2024年3月

市場レポート

日本の中小企業におけるサイバーレジリエンス

不安を乗り越えてAI活用の未来へ

Barracuda®
Your journey, secured.

目次

エグゼクティブサマリー……1

はじめに……2

調査結果1: AIは中小企業の人員を削減し知見拡大に貢献するが、メリットの享受には支援が必要……3

調査結果2: 62% が生成 AI のビジネス利用は非公式であると回答し、多数がリスクを懸念……4

調査結果3: 半数以上が一般的なサイバー脅威における攻撃者の AIの活用について不安視……5

調査結果4: メールベースの脅威はセキュリティ上の最大の懸念事項。36%がAIによる保護の強化を期待……6

調査結果5: AIベースの脅威に備えている企業は少なく、スキルやポリシーが不足……8

まとめ: AI時代のサイバーレジリエンスを高める……10

バラクーダについて……11

エグゼクティブサマリー

2022年11月に、生成人工知能（AI）ツール「ChatGPT」がリリースされたことで、AIに対する世界の認識が変わりました。一夜にして、AIがコンピュータサイエンスの主流分野になったようです。 今日、すべての組織や政府が直面している課題は、AI によってもたらされる、または促進されるリスクや不確実性を理解して対処すると同時に、その可能性をよい方向に活用する方法です。

日本の中小企業がこの課題にどのように対処しているかについて理解を深めるために、私たちは従業員200人未満の日本の企業におけるAIに対するさまざまな認識、懸念、利用についての調査を委託しました。 調査結果によると、回答者はAIについておおむね前向きで楽観的ですが、AIがビジネスやサイバー脅威にどのように影響するか、またそれに対処するスキルがあるかどうかについては、かなりの疑問と懸念があります。

主な調査結果は次のとおりです。

- 66%が、AIによる人員削減を予想しています。
- 76%が、AIによって顧客インサイトをより簡単かつ迅速に収集できるようになると予想しています。
- 77%が、AIソリューションの実装と管理を支援するパートナーを必要としています。
- 62%が、生成AIのビジネス利用は非公式であると回答し、69%がリスクを懸念しています。
- 55%が、攻撃者がメールベースの攻撃でAIをどのように利用するかわからないと回答していますが、36%はAIによってそのような脅威に対する防御が強化されると考えています。
- 63%は、AIベースのサイバー攻撃に対処するために必要なスキルの一部またはすべてが不足していると回答しています。

本レポートは、調査結果とその背景、AI 時代における組織のサイバーレジリエンスへの影響をまとめています。 企業が自社の AI 成熟度をベンチマークし、対策や支援の必要な分野を特定する一助となることを願っています。

調査方法

Barracudaは、独立系市場調査会社のTech Research Asiaに依頼して、日本の従業員数50～200人の組織で働く500人のITプロフェッショナルを対象に調査を実施しました。

回答者の半数弱（47%）は経営幹部の役割を担っており、調査は2023年11月に実施されました。

はじめに

人工知能と世界への影響

人工知能（AI）とは、コンピュータサイエンスの一分野であり、推論、学習、知覚、自然言語処理、問題解決、意思決定など、従来は人間にしかできなかった複雑な作業や時間のかかる作業を実行できます。

AIは、コンピュータサイエンスと堅牢な、多くの場合膨大なデータセットを組み合わせます。AIの下位分野には、生成 AI（GenAI）、機械学習、ニューラルネットワーク、自然言語処理、コンピュータビジョン、深層学習、コグニティブコンピューティングなど多くのものがあります。 各下位分野には独自の目標、方法、および用途があります。

AIの開発と実装は急速に進化しています。 企業や社会にとって見返りが得られる可能性は大きいですが、それに伴うリスクもいくつかあります。

例えば、AIはプロセスの最適化と自動化、コストの削減、品質の向上、新しいインサイトやアイデアの生成によって、ビジネスの成果と競争力を向上させることができます。チャットボットを通じて顧客サービスと対話を強化し、顧客データを深いインサイトに変えることもできます。また、サイバーセキュリティなど、高度なインテリジェンスを必要とする、困難で複雑かつ斬新な問題に企業が取り組む際にも役立ちます。

