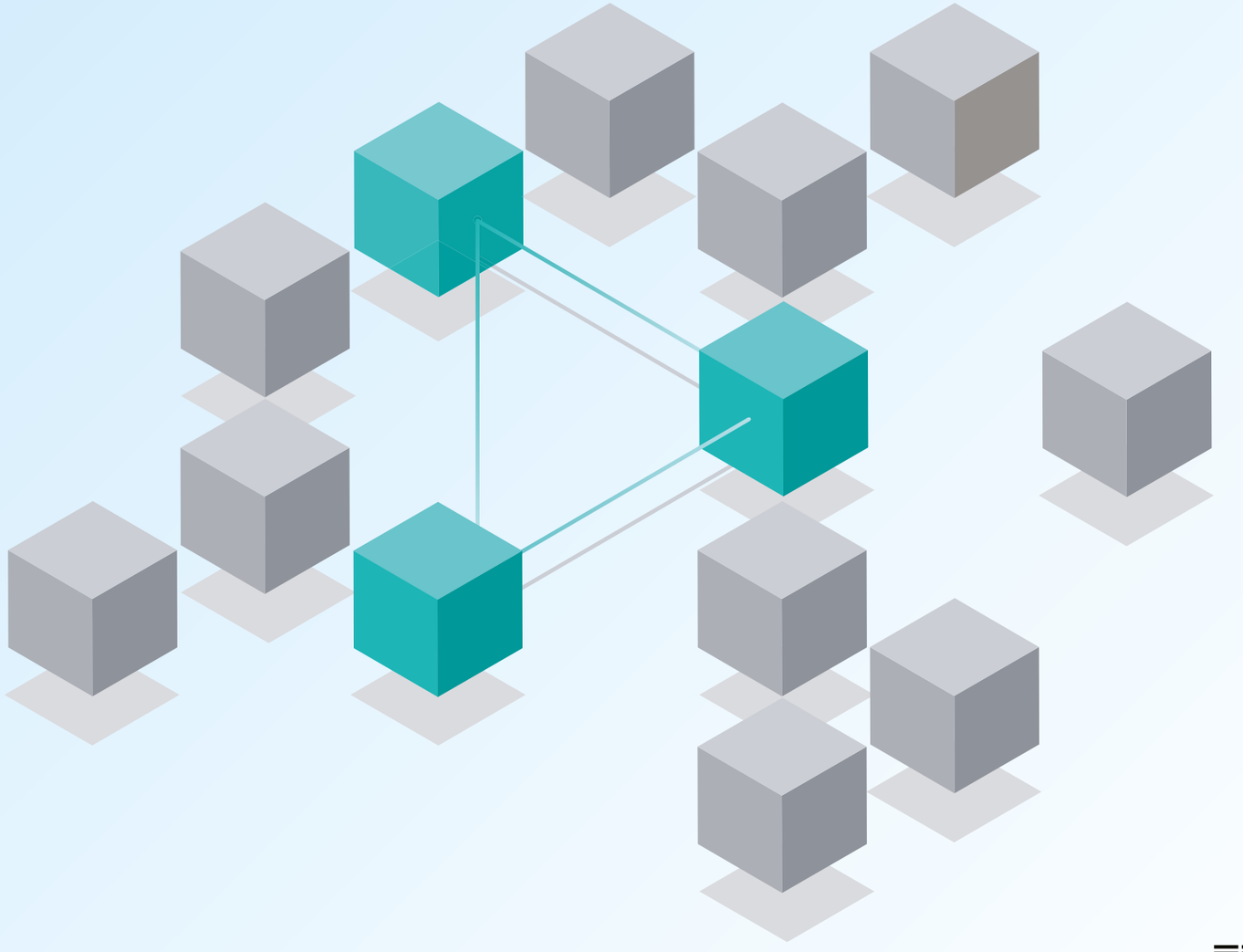
EDR購入者ガイド

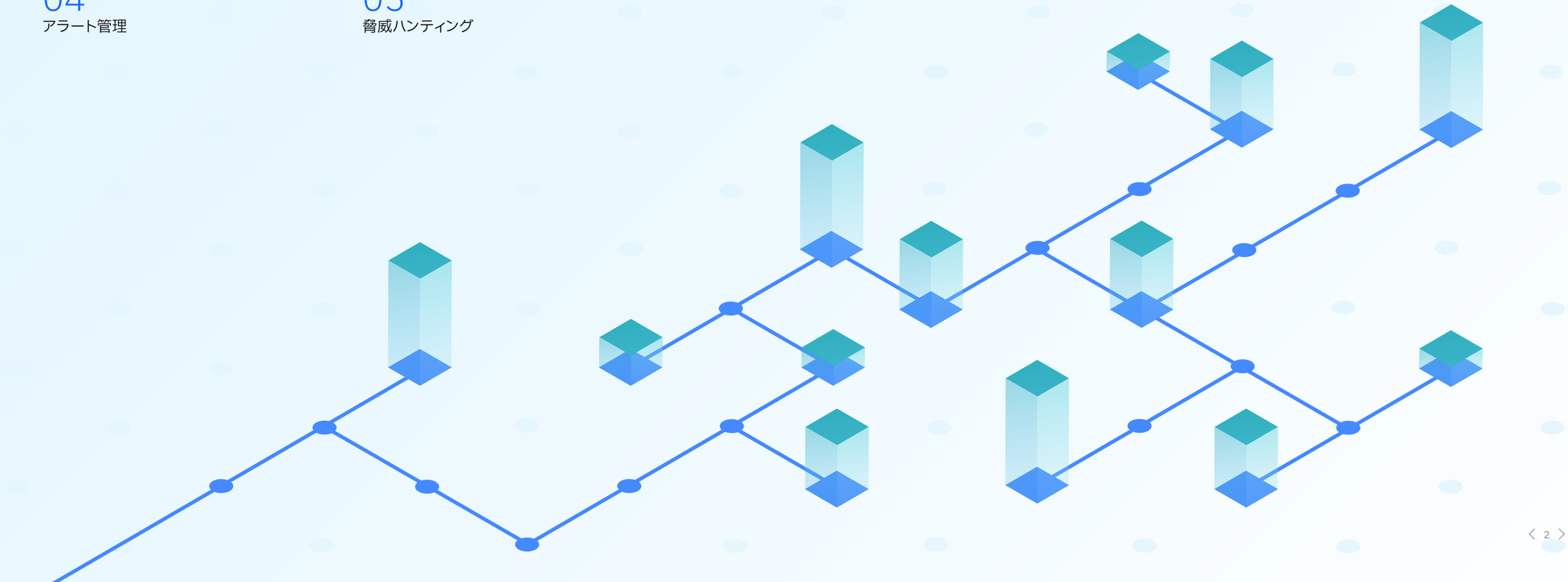
お客様のビジネスにぴったりのEDR（エンドポイントでの検知およびレスポンス）ソリューションを選択するには



REAQTA
an IBM Company

IBM

目次



01
はじめに

