2016 年 5 月

コグニティブ・セキュリティー

理解し、考え、学ぶセキュリティーにより、防御を進化させる

目次

新たな必須要件

ほぼ一世紀にわたり、IBM は、複雑な問題を解決できるように、コンピューターのプログラミングを続けてきました。現在では、天気のシミュレーション、ゲノム配列の解析、世界中で瞬時にデータを共有することができるようになっています。しかし、画像の認識、読書や詩の意味の説明など、人間が日々行っているようなことをコンピューターにさせるということになると事情が異なります。従来のシステムでは不十分なのです。

セキュリティーについても同様です。数十年にわたり、IBM では、ウィルス、マルウェアやエクスプロイトを認識するようにコンピューターのプログラミングを継続してきました。より正確になるようにコンピューターの調整を続けていますが、それでは十分ではありません。敵は常に攻撃を変化させ、防御を突破するためのクリエイティブな方法を見つけ出します。企業が必要としているのは、活動の微妙な変化を検知し、可能な限り多くのコンテキストで分析し、新たな脅威を識別して取り除く能力です。

世界のデータの 80% は 見えていませんでした。

これまでは。

被害を受ける前に攻撃や異常な振る舞いを見つけ出すには、継続的に監視を行い、データを最大限に活用することが必要です。しかし、世界では毎日 250 京バイトのデータが生み出されており、その内の 80% が構造化されていません。これは、人間が容易に理解できる話し言葉、書き言葉、視覚的言語などの自然言語でデータが表現されていることを意味していますが、脅威に対するインテリジェンスが詳述された何千ものブログが毎日投稿されているにも関わらず、従来のセキュリティー・システムは理解することができません。現実には、セキュリティー・アナリストがその内容をすべて把握することは不可能であり、従来のセキュリティーでは、アナリストが行うようなやり方でこのような洞察を分析、利用することはできないのです。

いまだに最も困難なセキュリティー上の問題では、対応の拠りどころとなるものやフォールス・アラームの見極めについて適切な判断を下すように迫られているという理由がここにあります。実際に、最も優秀なセキュリティーの専門家は、同僚と話し、会議に参加し、研究を逐一把握しながら、経験を通して知識体系を日々構築しています。

IBM Security では、絶えず進化し続けるセキュリティー脅威について理解し、考え、学ぶ新世代のシステムのトレーニングを行っています。セキュリティーに対する直観力と専門知識を新たな防御の中に組み入れ始めています。この防御はセキュリティーの専門家が日々行っているように、ただし、これまでにない規模で、調査レポート、Web ページ中のテキスト、脅威データやその他のセキュリティーに関連する構造化および非構造化データを分析するのです。 これがコグニティブ・セキュリティーの本質です。

結果: アナリストたちは脅威に関する理解を補強し、さらには自動化できるようにコグニティブ・システムに要請するようになり、最新の攻撃についてより賢く、貴重な時間を他の差し迫った問題に割けるようになります。

コグニティブ・セキュリティーとは

コグニティブ・システムとは、データ・マイニング、機械学習、自然言語処理およびヒューマン・コンピューター・インタラクションを使用して、人間の脳の働きを模倣する自己学習システムです。

コグニティブ・セキュリティーとは、2 つの広範かつ関連する機能の実現です。

- コグニティブ・システムを活用することで、セキュリティー動向を分析し、膨大な構造化および非構造化データから不必要な要素が取り除かれた情報にした上で、実用的な知識に抽出し継続的なセキュリティーと業務改善を可能にします。
- 自動化されたデータ駆動型のセキュリティー・テクノロジー、手法やプロセスを活用することで、コグニティブ・システムが最高レベルのコンテキストと正確性を保有できるようにサポートします。

コンプライアンスからコグニティブへ

初期のネットワークやそれに続いたハッカーの時代から、IBM は攻撃を止めるセキュリティー・テクノロジーを発展させてきました。今日まで、サイバー・セキュリティーには、境界コントロールおよびセキュリティー・インテリジェンスという明確に異なる 2 つの時代が続きました。コグニティブ・セキュリティーという第 3 の時代に入ると、これらのセキュリティーは構成要素として役割を果たします。

