ホワイトペーパー

サイバーセキュリティとサイバーレジリエンスにおけるベストプラクティス

データセキュリティアライアンスのホワイトペーパー

目次

要旨

企業や政府機関を F1 レースカーに例えてみてください。 最高クラスの国際レースに出場するために、毎日何時間もかけて準備をしますが、同じトラックはありません。競争はさまざまです。ドライバーは人間です。天気も変わります。しかし、他のどんな要素よりも、成功の鍵を握っているのは、優れたピットクルーの存在です。

サイバーレジリエンスにも同じことが言えます。F1のピットクルーと同じように、優れたデータセキュリティとデータ管理を組み合わせた技術的に統合されたサイバー防御を持つことは、組織が順調にコースを走り、力強くゴールするのを確実にするのに役立ちます。

2022年11月、セキュリティ業界のトップ企業 十数社で、企業や政府がサイバー攻撃との競争に勝つためのより多くの方法を提供するために、データセキュリティアライアンスを結成しました。そのミッションは明確で、データのセキュリティと保護を目的としています。本アライアンスは、データセキュリティとデータ管理をサイバーセキュリティと統合し、サイバーレジリエンスを向上させ、重要な技術の統合とアーキテクチャ、ベストプラクティス、そして共通の目標を中心としたソートリーダーシップを提供することによって、これを達成します。

データセキュリティアライアンスが発表したこのホワイトペーパーでは、シニアリーダーが、よりスマートなサイバーレジリエンスへの投資を通じて、リスクの低減やコンプライアンスの強化など、ビジネスの最優先課題に取り組む方法を概説します。また、NIST の新しいサイバーレジリエンスのエンジニアリング分野も考慮に入れ、データセキュリティアライアンスの総合的なビジョンとテクノロジーに沿ったベストプラクティスを紹介します。そして、メンバー組織が脅威に対抗するためのアイデアや戦略を、個々の企業レベルから業界レベルにまで高め、NISTサイバーセキュリティフレームワークと同期しながら、特定、防御、検知、対応、復旧に焦点を当てて解説します。

サイバーレジリエンスの重要性

今日のデジタル世界では、コンシューマーも企業も、あらゆる種類や規模の組織がシステムの停止なくオペレーションが行えることを期待しています。サービスレベル契約などの契約上の義務でさえ、それを要求します。しかし、計画的なものであれ、計画外のものであれ、インシデントが発生するとダウンタイムを引き起こす可能性があります。このようなときに重要になるのが、サイバーレジリエンスです。

> **「データをセキュアかつ倫理的な方法で価値に変換することは、今後10年間、ビジネスの急務になります。データのライフサイクルをコントロールする人が、その運命を最も方向づけることになります。データの価値に対する認識が高まるにつれて、データは企業スパイや国家によるサイバー攻撃の標的にされやすくなります」**[1]
>
> – **Jan-Peter Ohrtmann博士**、パートナー、PwC

サイバーレジリエンスの目標は、脅威が増大する中で、最高レベルのオペレーションとビジネスの継続性を達成することです。サイバーセキュリティは、定期的なパッチの適用、脅威の検出、脆弱性の発見などを含む、実用的で必須のサイバー衛生の慣行で、サイバーレジリエンスの基礎となるものですが、完全とはいえません。サイバーレジリエンスは、ディザスタリカバリの域をはるかに超えるもので、組織は、数日や数週間単位ではなく、数分または数時間単位で障害を予測し、それに耐え、障害から回復し、障害に迅速に適応することも必要になります。

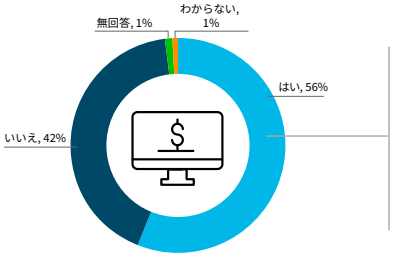
[1] PwC. “Privacy Megatrends 2030: A Roadmap for CEOs,” Dr. Jan-Peter Ohrtmann, 21 Jan 2021.

