DARKTRACE

クラウド調査&対応の自動化が必要な5つの理由

クラウドコンピューティングはアプリケーションとサービスの管理と提供方法に真の革命をもたらしました。クラウドへの移行の魅力は明らかです – **より優れたスピード、敏捷性、柔軟性、コスト、その他多くのメリットがあります。**

> “2027 年までに、エンタープライズ企業の 70% 以上が自社のビジネスを加速させるためにインダストリクラウドプラットフォームを使用するようになると予想されています（2023 年には 15% 未満）。”
>
> ■ Gartner[1]

しかし、デジタル変革は新たなセキュリティ課題ももたらし、特にフォレンジックやインシデント対応が問題となります。クラウドは複雑です。

仮想マシン、コンテナ、関数などはアクセスがきわめて難しく、場合によっては一瞬で消えてしまいます。新たなブラインドスポットが攻撃者にさらなる攻撃の機会を作り出しているこの現代のサイバー世界において、セキュリティチームが侵害の可能性を調査し対応するための適切な可視性を持つことは必須の条件です。本データシートでは、組織がクラウド脅威を効率的に理解しそれらに対応するために、CIRA（Cloud Investigation and Response Automation）がなぜ必要なのか、その 5 つの理由を説明します。

CIRA とは？

CIRA はクラウドセキュリティの中の新しいカテゴリです。

CIRA テクノロジーは、クラウド環境内のフォレンジックデータの収集と分析を自動化することにより、対応を迅速化することを可能にします。このカテゴリーは Gartner® 社により 2023 年に最初に定義されました。

クラウド環境で見られる攻撃手法の急速な変化に、規制要件の数と範囲の拡大が重なり、多くの組織において、クラウドでのインシデント対応に現代的アプローチを早急に取り入れなければならないという危機感が高まりました。CIRA テクノロジーは組織がクラウドリスクを徹底的に理解し緩和するための鍵となる能力を提供します。

CIRA テクノロジーの核となる能力には次が含まれます：

- マルチクラウド環境からのフォレンジックデータ収集および分析
- コンテナ等の動的かつ短命なリソースから取得された証拠を保全する能力
- クラウドリソースおよびログの両方から取得されたさまざまなデータソースをシームレスに調査する能力
- 迅速な対応を可能にする自動化された緩和アクション

理由その 1

セキュリティチームはクラウドに対してさらなる可視性を必要としている

それは理想的な出会いでした：クラウドコンピューティングと DevOps の組み合わせにより、スケール性、アクセス性、そして自動化という利点が得られ、新しいソフトウェアをクラウドのスピードで実装できるようになりました。これまで何か月または何年もかかっていたものが、わずか数週間でプロトタイプを作成できるのです。夢のような話ですが、それはサイバーセキュリティがイノベーションのスピードについていければの話です。

これまでのセキュリティチームの努力の大部分は DevOps およびソフトウェア開発ライフサイクル初期のフィードバックループを保護することに向けられていました。そのため、多くの組織は CSPM（Cloud Security Posture Management）や CWPP（Cloud Workload Protection Platforms）などのクラウド向け保護および検知テクノロジーを導入しました。

1 Gartner, June 5, 2024, “The Expanding Enterprise Investment in Cloud Security,”
参照先： https://www.gartner.com/en/newsroom/press-releases/2024-06-05-the-expanding-enterprise-investment-in-cloud-security

しかし、調査と対処の点では、非常に大きなギャップが存在します。有害な事象が識別されても、多くの場合組織はインシデントの真の範囲と根本原因を理解する能力を持っていません。

今日、サイバーインシデントが発生した際、セキュリティチームはしばしば「リフトアンドシフト」アプローチに頼らざるを得ず、既存のオンプレミス用調査および検知ツールを使ってクラウドの可視性を得ようとしています。しかし、これらのツールは、仮想マシン、コンテナ、およびサーバーレスリソースを含む動的なクラウド環境のために設計されたものではありません。つまりセキュリティチームは多くの場合、その全体像を理解せずにインシデントに対処しており、攻撃者が利用できる要素を残してしまうことを意味します。

80%

例えば、ある研究では、支払いを行ったランサムウェアの被害者の80%が再度攻撃を受けていることがわかっています。

今日のクラウドファーストの世界でリスクを適切に管理するためには、セキュリティチームには次世代技術全体にわたる深い可視性が必要となります。[2] 今日のクラウドファーストの世界でリスクを適切に管理するためには、セキュリティチームには次世代技術全体にわたる深い可視性が必要となります。そこで CIRA が登場します。クラウドでフォレンジックデータを取得することは気が遠くなるようなな作業に思えるかもしれませんが、クラウドプロバイダーは現在、さまざまな自動化オプションを提供しており、これらの自動化テクニックによってセキュリティチームによる深掘りが可能になります。検知プラットフォームが提供できる以上の可視性を持つことで、セキュリティチームはより情報に基づいた対応決定を行うことができ、その結果、複雑な環境全体でリスクをより良く管理することができます。

