2024 年 3 月 25 日
サイバーリーズン合同会社

サイバーリーズンと Observe が 新しいソリューション「Cybereason SDR」を発表、 生成 AI の時代に SIEM と XDR を融合することで、可観測性を 通じてセキュリティに革命を起こす

※本資料は日本時間 2023 年 3 月 25 日に Cybereason Inc.（米国本社）が発表したリリース文の抄訳です。

日本、東京（2024 年 3 月 25 日）- サイバー攻撃対策ソリューションのリーディングカンパニーである Cybereason Inc.（以下「サイバーリーズン」）は、本日、Observe Inc.（以下「Observe」）と共同で、新しいソリューション SDR（SIEM Detection and Response、以下「Cybereason SDR」）を発表しました。

Cybereason SDR の SaaS ソリューションは、従来型の SIEM アーキテクチャの課題を解決し、組織のあらゆる IT インフラストラクチャデータの自動取り込みと価値の向上を通じて SOC の有効性を強化します。

すべてのセキュリティデータを中央データレイクへと統合： Cybereason SDR は、従来型の SIEM アーキテクチャの課題を解決し、すべてのセキュリティログ、イベント、トレースを取り込むためのコストの障壁を取り除きます。これにより、自社全体を通じて有意義な可視性を確保できるようになります。Cybereason SDR は、すべてのサイロ化されたデータを 1 つの統一的な可観測性プラットフォームへと統合することで、検知、調査、対応を合理化します。これにより、サイバー侵害を早期に阻止しつつ、ビジネスの回復力を確保できるようになります。

オープンアーキテクチャ：Cybereason が持つオープンアーキテクチャにより、構造化データおよび非構造化データを取り込むことで、既存のエンタープライズ IT スタックおよびセキュリティスタック全体を通じて重要なインサイトを得ることができます。制限の多いベンダープラットフォームに縛られることはありません。このアプローチにより、企業は SDR を既存のインフラストラクチャへとシームレスに統合することで、投資利益率を最大化しつつ混乱を最小限に抑えることができます。

AI 駆動型の高度なアナリティクス：サイバーリーズンのコアテクノロジーと可観測性を組み合わせることで、SecOps チームは、IT 資産全体にわたって AI 駆動型のアナリティクスを利用できるようになります。MalOp™検知エンジンを搭載したサイバーリーズンのコアテクノロジーは、自動化されたトリ

アージと調査ワークフローを可能にすることで、攻撃の完全なストーリーを構築します。これには、根本原因、攻撃のタイムライン、影響を受けたデバイス、ユーザー、およびその他の資産などが含まれます。

この自動化されたアプローチにより、平均検知時間（MTTD）を大幅に短縮できます。また、サイバーリーズンが提供する統一的なポータルにより、複雑で高度なサイバー攻撃に対処するためにガイド付き修正を含む迅速な対応が可能となります（MTTR を短縮）。

■製品詳細ウェブページ
URL： https://www.cybereason.co.jp/products/sdr/

サイバーリーズンの会長兼 CEO である Eric Gan（エリック・ガン）は次のように述べています。
「私たちは、この強力なソリューションを発表できることをとても嬉しく思っています。当社は、パートナー企業との数ヶ月に及ぶ共同作業により、飛躍的なデータの増大、IT の複雑性、高度な生成 AI がもたらす脅威など、顧客の実際のニーズに合ったテクノロジーを構築する機会を得ることができました。この新しいソリューションは、スケーラブルな可観測性プラットフォームを提供します。これを利用することで、多様な IT プラットフォーム全体を通じて脅威の相互関連付けを迅速に行えるようになると同時に、データコストを削減し、ソフトウェアの統合を実現できるようになります。

Observe の CEO（最高経営責任者）である Jeremy Burton（ジェレミー・バートン）氏は次のように述べています。
「サイバーリーズンは、セキュリティはデータの課題であると認識しており、 Observe は、すべてのセキュリティ・イベント・データを単一の中央データレイクに統合することができます。 これにより、組織のセキュリティ状況の可視性が向上し、最新のクラウドアーキテクチャによりコストも削減されます。」

＜サイバーリーズンについて＞
サイバーリーズンは、将来を見据えたサイバー攻撃対策ソリューション分野におけるリーディングカンパニーであり、エンドポイント上、クラウド環境、そして企業のエコシステム全体においてサイバー攻撃を阻止するために、防御者と一丸となって尽力しています。現時点で最新のランサムウェアや高度な攻撃手法にも負けることのない、予測的な防御、検知、対応を提供できるソリューションは、AI 駆動型の Cybereason Defense Platform のみです。サイバーリーズンの MalOp™は、影響を受けるすべてのデバイス、ユーザー、システムに対して、コンテキストリッチな攻撃インテリジェンスを比類のないスピードと精度で即座に提供します。それにより脅威データをビジネススピードで実用的な意思決定の手段へと変えることができます。またサイバーリーズンは、カリフォルニア州に本社を

置き、世界 40 ヶ国以上に顧客を持つ非上場の国際企業です。詳しくは、https://www.cybereason.com/をご覧ください。

＜Observe について＞

Observe は、アプリケーションから放出される機械生成データを統合し、そのデータを人間が理解できるものへと変えます。数 10 億件ものイベントの中から有意義なヒントを探し出す代わりに、エンジニアは今や、顧客、コンテナ、ビルド、チケットなどの、慣れ親しんだリソースについて質問できるようになっています。Observe は、これらのリソース間における関係を表すグラフを維持し、それらの関係が時間と共にどのように変化するかを記録します。この機能は、未知の問題を調査する際に、コンテキストを簡単に提供するために重要となります。なお、Observe が持つ独自のクラウドネイティブアーキテクチャのおかげで、当社が提供する製品の価格は、同業他社よりも最大で 1 桁安価となっています。詳しくは、https://www.observeinc.com/about-us/をご覧ください。