Forrester社のステファニー・バラウラス副社長 (グループダイレクター) は、2020年5月に「レジリエントな企業は、リスクの特定と軽減のための戦略と枠組み、徹底した事業継続計画と準備、柔軟な危機と事故対応能力、冗長性とディペンダビリティ (信頼性) のために設計された業務システムを備えてる」と書いています[2]。それからわずか数年で、何十万件ものランサムウェア攻撃が発生するようになり、企業にはサイバーレジリエントな戦略とフレームワークも必要になっています。

サイバー脅威、特にランサムウェアは、より頻繁に、より巧妙になり続けています。そのため世界中の組織は、24時間365日体制でサイバーレジリエンスを最大化するために、通常サイロ化されているセキュリティチームとデータ管理チームとソリューションの新たな連携を進める必要があります。テクノロジーとプロセスの統合によってのみ、組織の最新のデジタル基盤は、サイバー攻撃、自然災害、システム障害に耐え、復旧することが可能です。

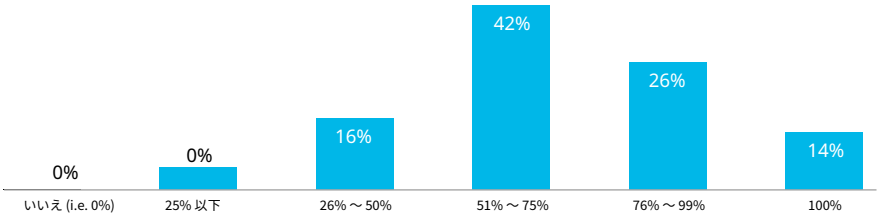
このような背景から、データ保護は急速にビジネスや政府のリーダーにとって最優先事項となっています。顧客ロイヤルティ、ブランドの評判、国家の安全性は、卓越したデータ保護にかかっており、戦略的リーダーは、サイバーレジリエンスの目標を達成するために必要な人材、ポリシー、ソリューションを導入するために、技術的な対応者である最高情報責任者 (CIO) や最高情報セキュリティ責任者 (CISO) に目を向けています。ランサムウェアの脅威が進化する中、サイロ化されがちで、脅威重視型で、複雑なスタンドアローン型のセキュリティソリューションを管理することは困難です。データセキュリティとデータ管理も同様に、サイバー犯罪者が多額の支払いを強要するのを発見し、防止し、阻止する上で、バラバラで一貫性がありません。Enterprise Strategy Group (ESG) によると、ランサムウェア攻撃の被害に遭った企業の半数以上が、データ、アプリケーション、システムへのアクセスを取り戻すために身代金を支払ったことを認めています[3]。さらに、Palo Alto Networksによると、身代金の平均支払額は2022年の最初の5カ月間で71%増加し、前例のない100万ドルの大台に近づいています[4]。しかし、身代金を支払った組織でさえ、データ復旧が保証されないことを知っています。支払い後にすべてのデータを取り戻したと回答したのは、ESG レポートの調査対象となった組織の 7 社に 1 社、つまり 14%だけでした[5]。

攻撃に遭った際、組織が身代金を支払ったことはありますか?



「ランサムウェアの攻撃を受けたことがある組織の**半数以上**が、データ、アプリケーション、システムへのアクセスを取り戻すために身代金を支払ったことを認めています」

身代金を支払った後に復旧したデータの割合



[2] Forrester社「Business Resilience Is No Longer Optional」Stephanie Balaouras、2020年5月12日
[3] Enterprise Strategy Group「ランサムウェア対策への長い道のり」、2022年3月。
[4] Palo Alto Networks社 「2022 Unit 42 Ransomware Threat Report」2022 年6月7日
[5] Enterprise Strategy Group「ランサムウェア対策への長い道のり」、2022年3月

テクニカルリーダーは、業界をリードするデータファーストの企業と手を組むことで、既存の予算内で (新しくセキュリティ予算を申請することなく)、急増するランサムウェアに賢く対処することができます。協力することで、サイバーレジリエンスエンジニアリングに焦点を当てたコントロールとプロセスを通じて、ランサムウェアの保護と復旧に取り組むことが可能になります。NISTは、生き残りが可能で信頼できるセキュアなシステムを開発するために、レジリエンスエンジニアリングを、システムセキュリティエンジニアリングと組み合わせて適用する新たな専門分野と定義しています。

データはデジタルビジネスと政府を動かしていますが、セキュリティ戦略ではデータにもっと焦点を当てる必要があります。データセキュリティアライアンスは、データを中心に置いて、セキュリティと経営戦略を結び付け、成果を向上させます。

> **「今日の絶え間ない巧妙化するサイバー脅威は、全員参加型のアプローチを必要としています。サイバーセキュリティの課題をすべて解決するのはベンダー 1社の責任ではなく、悪者と戦うにはいろんな人の協力が必要です」**
>
> – **Sanjay Poonen**、CEO兼プレジデント、Cohesity

