VECTRA
SECURITY THAT THINKS®

業界洞察

製造業における脅威検知

製造業とサイバーセキュリティの複雑な関係

この一年、多くの業界において利用が加速した新技術は、人々の安全、つながり、そして生産性を維持するためのものでした。製造業において必要な技術は、生活に密接につながっているというその本質的な性質ゆえの課題も伴っています。例えば、医療用品、輸送、エネルギー、農業などの生活必須職を含む製造業では、他の業界が停止しているときでも、自社の業務だけでなく、サプライチェーンの機能を維持し続ける必要がありました。

そのため製造業においては、製造を停止するのではなく、業務を続けつつも技術面などで必要な調整を行いました。技術面においては、他の業種と同様に製造業も、スピードを向上し、スケールの柔軟性を高めるためにクラウドの利用が増加しています。これは、既に分散している運用技術インフラに、さらなる攻撃対象となりうるレイヤーが追加されることになります。サイバーセキュリティの観点から、機器の故障によるダウンタイムを最小限に抑えることを優先する製造業にとって、クラウドへの移行はどのような課題をもたらすのでしょうか。

製造業もスピードを向上し、スケールの柔軟性を高めるためにクラウドの利用を増やし続けています。これは、既に分散している運用技術インフラに、さらなる攻撃対象となりうるレイヤーが追加されることになります。

*本レポートは、Vectra AI社の2021年第2四半期 スポットライトレポート「ビジョンと可視性：Microsoft Azure ADとOffice 365の脅威検知トップ10」において収集した調査に基づく洞察となります。

ハイライト

- **脅威検知のトップ10：** 製造業におけるMicrosoft Azure ADおよびOffice 365での異常、または安全でない活動は何か？
- **不審かつ高リスクな活動：**Office 365における不審な共有が多く検知され、これは攻撃者がデータの流出やアクセスを維持するためにSharePointを使用している可能性があります。
- **ギャップ（死角）の解消：**人工知能（AI）は、クラウド環境で真に何が起こっているかを知るために必要なビジョンと可視性を提供できます。

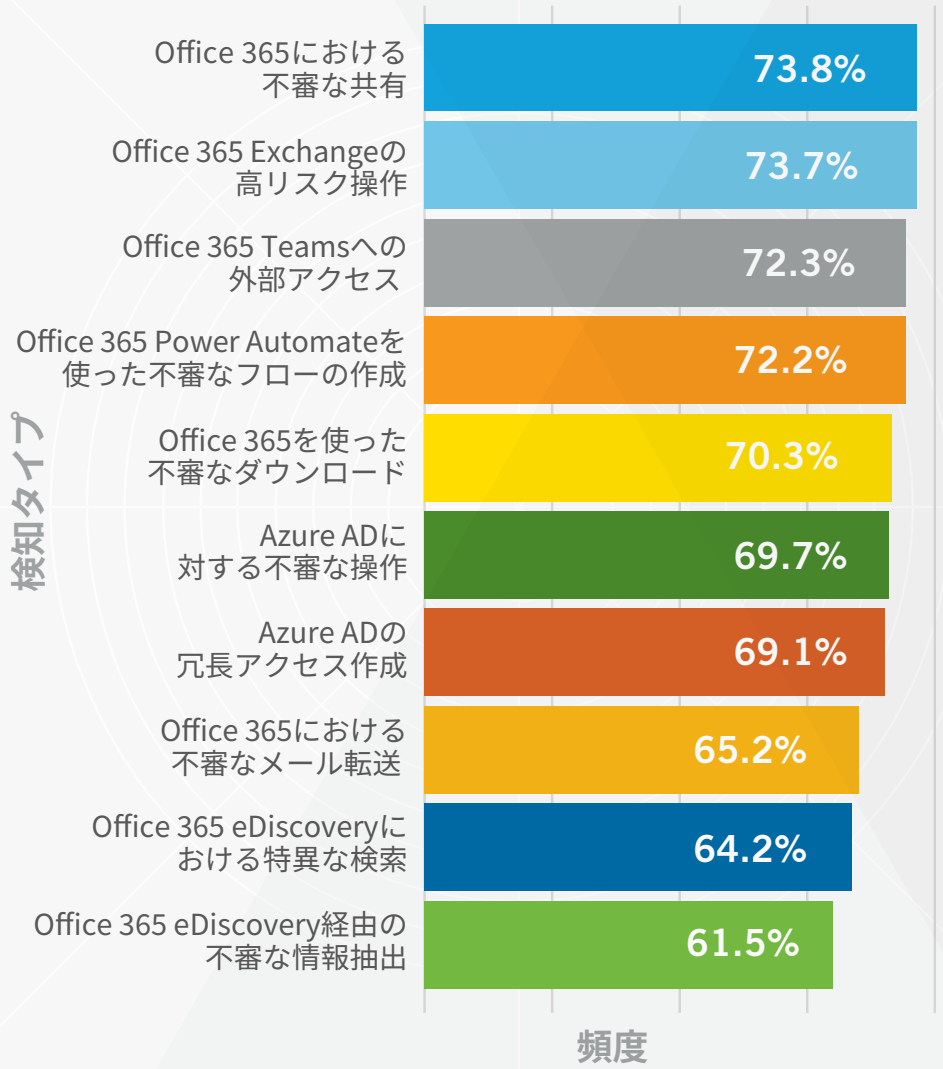
Vectra AI社の2021年第2四半期 スポットライトレポート「ビジョンと可視性：Microsoft Azure ADとOffice 365の脅威検知トップ10」では、すべての業界を網羅して詳細に検証しています。本レポートは、製造業に焦点を当てるものとなっており、当社の製造業のお客様で見られるMicrosoft Azure ADおよびOffice 365における脅威検知の上位の洞察を紹介しています。この検知によって得た情報は、適切なビジョンと可視性とともに活用することで、事業を順調に進めることができます。つまり、許可されたユーザーの利用方法をビジョンとして明確に理解し、それ以外の行動を監視・測定することで、攻撃者の振る舞いを特定し、見えるようにするという可視性が必要です。クラウドがセキュリティに関する私たちの常識を変え続ける中、適切なデータと実用的なAIがクラウドに明確さをもたらすのです。

