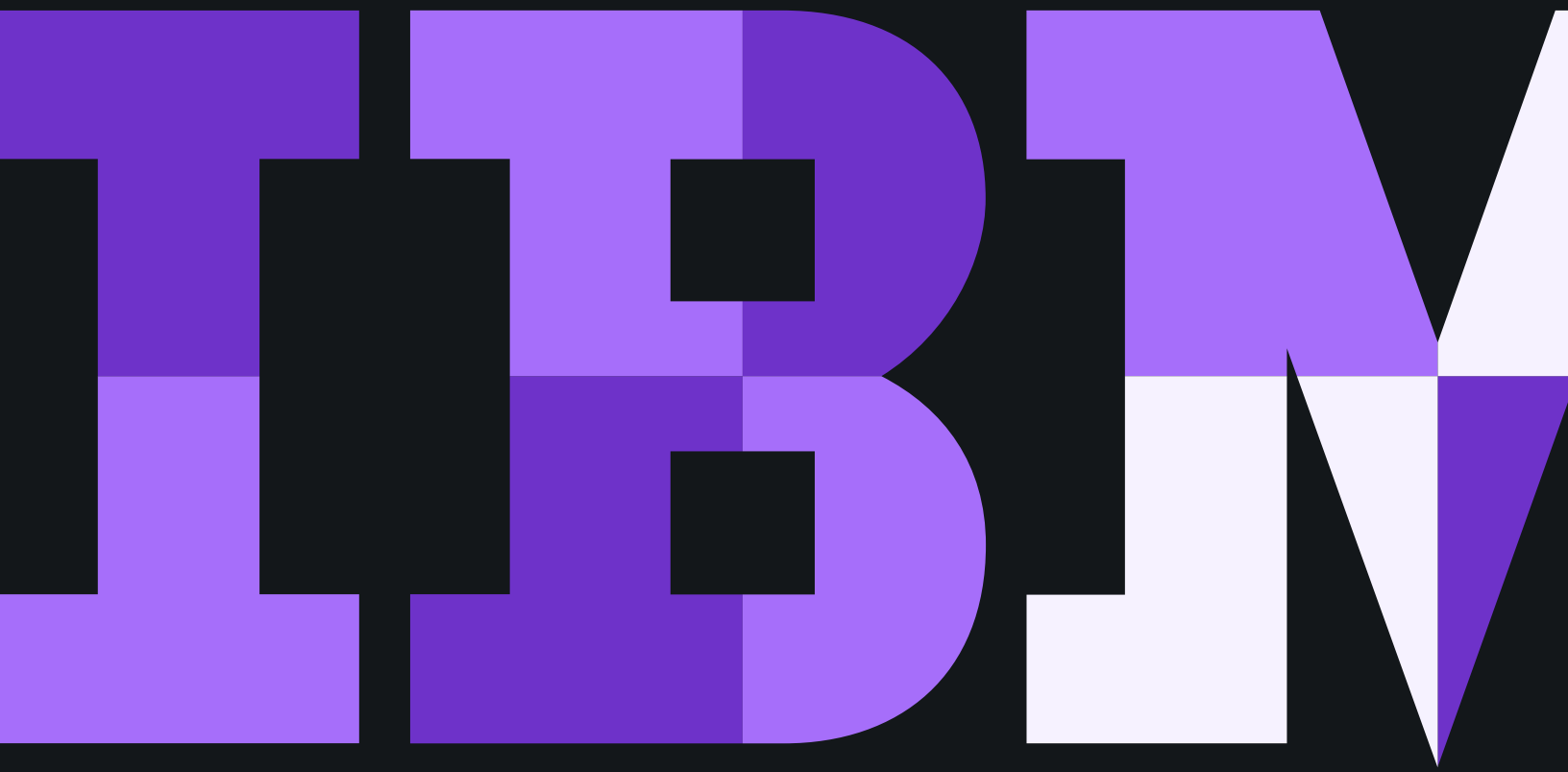
IBM Security

2020 年 1 月

保護の推進

脅威マネジメントのパフォーマンス高速化



IBM

目次

お客様のセキュリティー環境は勝つために構築されていますか?

カー・レースで勝つためには、レースが始まる前に多くの作業が行われます。レーシング・チームは、レース・トラックで優位に立つために、最高のエンジン、最高のタイヤ、最高のチームと頭脳が総動員されます。セキュリティー・チームも同様です。脅威を阻止するレースが始まったときに処理パフォーマンスが最高に達するよう最高の製品、人材、実施方法が集められます。

ここで、何がセキュリティー・パフォーマンスを引き上げる要素であるかということが問題になります。セキュリティー・エンジンがたくさんの異なるパーツから組み立てられた場合、それは、最適な能力と効率性で実行されるよう調整、統合されているでしょうか。パフォーマンス測定基準と状態を単一のダッシュボードに表示し、効果的に問題をトラブルシューティングし、問題を隔離し、緊急事態にリアルタイムで対応できますか?チーム・メンバーはランサムウェアや次の大きな脅威に対抗する準備ができていますか?自信を持って毎回脅威を処理できる準備ができていなければ、最高のセキュリティー対策でも失敗するでしょう。

今日の複雑な SOC 環境では、多数の異なるツールが使用されています。[1] お客様のセキュリティー対策の成功要因は何ですか?