しかし、AI システムは開発と実装に時間とコストがかかり、多くの場合、専門的なスキルとリソースを必要としますが、採用が難しい可能性もあります。AI は一部の職務の必要性を減らす見込みであり、これは長期的な社会的影響を及ぼします。さらに、膨大な量の個人情報、センシティブデータ、機密情報の使用と保管に関連するプライバシーとデータ保護の懸念や、説明責任と透明性などの倫理的問題と法的問題があります。

サイバーセキュリティに関しては、脅威の防御、検出、対応を強化できる AI ツールが、これまで以上に巧妙で標的を絞った攻撃をより迅速に仕掛けるために、サイバー攻撃者によって利用される可能性もあります。

日本のAI情勢

日本も含め、あらゆる組織や政府が直面している課題は、有益なイノベーションと導入を加速しつつ、急速に進化する AI 分野のリスクと不確実性に対処する方法です。

日本はリスクを回避するだけでなくイノベーションにも長けているという長年の評判があり、AIの分野ではスマートロボティクスと自動車技術のリーダーです。しかし、一部の報道によるとAIを活用したハードウェアで日本が成功を収めたほどには、AIベースのソフトウェアでは成功していないと言われています。たとえば、日本は生成 AI に関しては依然として外国の大規模言語モデルに比較的依存しています。日本は、AI の開発と導入において、データの可用性の欠如やビジネスリスクの許容レベルに関する文化的要因など、他にもいくつかの特有の課題を抱えています。

しかし日本の当局は、 リスクベースで機敏かつ協調的な AI 関連規制の導入に熱心であり「Society 5.0」に向けた取り組みの一環として、社会や企業が人工知能の恩恵を最大限に享受できるようにしようとしています。

調査結果 #1

AIは中小企業の人員を削減し知見拡大に貢献するが、メリットの享受には支援が必要

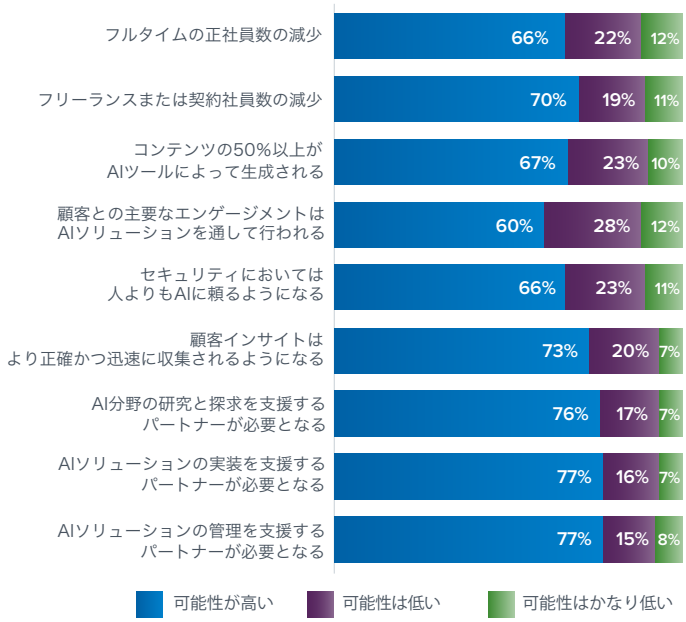
この調査結果は、日本の多くの中小企業がAIのビジネスへの影響について楽観的であることを示唆しています。

AIソリューションの使用により、今後2年間で正社員（回答者の66%）とフリーランサーまたは契約社員（70%）の両方の従業員数が削減されると予想しています。 雇用主にとってはコストと人的資源の負担を軽減することになる一方で、その役割が脅かされるかもしれない従業員にとっては、先行き不透明であることを意味します。

マーケティングや顧客関係管理等の分野でも、AIによる業務効率向上が期待されています。67%は今後2年以内にコンテンツの半分以上が、AIツールによって生成されると予想しており、60%は顧客が主要なコミュニケーションチャネルとして、主にAIソリューション（チャットボットなど）を利用するようになると考えています。これに加えて、76%が顧客インサイトがより正確かつ迅速に収集されるようになると予想しています。