境界コントロール: 制限によるセキュリティー (2005 年以前)

IBM は、ファイアウォール、ウィルス対策ソフトウェアや Web ゲートウェイなど、データの流れを防御または制限する静的防御から始めました。企業内部における情報セキュリティーの進化は、コンプライアンス活動として始まり、パスワードや広範なアクセス制御戦略によって機密情報へのアクセスをロックダウンし、制限することが目的でした。
成功とは、監査に通ることを意味していたのです。境界防御がまだ使用され続けていますが、それだけでは現在の環境には十分ではありません。

セキュリティー・インテリジェンス: 思考の一助となるセキュリティー (2005 年以降)

時間と共に、脆弱性を見つけ出し、潜在的な攻撃の優先順位付けを行うために膨大なデータを収集し、綿密にチェックすることができる高度な監視システムに発展しました。この変化により、疑わしいアクティビティーを検知するリアルタイム情報に焦点が置かれるようになりました。現在では、セキュリティー・インテリジェンスとは、ユーザー、アプリケーションやインフラストラクチャーが生成した構造化データのリアルタイムの収集、正規化および分析を意味するようになっています。

セキュリティー・インテリジェンスは規則的なパターンの逸脱を検出し、ネットワーク・トラフィックの変化を明らかにして、設定したレベルを超えるアクティビティーを見つけるアナリティクスを活用します。セキュリティー・インテリジェンスのインフラストラクチャー内部では、コンテキストの中で企業データを理解し、日々のアクティビティーの優先順位を決定する目的で、アナリティクスが膨大な情報に適用されます。セキュリティー・インテリジェンスは有意な逸脱を判断することで、より迅速に侵害を検知できるようになるだけでなく、フォールス・ポジティブ（誤検知）を減少させて時間とリソースを節約します。

コグニティブ・セキュリティー: 大規模に理解し、考え、学ぶセキュリティー (2015 年以降)

コグニティブ・セキュリティーはビッグ・データ・アナリティクスを活用するセキュリティー・インテリジェンスをベースに構築されており、理解し、考え、学ぶことができるテクノロジーを特徴としています。書き言葉や話し言葉など、構造化されていない現在のデータの 80% を処理して解釈することができるコグニティブ・システムにより、遥かに大きなスケールの関連セキュリティー・データにアクセスできるようになっています。

コグニティブ・セキュリティー・システムは、所定のテーマについて専門家が監修した知識のデータ集を取り込んだ後、一連の質問と答えの組み合わせを投入されることで訓練されます。その後、セキュリティーの専門家がシステムの応答の正確性についてフィードバックを与え、システムとやり取りをして、この機械の「知識」が高められます。
主な違い: コグニティブ・システムは人間を遥かに上回る速度で新しい情報を理解し、処理します。今や技術的防御は、日々生み出されている何千もの調査レポート、会議資料、学術論文、新しい記事、ブログ投稿メッセージ、業界のアラート情報を分析するように訓練することができるのです。

コグニティブ・システムが有害なものと価値のあるものを区別しながら、イベントや振る舞いの観察を継続するにつれ、統合防御を活用して新たな脅威をブロックする機能はますます強化されていきます。コグニティブ・セキュリティーは、セキュリティー・アナリストがより効率を上げられるように支援し、新たな脅威に対する対応を促進することで、現在のセキュリティー・スキルのギャップに対応し、信用を高め、リスク管理を実現します。(図 1 参照)

