IBM Security

ブームを超えて: SOC における AI 活用

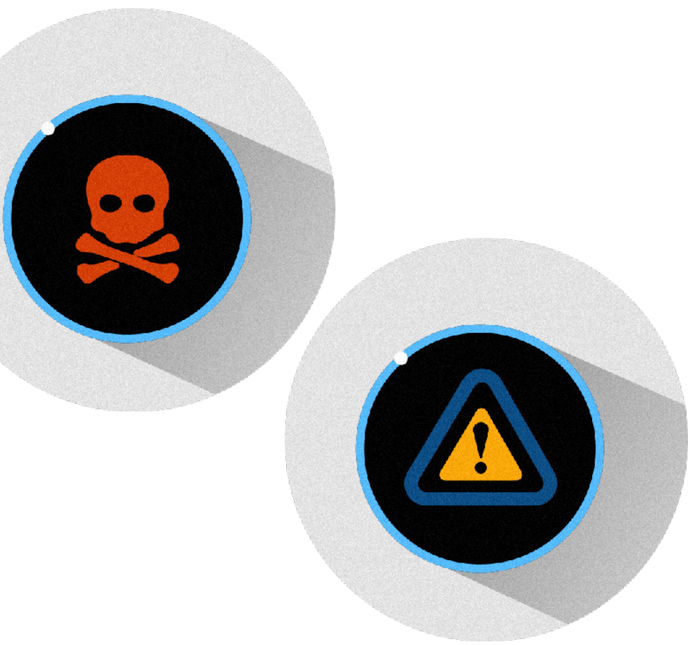
コグニティブなサイバーセキュリティー・ソリューションを採用する前に以下の 7 つの質問に答えてください。

1

リスクやセキュリティーのバランスに自信があるか?

CISO は、テクノロジー業界で最も困難な任務を遂行しています。ユーザーが重要なデータにアクセスできるようにすると同時に、インサイダー脅威、認証情報の悪用、操作ミスからデータを保護する必要があり、これは容易なことではありません。CISO の仕事は、すべての脅威を検知し、それに対応することですが、最も困難な点は、少ない人材と能力でこれを遂行しなければならないことです。

リスクは今までになく高くなっており、言い訳はききません。組織やクライアント、その顧客からのセキュリティー要求に応えなければならず、規制機関からの監視を受ける中、サイバーセキュリティーの事象件数は増加する一方です。投資家や弁護士も目を光らせています。経営層の役員から一般社員まで、すべての従業員に対し絶対的で厳重なセキュリティーを提供する必要がありますが、全従業員自身が脆弱性を媒介する危険性を持っています。



これらの 3 つの項目をチェックリストに入れることを考えてください。

能力不足

第一階層または前線のアナリストは多くの場合、この業界での経験が長くありません。SOC 全体で必要とされる真のスキルを習得し、調査能力の信頼性や成熟度を達成するには、時間がかかります。2018 年の ESG の調査によると、組織の 51% が「サイバーセキュリティーの分野において深刻なスキル不足がある」と回答しています。この回答は、2017 年には 45% に上昇しています。実際にサイバーセキュリティーの能力が不足しており、ESG によると、サイバーセキュリティー・プロフェッショナルの 38% が、スキル不足のために燃え尽き症候群の比率が増加し、人員不足が発生していると答えています。

悩んでいる時間が長すぎ、コストがかかっている

平均で 50 ～ 200 日間も討議にかかっています。データ漏えいを 100 日未満で検知した企業では、100 日以上かかった企業に比較して、100 万ドル以上のコストが節減できています。

チームは知見過負荷がかかっており、救済策がありません

お客様の組織でもサイバーセキュリティー人員の疲弊が起こっている可能性が高く、これは珍しいことではありません。サイバーセキュリティー人員は同じ作業の繰り返しに圧倒され、規定されたプロセスの崩壊が起こっています。これらすべてが積み重なって、重要な侵害指標 (IoC) が見逃される可能性が高くなります。そして、最新の高度な脅威に対応しようと、新しいソリューション・ポイントを追加すると、事態はさらに悪化します。この理由は、データ・サイロや統合の複雑性、アナリストが解析しなければならない知見数が増加するからです。

自分の組織で SIEM や AI が必要か?どの部分が単なる流行で、どの部分が本当に重要か?