ランサムウェアの増加

ランサムウェアは今年、全世界で300億ドル以上の被害をもたらすと予想されています。企業への攻撃は、2022 年の 11 秒に 1 回から、2031 年には 2 秒に 1 回になると予測されています[6]。サイバーレジリエンスを追求する組織は、数多くの課題に直面しています。そのいくつかを以下に挙げていきます。

人の課題

人は完璧ではありません。最も一般的なランサムウェア攻撃は、フィッシングメールや盗まれた認証情報によって発生しており、後者がランサムウェア攻撃の40%を占めています[7]。

- 組織は、攻撃 (フィッシングなど) に対抗するためのセキュリティに関する認識について、従業員やパートナーを適切に教育し訓練するための時間とリソースが不足しています。
- ITとセキュリティの役割がサイロ化しています。最近実施された調査では、SecOpsの回答者の約3分の1 (31%) が、IT部門との連携は強力ではないと考え、そのうち9%は「弱い」と回答しています[8]。

組織とプロセスの課題

ランサムウェアの滞留時間は着実に減少しているものの、調査レポートによれば、21日〜11日のラグタイムが依然として存在しています。こうした脅威に対抗できるよう設計されていないセキュリティワークフローや情報共有プロセスが主な原因となっています。例えば:

- 脆弱なアプリケーションやシステムにパッチを適用するのは、時間もコストもかかります。
- バックアップなどの防御に役立つレガシーシステムは、IT専門家を必要とします。
- 攻撃対象が広がり、あらゆる場所のデータを保護するのが難しくなっています。
- 災害復旧の ”ランブック (作業手順書)” は一般的ですが、そのほとんどはランサムウェアへの対応と復旧の複雑さを考慮していません。

[6] Cybersecurity Ventures「Ransomware will strike every 2 seconds by 2031」 2023年1月3日
[7] Verizon「Data Breach Investigations Report」2022年
[8] Censuswide「Cohesity survey」2022年6月

テクノロジーの課題

IDCによると、Global DataSphereの規模は2022年から2026年にかけて2倍以上に拡大し、エンタープライズ組織がデータ増加の大部分を牽引すると予想されています[9]。多くのテクノロジー環境、特にベストオブブリードの製品を寄せ集め、セキュリティやインフラのプラットフォームがバラバラな環境では、オンプレミス、クラウド、エッジのデータをこのような規模で扱えるように設計されていません。データは爆発的に増加しており、その種類は非常に多く、場所も多岐にわたっているため、これらの環境はランサムウェアの圧力に屈しています。

- 既存のソリューションはうまく統合されておらず、複雑さが持続しています。
- クラウドやハイブリッド環境は、ランサムウェアの保護と復旧に新たな課題をもたらしています。
- 経済的な不確実性により、セキュリティへの投資を増やすべきか、現在あるものを最適化すべきかが問われています。
- ほとんどのテクノロジーは、人工知能と機械学習 (AI/ML) が可能にする効率性と拡張性を活用できていません。

総力を挙げる

ランサムウェアの勢いは衰えず、軽視されるべきではないという顕著な兆候の中で、米国立標準技術研究所 (NIST) は最近、「Developing Cyber-Resilient Systems: A Systems Security Engineering Approach (サイバーレジリエントなシステムの開発: システムセキュリティ工学のアプローチ)」を更新し、サイバーレジリエンス工学に焦点を当てました。この新たなシステム工学の専門分野は、システムセキュリティ工学と組み合わせて適用され、生き残り可能で信頼できるセキュアなシステムを開発します。

サイバーレジリエンス工学は、システムの信頼性を構築、設計、開発、実装、維持、持続させることを目的としています。これにより、サイバーリソースを使用する、あるいはサイバーリソースによって引き起こされる不利な状況、ストレス、攻撃、侵害を予測し、それに耐え、回復し、適応することができます。リスク管理の観点から、サイバーレジリエンスは、サイバーリソースに依存することによるミッション、ビジネス、組織、企業、または特定分野のリスクを軽減することを目的としています。