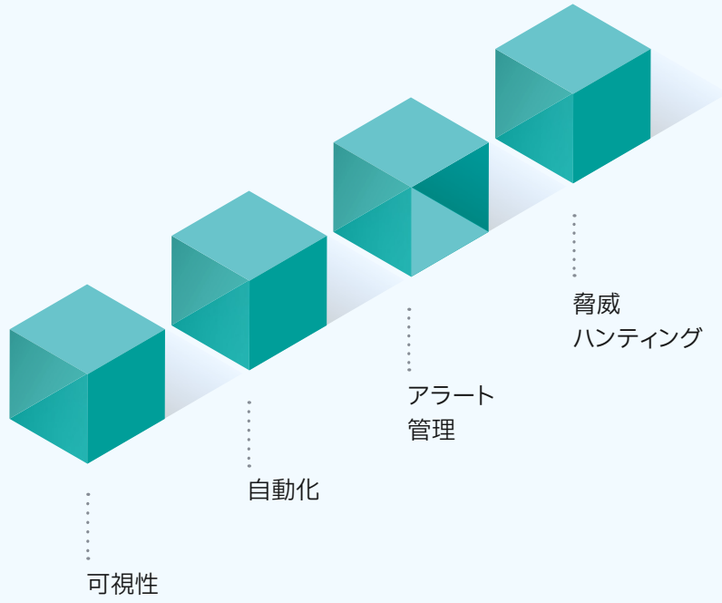
EDRとは何か、そしてEDRが必要な理由
近年、エンドポイントやデータが拡大し、相互接続も増えてきたのに伴い、悪意ある活動も増えてきています。このような要因のため、大企業であれ中小企業であれ、ビジネス・コミュニティーは重大な脅威にさらされてきました。個人や国家が行うサイバー攻撃の犠牲となる企業の数は、増加の一途をたどっています。

