VECTRA
SECURITY THAT THINKS®

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

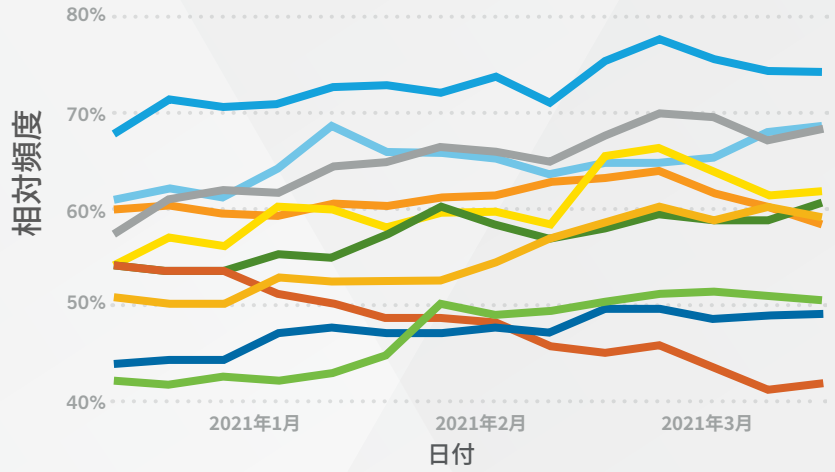
エグゼクティブサマリー

クラウドの普及によってセキュリティの常識が覆されつつあり、これまでクラウド利用に消極的だった企業でさえ、クラウドを導入した上で、社内資産や従業員を守るための方法を新たに模索し始めています。クラウド環境でのセキュリティ対策は大変そうに見えるかもしれませんが、実用的な人工知能 (AI) を使って適切なデータを収集することで、クラウドアプリケーション全体を「見える化」し、危険性のある活動を検知するためのビジョンと可視性を実現できます。

このスポットライトレポートでは、攻撃の実態把握にお役立ていただけるよう、当社のお客様全般で確認されたMicrosoft Azure ADおよびMicrosoft Office 365に関する脅威検知のトップ10項目について解説します。Vectra AIの検知サービスが提供するこれらの情報をもとに、クラウド環境で発生している活動が攻撃者または特権ユーザーどちらによるものかをお客様側でご判断いただけます。ご紹介するデータはすべて、通常とは異なる挙動を検知した際にお客様のセキュリティ部門に通知する脅威の実例です。以下は、レポートの主な内容です。

- **検知された脅威項目トップ10：** Microsoft Azure ADおよびOffice 365で検知された、普段あまり発生しない異常もしくは安全でない振る舞いのトップ10リスト。企業環境への影響についてもそれぞれ解説します。
- **企業規模別の脅威分析：**トップ10項目を企業規模別に分類。皆様のクラウド環境においてどのような検知内容に相当するのかをご確認いただけます。
- **侵害の検知：** 脅威項目別のリスクを把握し、多額の損失につながるサプライチェーン攻撃のような侵害を回避するための方法をご紹介。

検知された脅威の相対頻度別トップ10



「スポットライトレポート：Microsoft Azure ADとOffice 365の脅威検知トップ10」では、Microsoftの汎用クラウドアプリケーションにおける脅威検知のきっかけ（トリガー）となる活動の種類について詳しく解説しています。

レポートを取得する

Vectra® AI社が提供するCognito® Detect for Office 365 は、サイバー攻撃者の隠れた振る舞いを自動的に検知して対応し、スピーディーなインシデント調査およびプロアクティブな脅威ハンティングを支援します。2020年に提供開始後、わずか90日間で400万件以上のOffice 365アカウントに適用され、その保護を行ってきました。

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