セキュリティー年表

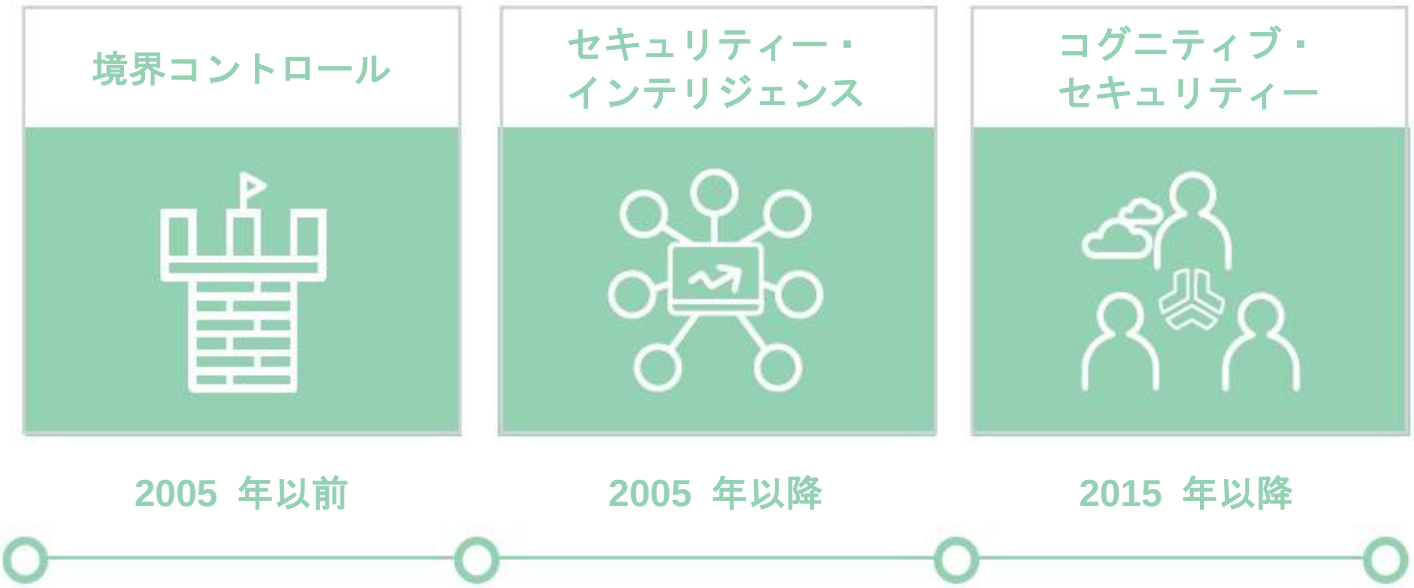

図 1

コグニティブは、最終的には、従来のセキュリティーを基に構築されたフレームワークに加わります。セキュリティー・インテリジェンスはコグニティブ・セキュリティーの重要な構成要素であり、消え去るようなことはありません。コグニティブの役割は、かつてないスピードと規模で、私たちに脅威に対するインテリジェンスと検知を選別する方法を与え、実用的な情報を提供することです。

図 2

セキュリティー・インテリジェンスとビッグ・データ・アナリティクスが従来から構造化されていなかったことから、コグニティブの要素によって、状況把握や対応方法に重要で付加的なレベルの理解がもたらされます。このようなフル・スタックを活用して、セキュリティー環境を最大限保護することができます。(図 2 参照)

コグニティブ・セキュリティーの強み

従来のプログラムで制御できるセキュリティー・システムは、予め設定されていたパラメーターに従い、要求に応答し、データを判断し、分析しています。コグニティブ・システムは、実質的にすべてのインタラクションからデータを解釈し、知識の基盤に追加し、洞察の深さに基づいて可能性を推測して、関連変数の考察を踏まえて対応できるようにお手伝いをします。

現世代のシステムが異常値や攻撃を検知し、対応するという受け身の防御であるのに対し、コグニティブ・セキュリティーの防御は積極的です。将来に焦点を合わせた、継続的なマルチタスクであるコグニティブ・システムは脆弱性を調査し、点と点を結び合わせ、変数を検出し、何十億ものイベントを取捨選択して、実用的な知識の土台を構築します。

コグニティブ・ソリューションは答えだけでなく、仮定し、根拠に基づいた推論と提案を生成します。現在では、以前は既存のシステムがアクセスすることができなかった、無数の情報ソースや場所から得られた構造化されていないデータの 80 パーセントを解釈し、構造化されたデータと統合する能力が実現されています。情報から価値がもたらされる傾向が強まっているグローバル経済において、データは世界で最も豊富で、価値があり、複雑な原料です。私たちは、今や、構造化・非構造化データの両方を利用し、継続的に特徴やパターンを抽出して、意思決定を向上させるコンテキストをリアルタイムで提供する方法を手にしているのです。