従来の防御のしかたは既知の脅威に対応していますが、複雑で未知の攻撃手法に脆弱で、資産への可視性が得られません。これは、こうしたシステムを保護する上で最も大きな障害のひとつと言えます。専門家に依頼してエンドポイントを保護できるのは普通、大企業か、潤沢な資金のある組織だけです。現在、多くの攻撃が機械化されたスピードで行われ、多くの可動部分が存在するという事実もあって、従来型のソリューションに依存し、人間が作業するチームでは対応しきれない、という状況が生まれています。

エンドポイント検知およびレスポンス(EDR)ソリューションは、マルウェアを事前に自動でブロックして隔離し、セキュリティー・チームに適切なツールを提供して、難局に自信を持って対処できるようにします。最新のEDRでは、アナリストの負担を増やしたり高度な技術を持つセキュリティー専門家を必要としたりすることなく、急増しつつある自動化された高度な脅威(ランサムウェア攻撃やファイルレス攻撃など)を効果的に抑制して、ビジネス・コミュニティーを守ることができます。

次のいずれかの問題でお悩みですか?
- 既存のソリューションが役に立たない
- 可視性が限られている
- スキルのある人材の不足
- アラート疲労
- 潜伏した脅威

最新の効果的なEDRは主に4つの要素で構成されており、それは次の章でご覧いただきます。



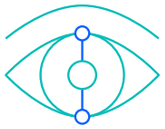
02
エンドポイント・エステート全体の完全な可視性

エンドポイントを保護する際の主な障害のひとつが、可視性の欠如です。そのため、最新のEDRソリューションでは、実行しているアプリケーションとプロセスへの完全かつ深い可視性を提供する必要があります。

脅威が現れたときに、攻撃の進展に伴いグラフィカル・ストーリーラインを使用して、リアルタイムで挙動のアラートを自動作成する必要があります。これにはアナリストに完全な可視性を提供し、何が起こっているかを把握できるようにするMITRE ATT&CKマッピングが含まれます。

すべてとは言わないまでも、大部分のエンドポイント・セキュリティー・ソフトウェアは、オペレーティング・システム内で動作し、エンドポイントのエージェントに対して境界を作ります。このため、エージェントの機能と可視性は制限され、同時にコンピューターのリソースも消費されます。ハイパーバイザー層で動作し、検出されないように設計されたエージェントを使用すれば、リソースの使用を低減するだけではなく、すべてのプロセスの動作を監視する優れた可視性を提供し、同時に攻撃者に対しては姿を隠すことができます。

確認事項:
- エンドポイントの完全な可視性
- リアルタイムのアラート
- ストーリーラインの作成
- トラブルのないエージェント
- 統合されたワークフロー



準備すべき質問:

→ 貴社のソリューションは、アプリケーションや実行中のプロセスに 完全で深い可視性を提供していますか。

→ 攻撃が展開されたときに、貴社のソリューションから脅威に対する理解を深めるための意味のあるリアルタイムの情報は得られますか。

→ 侵害を検知して警告することに加えて、お使いのMSSPではエンドツーエンドのレスポンスと修復が利用できますか。

03
自動化および使いやすさ

高度な脅威と攻撃対象領域が2022年以降増大する見込みがある中、多くの組織はサイバー犯罪者に一歩先んじることに苦心しています。最新のEDRは、増え続けるワークロードをスマートな自動化で軽減し、高度なスキルをもつセキュリティーの専門家の必要性を極力抑えて、使いやすくしなければなりません。

購入したEDRから価値を得るために重要なことは、自動化と単純化です。AIによる自動化で、作業の大半はアルゴリズムによって行われ、人間による対応は最小限となります。そのようなAIのアルゴリズムを使用することで、ソフトウェアは使いやすくなり、時間のかかる有効化の手続きなしで、すぐに作業を開始できます。

攻撃されたとき、事態を左右するのがレスポンス時間です。高度な脅威が貴社のインフラに損害を与える前にそれを取り除くための調査時間は、1分をかなり切る必要があります。

自律的に実行され、自動化された検出および応答機能を持つEDRを探して購入しなければなりません。そうすれば、アナリストは攻撃が進化したときでも、クリアでリアルタイムの概要を入手でき、ガイド付きの修復機能で、すばやく常態を回復することができます。

確認事項:
- 自律型検出
- ガイド付き修復機能
- エージェント分析
- すばやいレスポンス時間
- 使いやすさ

準備すべき質問:

→ EDRを操作するには、高度な技術が必要ですか。

→ アナリストの負担を軽減するために、EDRを自律的に実行できますか。

→ レスポンス時間に関して、脅威が分析されるのはクラウド内ですか、それともエージェントでですか?

