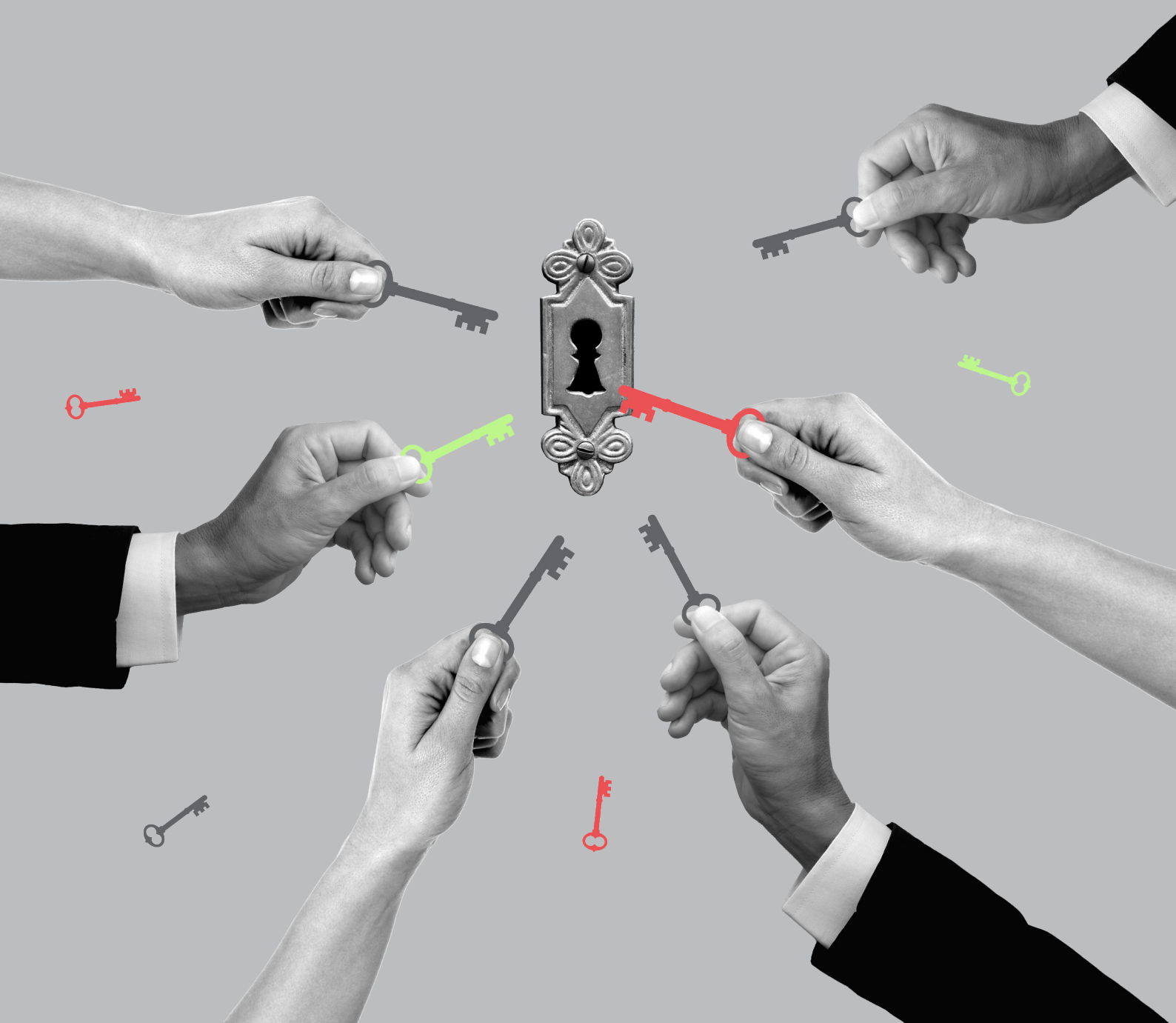
sysdig

2024年度版クラウドネイティブセキュリティおよび利用状況レポート



目次

主なトレンド

01

シフトレフトは今なお目標のままであり、現実となっていない

ランタイムスキャンの失敗率は91%で、CI/CDパイプラインスキャンの失敗率を上回っています。しかし、ランタイムの優先順位付けにより、使用されている重大で深刻度の高い脆弱性が50%近く減少しています。

91%がランタイムスキャンに失敗

02

ID管理は、最も見過ごされているクラウド攻撃のリスクである

98%の権限が使われておらず、CNAPPユーザーのうちCIEMを優先しているのはわずか20%です。

03

脅威検知プログラムは成熟しつつある

クラウド攻撃の35%はIoCにより特定できますが、残りの65%の攻撃を検知するには、繊細な振る舞いを検知対応するメカニズムの追加が必要となります。

35%がIoCマッチングにより識別可能な攻撃

65%が検知を必要とする攻撃

04

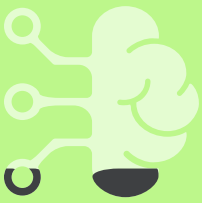
短命のコンテナは攻撃者を阻止できない

コンテナの70%は5分未満の寿命ですが、クラウド攻撃は自動化を利用してわずか10分で迅速に動作します。

05

企業における生成AIの導入が予想よりも遅れている

クラウドユーザーの31%がさまざまなAIフレームワークやAIパッケージを統合していますが、その中で生成AIを統合しているのは15%に過ぎません。



エグゼクティブサマリー

Sysdigの『2024年度版クラウドネイティブセキュリティおよび利用状況レポート』をお届けします。このレポートは、サイバーセキュリティが世界中のマスコミを賑わした1年を経た後、絶好のタイミングで発表されるものです。本レポートは、クラウド化によりセキュリティを取り巻く環境が短期間のうちにいかに広範なものになったかを示しています。

これまでと同様、本レポートでは、クラウドセキュリティの現状について結論を導き出すために、実際のデータを調査しています。当社では、多くの企業や組織がシフトレフトの概念と格闘し続けていると見ています。ランタイムの脅威の優先順位付けにより脆弱性は大幅に削減されたものの、強力で迅速なクラウドの脅威検知と対応（TDR）が依然として急務となっています。