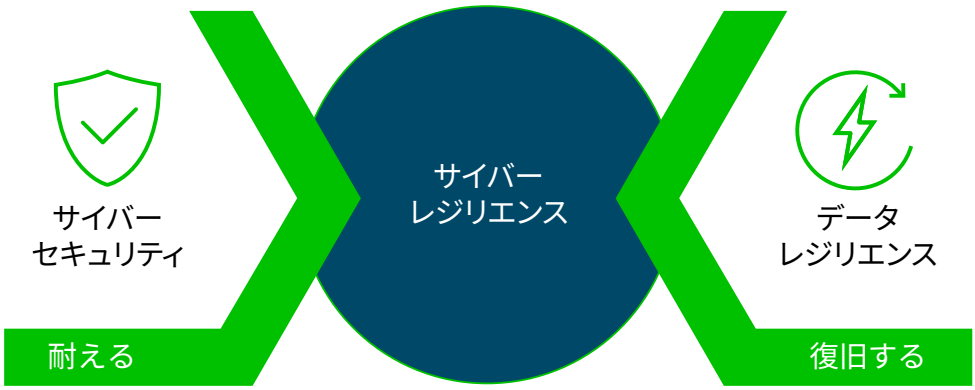
人材不足がITチームとセキュリティチームの連携に影響を及ぼしているため、これは組織にとって救いとなります。最近のレポートでは、IT部門の意思決定者の77%とSecOpsの専門家の78%が、その影響に同意しています[10]。同レポートは、このようなIT部門とSecOps間の連携不足により、回答者が自分たちの組織がサイバー脅威にさらされやすくなっていると考える原因になっていると指摘しています。回答者全員が特に恐れていることは下記の通りです:

- データの損失 (42%)
- 事業の中断 (42%)
- 顧客が他でビジネスを行うようになる (40%)
- ミスが発生した場合の責任追及とチームへの非難 (35%)
- 身代金の支払い (32%)
- 両チーム (ITとSecOps) の人材解雇 (30%)

[9] IDC「Worldwide IDC Global DataSphere Forecast, 2022–2026」 2022年5月
[10] Censuswide「Cohesity survey」 2022年6月

NIST のサイバーセキュリティレジリエンスフレームワークのアプローチの 1 つは、組織がサイバーセキュリティリスクを管理し、低減できるように設計された一連のガイドライン、基準、ベストプラクティスです。このフレームワークは、異なるセクターや業種にまたがるサイバーセキュリティリスクを管理するための共通言語と体系的なアプローチを提供します。このフレームワークは、特定、防御、検知、対応、復旧というコアの機能に基づいています。これらの機能は、組織がサイバーセキュリティリスクを理解し、資産を守り、サイバーセキュリティインシデントを検知して対応し、タイムリーにそこから復旧するのに役立ちます。

最も高いレベルでは、強固なサイバーレジリエンスのフレームワークは、攻撃に耐えることと、攻撃から復旧することという 2 つの重要な概念を包含しています。



最新の考え方: セキュリティ戦略の中心にデータを置く

F1レースでは、車が重要視されます。いかにしてスピードを最大化するか? パフォーマンスを最適化するには? そのすべてをいかに安全に行うか? ビジネスと政府において、データはF1車です。データがデジタルビジネスと政府を動かしています。しかし、データは多くのセキュリティ戦略や管理戦略の最前線にはありません。インフラやシステム、特にクラウド全体に焦点を当てすぎています。

データセキュリティアライアンスの使命はデータを中心に置くことであり、特にサイバーレジリエンスの背後にあるデータ管理とデータセキュリティを統合することにあります。そのビジョンは、業界を変えるような技術的な統合やアーキテクチャ、強固なデータとセキュリティのコラボレーション、ベストプラクティス、データに関するソートリーダーシップを提供することです。

このビジョンは、セキュアなクラウドコンピューティング環境を確保するためのベストプラクティスを定義し、その認知度を高めることを目的とするCloud Security Alliance (CSA) のビジョンとは異なりますが、それを補完するものです。組織は、クラウド上の機密データのセキュリティと追跡に苦慮しています。CSAによる調査レポート「State of Cloud Data Security」によると、すべてのクラウドデータのセキュリティが十分だと考えているのはわずか4%で、4分の1以上の組織が規制対象のデータを追跡しておらず、3分の1近くが機密データや内部データを追跡しておらず、45%が未分類データを追跡していません。

データセキュリティアライアンスの統合とベストプラクティスは、組織がサイバーインシデントの影響を最小限に抑えるために、一連のプロセスやコントロールを緊密に連携させるのに役立ちます。また、パブリック、プライベート、ハイブリッドのコンピューティング環境を問わず、あらゆる場所に保存されたデータに対する組織の自信を高めることができます。

> “サイバーレジリエンスは、特にデータに関する基本を正しく理解することから始まります。自社の機密データがどこにあり、どのようなもので、誰がアクセスでき、どのようなリスクがあるのかを理解することが重要です。セキュリティコミュニティとして、私たちはデータをセキュリティ戦略の中心に据える必要があります”
>
> – **Tyler Young**, BigID CISO

