

2022年3月29日
サイバーリーズン・ジャパン株式会社

「サイバーリーズン・ジャパン 事業戦略発表会」を開催
～ランサムウェア攻撃や国家を背景とした高度なサイバー攻撃が増加のなか、
サイバー攻撃の検知・把握・予測を実現する“AI 駆動型 XDR”の事業戦略を発表～

AI(人工知能)を活用したサイバー攻撃対策プラットフォーム「Cybereason」を国内向けに提供するサイバーリーズン・ジャパン株式会社(本社:東京都中央区、CEO:アロン・ラスキン、以下「サイバーリーズン・ジャパン」)は、2022年3月28日(月)に「サイバーリーズン・ジャパン 事業戦略発表会」を開催し、サイバーリーズン・ジャパンの日本市場における事業戦略や、Google Cloudと共同で開発を進めている「Cybereason XDR powered by Google Chronicle」(以下、Cybereason XDR)の概要について発表いたしました。



近年、サイバー攻撃の手口がより巧妙化し、ランサムウェア攻撃や国家を背景にした高度なサイバー攻撃など、規模の大小問わず、企業のシステムあるいは事業停止に追いやれる被害が多く報じられており、さらには企業のDX(デジタル・トランスフォーメーション)推進やコロナ禍によるテレワークの常態化によって、セキュリティの脅威に晒されるリスクも高まっています。こうした状況下のなか、サイバーセキュリティ対策は企業が存続していく上でも、必要不可欠な取り組みとなっております。国家、犯罪組織が絡んだサイバー攻撃の組織化や多様化に合わせ、今後のセキュリティ対策はますます重要性を帯びているなか、サイバーリーズン・ジャパンはGoogle Cloudと戦略的パートナーシップを結び、AIの高精度な技術によってサイバー攻撃の検知・把握・予測を今までにないスピードで行うことができるAI駆動型の「Cybereason XDR」を共同開発いたしました。本製品は今年の7月頃に提供

を開始いたします。提供にあたって、近年のサイバーセキュリティにおける現状と「Cybereason XDR」の概要や事業戦略を発表いたしました。

■ サービス詳細ウェブページ

<https://www.cybereason.co.jp/products/xdr/>

■ 人と情報がサイバー攻撃に屈しない未来を創造する

冒頭では Cybereason Inc. 共同創業者兼 CEO リオ・ディヴが登場。世界有数のサイバーセキュリティ技術を持つイスラエル軍の 8200 部隊にてキャリアをスタートしたリオは、2013 年にサイバーリーズンを創業し、世界各国で発生する巧妙かつ悪質なサイバー攻撃を阻止してきました。

テクノロジーなくしては、豊かな生活が送れなくなった今、常にサイバー攻撃の脅威と隣り合わせになっているとも言えます。強固なセキュリティをも突破する、技術と知見を持った攻撃者が優位に立つ状況を打破するという思いを強く胸に持っているリオは「誰もがつながっているオープンな世界で、人々や情報を守る」と、人と情報がサイバー攻撃に屈しない未来を目指していくことを語りました。

今回、日本市場にも提供開始が開始される Cybereason XDR について、リオは「唯一無二の技術であり、ハッカーからのあらゆる攻撃を予測し、対処することができる」と述べました。

■ Cybereason XDR が見出す 3 つの特長と製品力

次いで、サイバーリーズン・ジャパン株式会社 CEO のアロン・ラスキンが壇上に上がり、日本市場での事業戦略と今後の展望についてプレゼンを行いました。

これまで日本法人にて、オペレーションとチーム全体を率いてきたなか、「今年はサイバーセキュリティにおける重要な転換期になる」と強調しました。2020 年から長期化するコロナ禍では、セキュリティインシデントが従前に比べて 300%増加。また、世界中のデータは 2025 年に 175ZB (ゼタバイト) まで膨れ上がり、データ爆発時代の到来が予見されています。このような状況化において、サイバーセキュリティにおける人材不足は深刻で、犯罪者によるサイバー攻撃から身を守るためには、サイバーセキュリティの強化が急務となっています。

インターネットが発展し、あらゆるデバイスや SaaS 系のクラウドサービスなどから簡単にさまざまな情報へアクセス可能になったことは、裏を返せばそれだけ攻撃の標的にされやすいとも言えます。攻撃の対象が増えれば、「従来のようなスマートフォンやタブレット、PC といったエンドポイントでのサイバー攻撃の検知や対応では、対処しきれなくなっている。今の時代、脆弱性が何なのかを理解し、対処療法的ではなく攻撃者に侵入される前に防御することが求められている」とアロン・ラスキンは説明しました。



そして、「サイバー攻撃を仕掛ける側は、0.001%のセキュリティの脆弱性を突き、バリアを打ち破ることができれば成功になる。攻撃の仕方が多様化し、ますます悪質になってきていることから、防御する側は攻撃の手口を予測し、対処していくことで100%被害を防がなければならない」と話しました。そこで、新たに提供を開始する Cybereason XDR は「次の3つの特長を兼ね備えている」と説明します。

①Planetary-Scale eXtendability (拡張性)

従来のエンドポイントにおけるログデータのみならず、ネットワーク、ID 管理・統合認証、クラウドサービスなど、IT 環境全体から膨大な量のデータを Google Chronicle に集約することができます。地球規模のデータ量に匹敵する 9.8PB (ペタバイト) のサイバー脅威情報を、週次で取り込み分析することで、広範囲にわたるサイバーセキュリティ強化を実現します。

②Operation-Centric Detection (攻撃オペレーションの検知)