同様に、ID管理にも成熟の機会が残されています。昨年のレポートでも指摘しましたが、過剰な権限が人間とマシンの両方のIDに対して付与され続けているからです。カジノから消費財に至るまで、企業を標的とした衝撃的でよく知られたID攻撃を振り返ると、過剰な権限がリスクの高い状況をもたらしているのは明らかであり、注意と対策が必要です。

短命のワークロードは、クラウド攻撃のスピードにはかないません。多くの企業や組織がデータ処理の自動化を進めていますが、生成AI（GenAI）をセキュリティ対策に応用している組織はほとんどありません。

今年のレポートでは、ランタイムの脆弱性の減少をはじめ、セキュリティチームが現時点で過剰な権限に関連するリスクをどの程度受け入れているかを取り上げているほか、リソースの消費傾向についても調査しています。この調査によれば、未使用で制限のないリソースは、攻撃の可能性と攻撃者の成功率を高めることが分かっています。リソース消費に関連する傾向は、脅威アクターがこのようなアクセス制御のギャップを利用した場合に、彼らが金銭的にも物質的にもいかに大きな影響を実現するかを示しています。

> 今年の傾向は、企業や組織がより迅速な開発とイノベーションを優先するために、セキュリティのベストプラクティスよりもスピードと利便性を依然として重視していることを示しています。

自動化、DevOpsサイクル、セキュリティツールのすべてが急速に変化しています。クラウドに特有の常に動的な状況は、セキュリティリーダーにとっても実務者にとっても同様に、あらゆるイノベーションがエクスプロイトと出会うという課題を突きつけています。**クラウドへの移行が進む中、攻撃は10分で起こりうるため、スピードが命となります。**業界として、私たちはクラウドに必要なスピードでイノベーションと成熟を進めています。セキュリティにおいては、私たちは猛烈なスピードで攻撃者と競争しており、そこでは1秒1秒が重要となっています。

01

脆弱性管理は優先事項である

企業や組織は、脆弱性を最小限に抑えつつ、自らのアタックサーフェスを縮小できる最も生産的で時間効率の高い方法を求めています。Sysdigの顧客の88%は、毎週脆弱性データに対処しており、その結果、実行時に使用される脆弱性の削減に成功しています。

シフトレフトは今もなお目標であり、完全なる実現には至っていない

脆弱性管理は、企業や組織のセキュリティプログラムとリスクの優先順位付けの基礎となるものです。その目標は、悪用される前に、ワークロード中の既知の脆弱性を特定した上で、コードへのパッチの適用、依存関係のアップデート、または何らかの他のセキュリティ制御を通じてリスクを軽減することにより、脆弱性を修正することです。理想的には、配信前のパイプラインスキャンにおいて脆弱性を特定することが望まれます。

早期に（すなわち本番環境への導入前に）スキャンすることにより、攻撃の機会を減らすことができるものの、誤検知率が高くなる可能性があります。多くの組織では、ランタイムセキュリティまたはシールドライトアプローチと呼ばれる、本番環境を継続的にスキャンすることで問題に対処しています。完全なシステムの一部として実行時にスキャンを行うことで、シフトレフトよりも精度が向上しますが、本番環境で悪用可能な問題が発生するという現実は避けられません。成熟したセキュリティプログラムの最高レベルでは、誤検知を減らしアタックサーフェスを縮小するために、両方のアプローチを使用することになります。

> “ 当社では、手作業で行っていたレビューを自動化し、本番環境に昇格したコンテナに対して、コンテナの脆弱性とコンプライアンスのチェックを行うようになりました。このような自動化されたチェックにより、より迅速に作業を進めることが可能となりました。
>
> SAP Concur エンジニアリング部ディレクター

脆弱性データ分析において、私たちは、約600万件のランタイムイメージスキャンと50万件以上のCI/CDビルドパイプラインスキャンを調べ、ポリシーの失敗率を検証しました。ランタイムスキャンの脆弱性ポリシー失敗率は91%であり、驚くべきことにCI/CDビルドパイプラインの失敗率はより低い71%でした。

シフトレフトの考え方に従えば、この数字は反転すると予想されます。企業や組織は、早期にかつ頻繁にスキャンを行い、失敗したビルドを認識し、コードを修正し、そして再導入を行う必要があります。**このアプローチでは、高いランタイム失敗率は期待されないでしょう。なぜなら、問題はデリバリーの前に、そして攻撃者にとって悪用可能な状態になる前に発見されるからです。**

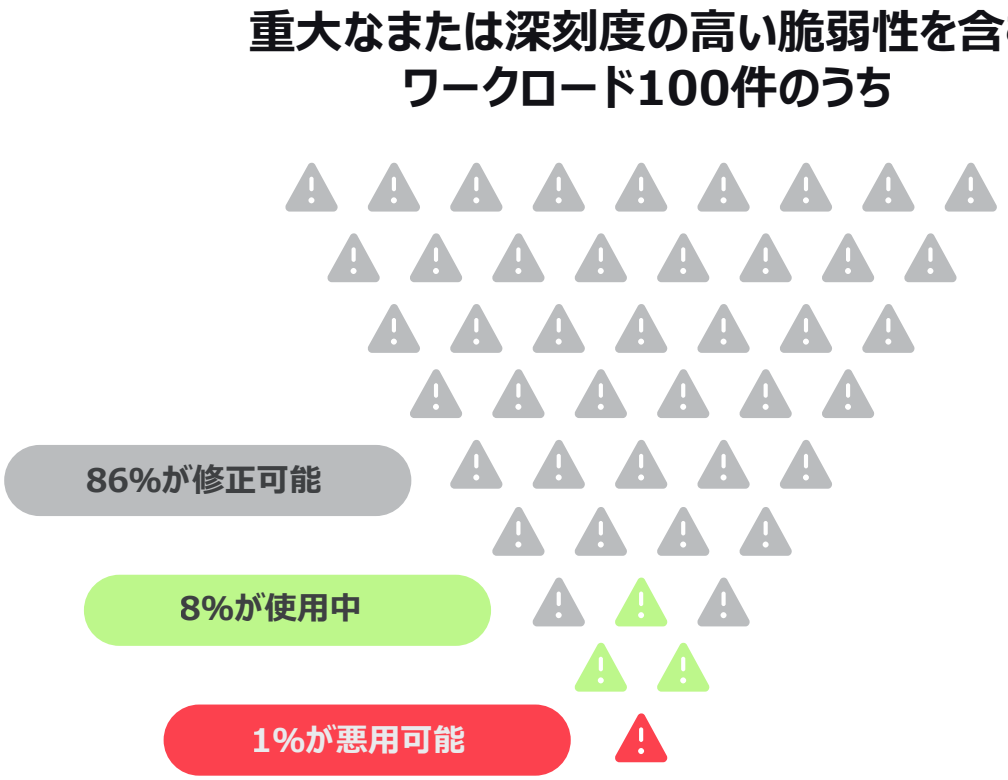
このデータを説明する1つの可能性として、パイプラインスキャンのスコープにない、追加の依存関係が参照されていることが考えられます。また、もう1つの理由として、精度を高めるために、あるいは開発チームの負担を減らすために、組織が単純にパイプラインスキャンを見送り、ランタイムチェックを選択していることも考えられます。最後に、すべてのパッケージが常にチェックされているわけではないことも挙げられます。多くの場合、NGINX、ロードバランサ、プロキシなどのミドルウェアコンポーネントでは、ソースが吟味されており、それなりにセキュアであると想定されているからです。