2

AI を使用することで適切なセキュリティー・バランスが実現できるか?

AI についてはいろいろな噂を聞くことがあっても、自分が投資した AI ソリューションが、自分の仕事に役立つインテリジェントな認知ソリューションであることに確証が持てるでしょうか。確実な答えは、AI が学習し、予防対策が取れるかにかかっています。重要な点は、AI によって疲労の原因となる反復タスクが自動化され、最も困難な課題である人材の問題が解決されるかという点です。

リーダーシップを示しながら組織のセキュリティー体制を維持し、SOC の日常業務をこなすのに精一杯で、拡大し続ける脅威環境に追いつくのはほぼ不可能です。SOC を守る準備が常にできているツールを備蓄している必要があります。

ここ数年間、AI が多くの話題にのぼり、過大評価されてきたことは、周知の通りです。ただ、SOC 内に適切に適用された AI は、独自に学習を続け、自己更新を継続的に行う、非常に有効なツールであることは間違いありません。AI は万能薬ではありませんが、セキュリティー武器庫の中で重要な役割を果たせます。

3

AI を使用することでセキュリティー・スタンスが強化されるか?

4

AI は人間のチームを 代替できるか?この ソリューションはチームの生活を脅かすものか?

AI はチームに対抗するものではなく、チームと協働できるものです。チームは反復タスクを AI に任せ、より多くの情報に基づいた意思決定を下せます。AI は、あらゆる場所から収集した外部データとネイティブ環境を統合し、次にどのような措置を取ればいいかを理解します。すべてのケースで、時間がかかるタスクからルーチン意思決定に至るまで、AI にどれだけの作業を任せるかを決めるのは人間です。つまり、AI はいつでも待機しており、人間がその経路を決め、指揮をとります。

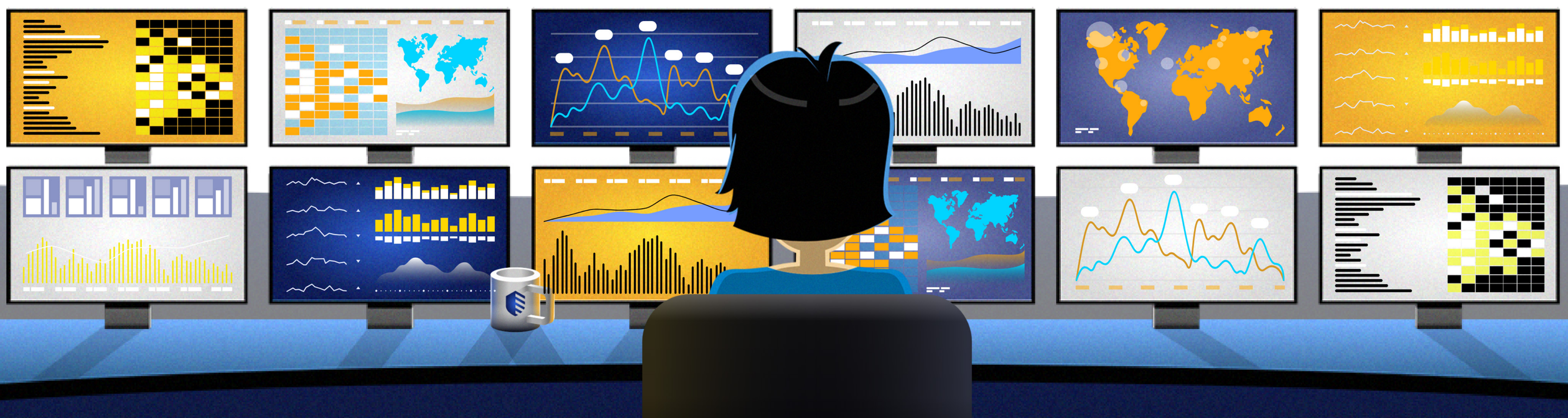
5

このソリューションは AI なのか、それとも機械学習なのか?違いを理解する必要があるか?

