DARKTRACE

■ レポート

クラウドでの調査と対応のために必要な 新たなアプローチ

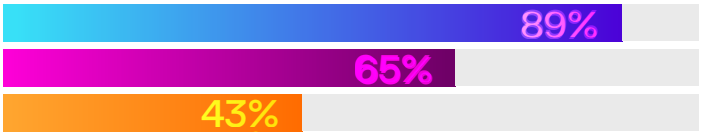
現在のインシデント対応は、あまりにも時間がかかる、人手に頼った作業となっており、見つかった脅威に対して効率的に調査し対応できないことにより、さらに被害が発生しかねない状況です。

また、企業がクラウドやコンテナベースのテクノロジーを取り入れ、マルチクラウド戦略を急速に進めるにつれ、インシデント対応の課題はさらに複雑化しています。とりわけ、インシデント報告に関する法的義務の数と範囲が世界的に拡大し、また、さまざまなクラウドやコンテナベース環境の複雑な構成を管理しなければならない状況下で、多くの組織は調査と対応に新しいアプローチが必要だということを認識しています。インシデント対応環境の現状を評価するため、当社は 2024 年に外部プロバイダーと協力してアンケートを実施しました。

調査の遅れは損害につながる

インシデント対応においては、スピードが最重要

しかし現在、これまでのアプローチを使った調査はあまりにも複雑で、時間がかかりすぎ、エキスパートの才能に依存しています。その結果、イベントの検知とその調査と対応の間に隙間が生じています。そのため、組織の 90% 近くは、クラウドでのインシデントを調査し封じ込めるまでの間に、一定程度の損害を被っていることが明らかになっています。さらに、その損害の半数近くが、重大なインシデントでした。このことは、より簡潔で効率的なインシデント対応戦略が、特にクラウド環境に対して、緊急に必要であるということを示しています。



89% の組織ではインシデントを封じ込め調査する前に被害が発生しています

65% の組織は、クラウド上で何かを調査する場合オンプレミスと比べて約 3-5 日余計に時間がかかっています

43% の組織は、調査されなかったクラウドインシデントアラートからの重大な損害の発生を経験しています

調査の遅れにつながる主な要因

調査の遅れにつながる主な要因の 1 つは、クラウド環境に対する可視性とコントロールの欠如であると報告されています。詳しく調べると、この可視性とコントロールの欠如は、クラウドベースの調査を行うために複数のツールやプラットフォームを使用しなければならないことでさらに悪化しており、特に複数のクラウドサービスプロバイダーのプラットフォームにわたってリソースが展開されている場合には問題が顕著です。さらに、クラウドに特化した問題への知識不足も関係してきます。従来のインシデント対応アプローチをクラウドに適用するには、深いレベルのクラウド専門知識が必要となります。残念なことに、セキュリティのトップ人材を採用することはそれだけでも非常に難しく、さらにクラウドインフラの深い知識を持ったセキュリティエキスパートを見つけることはさらに困難なタスクとなります。

クラウドベースの脅威に対応する際のその他のオペレーション上の課題：

82% **の組織**
はクラウドベースの脅威に対するフォレンジック調査を行うために複数のプラットフォームおよび / またはツールを使用していました

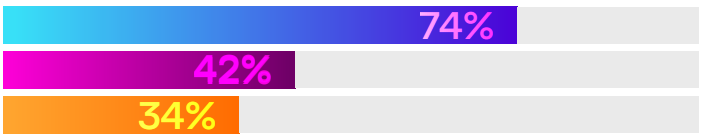
36% **の組織**
はクラウドベースの脅威に対するタイムリーな調査に関して、クラウド環境に対する可視性とコントロールの欠如が最大の課題であると回答しました

最大のコンプライアンス課題

セキュリティチームは、法的報告義務の範囲と数の世界的拡大によるプレッシャーに直面しています。コンプライアンス違反は高額な罰金につながり企業の評判や収益に大きな損害を与える可能性があるからです。

回答者は、組織が規制要件に対応する上で最大の課題はデータに対する可視性の欠如であると答えています。サイバーセキュリティリーダーの 70% 以上が、データプライバシー規制がインシデント対応を複雑化させていると答えたのに対し、規制要件への不適合で実際に罰金を科されたと答えたのは 1/3 をわずかに上回る程度でした。

今後さらに多くの組織が特にクラウドベース環境におけるインシデント対応に新たな戦略を適用し、また規制当局がクラウドセキュリティにより重点を置くようになるなかで、これらの数字がどのように変化していくかは興味深いところです。



74% の組織がデータプライバシー規制がインシデント対応を複雑化させると回答しています

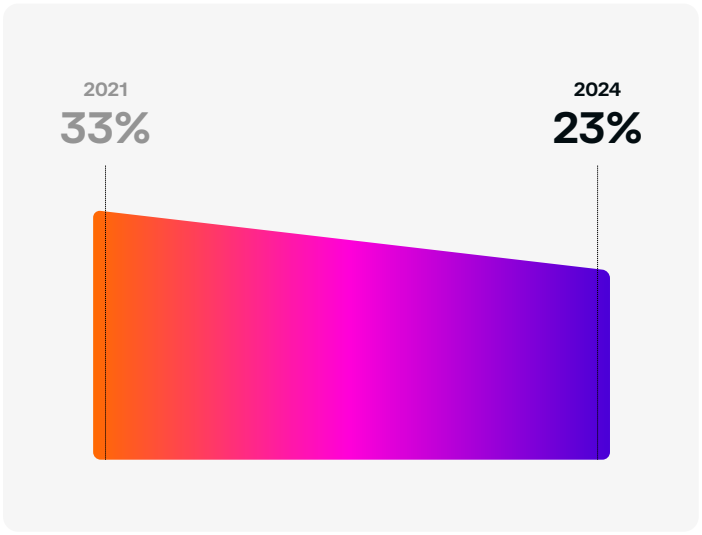
42% の組織がクラウド普及後の主なコンプライアンス課題はデータへの可視性であると回答しています