データをサイバーセキュリティ戦略の中心に据えることで、組織は以下のことを積極的に実現できます:

- リスクの削減
- アジリティの向上
- レジリエンスの向上

ランサムウェア侵入の各段階を通じて、プロアクティブに脅威を先取りすることで、以下のメリットを得ることができます:

サイバーレジリエンスの6つのベストプラクティス

データを重視し、優れたセキュリティパートナーとデータ管理パートナーがアーキテクトのピットクルーとして働けば、組織は何事にも対応できるサイバーレジリエンスの基盤を手に入れることができます。以下に、サイバーレジリエントな環境を構築するための 6 つのベストプラクティスを示します。(このベストプラクティスは、NIST のサイバーレジリエンスのベストプラクティスを補完するもので、ポリシーと手順の策定と実施から、インシデント対応計画の定期的なテストと更新、脅威インテリジェンスを共有するための他組織とのパートナーシップの確立まで、さまざまなアクションが含まれています)

1. 常に警戒する: セキュリティ体制を継続的に監視

脅威の状況は常に進化しており、組織は限られた予算とリソースの中で対応に苦慮し、時間のかかる手作業でデータを複数のスプレッドシートにエクスポートしたり、脅威を追いかけ続けたり (潜在的な攻撃や侵害を予測するのではなく) しています。これは、組織のあらゆるレベルにおいて、焦点の定まらない意思決定と不十分な戦略的計画につながります。 NIST は、サイバーセキュリティのポリシーと手順を策定し実施するようチームに助言しています。しかし、サ

イバーセキュリティチームには、現在と新たなサイバーリスクに積極的に対処し、管理するための新しいアプローチが必要です。攻撃を軽減し、迅速に対応する必要のあるインシデントの数を劇的に減らすためには、取り組みの優先順位をどこに置くか、長期的な進捗状況をどのように客観的に測定するか、結果を関係者に効果的に伝えるタイミングはいつかをより十分に理解する必要があります。

サイバー攻撃を防止することは、NISTが推奨する従業員のサイバーセキュリティ研修や意識向上、アクセス制御や監視システムの導入だけではありません。資産とエクスポージャの完全な可視化、潜在的なセキュリティ脅威に関する広範なコンテクスト、サイバーリスクを客観的に測定する明確な指標も必要です。サイバー攻撃を予測し、意思決定を支援するためにそれらのリスクを伝達することができる組織は、新たな脅威から身を守るために最適な体制を整えることができます。

データはあらゆる資産の中で最も動的な資産なので、特に管理が困難です。機密データは急速に増加し拡散するため、組織はデータの保存場所、分類、アクセス方法などを把握し、リスクと保護の必要性を理解する必要があります。

最も成功するサイバーレジリエンス計画は、アセスメントから始まります。チームは、サイバー上の強み、弱み、機会、脅威を確認するだけでなく、サイバーセキュリティ防御を構築し、サイバー攻撃に効果的に対応するために必要なソリューションを特定する必要があります (具体的な内容については巻末のチェックリストを参照してください)。業界をリードする脅威の経験と、オンサイトでもクラウド間でも機能するインテリジェントなデータセキュリティとデータ管理ソリューションに関する専門知識を組み合わせることで、組織がより効果的なサイバーに備えたプログラムを開発するのに役立ちます。

2. 決して信用せず、常に検証する: ゼロトラストの原則に基づくアーキテクト

信用せよ。しかし、検証もせよ、という考え方を中心としたセキュリティのレガシーモデルは、今日のビジネスや政府の環境ではもはや通用しません。なぜなら、ペリメータ (境界) がもはや存在しないからです。デジタルビジネスのベストプラクティスには、誰がいつどのような情報にアクセスしたかを確実に把握するために、決して信頼せず常に検証することや最小のアクセス権限など、ゼロトラストの原則に基づいたアーキテクトが求められています。

侵害された機密情報は、ビジネスの評判や優位性だけでなく、政府のアジリティや状況認識にも悪影響を及ぼします。そのため、最も広範なデバイスと環境にわたって、人であれマシンであれ、あらゆる ID を保護することが不可欠になっています。デジタルIDとは、オンライン上に存在する個人、組織、電子デバイスに関する情報のことです。多くの企業がデジタルトランスフォーメーションを進める中、以前にも増してデータにアクセスできるIDが急増しています。今日、複数のデバイスに特権的なアクセスやコントロールを持つIDの数は、ユーザの数をはるかに超えており、セキュリティチームには、より広い攻撃対象領域をより適切に守る責任が課されています。さらに、データ資産のIDセキュリティ管理に複数のレガシーツールを使用すると、ハッカーが悪用できる複雑さと非効率性が生じます。包括的なロールベースのアクセス制御と、信頼せず常に検証するポリシーを組み合わせることで、ランサムウェアや内部脅威から組織をより確実に保護することができます。