使用中の脆弱性は克服されつつある

多くの組織では、CVSS（Common Vulnerability Scoring System：共通脆弱性スコアリングシステム）に従って、重大で深刻度の高い脆弱性の修正に優先順位付けていますが、これは数10万件の脆弱性リストから数万件に絞り込むだけであり、それらの脆弱性のほとんどはビジネスに真のリスクをもたらしません。クラウドセキュリティプログラムには、リストを絞り込むよりも効果的な方法が必要です。

昨年、私たちはリスクの優先順位を付ける方法として、使用中の脆弱性の露出を利用することを報告しました。悪用可能な脆弱性への絞り込みを行い、そのコードがアプリケーションで使用されている場所を特定することで、ToDoリストが管理しやすくなり、実行しやすくなります。喜ばしいことに、修正可能で重大なまたは深刻度の高い脆弱性が存在する使用中のパッケージを含むワークロードが、昨年1年間で15%から8.2%へとほぼ半減しました。これは、実行可能で適切にスコーピングされた修正の優先順位が提示された場合、技術チームは、高リスクの脆弱性の負債を迅速に返済できることを示しています。

脆弱性管理で改善が見られた分野は他にもあります。修正が可能で、重大なまたは深刻度の高い脆弱性を含み、エクスプロイトが知られているコードを実行するワークロードは、2%から1.2%に減少しました。一方、修正が提供されておらず、重大なまたは深刻度の高い脆弱性を含むワークロードの実行は、1%から0.5%に減少しました。私たちは、このような傾向が続くことを期待しています。なぜなら、脆弱性のあるイメージを実行することは、依然として大きなセキュリティリスクだからです。しかし、組織や環境にとって最も重要なものに優先順位を付けることにより、攻撃リスクを間違いなく減らすことができます。



重大で深刻度の高い使用中の脆弱性の件数を昨年の

半分

に減らすことができました

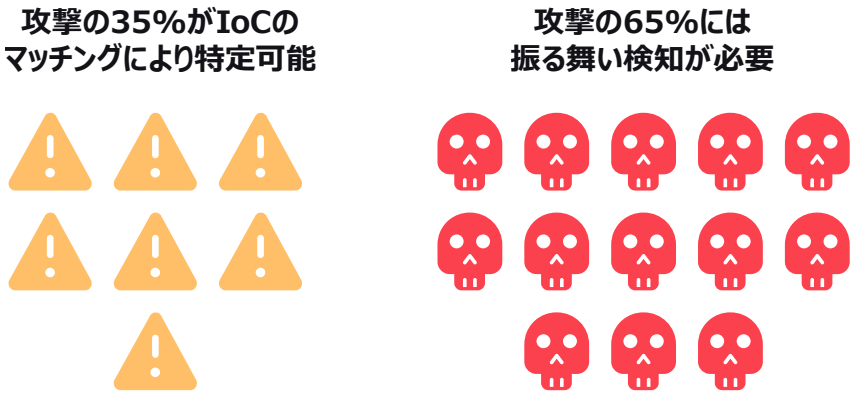
これは、実行可能で適切にスコーピングされた修正の優先順位が提示された場合、技術チームは、高リスクの脆弱性債務を迅速に清算することができ、また、その意思もあることを示しています。