34% の企業が規制要件への不適合で罰金を科されています

多くの企業はクラウド調査機能の強化に取り組んでいる

企業のクラウドへの移行が急速に進む一方で、脅威アクターはクラウド環境をエクスプロイトするための専用のツールやテクニックを開発しています。クラウドベースの脅威が増加するなかで、これらの進化する脅威に対する防御には新しいテクニックが必要だということは明白です。2021 年に実施された類似のリサーチと比較すると、調査されなかったクラウドアラートの量は減少しており、多くの組織においてクラウドベースの環境で調査を行う能力は多少向上しているとみられます。

今回、クラウドアラートの 23% がまったく調査されていないという結果でしたが、2021 年の結果では 33% 以上であり、クラウドで調査を行う能力は向上していることがわかります。



クラウドフォレンジックに対する予算措置

クラウドでの調査と対応における可視性の問題から、フォレンジックツールに目を向ける組織が増えています。この点については、大多数の組織(83%)がクラウドフォレンジックだけのために予算を取っています。さらに、77% の組織がこの分野の予算全体が 2024 年に増加すると予測しています。この投資傾向はクラウドセキュリティを管理する上でのフォレンジック機能の重要性が高まっていることを示しています。

83%

クラウドフォレンジックの予算
83%の組織がクラウドフォレンジックに対する予算を持っています

77%

全体予算の増加予測
77%の組織がクラウドフォレンジックとインシデント対応のITセキュリティ予算が2024年には増えると予測

クラウド調査および対応の今後の戦略

多くの組織においてクラウド環境で調査と対応を行うためのさまざまな戦略が検討されています。当然の流れとしてセキュリティチームは SOAR (Security Orchestration, Automation, and Response) 等の既存のツールを利用してこれらの課題に取り組もうとしました。しかし、クラウド調査に対しては、インシデント対応の自動化のほうが SOAR よりも 2 倍程度効果的であることが分かっています。クラウド脅威に対応する組織の能力を強化するために自動化を導入することは不可欠ですが、この自動化は一般的な自動化ソリューションを適用するのではなく、インシデント対応のためにカスタマイズされたものでなければなりません。さらに、ほとんどの組織 (95%) は近い将来、クラウドインシデント対応において AI が主要な役割を果たすと考えています。

2X クラウド脅威調査に対してはSOARよりも自動化が2倍効果的です

回答者の95%は今後2年間でクラウドインシデント対応にAIが主要な役割を果たすようになると考えています

Darktrace の活用法

Darktrace は単一のサイバーセキュリティプラットフォームでクラウドもカバーし、サイバーレジリエンスに対するプロアクティブなアプローチを提供します。

/ CLOUD

Darktrace / CLOUD は、すべてのセキュリティチームと SOC がクラウドセキュリティを利用できるようにするために先進的 AI を用いて構築された、リアルタイム CDR（Cloud Detection and Response）ソリューションです。さまざまな機械学習テクニックを駆使し、Darktrace はハイブリッドおよびマルチクラウド環境に前例のない可視性、脅威検知、調査、インシデント対応を提供します。

Darktrace のクラウド製品は Cado Security Ltd. の買収によりさらに強化され、セキュリティチームはマルチクラウド、コンテナ、サーバーレス、SaaS、オンプレミス環境においてフォレンジックレベルのデータに即座にアクセスできるようになりました。

ソリューション概要を読む ↗

デモを予約する ↗

リサーチ手法

このアンケートは Cado Security が TrendCandy の協力により 2024 年に実施したものであり、米国および英国に所在する組織に勤務するセキュリティ意思決定者 300 名を対象に調査を行いました。

このアンケートに回答するには、役職がマネージャー以上、情報セキュリティまたはサイバーセキュリティ部門勤務、そしてクラウドセキュリティに関与していることが条件でした。

さらに、対象組織の条件はビジネスオペレーションにパブリッククラウド(例、AWS、Azure、GCP 等)を使用していることでした。

“Darktrace / CLOUDにより、**明確な報告書づくりと、監査に対応できるトレーサビリティ** が実現できました。これは欧州法規制と欧州銀行監督局のガイドラインに従うために当社がまさに必要としていたことです。”

■ **リスクおよびコンプライアンス責任者**

金融テクノロジー企業

■ **ダークトレースについて**

ダークトレースは AI サイバーセキュリティのグローバルリーダーであり、日々変化する脅威ランドスケープに立ち向かう組織を支援しています。2013 年に英国ケンブリッジで設立されたダークトレースは、それぞれのビジネスからリアルタイムに学習する AI を使用して未知の脅威から組織を保護する、必要不可欠なサイバーセキュリティプラットフォームを提供しています。ダークトレースのプラットフォームおよびサービスは 2,700 名を超える従業員により支えられ、世界でおよそ 10,000 社の組織を保護しています。より詳しい情報については、www.darktrace.com/ja をご覧ください。

北米：+1 (415) 229 9100　ヨーロッパ： +44 (0) 1223 394 100　日本： (03) 5456 5537　ラテンアメリカ：+55 (11) 4949 7696

darktrace.com/ja | japan@darktrace.com