脅威固有のレベルではなく、一般的なレベルで、65%がセキュリティ面でAIツールに頼ることができれば、追加のセキュリティスタッフを雇用したり、サードパーティに依頼する必要性が減ると考えています。AIはサイバーセキュリティ、特に脅威の自動検出、分析、対応において重要な役割を果たすようになっています。これらのタスクは従来は手作業であり、時間とリソースを大量に消費し、誤検知が発生しやすいものでした。日本は世界で最も深刻なサイバーセキュリティ人材不足に直面しているため（8ページを参照）、AI を活用してあらゆる規模の組織がセキュリティリソースを最大限に活用できるようにすることが、防御のために重要です。

セキュリティ以外の分野も含め、AIは今後2年間であなたの組織にどのような影響を与えると考えますか？



n=500

パートナーシップの力

多くの企業は、AIのビジネス上のメリットを十分に享受するために支援が必要だと考えています。調査対象企業の4分の3が、AI分野の研究と探求を支援するパートナー（回答者の76%）、AI ソリューションの実装や構築を支援してくれるパートナー（77%）AIソリューションを管理するための継続的なサービスを支援してくれるパートナー（77%）が必要だと答えています。

日本のセキュリティベンダーやマネージドサービスプロバイダーなどには、中小企業が AI を活用してその恩恵を享受できるようサポートする絶好の機会があります。

調査結果 #2

62%が生成 AI のビジネス利用は非公式であると回答し、多数がリスクを懸念

2022 年11月、OpenAIは生成AIツール「ChatGPT」の無料のリサーチプレビューをリリースしました。ChatGPT は、大規模言語モデルを使用し、ユーザのプロンプトに基づいて自然で魅力的な会話を生成するチャットボットです。 ChatGPTやBingなどの生成AIツールの機能性とスピードは、世界を席巻しました。

しかし、ニュースの背後では、生成型AIと職場でのそのようなツールの使用に関して、確信はなく懸念が高まっています。

生成AIについての認識は、人工知能分野に対する幅広い理解とは異なります。 回答者の56%が、生成AIと機械学習などの他の形式の AI の違いを理解していると回答しましたが、44%は知らないか、なんとなくしかわからないと認めました。

この調査結果は、日本の企業がAIの潜在的な利益を理解している一方で、それに伴うリスクも認識していることを示しています。そして、使用が制限される場合が多いことを意味します。

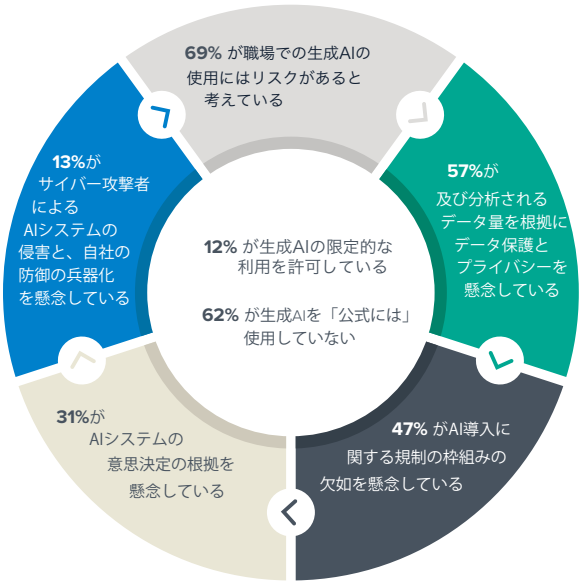
生成 AI のリスクと制約

回答者の69%が、職場での生成型 AI の使用にはリスクがあると考えています。

それにもかかわらず、回答者全体の18%は職場での生成AIの使用を許可していると回答しています。6%は広範囲に使用されていると回答し、12%は特定のチームまたは個人のみによる使用を許可しています。