コグニティブ・セキュリティーの次の 3 本の柱は、人間の思考パターンのように高速で機能します。

1. 非構造化データおよび自然言語テキストを**理解**し、解析します。本、レポート、ブログや関連業界データを「読む」こと、コンテキスト内の画像を「見る」ことや自然音声を「聞く」ことを通して、情報を取り込み、処理する能力が含まれています。
2. 情報を解釈して整理する能力を基に**推測**し、結論の論理的根拠と共にその意味を説明します。
3. データを蓄積し、インタラクションから洞察を導き出しながら、継続的に**学習**します。

より深く掘り下げ、より広い範囲へ

マルウェア、悪意のある脅威、外れ値や異常値を検出することだけに焦点を当てていると、得てして大量のフォールス・ポジティブにつながりますが、それこそが、コグニティブ・システムが活動する多次元の場の利点なのです。

今日の世界では、白と黒を区別する能力は、統合型セキュリティー・インフラストラクチャーに必要とされる専門知識の側面の 1 つに過ぎません。グレーの領域は増大しており、そこでコグニティブの出番になります。

コグニティブ・システムは高められた直観、インテリジェンスや洞察で強化されており、新たな脅威を示している可能性のある微妙な変化を区別できるように、継続的にデータを使用して向上するように設計されています。その結果として、全体像についてより大きな視野とプロアクティブな視点がもたらされます。

スキルのギャップに対応する

今日のセキュリティー環境に追いつくように求められているのはシステムだけではありません。スタッフの側の課題も存在します。世界中の情報セキュリティー・スタッフの欠員数は 208,000 人と見られており、2020 年までに 150 万人に増加すると予想されています。コグニティブ・セキュリティーならこの問題の解決に役立ちます。

コグニティブ・システムは、人間の能力を支援する拡張性のあるリソースとしての役割を果たし、人員が不足しがちなセキュリティー部門を臨時に増強したように機能することができます。使用しているシステムの内部で起きていることを監視し続けるだけでは、もはや十分でないため、この新たな特徴は重要です。潜在的な攻撃に備えるために、グローバルな規模で脅威を監視する必要があります。コグニティブ・システムは、世界中の何千もの顧客のために、膨大な数のセキュリティー・イベントを毎秒分析するグローバル・エクスチェンジ・ネットワークを利用することができます。

コグニティブは、高度な可視化、インタラクティブな脆弱性分析、リスク評価、是正策や可能性のある属性など、人間が主体のコミュニケーションを提供することで、セキュリティー・アナリストの仕事を軽減することができます。コグニティブ・システムは異常値や誤ったロジックを特定し、エビデンスに基づいた推論を提供できるようになります。これにより、アナリストは別の結果を比較検討し、意思決定を向上させることができるのです。

ユース・ケース:

解き放たれたコグニティブ

SOC アナリストの向上

コグニティブ・システムは、広大な構造化および非構造化データの海を理解し、若手アナリストの価値をレベル 1 からレベル 2 または 3 へ迅速に移行させるお手伝いをすることができます。コグニティブ・システムは、調査レポートやベスト・プラクティスなどの情報の取り込みを自動化して、リアルタイムのインプットを与えることができます。以前は、この知識と洞察は長年の経験からのみ得られるものでした。

外部インテリジェンスを使用する高速応答

Heartbleed のような脆弱性 が見つかったら、人々は防御方法をブログに投稿するでしょう。シグネチャーがまだ入手できない場合でも、オンラインには疑問点の答えを見つけられる自然言語の情報があります。コグニティブ・システムはクローリングして、次のゼロデイ攻撃から保護する方法を素早く見つけることができます。