02

脅威検知の強化

高度なクラウド脅威検知戦略

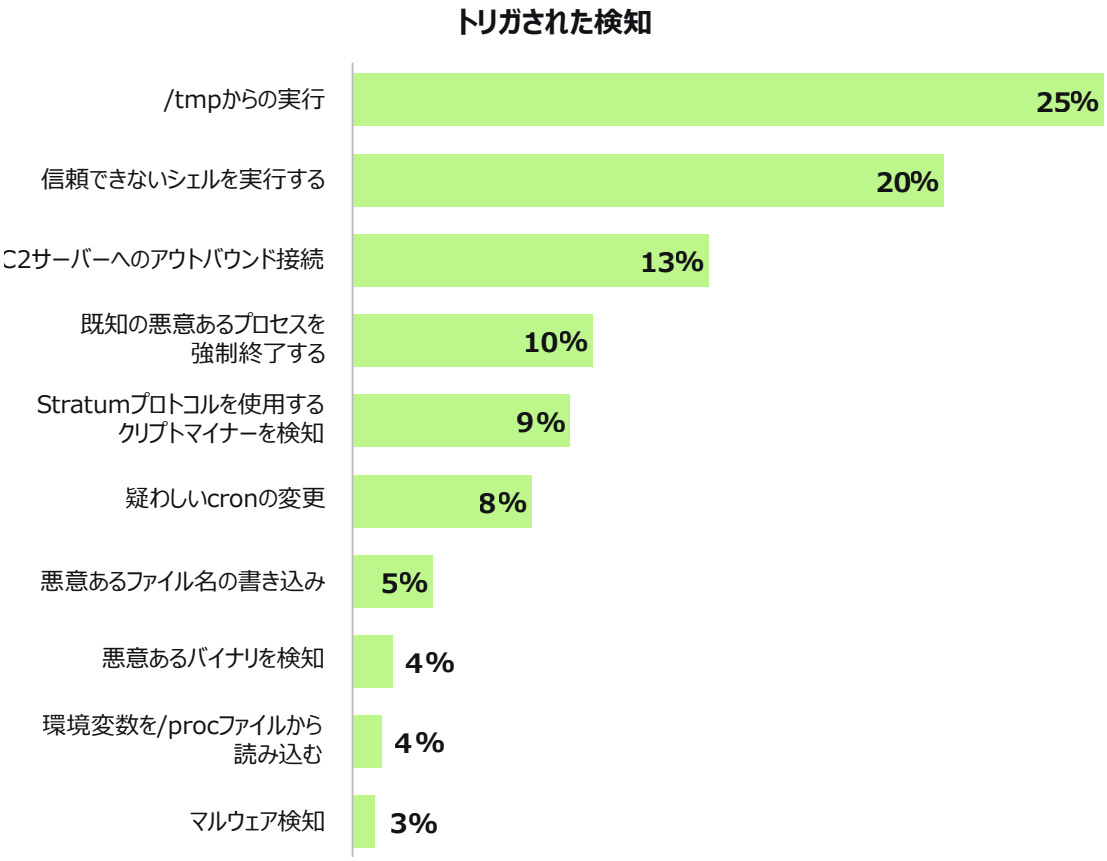
クラウドセキュリティは明らかに予防の域を超えて成熟しつつあり、クラウドの検知と対応の必要性がより緊急性を増しています。そのため、Sysdigの顧客の90%近くが毎週TDR関連のインサイトを活用しています。包括的な脅威検知には、脅威インテリジェンス、侵害指標（IoC）、振る舞い検知など、複数のアプローチが必要です。私たちのデータセットでは、攻撃の35%はIoCのマッチングによって特定可能でしたが、残りの65%はさらに繊細な振る舞い検知のメカニズムが必要でした。これは、脅威インテリジェンスのフィードは非常に有用ではあるものの、完全な検知カバレッジを実現するには至らないことを示しています。



> 当社が設定した基準を満たすために、手作業でログやアラートを調べるのはあまりに面倒です。それには専任の担当者が必要となり、時間を有効に使うこともできません。当社ではすべてのプロセスを自動化することで、より正確なレベルのインサイトに、より迅速に到達できるようになりました。
>
> BEEKEEPER　セキュリティアーキテクト

未知の脅威を捕捉するための振る舞い検知に対する高い要件に伴い、プラクティスとしての検知エンジニアリングが、クラウドセキュリティオペレーションセンター（SOC）内で一般的になりつつあります。カスタム脅威検知の継続的な作成とテストは、TDRユーザーの約65%が共有しているプラクティスであり、プロアクティブで成熟した脅威検知プログラムにおける肯定的な指標となっています。

未知の脅威を捕捉するための振る舞い検知に対する高い要件に伴い、プラクティスとしての検知エンジニアリングが、クラウドセキュリティオペレーションセンター（SOC）内で一般的になりつつあります。カスタム脅威検知の継続的な作成とテストは、TDRユーザーの約65%が共有しているプラクティスであり、プロアクティブで成熟した脅威検知プログラムにおける肯定的な指標となっています。

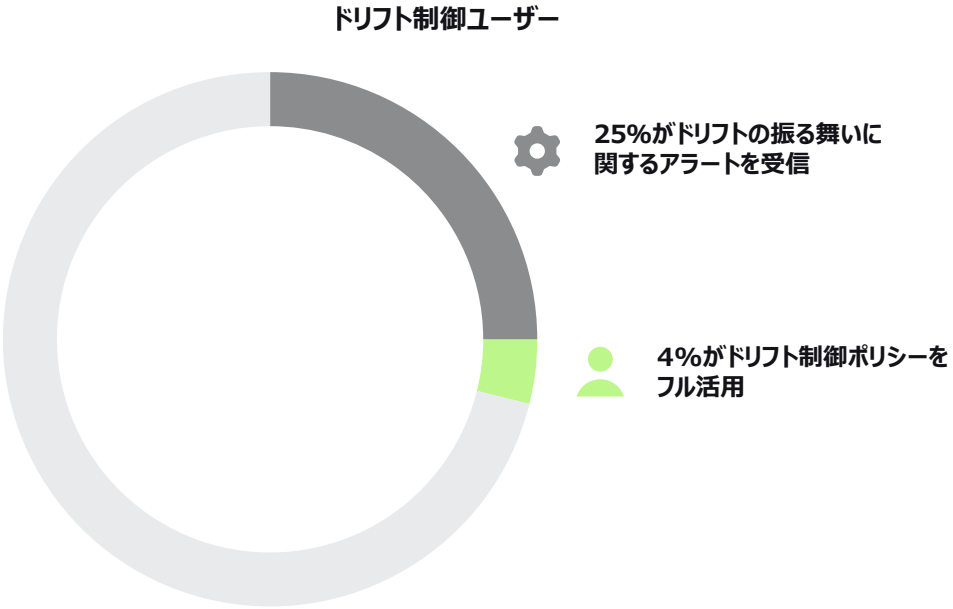


私たちは、セキュリティスキャンとテストがこれらのトリガの大部分を引き起こしていると考えています。これは、これらの組織が、手遅れになる前に攻撃に対応できることを期待して、攻撃の連鎖の早い段階で現れる手口を検知することに集中していることを示しています。

コンテナセキュリティでドリフトに先手を打つ

ドリフト制御は、DIE（Distributed, Immutable, Ephemeral）運用哲学を採用しているチームにとって、強力なセキュリティツールとなり得ます。DIEとは、不変のワークロードはランタイム中に変化すべきではないという考え方です。したがって、観測されたあらゆる変化が悪意ある活動である可能性があります。このようなアクティビティを完全に防止するか、または検知時に単にアラートを発行するように、ドリフトポリシーを設定できます。要するに、ドリフト制御の実装は、より強固な検知がより優れた防止を支援することを例証しています。コンテナドリフトを検知してブロックすることは、コンテナセキュリティにおける強力な予防手段となります。