さらに62%が「公式には」使用していないと回答しており、多くの企業は従業員が生成AIを使用している可能性があることを認識しているものの、その方法は監視も管理もされておらず、潜在的なセキュリティリスクが増大していることを示唆しています。

生成AIに関連するその他の懸念事項としては、保存・分析される大量の情報を根拠とするデータ保護とプライバシーの懸念（回答者の57%）、AI導入に関する規制の枠組みの欠如（47%）、AIシステムがどのように意思決定を行うかについての理解不足（31%）が挙げられます。13%は、サイバー攻撃者が AI システムを侵害して、自社の防御を兵器化するのではないかと懸念しています。

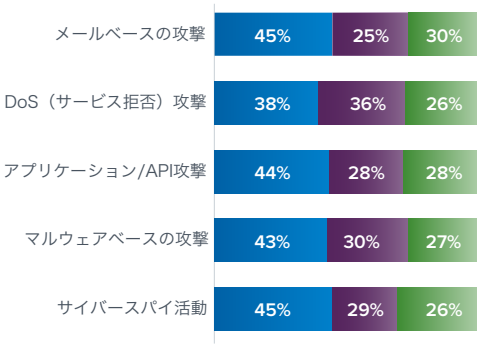


調査結果 #3

半数以上が一般的なサイバー脅威における攻撃者のAIの活用について不安視

企業は、AIによって一般的なサイバー脅威がどのように変わるかについて不安を感じています。たとえば、回答者の55%は、攻撃者がメールベースの攻撃にAIをどのように使用するかわからない、または確信がないと回答しています。同じ割合の人が、サービス拒否（DoS）攻撃（62%）や、マルウェアベースの攻撃（57%）、アプリケーション/API 攻撃（56%）、サイバースパイ活動（55%）についても、同様に不安視しています。

これらの攻撃にどのようにAIが使用されるか知っていますか？



n=500

調査結果 #4

メールベースの脅威は セキュリティ上の最大の懸念事項。36%がAIによる保護の強化を期待

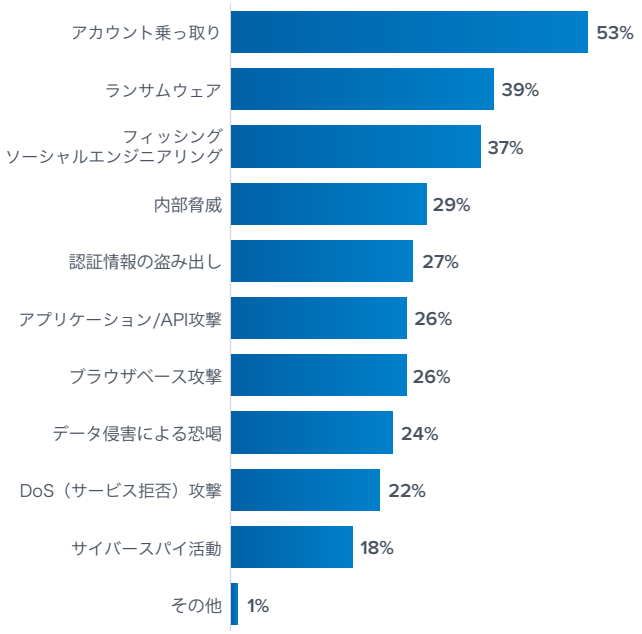
日本の中小企業にとってメールベースの脅威はセキュリティ上の懸念事項のトップを占めているため、これは気になる調査結果です。回答者の53%は、アカウント乗っ取り攻撃を懸念事項のトップ 3 に挙げています。

アカウント乗っ取りは、高度なメールの脅威です。なりすましや詐欺の一種で、悪意のある第三者がユーザのアカウント情報へのアクセスに成功します。本物のユーザを装うことで、攻撃者はアカウントの詳細変更やフィッシングメールの送信、財務情報やセンシティブデータの盗用、盗んだ情報を使用して組織内の他のアカウントへのアクセスができます。