先進的なアナリティクスで脅威を特定

コグニティブ・システムは、機械学習、クラスタリング、グラフ・マイニングおよびエンティティー関係モデルなどの分析手法を使用して、潜在的な脅威を特定することができます。これらのシステムは、被害が発生する前に、リスクの高いユーザーの振る舞いを素早く検出したり、データ流出およびマルウェアを検出したりできるように支援します。

アプリケーション・セキュリティーの強化

コグニティブ・システムは、コードやコード構造の理解を深めながら、アナリティクスやデータの意味コンテキストを理解することができます。何千もの脆弱性の知見を理解し、結果を使用可能な小さな項目に精緻化して、使用しているコードの中の修正個所を見つけ出します。

企業リスクの改善

将来的には、組織、企業活動に関するリスク・プロファイル、トレーニングや再教育を策定するために、コグニティブ・システムは対話のコーパス、対話の性質や影響の受けやすさなどを分析できるようになります。また、自然言語処理を使用して、組織の機密データを見つけて編集できるようになります。

未来: 逆転するサイバー犯罪経済

微妙な共通性を検知するために、コグニティブ・システムは、マルウェアとして知られている、膨大な悪意のあるソフトウェアから特徴または特性を分析することができます。共通性の検知が重要な理由は、悪意のあるソフトウェアは非常に多様性に富んでいますが、サイバー犯罪のグループはコードを進化させており、現在稼働しているマルウェアの大半が実質的に他のマルウェアと関連しているからです。コグニティブ・システムを使用すれば、不審な実行ファイルの膨大な機能を分析し、それらを集めて、パターンを見つけ出すことができます。人間がそれらの機能の正体や、どのように、なぜ一致するのかを知らなくても、システムは新たなマルウェアの亜種を見つけ、分類できるパターンを特定できます。

コグニティブ・セキュリティーのコミュニティーが拡大し、新たな攻撃の実行可能性が減少するにつれ、サイバー犯罪は新たな経済の現実を迎えることになります。検出を回避するマルウェアを開発する努力はますます複雑になり、費用がかかるようになるでしょう。Ponemon Institute の 2015 年の「データ漏えいコストに関する調査報告書」によると、企業は APT 攻撃の検出に平均で 256 日を要し、アメリカのデータ漏えいの平均コストは 650 万ドルになります。コグニティブ・セキュリティーは、潜在的な攻撃の警告情報を早期に見つけ、検出を大幅に加速させる能力をセキュリティー・アナリストに与えます。サイバー犯罪者は利益を得ることがますます難しくなっていることに気付くことになるでしょう。

コグニティブ・コンピューティングは、データだけでなく、意味、知識、プロセス・フローやアクティビティーの進行を電光石火の速度とスコープで活用することで、大きな変化を推進しています。コグニティブ機能を活用する企業にとっては、競争優位性が飛躍的に向上し、広範に及ぶことになります。

コグニティブ・エコシステムに向けた統合化と専門知識

統合と専門知識はセキュリティーを正しく実施するために最も重要です。あまりにも多くのセキュリティー・プラクティスが統合化されていないポイント製品の集合体の上に構築されており、迅速に対応するために必要な可視性も実用的なインテリジェンスも提供していません。

ドメインの機能がエコシステム全体で企業の壁を超えた拡がりを持ち、ハイブリッド IT 環境全体で相互に作用してやり取りを行うことができるようになるまでは、完全な統合ではありません。
統合化を適切に行えば、セキュリティー・インシデントの発生時に迅速な対応を取るために必要な可視性を得ることができます。統合化によって、少ない労力でより多くのことができるようになります。これはセキュリティー・スキルのギャップに対応する基本的な方法なのです。

新たな脅威は毎日見つかっており、セキュリティーの専門知識や脅威に対するインテリジェンスの共有が必要不可欠であることを示しています。一連のソリューションや認識に投入するトップクラスの専門知識がないなら、すぐに後れを取ることになります。IBM X-Force Exchange は、現在、88,000 件以上の脆弱性、250 億以上の Web ページおよび 1 億ものエンドポイントからのデータに関する情報を分類し、すぐに利用できるリアルタイムで、世界全体をカバーした専門知識を実現しています。