クラウドユーザーの約25%が、ドリフトの振る舞いに関するアラートを受信しています。一方、予期しない実行を自動的にブロックすることで、ドリフト制御ポリシーをフル活用しているチームは約4%です。この数字は低く見えるかもしれませんが、組織がすでにDIEを導入している場合、ドリフト制御によりアラート疲れと攻撃リスクが大幅に軽減されることを理解する必要があります。



ただし、変更可能なワークロードに対してドリフト制御の検知をオンにすると、誤検知が発生する可能性があります。一方、ドリフト制御の防止機能は、可用性に影響を与え、深刻なダウンタイムを引き起こす可能性があります。エンジニアがワークロードを直接変更したり、確立されたバージョン管理メカニズムの外で変更を加えたりした場合、システムは毎日数万件から数百万件ものドリフト検知アラートを生成する可能性があります。逆に、個人が組織の正式なリリースプロセスを遵守し、実行中のワークロードに変更を加えないようにすれば、ドリフトアラートの精度は大幅に向上します。成熟した開発環境で予防的なドリフト制御対策を有効にすると、インシデントレスポンスによる介入を必要とするような潜在的に悪質なイベントの量を約9%削減できます。

これらの低い数値は、継続的なデリバリーとインフラ自動化の実践に関するセキュリティ成熟度の状況を広く物語っています。一方、一部の企業や組織にとっては、今もなお長い道のりがあるように見えます。

予防的ドリフト制御で対応作業を9%削減

03

基礎の軽視：見過ごされてきたID管理のリスク

企業や組織が脆弱性を減らし、脅威検知作業に優先順位を付けることに関して大きく前進している一方で、ID管理は道半ばにあるように見えます。当社のデータによると、権限は依然として過剰に付与されており、かつ適切に管理されていないため、設定ミスや攻撃者にとっての権限昇格の機会が多く残されています。検知によりこのようなリスクはある程度軽減されますが、ID管理への取り組み（特に過剰な権限の修正）を改善することにより全体的なセキュリティポスチャーを改善し、アタックサーフェスを縮小できます。

ヒューマンIDとノンヒューマン（マシン）ID

私たちのデータによると、脅威の検知や脆弱性の管理に高い優先順位が与えられているのとは異なり、**クラウドネイティブアプリケーションプロテクションプラットフォーム（CNAPP）ユーザーのうち、毎週IDのレビューと管理に力を入れているのはわずか20%に過ぎません。**これは、このデータの管理頻度がはるかに低いためか、あるいは企業や組織がデータを確認するために他のツールを使用しているためだと思われます。いずれにせよ、多くの企業や組織が、過剰な権限を修正するための措置を取っていないことは確かです。

シフトレフトのアプローチと同様に、最小権限の実施もまた、あらゆる組織のセキュリティ施策では優先順位の高いものであり、ゼロトラスト設計の基礎となるものです。昨年、私たちは権限が過剰に付与され、未使用のままになっていることを報告しました。今年のデータを分析したところ、適切な権限の割り当てと管理に苦労している状況は悪化の一途をたどっていることが分かりました。私たちは、その理由として、定期的かつ継続的なID管理の欠如と、IDに高い権限を付与することで著しく時間を節約できるという利便性があると考えています。権限制限がなければ、従業員はプロジェクト中に追加権限を要求する必要なく、シームレスに仕事を進めることができますが、その反面、過剰な権限付与によるこの利便性と時間の節約は、リスクの増大をもたらします。

> “ 最小権限の原則に従うのであれば、過剰な権限を排除することが重要な優先事項となります。過度に寛容なIDがどこにあるのかを理解することは非常に重要であり、その組織規模の大きさゆえに、それらを管理する自動化された方法が必要なのです。
>
> **Booking.com** シニアプロダクトマネージャー

過剰な権限

人間もマシンも、与えられた権限の2%しか使用していません。過剰な権限と管理者権限は、ツールやアプリケーションのデフォルトセットアップとして毎回付与されており、これらが変更されることはほとんどありません。いくつかのケースでは、ノンヒューマン（人間以外）のアプリケーション、ツール、およびサービスは、最初の実装時に何万件もの権限へのアクセスが付与されていましたが、それらが無効にされたりデプロビジョニングされたりすることはありませんでした。私たちは、1年以上まったく手が触れられていない、数十万件もの不要な権限を持つマシンIDを発見しました。

ヒューマンIDにおける過剰なスコープは、過剰な権限付与が従業員に迅速かつ中断なく働いてもらうために最も簡単な方法であったことを考えれば、それほど驚くべきことではありません。一方、マシンIDは、このような扱いを受ける理由がありません。なぜなら、マシンIDは特定の範囲を念頭に置いて作成されるべきであり、プロジェクトやロールの間を移動する可能性があるヒューマンユーザーとは異なり、ノンヒューマンIDはスコープを頻繁に変更する必要がないためです。

重大な影響を及ぼす深刻なクラウドセキュリティ・インシデントの多くが、ID、アクセス、および特権管理の不備に関連している場合、このような運用は過度のリスクを引き起こします。私たちは、攻撃者が脆弱なアクセス制御やアクセス権限のミスを悪用するのを、ここ数年で数え切れないほど見てきました。このアクセスや権限の悪用は多くの場合、攻撃チェーンの最初の攻撃ベクトルであり、IDのハッキングは、必然的にアプリケーションの悪用、システムのハッキング、またはデータの流出につながります。セキュリティインシデントが組織の財務に重大な影響を与えたり、投資家の懸念を招いたりする可能性がある場合、重要課題の評価と開示として満たすべき規制上の要件が追加されることになります。企業や組織はすでに、既存のプライバシーとデータセキュリティ規制を満たすのに苦労しています。これは、米国で発生した1996年医療保険の携行性と責任に関する法律（HIPAA：Health Insurance Portability and Accountability Act）違反のトレンドを有する、保護された医療情報などの分野において明らかです。アクセス制御のギャップは、企業や組織への潜在的な影響に関して、災害を増幅させます。

ノンヒューマン（マシン）IDがトップを維持

ノンヒューマンIDは、今年、クラウドのユーザーとロールの63%を占めています。この3年間、ヒューマンアイデンティティとマシンアイデンティティの数に関するデータを収集した結果、組織がクラウドサービスやツールを拡大、拡張、自動化するにつれ、マシンIDがIDの大半を占めるようになる、と私たちは自信を持って予測しています。しかし、マシンIDが不注意に生み出す膨大なアタックサーフェスを縮小するには、ノンヒューマンユーザーを新規作成する際に付与されるデフォルトのアクセス許可を、最初のプロビジョニング後も継続的に見直す必要があります。

