ネットワークに接続するデバイスを把握するエンタープライズ IoT セキュリティー

自社ネットワークの内外およびエアスペースにある企業の IoT デバイスとアンマネージドのデバイスを可視化しましょう。

IBM Security X-Force Threat Management for IoT

デバイスは何かだけでなく、デバイスが何を行っているかをお伝えします。デバイスの動作とその接続を継続的に追跡し、疑わしい動作や悪意のある動作を特定できます。

機械学習を使用して、デバイスについて学習し、企業規模でその動作を監視します。IBM Security X-Force Threat Management for IoT 脅威管理サービスは、コネクテッド・デバイスを採用する際に IoT セキュリティーの盲点をなくして、ビジネス革新の推進を支援します。

今すぐ始めましょう

フルマネージド IoT 脅威管理サービスのメリットについてご紹介しています。

Solution Brief をダウンロードする:
ibm.biz/XF-IoT-SolutionBrief-J

IBM Security Services のお問い合わせ:
ibm.biz/Security-Mail-Form

CISO（最高セキュリティー責任者） がアンマネージドのデバイスと IoT デバイスのセキュリティーのために IBM Security X-Force Threat Management for IoT を選択している 6 つの理由

1 デバイスの検出と分類

何がネットワークに接続しているかと、その場所を可視化。IBM Security X-Force Threat Management for IoT は、ネットワーク内外とエアスペースの環境内で、マネージドだけでなくアンマネージドの IoT デバイスも検出します。そこに何があり、何を行っているのか、どのソフトウェアが実行され、どのように通信しているのかを検出します。

2 統合された脅威インテリジェンス

各デバイスのリスクと脆弱性を明確化。IBM Security X-Force Threat Management for IoT は、外部の脅威フィード、脆弱性データベース、RSS フィード、および内部の脅威調査からのインテリジェンスに基づいて、デバイスに関連するリスクと脆弱性を検出し、各デバイスにリスク・スコアを割り当てます。

3 継続的な動作分析

IoT デバイスから生じる脅威を迅速に検出して対応するための継続的なリアルタイム監視。IBM Security X-Force Threat Management for IoT は、環境内のデバイスの動作を継続的に分析し、機械学習を使用して、デバイスが標準から逸脱しているかどうかを識別します。このサービスは、1,000 万を超える個別デバイスのプロファイルからなる膨大な知識ベースを蓄積しています。これは、大規模な「クラウド・ソーシング」の知識ベースで、お客様環境のデバイスから継続的に学習しています。これにより、高い精度で脅威を検出できます。

4 エージェントレスでパッシブな監視

従来型のセキュリティー・エージェントを受け入れることができない、機器が故障する懸念があるなどの理由で、アンマネージドのデバイスおよび IoT デバイスを監視するためのツールが不十分な状況に対処します。IBM Security X-Force Threat Management for IoT は、エージェントやハードウェアを必要としないため、簡単かつ迅速に導入できます。これは、エージェントに対応できない IoT デバイスで動作することも意味します。通常、企業内の全デバイスの 40% はエージェントに対応できず、その数は大幅に増加する一方であると予想されます。[1] このサービスは、帯域外のネットワークにある「コレクター」と呼ばれる仮想アプライアンスを使用します。ワイヤレス LAN コントローラー（WLC）、スイッチ、その他のネットワーク・インフラストラクチャーと統合します。これらの接続を通じて、ネットワークから情報を収集します (100% パッシブの監視)。IBM の仮想アプライアンスはパケットを調べ、すべてのデータ・ペイロードを取り除き、メタデータをクラウド・ベースの分析エンジンに送信します。クラウドベースの分析エンジンが、ネットワーク上のリスクの高まりや攻撃やポリシー違反があると判断すると、トリアージと対応に関するセキュリティー・アラートを生成します。

5 有線および無線のトラフィックの確認

WiFi または Bluetooth 経由でネットワーク接続されたデバイスが無線攻撃の原因となったり、無許可のデバイスやネットワークに誤って接続して、いわゆる「シャドー・ネットワーク」を作成したりするリスクに対処します。IBM Security X-Force Threat Management for IoT は、SPAN ポートを介して有線ネットワークに接続します。また、標準のユーザー・アカウントを使用して WLC に接続します。既存のワイヤレス・インフラストラクチャーを使用して、ネットワーク内外やエアスペース内のデバイス（Bluetooth デバイスや現在監視する方法がないその他の IoT ワイヤレス・プロトコルが含まれる）について把握する必要があるすべての情報を伝え、すべてのネットワーク上のデバイスを可視化できるようにします。

6 マネージド・サービスとして提供

信頼できるセキュリティー・パートナーが必要です。IBM Security X-Force Threat Management for IoT は、IoT セキュリティーに特化した専門知識を持つ専属のセキュリティー・アナリストによってマネージド・サービスとして提供されます。IBM の脅威アナリストは、IoT に関連するセキュリティー・インシデントの迅速な検出と対応のために、環境からのアラートを監視、検出、そしてトリアージを行い、重要なビジネス情報の保護を支援します。

[1] Armis, Why Armis