2023 年 4 月 20 日
サイバーリーズン合同会社

サイバーリーズンによる最新調査で ランサムウェア攻撃とサイバーセキュリティ人材不足が セキュリティオペレーションセンター（SOC）を 圧迫していることが明らかに

※本資料は米国時間 2023 年 3 月 14 日に Cybereason Inc.（米国本社）が発表したリリース文の抄訳です。

米国、マサチューセッツ州、ボストン（2023 年 3 月 14 日） - XDR 分野における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、セキュリティオペレーションセンター（SOC）に関するグローバル調査の結果と、サイバー攻撃やサイバーセキュリティの人材不足が SOC を最新化するために与えた影響について発表しました。本調査では、ランサムウェア攻撃によるサイバーセキュリティの人材不足、可視性や自動化の欠如、ツールの増加、アラート過多などから、組織が直面する継続的な課題を取り上げています。

「2023 年版 ランサムウェアと最新の SOC～ランサムウェアが SOC を最新化するために与えた影響～」と題されたこの調査は、1,203 人のサイバーセキュリティ担当者を対象に実施され、彼らが直面する最大の脅威としては、49％の回答者がランサムウェアと回答し、次いでサプライチェーン攻撃が 46％、日常的な標的型攻撃が 31％であることが明らかになりました。回答者の 30%以上が、拡大するランサムウェアの脅威に対処するために、より多くの人材およびサービスを必要としています。

全体としては、調査回答者の 31%が、ランサムウェアの脅威を契機に、組織に対するサイバー攻撃の全容をよりよく把握し、可視化する必要があることが明白になったと回答しています。平均して米国の 35%の回答者が、より深い攻撃の洞察力と可視性を必要としています。イタリアでは、この数字は 46%と大きく上昇しています。旅行・運輸業界では、57%以上の回答者が脅威の可視化を必要としており、次いで小売、飲食、レジャー業界の回答者が 39%となっています。

「ポストコロナ時代の世界において、最新の SOC は、業界をリードする検知、予防、可視化、自動化技術を活用する分散型の機能ベースの組織である必要があり、これらの技術はすべてマネージドサービスによって強化されることが多いと言えるでしょう」と Cybereason Inc.の CISO であるイスラエル・バラックは述べています。

このレポートの全文は下記のリンクから入手できます。
【グローバル調査結果】

2023 年版 ランサムウェアと最新の SOC～ランサムウェアが SOC を最新化するために与えた影響～

https://www.cybereason.co.jp/product-documents/survey-report/10369/

調査方法について

本調査は、2022 年 9 月から 10 月に Censuswide 社が実施したものであり、米国、英国、フランス、ドイツ、イタリア、南アフリカ、アラブ首長国連邦、シンガポールの各国におけるサイバーセキュリティ担当者が回答者として参加しました。また本調査で対象となった主な業種としては、テクノロジー、製造、金融サービス、小売、ヘルスケア、自動車、法務、政府機関などです。

Cybereason について

サイバーリーズンは、ボストンに本社を置き、40 カ国以上に顧客を持つ非上場の国際企業で、エンドポイントやクラウドなど企業のエコシステム全体を標的にしたサイバー攻撃を終息させるため、XDR、EDR、EPP ソリューションと MDR サービスなどのセキュリティサービスを提供しています。Cybereason Defense Platform は、進化し続けるランサムウェア攻撃や高度な攻撃手法に対して圧倒的な防御、検知、対応能力をお客様に提供するとともに、すべてのデバイス、ユーザー、システムへの一連のサイバー攻撃をコンテキストに富んだインテリジェンス（MalOp）として比類のない速度と精度で可視化することで、サイバー脅威データをビジネスにおける実用的な意思決定手段に変えることができます。