クラウドのユーザーとロール

63%がノンヒューマンID　　**37%がヒューマンID**

企業や組織はすぐに、自分たちがクラウドインフラストラクチャエンタイトルメント管理（CIEM）、特権アクセス管理（PAM）、シークレット管理、アイデンティティガバナンスおよび管理（IGA）を含むIDおよびアクセス管理（IAM）ツールの派生物と格闘していることに気付きます。CIEMは、アイデンティティ・ファブリックが標準的なクラウド環境、特にマルチクラウド・アプローチにおいて、アイデンティティの種類が混在することで生じる複雑性に対処するために特別に設計されました。Gartner®社は、「2027年までに、アイデンティティ・ファブリックの免疫原則は、新たな攻撃の85%を防止し、その結果、侵害の財務的影響を80%削減する」と予測しています[1]。IDタイプの混合、異なる使用パターン、および最新のテクノロジスタックによる動的アクセス制御の必要性を考慮すると、人中心のIAMアプローチはマシンIDに関しては十分ではありません。IDテクノロジーは、ID脅威の検知と対応（ITDR）戦略を強化するために協調して機能する必要があり、CIEMはクラウドにおけるIDリスクに対処するために不可欠な機能となっています。

2023年11月、イランの脅威者アクターが水道局を含む複数の米国組織をハッキングしました。これは、産業用制御機器のデフォルトパスワードが変更されなかったことが原因でした。

1　Gartner, Invest Implications：Top Trends in Cybersecurity 2023, Frank Marsala, 23 March 2023. GARTNER は、米国およびその他の国における Gartner, Inc. および / またはその関連会社の登録商標およびサービスマークであり、本書では許可を得て使用しています。無断複写転載を禁じます。

04

セキュアなデリバリーと開発者の習慣

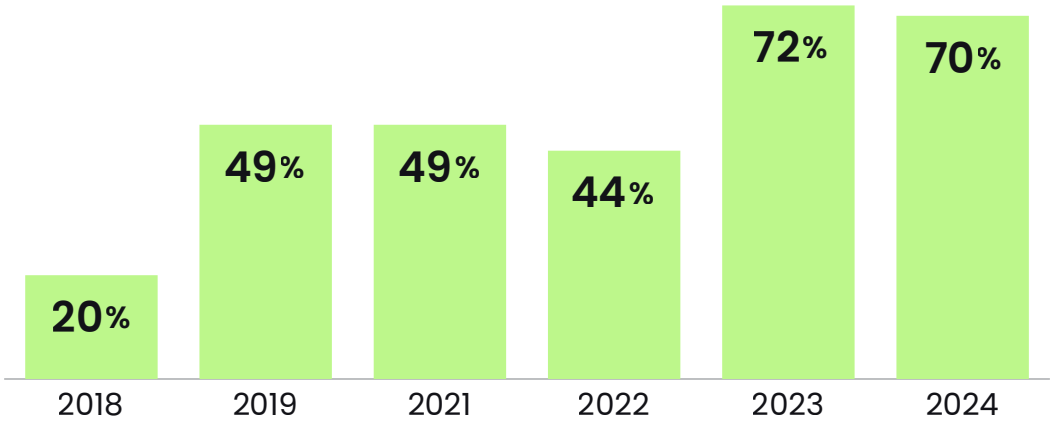
多種類のリスクのバランスを取ることは綱渡りのような作業

私たちが今年までに収集した利用データには、一貫した重要な事実が存在しています。当社の顧客の大半は、一般に公開されているレジストリをイメージのために使用しており、CPUやメモリの使用量を制限していません。オープンソースプロジェクトにおける開発、コードコミット、ビルドのペースは速く、制限がないため、開発者はクラウドのスピードで作業できます。しかし、このことは、企業や組織にガバナンスの課題とセキュリティリスクをもたらし、サイバーセキュリティに必要な要素である運用の回復力に対する脅威を高めることになります。

攻撃者はコンテナの寿命に打ち勝つ

コンテナの平均寿命は年々短くなっています。今年、70%のコンテナが短命であり、5分以内にスピンダウンしています。Sysdigの脅威研究チーム（TRT）は、『2023度版グローバルクラウド脅威レポート』の中で、クラウド攻撃にかかる時間はわずか10分であると報告しています。攻撃者がラテラルムーブメントを実施していなければ、攻撃はコンテナが実行されている間に開始され、コンテナの終了と共に強制終了されます。しかし、クラウドでは攻撃者が発見と偵察を自動化しているため、攻撃者が環境に侵入してラテラルムーブメントを実行するのは迅速かつ容易であることが分かっています。攻撃者が環境に侵入すると、ほとんど一瞬で、その侵入先の状況を把握し、前進する準備が整います。このことは、リアルタイムセキュリティと継続的スキャンの重要性を浮き彫りにしています。脆弱なワークロードを稼動させることは、いかに短期間であっても、企業や組織を攻撃のリスクにさらすことになります。