製造業全般で検知された脅威

既に述べた通り、本レポートでは製造業のお客様に焦点を当てていますが、他の業種と同様に、明らかに悪質な攻撃行動は簡単に検知できるということが大前提です。そのため、現代のネットワーク防衛においてきわめて重要なのは、攻撃者がその目的を遂行するために取っている行動と、許可されたユーザーによる日常的な振る舞いを正しく区別することです。このレポートで取り上げられている検知の多くは、異常な動作を示しているものの、検知のすべてが悪意のある活動によるものではありません。頻繁に検知されている内容の詳細を見てみましょう。

製造業においては「Office 365における不審な共有」、「Office365 Exchangeの高リスク操作」、「Office 365 Teamsへの外部アクセス」が多く検知されました。

製造業界脅威項目トップ10



ファイルの共有をきちんと把握していますか？

結果：製造業においては、「Office 365における不審な共有」、「Office 365 Exchangeの高リスク操作」、「Office 365 Teamsへの外部アクセス」が多く検知されました。

分析：「Office 365における不審な共有」は、アカウントが通常よりも高い割合でファイルやフォルダを共有している場合に検知されます。この脅威を検知しなければならないのは、攻撃者がSharePointを利用してデータを流出させたり、攻撃者による最初のアクセスをブロックした後もアクセスが維持されていることを示している可能性があるからです。「Office 365 Exchangeの高リスク操作」もリストの上位に入っていますが、このリスクは、電子メールを介して機密情報にアクセスしている可能性を示しています。攻撃者がデータへのアクセスを得るためにExchangeを操作し、最終的に攻撃を進め、バックドアを作成したり、永続的なアクセス方法を確立している可能性があります。

また、「Office 365 Teamsへの外部アクセス」は、攻撃者が管理するアカウントが追加されている可能性を示します。トップ3のうち2つの検知が共有に関するものであったということは、この業種では共有活動があまり一般的ではないことを意味しており、だからこそお客様が把握することが重要なのです。