データは今やあらゆる場所に存在するため、組織はエンドポイントからクラウドワークロードまで、バックアップから本番環境まで、IDからデータまで、データ管理とデータセキュリティを包括的に統合し、悪意のある行為者を阻止する方法を見つける必要があります。データを保護するために暗号化やその他のセキュリティコントロールを導入することを推奨するNISTの勧告を補完する、攻撃防止のためのデータファーストのアプローチには、すべてのデータの可視化とコントロールを必要としています。完全な可視性があれば、データセキュリティ、プライバシー、コンプライアンス、ガバナンスのために、クラウドとオンプレミスのすべてのシステムでデータリスクを最小限に抑えることができます。

3. データを知る: インテリジェンスを深める

NISTは、インシデント対応計画の定期的なテストと更新、脆弱性評価と侵入テストの定期的な実施を推奨しています。これが非常に重要なのは、マルウェアを迅速に検出することで、身代金の支払いを拒否する自信を得ることができるからです。本番システムに対するこのガイダンスの他にも、既知の脆弱性に対して本番データやバックアップスナップショットのオンデマンドスキャンや自動スキャンを実行することで、本番環境内のサイバーエクスポージャーや盲点を発見することができます。また、これらのスキャンにより、本番環境に影響を与えることなく、簡単にリスク体制を評価し、厳格なセキュリティおよびコンプライアンス要件を満たすことができます。

本番環境とバックアップスナップをスキャンすることで、健全性と回復性を評価します。そして、バックアップを検証し、リストア時に既知の脆弱性が本番環境に再導入されないようにします。これらはすべて、より深いインテリジェンスと、本番環境内のすべてのサイバーエクスポージャのグローバルビューを提供するため、悪意のある行為者に悪用される前に対処することができます。

人工知能と機械学習 (AI/ML) を活用したデータ分類は、ランサムウェアからの保護、検出、対応能力も加速し、サイバー犯罪者の一歩先を行くことができます。個人を特定できる情報 (PII)、保護対象保健情報 (PHI)、PCIデータなどの機密データや規制対象データを継続的に検出し、MLベースのデータ分類によって誤検出を減らすことができます。このデータインテリジェンスは、セキュリティ体制を通知し、情報漏えい対策 (DLP: Data Loss Prevention) などの依存するセキュリティ制御を最新の状態に保つのに役立つだけでなく、対応チームがランサムウェア攻撃やサイバーインシデントの影響を理解するのにも役立ちます。

4. コラボレーションを強化する: サイバーレジリエンスをチームスポーツに

レジリエンスには、準備、対応力、強靭さ、適応性が必要です。現代のつながっている世界では、セキュリティリーダーは、オンプレミス、クラウド、SaaS の各環境を包括するアーキテクチャとプロセスを活用し、ビジネスの継続性に重点を置いたセキュリティプロセスを実装する必要があります。SecOpsプログラムでは、可能な限り敵の行動を阻止する予防策を提供するソリューションとプロセスを活用する必要がありますが、予防ができない場合に、必要に応じて検知と対応も行う必要があります。

レジリエンスは、敵がターゲットとした環境で目的を達成する前に阻止することによって達成されます。組織は、レジリエンスへの取り組みを支援するために、個々の脅威の状況と攻撃ベクトル をしっかりと理解する必要があります。この2つは、洗練された脅威インテリジェンスと攻撃対象領域を理解することで 達成可能ですが、一般化されたものではなく、その組織に固有のものである必要があります。最後に、ビジネスレジリエンスを支援するプロセスは、セキュリティプログラムの重要な成果です。インシデント対応の計画と連携は、ビジネスとセキュリティプログラムの存続可能性の両方を支援するための鍵となります。

NISTは、脅威インテリジェンスやベストプラクティスを共有するために、他の組織とのパートナーシップやコラボレーションを確立することを推奨しています。プロセスを再構築し、ITとSecOps とのコラボレーションに適応させれば、ランサムウェアの攻撃者からデータを守るチャンスが広がります。また、ビジネスリーダーも夜、安心して眠れるようになります。