回答者の37%が、フィッシングやソーシャルエンジニアリング全般など、その他のメールベースの脅威を、懸念事項トップ3に挙げています。メールベースの攻撃は、ランサムウェア、データ侵害、サイバースパイなど、他より深刻なインシデントの出発点となることが多いため、メールベースの攻撃に対して不安を感じるのは無理もありません。たとえば、回答者の39%がランサムウェアの脅威を懸念事項のトップ3に挙げており、当社の調査によると、2022年に成功したランサムウェア攻撃のうち69%がメールから始まっています。

メールベースのセキュリティ脅威の詳細についてはバラクーダの「今すぐ知っておくべき13タイプのメール攻撃」を参照してください 。

どのサイバー脅威を最も懸念していますか？



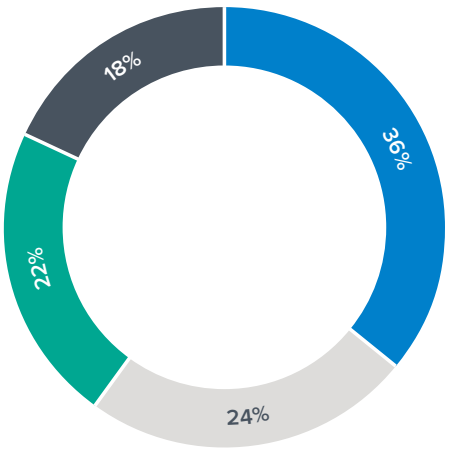
n=500

防御強化におけるAIの役割

サイバー防御の強化における AI の役割は、特にメールセキュリティと従業員向けのサイバーセキュリティ意識向上トレーニングに関して、調査回答者の間で比較的よく理解されています。AI が他の分野でどのように役立つかについては不透明な部分もありますが、それらの分野自体が中小企業にはあまり理解されていないことが原因かもしれません。

AIを活用したサイバー防御のうち、組織のセキュリティを最も向上させるものを選んでもらったところ、36%が、特にディープフェイクなどの高度な AI ベースの脅威に対する防御のために、AIを活用したメールセキュリティを選びました。24%は、AIによって、よりパーソナライズされたトレーニングの回数を増やせると回答しました。セキュリティオペレーションセンター（SOC）によって行われるような、脅威インテリジェンスや24時間年中無休の脅威の検出と対応における AI の役割は、あまりよく理解されていませんでした。

サイバー防御の強化における以下のAIの活用のうち組織のセキュリティに最も変化をもたらすと思うものはどれですか？



- AIにより、セキュリティ技術がディープフェイクなどの高度なメールの脅威をより迅速に、自動的に、そして大規模に特定して対応できるようになる。
- AIは、パーソナライズされたトレーニングコンテンツを使用してユーザをより頻繁に教育するのに役立つ。
- AIにより、防御者は脅威インテリジェンスの最新情報を他の組織や顧客とリアルタイムで共有し、使用できるようになる。
- AIは、過去の意思決定プロセスや結果を深く理解し、学習した上で、セキュリティ・アラートをコンテキストに合わせて表示し、改善策をアドバイスすることで、24時間年中無休の人間の脅威アナリストの仕事を強化する。

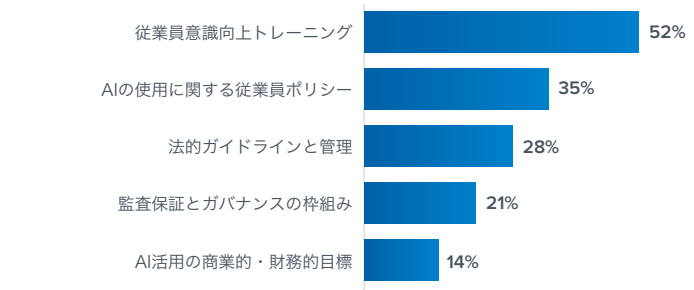
n=500

調査結果 #5

AIベースの脅威に備えている企業は少なく、スキルやポリシーが不足

全体として、調査回答者は、責任を持ってAIを使用するために必要な AI 特有の実践やポリシーを欠いています。AIの使用と脆弱性に関する従業員意識向上トレーニングを実施しているのは52%と比較的安心できる一方、従業員がAIを使ってできること、できないことに関する会社方針を定めているのは35%に過ぎません。法的なガイドラインやフレームワークなどを含むガバナンスの安全措置を備えている企業はさらに少数です。これは、AIのビジネスへの応用が制御や管理されていない場合が多いことを示唆しています。