理由 02

クラウドエキスパートを見つけるのは困難

サイバーセキュリティ分野の人材不足はよく知られた問題です。2024 年に実施された調査、ISC2 Cybersecurity Workforce Study によると、世界的に 480 万人のサイバーセキュリティ労働者が不足しており、前年から 19% 拡大しています。[3]

そして、クラウドへの急速な移行に伴い、組織は他のすべての要素に加えて、深いクラウド知識を持つセキュリティ人材の採用を求められています。セキュリティチームが持っているこれまでの知識、ツール、リソースでは、クラウドでのフォレンジックやインシデント対応を実行できないことがしばしばです。

たとえば、アナリストが調査を始める前に、まず最も価値があると思われるクラウドデータソースの種類を特定する必要がありますが、変化し続ける今日のクラウド環境では、これは簡単な作業ではありません。たとえば、AWS には 200 以上の製品とサービスがあり、それぞれに異なるセキュリティのベストプラクティスとデータソースがあります。セキュリティーチームが分析したいデータソースの種類を特定できたとして、そこへのアクセスを得ることはまた別の障害となります。クラウド API はオンプレミス向けの API よりもはるかに優れていますが、それを活用するには各クラウドプロバイダーの機能に対する深い理解と、API を呼び出すスクリプトを記述するスキルが必要です。

正しく行うことができれば、その利点は数え切れないほどあります。

セキュリティチームは、データの取得、処理、分析、そして対処アクションまで、プロセスの各要素をエンドツーエンドで自動化できます。クラウドにおけるさまざまなデータソース（例：AWS CloudWatch、Azure Monitor Logs、Kubernetes Logs などの主要ログプラットフォーム）について基本的な理解を持つことは重要ですが、クラウドでのインシデント対応調査を行うためのすべてのクラウド専門知識を 1 人の個人が持つことを期待するのは非現実的です。従来のインシデント対応アプローチを考えると、これらの異なるデータソースをすべて分析することはほぼ不可能に感じられますが、CIRA を使用することですべてのレベルのアナリストがクラウドでフォレンジック調査を行うことができます。CIRA ソリューションは、クラウドプロバイダーのログ、ディスク、メモリその他、何百ものデータソースを単一の画面に統合します。

さらに、この現代的なアプローチは、セキュリティチームがクラウドを活用してインシデントの重要な証拠を安全で柔軟かつ効率的に収集、処理、保存できるようにすると同時に、コラボレーションを容易にします。

理由その 3

リスクはクラウドのスピードでエスカレートする

クラウド、コンテナ、サーバーレスアーキテクチャによって、ビジネスアプリケーションの構築方法が完全に変化しましたが、攻撃や敵対者の手法も根本的に変わりました。攻撃者は急速に進化しています。この次世代テクノロジーを侵害するための新しいツール、戦術、技術を着実に開発しているのです。

例えば、Cado 社の研究者たちは、Darktrace による買収後、公に知られたものとしては最初の、AWS Lambda 環境で実行するように特別に設計されたマルウェアを発見しました。[4] 最初に発見されたサンプルは、クリプトマイニングソフトウェアのみを実行するという点で比較的無害でしたが、攻撃者が高度なクラウド特有の知識を利用して複雑なクラウドインフラを侵害できることを示しており、将来的により悪質な攻撃が発生する可能性を示唆しています。

```
2022/04/01 11:37:21 expected AWS Lambda
environment variables [_LAMBDA_SERVER_
PORT AWS_LAMBDA_RUNTIME_API] are not
defined
```

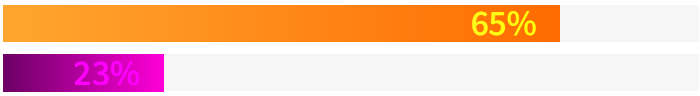
AWS Lambda 環境で実行するように設計された、公知となった最初のマルウェア、Denonia からの Lambda 特有のログステートメント。

2 CBS News, June 17, 2021, “80% of ransomware victims suffer repeat attacks, according to new report,” 参照先： https://www.cbsnews.com/news/ransomware-victims-suffer-repeat-attacks-new-report/

3 ISC2, September 11, 2024, “Employers Must Act as cybersecurity Workforce Growth Stalls and Skills Gaps Widen,” 参照先： https://www.isc2.org/Insights/2024/09/Employers-Must-Act-Cybersecurity-Workforce-Growth-Stalls-as-Skills-Gaps-Widen