ランサムウェアに対抗するためにシームレスに連携する信頼できるセキュリティ製品を見つけ、投資することが必要です。これには、ランサムウェア攻撃の発見、調査、修復までの時間を短縮してくれるSIEM (セキュリティ情報イベント管理) やSOAR (セキュリティオーケストレーション自動応答) ソリューションが含まれます。拡張可能な事前に組み込み済みの統合ワークフローは、インシデント対応の自動化や、セキュリティ、IT、ネットワークの各チームを横断した統合

運用のために、SecOpsを強化するのに役立ちます。さらに、セキュアなSDK (ソフトウェア開発キット) とカスタマイズ可能な管理APIを使用して、事前に組み込みされた統合が可能であることを確認してください。これを使用することで、サイバー犯罪と戦うために必要な環境を柔軟に運用することができます。

5. 統合しシンプルにする: 最新のデータセキュリティと 管理プラットフォームの活用

ランサムウェア攻撃に対抗するには、規模と互換性がさらなる鍵となります。サイバーレジリエンスにはコラボレーションが必要であるため、APIリッチでAPIファーストなアーキテクチャを備えた、拡張性の高い最新のデータセキュリティとデータ管理プラットフォームを活用することが重要です。これは、場所に関係なく機能し、最も幅広いデータソースに対応していることが必要です。多くのデータ管理機能を単一のプラットフォームに統合することで、運用をシンプルにすることができます。また、データのコピーを作成して移動する代わりに、データをインプレースで (その場で) 再利用し、ウイルススキャンやデータマスキングからファイル監査ログの分析やデータの分類に至るまで、日常的なタスクからより困難なタスクまで、付加価値の高いアプリケーションをデータにもたらすことができるソリューションを手に入れることが大切です。さらに、単一の拡張可能なプラットフォームにより、データのフットプリントを削減し、ランサムウェアの攻撃対象を減少させることができます。

6. スピードと確信を手に入れる: バックアップインフラを、セキュリティインフラとオペレーションに統合

データセキュリティとデータ管理の複雑さは、特にデータ侵害が発生した場合、単独では解決できません。目標復旧時間と目標復旧時点 (RTO/RPO) の範囲内で、できるだけ早く運用可能な状態に戻すには、バックアップをサイロ化するのではなく、セキュリティインフラとオペレーションの本質的な部分とする統合的なアプローチが必要です。

データセキュリティとデータ管理に投資する組織は、セキュリティフレームワークの全領域をカバーする緊密に統合されたソリューションから利益を得ることができます。よく知られているのは、SANS Instituteのインシデント対応サイクル (PICERL) です：

- **事前調査 (Preparation)** – 評価、計画、教育、ID管理など
- **インシデントの特定 (Identification)** – 意識監視、早期発見など
- **封じ込め (Containment)** – 通知、バックアップ、フォレンジックなど
- **根絶 (Eradication)** – 復旧、根本原因の分析、マルウェア除去など
- **復旧 (Recovery)** – 脆弱性スキャン、オペレーションの復帰、ベースラインなど
- **教訓の学習 (Lessons Learned)** – 報告、手順の更新など

入念に検討された統合により、計画から復旧に至るまで、攻撃に対抗するスピードと自信を得ることができます。また、自動化されたAI/MLを使用して、データまわりの異常なパターンをチームに警告することで、潜在的なサイバー攻撃を検出することもできます。侵害が発生した場合、システムの再感染を回避するために脆弱性スキャンが行われたクリーンなデータを、任意の時点および場所にリカバリする手段もあれば、ダウンタイムを短縮できます。

サイバーレジリエンス能力のチェックリスト

主要な自動化と包括的な機能は以下の能力を備え、ランサムウェアに効果的に対抗できます:

	要件	主要機能
サイバーセキュリティ (耐える)	戦略	• サイバーセキュリティの防御を構築し、サイバー攻撃に効果的に対応するためのアドバイザリー、インプリメンテーション、マネージドセキュリティサービス
	ID管理とセキュリティ	• 従業員のIDと顧客のIDのためのプラットフォームとサービス • 幅広いデバイスや環境において、あらゆるID (人とマシン) を保護します。
	可視化とエクスポージャー管理	• すべてのIT資産 (ハードウェア、ソフトウェア、アプリケーション、データ) をインベントリ化する機能 • クラウドまたはオンプレミス、ITからOT、さらにその先に至るまで、攻撃対象領域全体にわたってリスクを評価するプラットフォームで、リスク体制の優先順位付けと検証に必要な可視性とインサイトを提供 • データセキュリティ体制管理 (DSPM: Data Security Posture Management) で強力なデータ発見、分類、インテリジェンスの実践を可能にし、データの所在、内容、アクセス権者、ワークフロー、リスクを把握
	XDR (拡張検出と応答)	• 検知、対応、復旧を迅速化する、セキュリティインフラ全体に対するXDR機能を備えたクラウドネイティブなソリューション • ランサムウェア攻撃発生時にデータとワークロードをリストアするワークフローを開始する方法
	次世代SIEM (セキュリティ情報イベント管理)	• 今日の複雑なハイブリッド環境における高度な脅威を防御するソリューションで、最先端のアナリティクスを使用し、スケーラブルで柔軟なクラウドネイティブのアーキテクチャ上に構築
	SOAR (セキュリティオーケストレーション自動応答)	• サイバー攻撃やランサムウェア攻撃をより迅速に管理できる自動化と柔軟性
	アクション可能な脅威インテリジェンス	• 包括的なインテリジェンスと専門知識により、より効果的なプログラムを開発し、サイバーへの備えに対する信頼感を築くためのダイナミックなソリューションを提供 • すべての機密データと重要データを可視化/制御し、データセキュリティ、プライバシー、コンプライアンス、ガバナンスのためのデータファーストアプローチにより、クラウドとオンプレミスにあるすべてのデータのリスクを理解
	フルスタックの可観測性	• 統合されたセキュリティ、フルスタックの可観測性、カスタムアプリケーションを提供する拡張可能なデータプラットフォーム
	ゼロトラスト (ZT) / ペリミター (境界) とエンドポイント保護	• エンドポイント、クラウドワークロード、ID、データなど、企業のリスクにおいて最も重要な領域を保護し、敵の先手を打って侵害を阻止する方法
	フォレンジック	• ランサムウェア駆除の前に、根本的な原因やランサムウェアのシグネチャを特定し、起訴の可能性を検討するためのセキュリティソリューション

	要件	主要機能
サイバーレジリエンス (復旧する)	バックアップ & リカバリ	• 包括的なサイバー脅威対策、MLベースの異常検知、迅速なランサムウェアからの復旧、ハイブリッドクラウドモビリティ • データのイミュータビリティ (変更不可) • データ隔離: 物理的、論理的にデータを隔離し、セキュリティレイヤーを追加 • ゼロトラスト原則 (多要素認証 [MFA] など) • クォーラム: 管理上または設定上の変更するために複数の人の承認が必要
	脆弱性スキャンと復元	• クリーンルーム、サービス再開までのステージング、データおよび／または設定の追加リカバリ、アプリケーションチームの承認、場合によってはデータセンターオペレーションによる環境間のシステム移動、セキュリティ、新しいオペレーションエリアへのアクセスを確保するためのネットワーク
	脅威からの保護	• MLベースの脅威インテリジェンスとスキャンにより、マルウェアや侵害の痕跡 (IOC) を検出し、バックアップデータ内の脅威を特定
	セキュリティ統合	• API、SDK、セキュリティオペレーションとセキュリティコントロールの統合により、インシデント対応を迅速化し、既存のコントロールとプロセスを活用

データをサイバーレジリエンス戦略の中心に据えることで、最大限の保護と最良の復旧を実現するためのアーキテクチャーを確実に行うことができます。データセキュリティアライアンスは、IT およびビジネスの意思決定者に対し、サイバーレジリエンスについて次のサイトでさらに学ぶことを奨励しています: www.cohesity.com/jp/company/data-security-alliance

データセキュリティアライアンスについて

データセキュリティアライアンスの使命は、データのセキュリティと保護です。本アライアンスは、データセキュリティとデータ管理をサイバーセキュリティと包括的に統合し、サイバー耐性を向上させ、重要な技術統合とアーキテクチャ、ベストプラクティス、共通のフォーカスを中心としたソートリーダーシップを提供することで、これを達成します。データセキュリティアライアンスは、業界をリードするサイバーセキュリティとサービスを提供する企業のクラス最高のソリューションと、Cohesityの卓越したデータセキュリティとデータ管理の専門知識を組み合わせるものです。データセキュリティアライアンスのメンバーは以下の通りです: BigID、Cisco、Cohesity、CrowdStrike、CyberArk、Okta、Palo Alto Networks、Securonix、Splunk、Tenable、Mandiant、Qualys、Netskope、ServiceNow、Zscaler、PwC

2000046-001-JP 8-2023