AI を使用している場合、
次のうちどれを導入していますか？



n=500

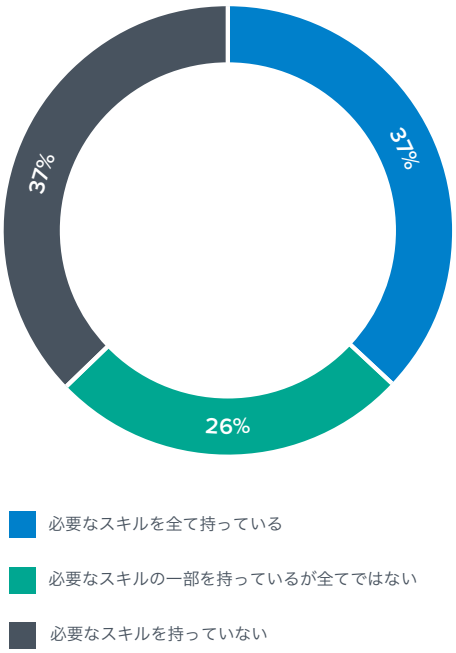
サイバーセキュリティのスキル不足

最新のICS2サイバーセキュリティ人材調査によると、日本のサイバーセキュリティ人材は50万人弱（480,659人）です。世界全体の増加率が8.7%であるのに対し、日本では前年比 23.8% 増と大きく伸びています。

しかし、需要が供給を大幅に上回っています。日本にいるサイバーセキュリティ専門家の人数と、日本が必要としている人数との差は、110,254 人です。世界全体の増加率が12.6%であるのと比較して、これは前年比97.6% の増加です。ICS2 が評価した中では、これほど大きなギャップがある国は他にありません。

この大局的な状況が、調査対象となった中小企業、特にAIベースのサイバー攻撃の日常の現実に、どのように反映されているかを見るのは興味深いことです。

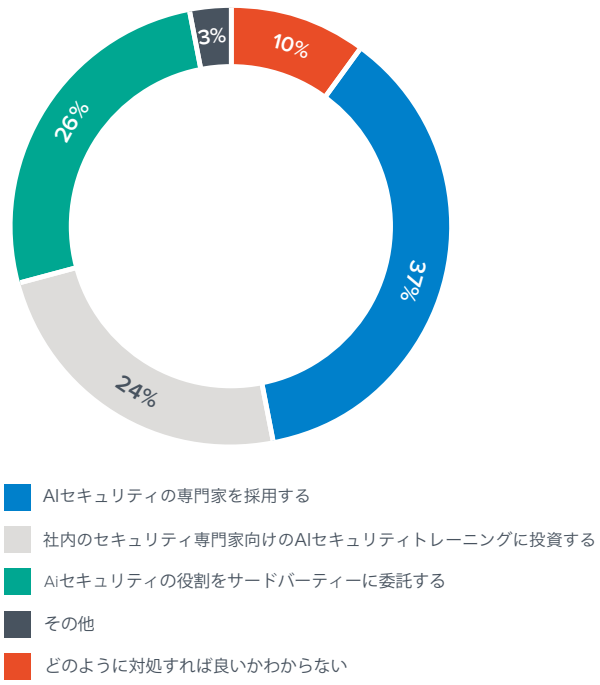
あなたの組織はAIベースの攻撃に対処するスキルを持っていると思いますか？



n=500

データによると、AIベースのサイバー脅威に対処するために必要なスキルをすべて持っていると感じている回答者はわずか37% で、63%は必要なスキルの一部またはすべてが欠けていると回答しています。

AIセキュリティスキルのギャップにどのように対処しますか？



n=500

スキルの課題への対処に関する数字は、あまりつじつまが合いません。

37%はビジネスに必要な AI セキュリティの専門家を外部から採用することを想定しており、26%はAIセキュリティの役割をサードパーティに委託することを検討しています。AIに精通したセキュリティの専門家という限られた人材をめぐって、各社がしのぎを削ることになりそうです。

