We bring security to life.

報道関係各位

2022/10/4
Trellix

※当資料は、米国時間 2022 年 9 月 28 日に米国で発表されたプレスリリースの抄訳です。

Trellix（トレリックス）、セキュリティオペレーションを変革する XDR プラットフォームを拡張

Trellix XDR で、エンドポイント、ネットワーク、データ上の脅威の検出・対応を統合し、シンプルなセキュリティ運用体験を提供

XDR（Extended Detection and Response）の未来を提供するサイバーセキュリティ企業である Trellix は、本日、XDR プラットフォームを拡張することを発表しました。「Trellix XDR」は、4 万を超えるお客様がより優れたサイバーレジリエンスを構築し、既存のセキュリティツールの価値を最大限に引き出し、検出と対応に要する平均時間を短縮することを実現します。

Trellix の CEO であるブライアン・パルマ（Bryan Palma）は次のように述べています。
「私たちは業界で最も包括的な XDR プラットフォームを保持しています。旧来の SIEM（Security Information and Event Management）技術は、セキュリティ運用の近代化に寄与していません。Trellix XDR はこの極めて重要なギャップを埋めることができると確信しています。」

Trellix XDR
2022 年第 4 四半期に登場するアップグレードした XDR エンジンは、セキュリティ運用チームに、ガイド付き調査のための強化されたプレイブック、マカフィーとファイア・アイのアセットの統合によってアップグレードされた脅威インテリジェンス、そして「Trellix Event Fabric」の提供を開始します。Trellix Event Fabric は、あらゆるクラウドサービスプロバイダーからの異なるセキュリティデータを連携し、セキュリティアナリストがどこからでもデータにアクセスし、データ間の関連付けを可能にします。この機械学習と自動化の組み合わせにより、セキュリティ運用チームは、平均検出時間の短縮、ならびに平均応答時間の改善を実現することができます。

Clario のセキュリティ＆リスク担当シニアディレクター、ケイト・ダウニング（Kate Downing）氏は次のように述べています。
「Trellix XDR は、脅威に対する可視性とコンテクスト情報を提供してくれます。以前なら対処できなかったような事象をより高度なレベルで認識でき、セキュリティチームが迅速に影響の拡大を排除することにより、攻撃の深刻さと範囲を縮小することができるのです。」

Trellix XConsole
XConsole はセキュリティ運用チームに単一のインターフェイスを提供し、Trellix XDR 全体の操作性を効率化します。共通の運用状況に関する情報を提供することで、これにより、お客様は使用中の Trellix のテクノロジー及びサードパーティのセキュリティツールへの投資を最大限に活用できます。また、単一のユーザーインターフェイスを活用することで、アナリストと対応担当者は、ネットワーク、エンドポイント、データ、電子メール、およびクラウドの攻撃対象領域の可視性を高め、さらに全体的な脅威状況を迅速に把握できます。Trellix XDR のコントロールセンターである XConsole は、2023 年初頭に利用可能となります。

Media@Trellix.com

当社のパートナーのひとつである Ingram Micro のシニアバイスプレジデント兼チーフカントリーエグゼクティブであるアリ・バグダディ（Ali Baghdadi）博士は次のように述べています。
「Trellix XDR は、統合的なセキュリティオペレーションコンソールを搭載し、組織内のすべてのツールからデータを取り込むことで全体の統合を実現します。この使いやすいプラットフォームは、当社のお客様にとって非常に魅力的です。」

Trellix Endpoint
2023 年初頭に提供を開始する「Trellix Endpoint」は、エンドポイント保護、エンドポイント検出と応答、分析全体における、マカフィーとファイア・アイの技術を統合し、業界内で最高レベルのエンドポイントの多層防御が可能となります。

Trellix Endpoint では、以下を提供します。

- 多層的なランサムウェア対策
- なりすましや不正使用を防止するための ID 検出と対応
- 攻撃対象領域管理による重要な脅威の優先順位決定
- デジタル・フォレンジックとインシデントレスポンスによる根本原因の迅速な特定

Trellix Network Detection & Response （NDR）
「Trellix Network Investigator」は、サイバーキルチェーンにおいて脅威を検出、調査、対処するための総合的なソリューションを提供します。Trellix の既存の機械学習モジュール、イベントベースのパケットキャプチャ、ネットワークトラフィック・ハンティング機能を単一のソリューションに統合することにより、お客様は既存の Trellix ネットワーク製品に NDR 機能をすぐに導入することができます。Trellix Intrusion Prevention System、Trellix Network Security、Trellix Network Forensics といった各製品からのシグナルを活用し、最初の感染後の活動を特定することで、お客様はラテラルムーブメントやデータ流出を防ぐことができるようになります。Trellix NDR ソリューションによるトリアージと調査機能との組み合わせで、感染後のさらなる被害拡大を防止できるようになります。Trellix Network Investigator は、当社の Detection as a Service のサブスクリプションによって補完されています。Trellix Intrusion Prevention System のすべてのお客様が Detection as a Service を利用でき、SaaS とプライベートクラウドのオプションで導入可能。お客様はゼロデイ保護とマルウェア分析を受けることができます。

Trellix Advanced Research Center について
Advanced Research Center は、セキュリティ研究者、アナリスト、対応者の精鋭チームを結集し、斬新な洞察と実用的なリアルタイムのインテリジェンスを生み出しています。Trellix のセンサーネットワークから得られるセキュリティテレメトリーに、他に類を見ない業界インテリジェンスを組み合わせて活用することで、Trellix のテクノロジーは最先端の脅威指標を備えることを約束します。Advanced Research Center は、Trellix の 4 万を超えるお客様に継続的な敵対研究、脅威情報、製品アップデート、機械学習アルゴリズムを提供しています。

参考情報

- Trellix Xpand Live Media Kit （英語）

Media@Trellix.com

Trellix について
Trellix は、サイバーセキュリティの未来を再定義するグローバル企業です。オープンかつネイティブな Trellix の XDR（Extended Detection and Response）プラットフォームは、現在最も高度な脅威に直面するお客様が業務の保護や回復に確信を持って対応するための支えとなります。Trellix のセキュリティ専門家は、広範なパートナーエコシステムとともに、データサイエンスと自動化によりテクノロジーイノベーションを加速させ、4 万を超える企業や政府機関のお客様の力となっています。

＜本情報のお問い合わせ＞
Trellix（McAfee Enterprise）
広報担当 戸田
Tel: 070-2680-0731
hiromi.toda@trellix.com

Trellix（McAfee Enterprise）広報担当
LaCreta 担当：野澤 / 近藤
Tel: 050-4560-2425
trellixjpn@lacreta.jp