コンテナの寿命は5分未満



ベストプラクティスにもかかわらず、パブリックソースを使用することは今もなお普通に行われている

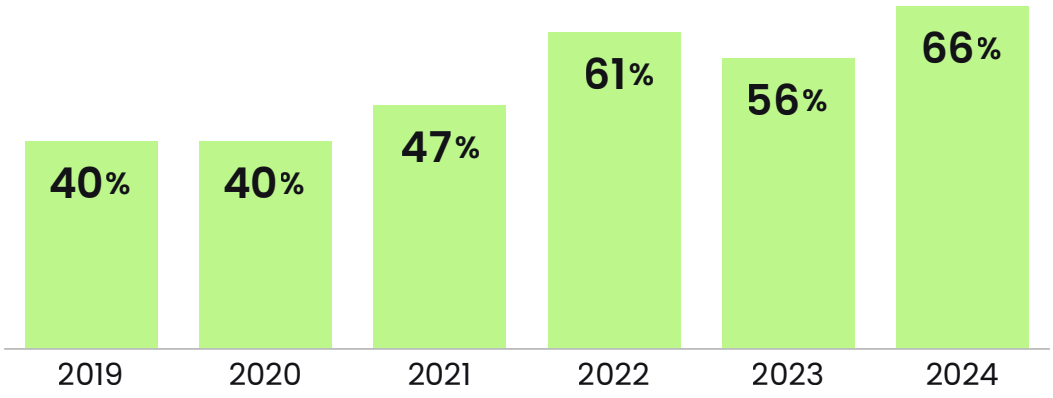
私たちは毎年、パブリックおよびプライベートレジストリとリポジトリの使用内訳を確認し、最もよくイメージがプルされている場所を特定しています。私たちは今年、260万個以上のコンテナにまたがる1,400以上のユニークな名前のレジストリを分析しました。その結果、コンテナイメージのホストと管理に使用されているレジストリの 66%がパブリックであることが分かりました。残りの 34% のレジストリは、パブリック レジストリのプライベートインスタンス、ベンダー管理のレジストリ、または独自のカスタマイズされたレジストリの組み合わせであり、通常は大規模な顧客やセキュリティに精通した顧客向けです。

レジストリの種類

66%がパブリック　　**34%がプライベート**

このデータを数年間検証した結果、セキュリティの成熟度に関係なく、パブリックレジストリとマネージドレジストリの利便性がコンテナユーザの大多数にとって魅力的であることは間違いありません。イメージにパブリックレジストリを使用することで、企業や組織は独自のレジストリの作成と保守にかかる時間を節約できるほか、ベンダーが管理するタイプのレジストリに費用を支払う必要がないためコストを削減できます。その一方で、パブリックレジストリを使用すると、セキュリティ制御の強制力が低下し、ソフトウエアのサプライチェーンリスクが生じることに注意する必要があります。

パブリックレジストリの使用



Sysdig TRTは、『2023年度版グローバルクラウド脅威レポート』の公開イメージ分析において、1万3千のDockerHub上の不審なコンテナイメージを、80万以上のダウンロードと共に特定しました。ランタイム分析を行った結果、これらのイメージのうち約6%が真に悪意あるものであると判定されました。悪意あるイメージの割合がこの程度であることを考えると、パブリックレジストリから取得するセキュリティリスクは些細なものに思えるかもしれませんが、それがコンテナイメージのセキュリティ管理に関連する大きなリスクであることに変わりはありません。ハッキングされたイメージが検査や保護なしに実行されると、企業や組織にとってセキュリティ上の大きな問題を引き起こす可能性があります。

2023年度版グローバルクラウド脅威レポート

今すぐ読む →

理想的なセキュリティアプローチは、ベンダーが管理するレジストリを使用するか、またはチームがコードのプルやインスタンス化を行える公開されているレジストリのプライベートインスタンスを使用することです。しかし、これらのプライベートレジストリには、パブリックレジストリから引き出されたコードのコピーが含まれているため、それらを環境に実装する前に、組織のポリシーに基づいて厳しくスキャンする必要があります。成熟した組織は、プライベートレジストリ内に「ゴールデンイメージ」または「ゴールデンソース」を保管しています。これは、GitOpsやPlatformOpsなどのようなその他のプラクティスのバックボーンにもなります。このアプローチにより、組織はソースパッケージとイメージに対するより強力なガバナンスを確立でき、その結果、攻撃者がパブリックリポジトリとレジストリのファイルをターゲットにした際に発生する脅威を軽減できます。

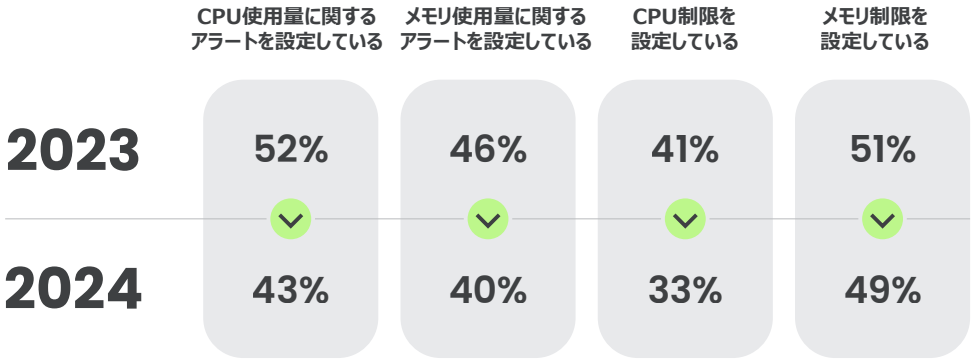
一部の組織が、ランタイムTDRに依存するなどして、サイバーセキュリティプログラムの一部として、パブリックレジストリからプルすることに関する相対的なリスクを受け入れ、おそらくは他の方法で軽減していることは理にかなっています。これは利便性のためか、運用の負担を減らすためか、あるいは組織の縦割りの副産物であるか、それともコスト削減努力の一環であるかもしれません。いずれにせよ、これは、伝統的な「徹底的な防御」というセキュリティの考え方とは相反するものであり、セキュアなデリバリープロセスに関する懸念を引き起こすものです。これはセキュリティのベストプラクティスではありませんが、強力なTDRを導入することで、パブリックレジストリに関連するリスクを何らかの形で軽減できます。

企業や組織は、TDRを通じてパブリックレジストリの利用に関するリスクを軽減する権利を守ろうとしていますが、理想としては複合的なアプローチを採用する必要があります。

リソースの制約がまだ甘すぎる

CPUとメモリの使用量をトリガとするアラートが設定されている環境は50%未満です。さらに、大半のユーザーはCPUやメモリの使用量に上限を設定していません。これは、アラートがうるさすぎると認識されている可能性が高く、組織は本番のアプリケーションに影響を与えないように容量を増やすことを好むためだと思われます。これもまた、セキュリティリスクと可用性リスクのトレードオフが当てはまるケースです。アラートや制限を設定しなければ、攻撃者が環境内で使用した分のリソースの代金を支払わなければならないというリスクが高まります。可用性を優先するという決定は、クラウド環境での利便性と開発スピードのサポート、そして伸縮性（エラスティック）に関わります。リソースの制限を減らしたり無視したりすることは、時間を節約するためのギャンブルとなります。