「AI」と「機械学習」という用語は、多くの場合、同義語として使用されています。さらに「機械学習」の代わりに「ML」という略語が使われたり、「AI」の代わりに「人工知能」という用語が使われたりします。しかし、AI（人工知能）と ML（機械学習）は同じでないため、本当に必要なものが AI

なのに機械学習ソリューションを購入してはなりません。機械学習では、データと交信できる機械の能力が中心になります。機械は「学習」でき、受信するデータの量が増えるに伴いアルゴリズムを変更できますが、機械学習は AI のサブセットであるため、最終的にこれが限界です。AI では、認知能力が成長、学習でき、アルゴリズムに基づいてタスクを実行できます。AI は、データベース、あるいは機械によって生成されたデータ（構造化）、またはソーシャル・メディアや雑誌記事（非構造化）のデータなど、ほぼ無限の種類の情報源から情報を収集し知識を蓄積し続けることによって SOC を支援します。AI は企業内のデータ、ブログ、レポート、リサーチ、セキュリティー・アラートなどの外部のあらゆる場所からのデータを使って学習できます。この要素が、機械学習と AI との違いです。

SOC に AI を装備することで、お客様の組織に特化して設計された推奨事項を提供できる組織メモリーのレポジトリにアクセスできます。AI を使用することで、セキュリティー運用とソリューションのバランスを取ることが可能になるため、本当の AI ソリューションを購入しているかを理解することが重要です。



6

AI を使用することでセキュリティーの取り組みにどのような改善が期待できるか?

異なる潜在的なインシデントを自動的に連携できます。

AI は、根本原因の自動化や統合以上のことができます。AI は脅威とリスク知見を紐づけられますが、疲れを知りません。AI は、人員の交代、未熟さ、時間の経過が原因で人間が見逃す相互関係を示すことができます。AI なしでは、経験の浅いアナリストは、単一の攻撃インスタンスだと思ってアラートを解決済みと設定してしまう可能性があります。AI は認知推論を使用して、トラブル・チケットが解決済みに設定されたのが一昨日前であろうと、何カ月も前であろうと、複数のインシデント間の共通点を見つけ、コンテキストに基づいた行動可能なフィードバックを提供します。AI は外部脅威インテリジェンスを収集して、人間の解析に文脈を追加し、人間が気付かなかった文脈を収集することができます。

人員関係の問題を解決。

AI は、脅威や組織について得た知識を基に根本原因分析を判断し、次の措置を調整できます。AI には休暇が必要ありません。AI は離職しません。重要な IOC を見逃していないか考慮する必要がありません。

いつでも一貫性のある詳細な調査を実行できます。

AI は、構造化データと非構造化データの両方を読み取ることができ、人間では不可能な量のデータを読み取れます。AI は学習します。AI は Mean Time to Detect と Mean Time to Respond (MTTD および MTTR) を低減して、必要な情報をより速く提供でき、エスカレーション・プロセスを促進します。AI は既知および未知の脅威を検知するための高度なアナリティクスを提供できます。AI は、いつでも一貫性のある詳細な調査を実行できるため、アナリストは勘ではなく、データに基づいて意思決定を下せます。