4 SC Media, April 6, 2022, “First malware targeting AWS Lambda serverless cloud environment discovered,” 参照先： https://www.scworld.com/news/first-malware-targeting-aws-lambda-serverless-cloud-environment-discovered

しかし、攻撃者がクラウドの速度で動いている一方で、組織はそのペースに追いつけていません。2024 に行われた調査によれば、組織の 89% はクラウドでのインシデントを調査し、封じ込める前に、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。理由の 1 つはフォレンジック調査を行うのに必要なデータを収集し処理するのに時間がかかりすぎるということかもしれません：



組織の 65% 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。さらに良くないのは、そのためにクラウドセキュリティアラートの約 23%はまったく調査されないということです。

敵のペースに後れをとらないためには、セキュリティチームにはインシデント調査を迅速かつ深く行うための能力が必要です。徹底したインシデント対応を行うには、セキュリティチームは攻撃者のあらゆる動きを追跡し、将来の侵害に対して組織を脆弱にするようなあらゆる隙を埋める必要があります。さらに、エフェメラルワークロードがスピンダウンされ攻撃者が残した手掛かりが破壊されてしまう前に、これを素早く行う必要があります。CIRA ソリューションは、セキュリティチームがクラウドのスピードと自動化を利用し、検知、調査、対処の間の時間をなくすことにより、この課題に対応しようというものです。

理由その 4

マルチクラウド使用が拡大しつつある

今日では、ほとんどの組織は複数のクラウドプロバイダーを利用しています。最近行われた研究によれば、組織の 89% は現在マルチクラウド環境を運用しています。

米国の金融業規制機構である FINRA[5] も、ブローカーおよびディーラーは必要に応じてクラウドプロバイダーを切り替えることができるべきであり、「ベンダーロックインのリスクを考慮」し、「不利益なロックインの状況を回避するための出口戦略」を含めて検討するべきだとしています。[6]

同様に、欧州銀行監督局も単一プロバイダーに伴うリスクを警告し、各銀行に対して「集中リスク」を考慮し「簡単に置き換えることのできない支配的なサービスプロバイダー」への依存を避けることを促しています。[7]

セキュリティチームはクラウド上でインシデント対応を行うのに必要なデータを収集するのに既に苦労していますが、マルチクラウドの拡大によりこの作業は次の主な理由によりさらに困難となるでしょう：

- **サイロ化したデータ：**各クラウドプロバイダーはそれぞれ独自の用語、セキュリティツール、監視ログ、APIを持っているため、どのデータソースが最もキャプチャする価値があるか、どのようにそれらをキャプチャしたらよいかという判断が難しく、そしてさらに、複数のクラウドプラットフォームおよび環境からの様々なソースにわたってどのように効果的に調査を行えるのか、という難しい問題があります。
- **スキルと知識のギャップ：**前述の通り、深いクラウドの知識を備えたサイバーセキュリティプロフェッショナルを探すのは既に非常に難しい状況にありますが、複数のクラウド環境を扱うスキルセットを持ったセキュリティ人材の確保は不可能に近いようにも思えます。

その結果、クラウド内でインシデントが発生すると、セキュリティおよびインシデント対応担当者はどちらに転んでも不利な選択を迫られます。インシデント全体の範囲と影響を完全に理解することなくクローズするのか、あるいは望んだような結果が得られないかもしれない調査に何日、何週間も費やすのか、という選択です。

多くの企業がマルチクラウド戦略を採用する中で、セキュリティチームはクロスクラウド対応のソリューションを必要としています。CIRA はマルチクラウド環境におけるフォレンジックおよびインシデント対応に関連した複雑さを取り除く上で鍵となるソリューションです。データの捕捉と処理を完全に自動化することにより、CIRA ソリューションはデータの場所に関係なく、セキュリティチームがインシデントデータにシームレスに取りかかることを可能にします。

理由その 5

エフェメラル環境とはデータが一瞬で消えてしまうことを意味する

セキュリティチームが直面する最大の課題の 1 つは、クラウド、コンテナベース、およびサーバーレスリソースで構成されるエフェメラル環境の保護です。これらのリソースは絶えずスピンアップ、スピンダウンが繰り返され、セキュリティエキスパートにとってインシデントを調査しどのアセットおよびデータが侵害されたかを理解することをほとんど不可能にしています。

これらのリソースのスピンアップおよびスピンダウンの間に悪意のあるアクティビティが発生した場合、データは永久に失われてしまいます。

攻撃者は痕跡を隠すのに役立つためこれを利用しています。コンテナまたはその他のエフェメラルリソースを利用した環境を調査する際、データ収集が検知の直後に行われ大事な証拠が破壊されないようにする必要があります。これは自動化により実現することができます。さらに、多くの組織では数千ものコンテナを持っているため、自動化によりデータ処理とエンリッチメントを効率化することもきわめて重要です。