さらに、サイバーリーズンの持つ攻撃予測型 AI により、Malop (悪意のある操作) を迅速に予測し、対処することでセキュリティ対策の効率化や効果を飛躍的に向上させます。

③Predictive Response (予測対処)

そして、サイバー攻撃を仕掛ける側の目的を予測し、完全に自動化された対処を講じることで、解決までの時間を 93%短縮します。24 時間 365 日、リアルタイムでのマネージドサービスを提供することで、「1 分以内に検知、5 分以内に解析、30 分以内に修復」という“1-5-30 モデル”を構築し、またダッシュボードやレポート機能を提供することで、攻撃の全体像や見えない脅威を可視化できます。

■今までに類を見ない強固なセキュリティ体制を構築できる

続いて、サイバーリーズン・ジャパン株式会社 マーケティング本部 プロダクトマーケティングマネージャーの菊川 悠一が登場。昨今、マルウェア「Emotet (エモテット)」による攻撃やランサムウェア攻撃の「二重脅迫」が取り沙汰されるなか、被害を最小限に食い止め、早期復旧を目指すためには「フ

アイアウォールや内部ネットワークなど、エンドポイントとなる端末以外の広範囲な可視化や相関解析を行い、根本的な原因を特定することが不可欠になっている」と説きます。



また近年では、大企業の関連会社や子会社へサイバー攻撃を仕掛け、その会社の操業ひいては事業をも止めてしまう可能性があるサプライチェーン攻撃も顕著になってきています。サイバーリーズンのグローバル調査によると、ランサムウェア攻撃に遭い、身代金を支払ってしまった組織の80%が、「再びサイバー攻撃を受けた」といいます。つまり、再発防止には現状のサイバーセキュリティの課題や何度もインシデントを起こす原因の特定が、非常に重要となります。Cybereason XDRは、単一のプラットフォーム上で、徹底したサイバーリスクや脅威を追求し、さらには組織内の重要な情報資産を多面的に監視することで、強固なサイバーセキュリティ体制の構築を促します。

また、世界中で利用される Google Cloud と共同開発した唯一の XDR ベンダーとしての優位性を生かし、Google Chronicle と連携するさまざまなソリューションとシームレスにつなぎ込むことが可能になります。情報セキュリティの考え方として広まる「ゼロトラスト」の課題は、IT ツールやデータがサイロ化（社内システムオペレーションが乱立してしまっている状態）していることにあります。Cybereason XDR を活用することで、「保護対象の一元化や網羅性、インシデント対応におけるスピードも強化が可能になる。さらに、サイバーリーズンで集約された広範囲に渡るデータを自動で相関解析することで、ログ解析における作業時間を大幅に削減できる」と菊川は説明しました。

■ パートナーエコシステムを拡張し、XDR テクノロジーを全国に広める

最後にサイバーリーズン・ジャパン株式会社 シニア・エグゼクティブ・バイスプレジデント 瀧本 昌嗣が「本市場での事業展開&パートナー戦略」について発表しました。

サイバーリーズン・ジャパンの事業成長の肝になるのは「パートナーエコシステムをさらに拡張し、全国の企業様に安全を届けること」だと話します。サイバーセキュリティにコストをかける大企業だけでなく、中堅企業向けにコストを抑えた製品の訴求を行うほか、新規のディストリビューターや販売店の開拓をしていくことで、XDR テクノロジーを全国に広める青写真を描いていると言います。



こうした販売店ネットワークを、2022 年度中に 151 社へと拡大することを念頭に、「日本全国 8 万社のお客様へ、安全で強固なセキュリティ環境を提供していきたい」と抱負を語りました。そして、セキュリティベンダーの中では唯一、ISMAP(政府情報システムのためのセキュリティ評価制度)の認定を受けている背景から、「行政機関へのシステム導入も視野に、サイバーリーズンの EDR、MDR サービスや XDR テクノロジーを普及させ、より安全なセキュリティ環境を提供できればと考えている」と述べ、発表会を締めくくりました。

<サイバーリーズン・ジャパン会社概要>

社名： サイバーリーズン・ジャパン株式会社

設立日： 2016 年 3 月 9 日

CEO： アロン・ラスキン

所在地： 東京都中央区京橋 1-18-1 八重洲宝町ビル 5F

資本金等:4 億 9 千万円

事業内容:サイバー攻撃対策プラットフォーム「Cybereason」の日本市場での提供およびそれに付帯する事業

URL: <https://www.cybereason.co.jp>

<「Cybereason」の概要>

「Cybereason」は、サイバー攻撃から企業や団体のシステムを安全かつ確実に保護するサイバー攻撃対策プラットフォームで、企業・団体内の膨大なデータをあらゆる角度から深く分析する機械学習エンジンとグラフ処理システムを構築し、提供します。次世代アンチウイルス(NGAV)や、ランサムウェア対策、悪意のある PowerShell への対策、EDR 機能などを搭載するフルスタックの振る舞い検知型ソリューションである「Cybereason」は、これまでにない脅威を可視化し、複雑化する高度なサイバー攻撃を阻止する力をお客さまへ提供します。

- Cybereason および Cybereason のロゴは、Cybereason Inc.の米国、日本およびその他の国における登録商標または商標です。
 - その他、このプレスリリースに記載されている会社名および製品・サービス名は、各社の登録商標または商標です。
 - このプレスリリースに記載されている内容、製品・サービスの価格、仕様、問い合わせ先およびその他の情報は、発表日時点のものであり、これらの情報は予告なしに変更される場合があります。
-