IBM が お手伝いできること

コグニティブの旅は始まったばかりですが、IBM はこの革命をセキュリティーにも適用させる知識と投資をしています。7,500 名以上の IBM のセキュリティー専門家たちが、世界各地にある 36 カ所のセキュリティー・センターで毎日 133 カ国および 350 億のイベントを監視しています。IBM が行ったコグニティブ・テクノロジーへの投資は数十年に及び、自然言語を処理する能力、音声や画像を処理する能力、非構造化データを簡単に照会できるナレッジ・グラフのようなツールにする能力など、過去 5 年の間に大きな進歩を遂げました。セキュリティー・ユース・ケースを継続的に向上させ、その情報をセキュリティー・アナリストに提供するために、IBM はコグニティブを活用します。

IBM Security は、今日のソリューションにコグニティブ機能を用意しています。脆弱性検出の正確性を向上させ、迅速に対応できるように脆弱性の優先順位付けを行う支援をするために機械学習を使用し、ネットワークで発生している脅威の周辺の異常値をプロアクティブに予測し、発見するために行動学習を使用します。

IBM Security は、詳細なアナリティクス、ID とアクセス、高度化した不正行為、データ、アプリケーション、ネットワーク、エンドポイント、クラウド、モバイルや研究に及ぶ免疫システム・アプローチとエンドツーエンドの防御を提供します。これらのプラットフォームの 1 つ 1 つが IBM のコグニティブ機能から恩恵を受けることになります。コグニティブ・セキュリティーのメリットにご興味をお持ちなら、コグニティブ・テクノロジーを採り入れて活性化されていく IBM のプラットフォームの導入をご検討ください。

今、取るべき 3 つのステップ

1. 脅威の裏をかくコグニティブ機能の利用について、詳細を確認する。
2. さらなるセキュリティーの成熟化に向けたロードマップを作成して、コグニティブの準備を整える。
3. セキュリティー・インフラストラクチャーの統合化を促進する。

詳細情報

IBM の営業担当員または IBM ビジネス・パートナーにお問い合わせいただくか、次の Web サイトをご覧ください。
ibm.biz/cognitivesec

IBM Security について

IBM セキュリティーでは、きわめて先進的で、かつ統合されたエンタープライズ・セキュリティー製品/サービス群を取り揃えています。これらの製品/サービス群は世界的に名高い IBM X-Force 研究/開発に支えられています。この支援を基に、これらの製品/サービス群では、組織におけるひと、インフラストラクチャー、データ、およびアプリケーションの全体的な保護に役立つセキュリティー・インテリジェンスを備えるさまざまなソリューションを、ID およびアクセス管理、データベース・セキュリティー、アプリケーション開発、リスク管理、エンドポイント管理、ネットワーク・セキュリティーなどの領域で提供しています。これらのソリューションを使用することによって、モバイル、クラウド、ソーシャル・メディア、およびその他のエンタープライズ・ビジネス・アーキテクチャーに対するリスクの管理と統合セキュリティーの実装を効果的に行えます。IBM は、セキュリティーの研究/開発/提供をきわめて広範に行っている世界有数のセキュリティー組織を運営しており、133 カ国で 1 日当たり 350 億件のセキュリティー・イベントをモニタリングし、3,700 件以上のセキュリティー関連の特許を保有しています。

また、IBM Global Financing では、可能な限り最も費用効率が高く、戦略的な方法で、お客様のビジネスが必要とするソフトウェア機能を入手するお手伝いをすることができます。私たちは、融資条件を満たしているお客様と提携して、お客様のビジネスと開発目標に合わせてファイナンス・ソリューションをカスタマイズし、効率的な資金繰りを実現し、総所有コストを改善します。IBM Global Financing と一緒に、重要な IT 投資の資金を確保して、お客様のビジネスを促進していきましょう。
詳細情報については、ibm.com/financing の Web サイトをご参照ください。

IBM Security
Route 100
〒103-8510 東京都中央区日本橋箱崎町 19 番 21 号

Produced in the United States of America
2016 年 4 月