5 Flexera, “Cloud computing trends:Flexera 2024 State of the Cloud Report,” 参照先：https://www.flexera.com/blog/finops/cloud-computing-trends-flexera-2024-state-of-the-cloud-report/

6 FINRA, “Cloud Computing in the Securities Industry,” https://www.finra.org/rules-guidance/key-topics/fintech/report/cloud-computing/regulatory-considerations

7 European Banking Authority, “EBA Guidelines on outsourcing arrangements,” 参照先：https://www.eba.europa.eu/sites/default/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf

CIRA ソリューションはエフェメラル環境でのインシデント対応を次のような機能により可能にします：

- **自動データキャプチャ：**自動化により、インシデントが検知された後、直ちに調査のための証拠を確保することができます。これにより、セキュリティチームは重要な証拠を保全しインシデントの封じ込めと解決にかかる期間を短縮できます。
- **コンテナアセットディスカバリー：**コンテナは共有ホストカーネルOS内の仮想化された環境として動作するため、スケールされた環境内のすべてのコンテナ化されたマシンで実行されているアセットワークロードを追跡管理することは難しい作業です。効率的にコンテナアセットを発見し追跡できるエージェントレスのディスカバリープロセスはすべてのコンテナアプリに対して適切なセキュリティプロトコルを適用することができます。
- **すばやく隔離する能力：**リソースが侵害を受けた場合、そのリソースをすばやく隔離して攻撃の進行を止めさらなる拡散と被害を食い止める能力を持つことはセキュリティチームにとってきわめて重要です。最初の検知の直後に隔離を行うことが適切な第一歩となることもあります。これによりセキュリティアナリストはより詳細な調査をバックグラウンドで実施し、インシデントの本当の範囲と影響をよく理解した上で適切な緩和と封じ込めのアクションを取ることができます。

まとめ

セキュリティチームが環境を保護するのにクラウドのエキスパートでなくてもよいはずです。アナリストも、侵害された可能性のあるシステムを調べるのに、複数のクラウドチームと交渉し苦労してアクセスを得たり、主要クラウドプロバイダーすべてに関して深い知識を持っていたりする必要はないはずです。

最新のセキュリティテクニックおよびテクノロジーを適用することにより、可能なところでは自動化を行い、クラウド上でフォレンジックおよびインシデント対応を行う複雑さと時間を劇的に縮小することができます。

クラウドに特化したサイバーセキュリティ戦略には、クラウドのために構築されたソリューションが必要です。CIRA を利用することにより、データキャプチャ、処理、分析を効率化し、非常に複雑なクラウド環境に対しても容易にリスクを理解することができるようになります。CIRA はクラウドのスピードと自動化を活用することにより、セキュリティチームはエンドツーエンドのインシデント対応プロセスを補強することができます。適切なデータのキャプチャからインシデントの根本原因、範囲、影響の特定に至るまで、可能な部分を自動化することで一般的な調査テクニックを再現することができます。

この自動化により、集中するための貴重な時間が解放され、セキュリティチームが最も重要なインシデントを優先して対応し、平均修復時間（MTTR）を大幅に短縮することができます。

Darktrace はどのように CIRA を提供するか

Darktrace はインシデント対応においてクラウド環境特有の課題を効果的に管理する力を組織に提供します。クラウドのスピードとスケールを活用し、データキャプチャおよび処理から分析と攻撃封じ込めに至るまで、インシデント対応ワークフローのできるだけ多くの部分を自動化することにより CIRA を実現することができます。このクラウドセキュリティソリューションにより、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ます。クラウドプロバイダーのログ、ディスク、メモリその他から抽出された証拠アイテムは並列に処理され、調査開始までの時間を劇的に短縮します。

Darktrace はインシデントに関連する最も重要なイベントを、原因、範囲、影響も含めて自動的に提示し、あらゆるレベルのセキュリティアナリストを支援します。また、Darktrace は緩和アクションもサポートしているため、組織は進行中の攻撃をすばやく封じ込めることができます。

Darktrace の CIRA 機能により、セキュリティチームは以下を行うことができます：

- **エンドツーエンドのインシデント調査および対処プロセスを自動化:** アラートの処理から証拠の収集と保全、データの分析、脅威の封じ込め、影響の食い止めまで。
- **インシデントに対する総合的な準備:** アクセスのセットアップ、自動化ルール作成、サードパーティシステム（インシデント管理プラットフォーム、XDR、SOAR、CNAPP、SIEM等）とのインテグレーションにより、堅牢かつ包括的、防御可能なプロセスおよびアーキテクチャを構築します。
- **組織の準備度をテストしリスクを理解:** ギャップがどこにあるか、露出を縮小するためにどこに投資する必要があるかを理解します。