2019 年でも、セキュリティー・チームが最新型の脅威を検出するために 206 日間が費やされ、ネットワークからその脅威を排除するにはさらに 73 日間かかりました。[2]

360 度の視野で死角なし

すべての自動車には、視野が妨げられる死角があります。セキュリティー・ソリューションも同様です。死角によって、検知が難しい脅威や、コンプライアンス問題が見えにくくなっている可能性があります。死角によって、セキュリティー・チームの、脅威を特定、阻止し、適切なタイミングでそれに対応する能力が低下します。

360 度のセキュリティー可視性を獲得するには、セキュリティー情報が単一のダッシュボードに収集され報告される、適切なテレメトリが必要です。 大部分のセキュリティー・チームが情報の断片化に直面します。たとえば、ネットワーク攻撃について報告するツールを持っていても、コンプライアンスを走査するのはもう 1 つのツールで、アクセス特権のエスカレーションを検知するにはもう 1 つのツールを使用する、という具合です。また、セキュリティー・データの全容を見渡せないため、セキュリティー・チームは複数のモニターや部品を寄せ集めて全体像を理解するために多くの時間を費やします。

IBM Security Threat Management を使用すれば、セキュリティー・チームは、成功に必要な可視性を獲得できます。セキュリティー・データを統合することにより、セキュリティー・チームは、リスクのあるデータだけでなく、何千というエンドポイントやクラウドをまたがるネットワーク全体の脆弱性を特定し、自信をもって方向性を決定できます。IBM Security の統合アプローチを使用することにより、セキュリティー・チームは、毎日のセキュリティー業務の「ノイズ」に埋もれてしまいがちな疑わしいアクティビティーや異常を検知することができます。IBM Security は、セキュリティー・チームがセキュリティー対策を強化しリスクを回避するために必要とする脅威インテリジェンスも提供します。

自動化、AI、アプリのAAA で防御

脅威管理では、カー・レースのように、人間の知性と機械が組み合わされます。**セキュリティー・アナリストと脅威ハンターは、時間に追われながらも人工知能や機械学習を使って自動化されたセキュリティー・タスクや対応によって対策の実行を高速化するドライバーに当たります。**IBM Security Threat Management ソリューションを導入することにより、大量の専門知識を提供する熟練した専門家や、迅速に対応する必要がある脅威への対処時間を短縮するために適切なタスクを自動化する最先端テクノロジーを活用できます。

大部分の組織には、さまざまなアプリケーションからのセキュリティー・データが殺到しています。組織では、あるベンダー製のセキュリティー・インシデントおよび事象管理 (SIEM) が、ユーザー行動分析 (UBA) には他のベンダー製のソリューションが、マルウェア検知にはまた別のベンダー製というようにばらばらのソリューションが使われていることがあります。このセキュリティー・データすべてをフィルター処理しないで解析しようとしても、ネットワークに巣食っているランサムウェアに始まり、貴重なデータへのカギを握っている認証情報の乗っ取りまで、本当の脅威を特定するのがさらに困難になります。IBM Security Threat Management は、このようなノイズを自動的に消去し、本当の脅威をリアルタイムで明るみにさらします。

適切なチームを編成し、力を与える

セキュリティー・チームは、非常時における緊急隊員のようなものです。セキュリティー・ツール、画面、ダッシュボード、データベースなどの複雑なシステムは、セキュリティー・チームが俊敏に動き事態を把握する妨げになります。セキュリティー・チームには、侵害インジケーター (IoC) やマルチチェーン攻撃などの脅威シグナルを掘り下げてすばやく調査するために適切なツールとテクノロジーが必要です。

IBM Security Threat Management は、SOAR (security orchestration, automation and response) から SIEM、高度のアナリティクスから人工知能にいたるまで、脅威をインテリジェントに調査するために必要なツールを提供し、単一のダッシュボードからサードパーティー製のセキュリティー・アプリケーションに接続できます。この結果、脅威対応時間を大幅に短縮し、隠れた脅威を検知し、セキュリティー・アナリストの脅威特定率を引き上げる統合され調整されたセキュリティー環境が構築されます。さらに、IBM X-Force の世界一流のセキュリティーの専門家が、適切なタイミングで脅威インテリジェンスやサイバー脅威と闘う上で有利となる現実的なトレーニングを提供し、お客様のセキュリティー・チームを支援します。

65%

の組織が攻撃の量と重大性が増加していると回答している[3]

77%

の組織が IT セキュリティー・プロフェッショナルを雇用し、再教育する難しさを訴えている[3]

