドの脅威の統合:** Web アクティビティのコンテキスト、アクセスの追加経路や制御コマンドの可視性の向上など、攻撃の包括的な概要を提供します。
- **ネットワークテレメトリの優先順位付け:** 必要な情報を収集、整理された脅威に自動的に関連付けることで、ネットワークの脅威をより深く理解し、優先順位付けと対応策の決定を向上させます。
- **SOC インフラの最適化:** チケットシステムや Secure Orchestration Automation Response（SOAR）ツールなどの既存の SOC インフラと統合することで、SOC への投資の利益率を最大化し、効率的な自動化と迅速な負担軽減を実現します。

マカフィーは、迅速な調査と解決でサイバーリスクを最小限に抑える包括的且つ積極的なアプローチにより SOC を支援するため、引き続き XDR の開発を積極的に進めます。

詳細は McAfee MVISION XDR をご覧ください。

1 Enterprise Strategy Group, “The Impact of XDR in the Modern SOC,” November 2020
2 Gartner Innovation Insight for Extended Detection and Response, Peter Firstbrook, Craig Lawson, 19 March 2020（英語）

参考情報：

- What Is Extended Detection and Response (XDR)?（英語）
- マカフィーブログ：XDR への道

マカフィーについて

マカフィーはデバイスからクラウドまでを保護するサイバーセキュリティ企業です。業界、製品、組織、そして個人の垣根を越えて共に力を合わせることで実現するより安全な世界を目指し、マカフィーは企業、そして個人向けのセキュリティ ソリューションを提供しています。
詳細は https://www.mcafee.com/enterprise/ja-jp/home.html をご覧ください。

＜本情報のお問い合わせ＞

マカフィー株式会社（ https://www.mcafee.com/enterprise/ja-jp/home.html ）
広報担当 戸田
Tel: 070-2680-0731
hiromi_toda@mcafee.com