24%は、AIセキュリティトレーニングに投資して、自社でスキルを磨くことを計画しています。新しく訓練を受けた専門家は、新しく身につけたそのスキルを採用したいと考えるサードパーティや他の企業から、採用のターゲットになる可能性があります。より高い給与とキャリアアップを提供できる大企業の方が、優秀な人材を引き付けやすいかもしれません。

10人に1人は、AIセキュリティスキルのギャップにどのように対処すればよいのかわからないと回答しました。

朗報は、日本のセキュリティ業界がこの課題の大きさを理解していることです。東京大学、京都大学、東京工業大学など、多くの日本の大学が世界の AI大学トップ 100 にランクインしています。また、能力格差に対処するための専門資格認定や国際協力のためのプログラムもあります。

まとめ

AI時代のサイバーレジリエンスを高める

AI 時代にサイバーレジリエンスを高めるには、組織はセキュリティの考え方を「予防」から「検知と対応」に転換する必要があります。 これは、サイバー攻撃のシグナルを初期段階（ MITRE ATT&CK 「サイバー・キル・チェーン」の左側）で捉えることができるツールを導入することを意味します。

サイバーキルチェーンの初期段階には、脆弱なアクセスポイントやパッチが適用されていない脆弱性を調べるなどの偵察、フィッシングで取得したユーザ認証情報などの攻撃者が攻撃を行うために必要な資産の収集、フィッシングやサプライチェーンの侵害などによる標的ネットワークへの初期アクセスなどが含まれます。

まずは、生成AI対応のセキュリティツールを採用して、ますます説得力を増すフィッシングメールなど、サイバー兵器を構築するためにすでに生成 AI を導入している攻撃者に対抗することから始めるのがよいでしょう。

これらのAI対応セキュリティツールを使用すると、攻撃の初期の兆候が検出されたときに、ITセキュリティ専門家は自然言語を使用して情報を収集できます。チームはすぐに信頼できるデータを入手し、利用することができます。そのため対応を早めて、さらなるダメージを防ぐことができます。純粋に予防的な考え方で脅威をブロックして対処するのではなく、免疫力を高めるようなものです。

生成AIは、組織がセキュリティ意識向上トレーニングで従業員に見通しとコンテキストを提供するのにも役立ちます。 脅威が急速に進化するAIの時代には、最新の脅威とトレンドに関する定期的な意識向上トレーニングがこれまで以上に重要になります。

さらに、組織はSaaSアプリケーションにも注意を払う必要があります。 盗んだ認証情報で武装した攻撃者が、新たに侵入する経路となるためです。

SaaSアプリケーションを検出、管理、保護する適切なツールの導入は、組織がMITRE ATT&CKフレームワークの左側に留まることにも役立ちます。AIを活用した脅威が到来したときに、組織はフレームワークの左側にいる必要があるのです。

関連資料

- 今すぐ知っておくべき13タイプのメール攻撃
- すべてを変えるAI時代のランサムウェア

バラクーダについて

バラクーダは世界をより安全な場所にするために尽力しています。

バラクーダは、すべてのお客様が購入、導入、使用しやすい、クラウドファーストかつエンタープライズレベルのセキュリティソリューションを使用できることが当然であると考えています。また、お客様のビジネスとともに成長および変化する革新的なソリューションによってメール、ネットワーク、データ、アプリケーションなどを保護しています。

世界中の20万を超えるお客様がバラクーダを信頼しています。お客様がリスクにさらされていることを知らない場合でも、バラクーダはお客様を保護できます。このため、お客様はビジネスを次の段階に移行することに注力できます。

詳細については、barracuda.co.jpをご参照ください。

Tech Research Asiaについて

Tech Research Asiaは、アジア太平洋地域で活動するテクノロジー・リサーチ、コンサルティング、アドバイザリー会社で、テクノロジーのトレンドとビジネス価値への影響の分析を専門としています。詳細は www.techresearchasia.comをご覧ください。

Barracuda
Your journey, secured.