脅威対応を高速化

複数のベンダーから寄せ集められたセキュリティー・ツールだけが情報の分断化の原因ではありません。多くのセキュリティー・チームが異なる地理的位置に分散しており、一貫性のある効果的な脅威対応を取りづらくしています。セキュリティー脅威が刻々と変化する中、統一された前線が提示されているでしょうか? それともセキュリティー・アナリストはそれぞれ孤立して作業しているでしょうか? **自動化されたインシデント対応、セキュリティー・データの一元化、修復中のリアルタイム通信を含む戦略的な計画が策定されていなければ、組織内で分断された防衛策が最大の脅威になります。**

IBM Security Threat Management を使用することで、組織全体にわたって一貫性のある脅威対応を迅速に取ることができます。動的なプレイブックと自動化されたセキュリティー・ツールを使用する IBM Security Threat Management は、人とプロセスをシームレスにつなげて真に統合されたセキュリティーを実現し、組織全体の対応をリアルタイムで実行できます。セキュリティー・データと脅威管理タスクを総合的に把握できるため、セキュリティー・アナリストは、異なる現場にいてもチーム一丸となった対応を調整できます。

脅威マネジメントの防御が統一されれば、企業は迅速に行動できます

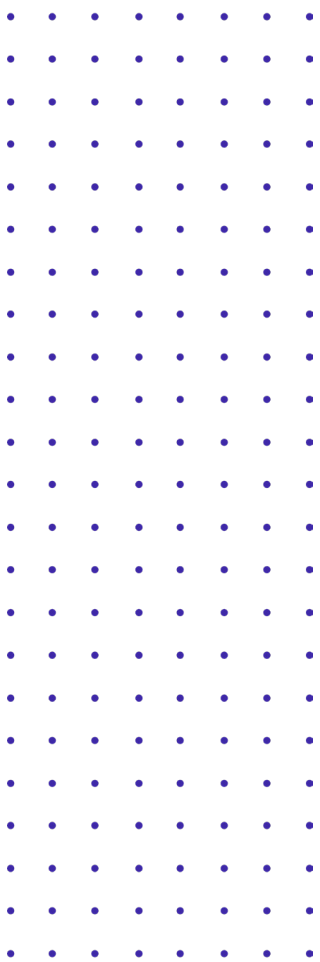
脅威マネジメントを統一することによって、企業はセキュリティー脅威に迅速かつ俊敏に対応でき、前に進むことができます。

動画を見る

動的なプレイブックと自動化されたセキュリティー・ツールを使用する IBM Security Threat Management は、組織全体の対応をリアルタイムで実行できます

IBM Security Threat Management ソリューション：勝つために構築

お客様独自の脅威マネジメント・ソリューションを構築するか、専門家によって精密に設計されたソリューションを選択することができます。IBM Security の実力は、世界の大手企業を代表するお客様や業界からの声からも明らかです。IBM の脅威マネジメント・ソリューションには、以下のように最先端の製品や優秀な人材が集結し、完璧に配置されています。



IBM Security QRadar: セキュリティー・チームが、競合社に比較して 50 分の 1 の時間で脅威を視覚化、検知、および自動的に対応できる、最新式のインテリジェント SIEM ソリューションです。

IBM Security Resilient: 動的で自動化されたプレイブックを通して組織全体のインシデント対応を高速化し、脅威から守る、業界をリードする SOAR ソリューションです。

IBM Security i2: 米国の保安および防衛分野、警察、業界不正行為チームなどから専門家が収集したインテリジェンスを活用して、効果的にすばやく行為を特定できる脅威インテリジェンス・プラットフォームです。

IBM Security Intelligence & Operations Consulting Services: お客様のセキュリティー環境のパフォーマンスを最高に保つため、評価、設計、構築、最適化するセキュリティー・プロフェッショナルです。

IBM X-Force Red： セキュリティー・リーダーが、デジタルおよび物理エコシステム全体のセキュリティー上の弱点を特定し修正するために必要な侵入テストと脆弱性管理プログラムを提供します。

IBM X-Force Threat Management Services: お客様のためにカスタマイズされた脅威管理である IBM X-Force は、セキュリティー防衛策からサイバー攻撃に対処する前線にいたるまで、最も必要な時にセキュリティー専門知識を提供します。

IBM X-Force Incident Response and Intelligence Services (IRIS): IBM X-Force の優秀な専門家チームは、豊富なセキュリティー・インテリジェンスと検証済みのインシデント対応計画を提供し、お客様のセキュリティー・チームの防衛策を強化し、攻撃者と闘い、攻撃後のバランスの回復に貢献します。

出典

1. Ponemon Study: 53 Percent of IT Security Leaders Don’t Know If Cybersecurity Tools are Working Despite an Average of $18.4 Million Annual Spend,” Business Wire (July 30, 2019).

2. Ponemon Institute, “2019 Cost of a Data Breach Study.

3. Ponemon Institute, “The Third Annual Study of the Cyber Resilient Organization.

IBM Security

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in Japan
January 2020

IBM

PO7JWB3W