→ 脅威がクラウド内で分析される場合、インターネット接続がないとどうなりますか。

04
アラート管理

従来型のアンチウイルス(AV)ソリューションとEDRの主な違いですが、まずAVは利用可能な署名に検出を依存しており、脅威をブロックするためにはそれについて知っている必要があります。一方、EDRでは、マルウェアやその他の潜在的な脅威をエンドポイントでの挙動によって識別する動作型アプローチを使用します。また、AVとは異なり、EDRは元々軽量で、頻繁なアップデートを必要としません。

したがって、最新のEDRで使用されるAIは、すばやく検出を行い、高い精度と忠実性でアラートの量(そしてアナリストの負担)を最小限に抑える必要があります。購入の際には使用されているAIと機械学習技術について知っておく必要があります。事前訓練モデルと分析に検出を依存するAIエンジンに比べ、初期学習モデルを使用して各エンドポイントの正常な挙動を特定するEDRでは、正常な動作から逸脱している場合に、より正確な検知とアラートが可能になります。

レスポンス時間を削減し、アナリストのアラート疲労を軽減するために、最新のEDRでは、アナリストから学習し、毎日のアラート処理でアナリストの意思決定を自律的に適用できる、堅牢なAI駆動のアラート管理システムが装備されている必要があります。完全に自動化されたAI駆動のアラート管理システムを導入することは、アラート疲労と戦い、従業員の離職を減らし、事態を再び掌握するために重要です。

確認事項:
- 高精度のアラート
- AIモデルの使用
- アラート疲労の防止
- 自動化されたアラート管理

準備すべき質問:

→ 貴社のソリューションに、自動的にアラートを処理してクローズする方法はありますか。

→ 貴社のソリューションはどのくらいアナリストの時間を節約しますか。

→ 貴社のソリューションはどれくらい誤検出を減らしますか。

→ 従業員が離職した場合、その人のインフラストラクチャーに関する知識を維持するにはどうしますか。

05

脅威ハンティング

脅威ハンティングは最新のEDRの重要な部分で、クリーンで脅威のない環境を維持するために必要です。脅威ハンティングを使うことで、新しい脅威が環境に侵入したかどうかをすばやく判断し、弱点を特定することができます。データ・マイニングによって、気づかない間に数ヶ月あるいは数年にもわたって環境に住み続け、攻撃者によって使用されることを待っているかもしれない潜伏した脅威を検索して削除できます。

本来、インメモリおよびファイルレス脅威を追跡するのは難しく、攻撃者が大規模なインフラストラクチャーを移動する際にさまざまなバリアントを使用する場合、さらに追跡が困難になります。最新のEDRはハンティング・ジョブを自動化し、データ・マイニングを使用することで、セキュリティー・チームが動作と機能レベルで他のインシデントと類似点を共有する脅威を自動的にハンティングし、数秒で対応できるようにしなければなりません。

脅威ハンティングの柔軟性は非常に重要です。購入の際、探すべきものは、事前構築されたプレイブックの大きなライブラリーを持ち、すぐに配置できるだけでなく、スクリプトの知識がなくても、自社特有のセキュリティー上のニーズに合わせて簡単に作成できるカスタム・プレイブックを備えたEDRです。

脅威ハンティングは干し草の山の中から針を見つけるようなものだ、とよく言われます。EDR検索では、特定のハンティング・パラメーターにドリルダウンし、こうしたパラメーターを包括的/排他的な方法で組み合わせることによって、包括的かつ粒度の高い結果をリアルタイムで提供する必要があります。アナリストを助けて時間を節約するには、結果をわかりやすいグラフィカル・ユーザー・インターフェース(GUI)で表示する必要があります。そうすれば、アナリストはどのエンドポイントからでも、いつでも任意のイベントを簡単かつ直感的に調べることができます。

確認事項:
- 潜伏した脅威の調査
- 自動化されたハンティング
- カスタム・プレイブックの作成機能
- スクリプト作成不要
- データ・マイニング
- リアルタイム機能
- グラフィック概要

準備すべき質問:

→ ユーザーは独自のカスタム検出方針とプレイブックを作成できますか。

→ 脅威ハンティングのシナリオを自動化できますか。

→ 高速トリアージ目的で脅威ハンティングのグラフィック概要を提供できますか。

→ プレイブックを作成するためにスクリプト作成の知識は必要ですか。

次のステップ

IBM Security ReaQtaの詳細および体験版の依頼についてはこちら。

日本アイ・ビー・エム株式会社
〒103-8510
東京都中央区日本橋箱崎町19-21