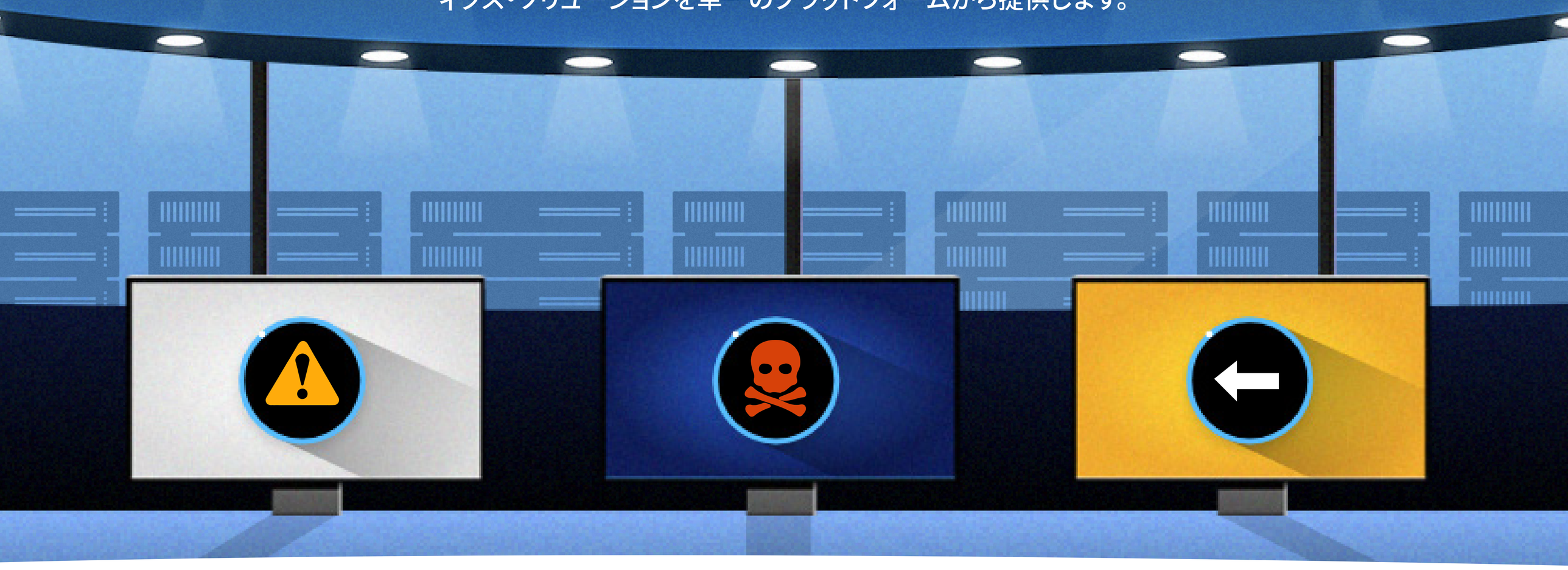
人、プロセス、テクノロジーをまたがる堅牢で自動化されたインシデント対応 (IR) ワークフロー

AI はデータとエビデンスに基づいた高速で完全な対応を通してセキュリティー・アナリストを導きます。AI はワークフローと修復を自動化します。AI は、SOC による評価を可能にし、IR プロセスの継続的な改善を実現します。

7

攻撃の発生前、発生中、発生後、AI はどのように SOC を改善するか

データ漏えいの発生前、発生中、発生後、AI を使用することで SOC をより効率的に準備でき、短時間で修復できます。IBM QRadar Security Intelligence Platform は、このテクノロジーをお客様の SOC に統合して、包括的なアナリティクス・ソリューションを単一のプラットフォームから提供します。



攻撃前 → 攻撃中 → 攻撃後

IBM QRadar SIEM は、完全な可視性を提供し、攻撃サイクルの早期に脅威や異常を検知します。

IBM QRadar SIEM がエビデンスを継続的に収集するため、フォレンジック・データを簡単に使用できます。AI は、ビジネスに与える影響を基に優先順位を決定します。

IBM QRadar SIEM は、得られた教訓を基に検知メカニズムを継続的に調整します。

IBM QRadar Advisor with Watson は、自動的にすべての異常を調査し、高リスク攻撃動作を特定します。

IBM QRadar Advisor with Watson は、自動化された根本原因解析によってチームの力を増強し、脅威の全容を明らかにします。

IBM QRadar Advisor with Watson は、将来起こる攻撃に、より正確に対応できるようモデルを適応させます。

IBM Resilient は、SOC による、人、プロセス、テクノロジーにわたる堅牢で自動化された IR ワークフローの構築を可能にします。

IBM Resilient は、高速で完全な対応を通してセキュリティー・アナリストを導き、インシデント・ワークフローと修復を自動化します。

IBM Resilient は SOC による IR プロセスの継続的な評価と改良を可能にします。

IBM QRadar with Watson について

AI を使用することで、増加する一方のサイバー脅威を阻止し、SOC 運用を最適化できます。IBM® QRadar® Advisor with Watson はルーチンの SOC タスクを自動化し、複数の調査にわたる共通点を特定し、アナリストに行動可能なフィードバックを提供してアナリストの作業を軽減するため、アナリストはより重要な操作の要素に集中することができ効率性が向上します。

詳細情報

参考資料

The State of Cyber security Professional Careers, ESG

IBM Security