トップ3のうち2つの検知が共有に関するものであったということは、この業種では共有活動があまり一般的ではないことを意味しています。

メールボックスの異常な変更が確認された場合は、セキュリティ管理を回避している可能性があるため、メール転送と併せて精査する必要があります。

リストでは下位にありますが、もう一つ注目すべきなのが「Office 365における不審なメール転送」です。これは、攻撃者がメールを収集したり、送信したりするための経路として使用される可能性を示します。実際、製造業のお客様の中には、契約社員や外注者に企業のメールアカウントを提供していることがあります。そして、その契約社員や外注者が、個人メールにメッセージを転送するように設定している場合が多く見受けられます。確かに、便利な方法かもしれませんが、企業としてはメール転送に関するポリシーが存在しないことを示すことになってしまいます。これがなぜ問題なのかというと、望ましくないデータの漏洩を発見することが難しくなるからです。また、これは、攻撃者が欲しいアカウントの電子メールのコピーを密かに取得するために使われる手法でもあります。

今後は、このような活動を常に見直し、許可された行動の範囲内であることを確認する必要があります。また、メールボックスの異常な変更が確認された場合は、セキュリティ管理を回避している可能性があるため、メール転送と併せて精査する必要があります。今回報告された検知結果と、製造業環境のITシステムに関する一般的な知識に基づいて、適切なコントロールが行われているかの監査を実施し、脅威の検知結果をレビューして、異常な共有やコラボレーションに関してセキュリティ担当者がきちんと把握しているのか確認する必要があります。

お客様のアカウントにおける振る舞いを知る

Office 365 や Azure AD などのクラウドプラットフォームは、製造業が最初に防御の対象とする分野ではないかもしれませんが、攻撃者にとっての攻撃対象であることに変わりはありません。攻撃者は、金銭を脅し取ったり、価値のある資産を盗んだりする機会があれば、どんな組織でも標的にするということを覚えておく必要があります。サイバー攻撃者が企業の運営能力に影響を与えるような攻撃ができてしまえば、それを利用した恐喝などにつながる可能性があり、特に製造業はその影響を受けやすい業種です。例えば、ランサムウェア攻撃によりデータを盗まれてしまい、それに対して企業は身代金を支払うか、業務を停止するかという脅迫を受けることが考えられます。

ランサムウェアに加えて、サプライチェーンへの攻撃によって企業のセキュリティ対策が突破できてしまえば、大規模な被害をもたらします。当社のスポットライトレポートでは、攻撃者がどのようにサプライチェーンを悪用しているかを詳しく説明し、さらに実際のサプライチェーン攻撃を分析して、Vectra AI社の脅威検知がどのように攻撃者に対応するかを紹介しています。攻撃者の振る舞いと許可されたアカウントの使用を区別するには、定義されたビジョンと可視性に沿った適切なデータ収集ができていなければ、曖昧な領域となってしまうのです。攻撃者が取るであろう振る舞いを理解するためには、許可された使用がどのようなものかを明確に把握することが必要です。

実用的なAIは、Azure ADとOffice 365アカウントのギャップ（死角）を解消し、通常とは異なることが起こったときに検知するための適切なデータを提供します。機密情報が外部と共有されたり、Microsoftクラウド内で特権が昇格されたりしたとき、あなたは気づくことができますか？どんな攻撃があり得るのか知っておいて損はないでしょう。

お問い合わせ：info-japan@vectra.ai　vectra.ai/jp

レポートを入手する

Vectra®のCognito® Detect for Office 365は、隠れたサイバー攻撃者の振る舞いを自動的に検知して対応することでインシデント調査を迅速化し、一歩先を行く脅威ハンティングを可能にします。

Vectra AIについて

Vectra AI社は、クラウドやデータセンターのワークロードからユーザー、IoTデバイスに至るまで幅広い範囲で発生する脅威の検知および対応サービスにおける世界的リーダーです。当社のCognitoプラットフォームは、AIを活用して収集・保存したネットワークメタデータに、既知および未知の脅威をリアルタイムで検知、ハンティング、調査するためのコンテキストを追加してデータを強化することで、検知および調査のプロセスをスピードアップします。Cognitoプラットフォームでは、重要なユースケースに対応するために4種類のアプリケーションを提供しています。Cognito Stream™は、セキュリティ情報が強化されたメタデータをデータレイクやSIEMに転送します。Cognito Recall™は、強化版メタデータの脅威情報を保存・調査するためのクラウドベースのアプリケーションです。Cognito Detect™はAIを活用し、隠れた攻撃や未知の攻撃行動を素早く特定し、優先度を決めスピードと共に対応します。Cognito Detect for Office365 and Azure AD™は、エンタープライズSaaSアプリケーションおよびMicrosoft 365エコシステムにおいて発生する攻撃を検知し、阻止します。詳細は、vectra.aiをご覧ください。.