CPUやメモリの使用量を気にしている組織は少ない



リソースの制約がないことは攻撃リスクの要因であり、制限を設けることはセキュリティの基本的なベストプラクティスであると考えられています。無制限のリソースは、攻撃者があなたの環境を利用するための絶好の機会を提供します。これには、クリプトジャッキング攻撃や、リソースを使用して組織のネットワーク内にある他のシステムを狙う複雑な攻撃チェーン（すなわちラテラルムーブメント）を永続化することなどが含まれます。この種の脅威は、チェックされていないリソースを迅速に発見し、除去しなければ、コストのかかる過ちとなることが証明されています。

これは一種の財務リスクでもあり、どのプロセスがメモリやCPUを使用しているかを確認した上で、コストを削減するためのビジネスチャンスが存在しています。現在のマクロ経済環境を考えると、ほとんどの企業や組織は、設備費と運用費を精査しています。クラウドやコンテナ環境では、リソースの消費を制御することが、財務上の目標を達成するための手段となります。

05

AIの導入は拡大しているが、それはあなたが考えているような方法ではない

自動化によりデータ処理と理解度が向上

驚くほど多くのAIパッケージやフレームワークが導入されていますが、これらのパッケージの85%は、生成AIのためではなく、機械学習（ML）を通じてデータ分析を強化し、相互関連付けや異常検知を強化するために使用されています。当社の顧客のおよそ3分の1がAIフレームワークとパッケージを統合しています。クラウド攻撃のスピードに対応するためには、いくつかのセキュリティプロセスを自動化する必要があります。大規模言語モデル（LLM）を使うと、実用的なインサイトを生成し、チームがリスクとセキュリティ問題をよりよく理解できるようになるほか、セキュリティ運用の対応にかかる時間を短縮できます。

> 攻撃時や日々のタスクに関連するコンテキストを提供するためにAIを使用することは、当社にとって非常に価値のあることです。当社では、これによりクラウド領域の知識のサイロ化を解消し、隠れたリスクを発見し、攻撃経路の点と点をつなげることができると期待しています。

onna　プリンシパルアーキテクト

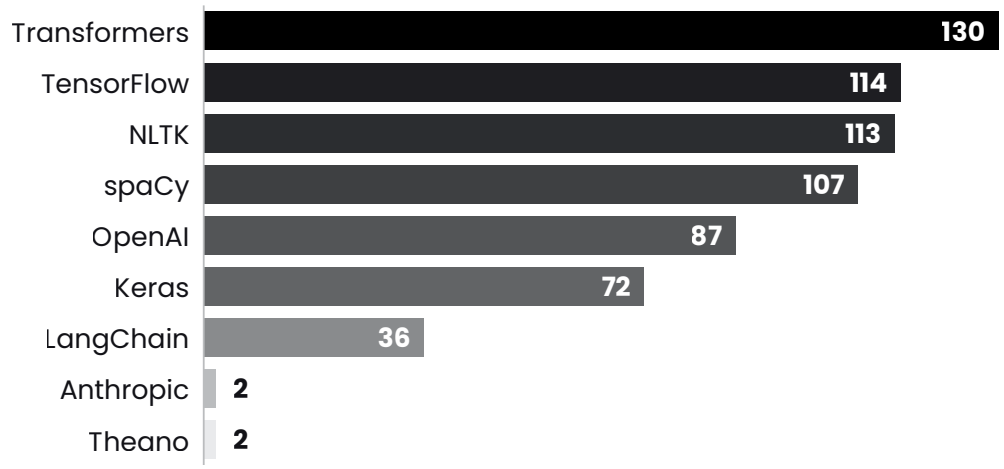
AIの採用

85%がデータ分析と相互関連付けに使用

15%が生成AIに使用

ここで報告している数字は、特にクラウドワークロード内の既知のパッケージに関するものです。多くの企業や組織は、現時点では独自の生成AIソリューションを構築することはなく、Anthropic（Claude）、OpenAI（ChatGPT）、またはクラウドサービスプロバイダーが提供するような、事前に構築され、事前に訓練されたサービスを利用することになるでしょう。その一方で、データ収集と理解の取り組みにおいてさまざまなタイプのAIパッケージを導入して使用している企業や組織は、そのような技術的能力を活用することでスタッフにかかるデータ解析の負担を軽減できるでしょう。

生成AIパッケージの種類



この表は、クラウド環境で見られる生成AIパッケージタイプの15%を表しています。

ブラウザベースのGenAIツールやインターフェースの個人的な使用は、ほぼ間違いなくはるかに増えていますが、私たちのデータは、企業が自社環境で実行されているワークロードにAIを明示的にホストするのが遅れていることを示しています。企業や組織がOpenAIのChatGPTのようなLLMをセキュリティの管理、検知の改善、脅威アクターの戦術、手法、手順（TTP）の理解と発見のために使用している可能性は低いと思われます。その代わりに、生成AIは、マーケティングキャンペーン活動、電子メール作成、文書作成、コード作成支援などのタスクに使用されています。Gartner社は、「2028年までに、企業のソフトウェアエンジニアの75%がAIコーディングアシスタントを利用するようになる。この数字は、2023年初頭には10%未満であった」と予測しています[2]。

2 Gartner, Invest Implications：Top Trends in Cybersecurity 2023, Frank Marsala, 23 March 2023. GARTNER は、米国およびその他の国における Gartner, Inc. および / またはその関連会社の登録商標およびサービスマークであり、本書では許可を得て使用しています。無断複写転載を禁じます。

調査方法

Sysdigは、実際の顧客データを共有することに専念しています。このようなデータを使用することで、当社は、独断的な調査結果や歪んだ調査結果ではなく、コンテナ、クラウド、セキュリティのトレンドの実際の変化について報告できます。コンテナ、クラウドアカウント、アプリケーションの使用状況を分析することで、私たちは、実行時に実際に使用されている脆弱性の件数や、コンピューティングリソースがどのように使用されているかなど、独自のインサイトを共有できるようになります。

本レポートのデータは、当社の顧客が毎日実行している数千件のアカウントと数百万件のコンテナの分析から得られたものです。当社のセキュリティとコンテナに関するインサイトは、技術系のスタートアップ企業から大企業に至るまで、幅広い業界の組織から得られたものです。この匿名化された顧客データは、世界中の地域でホスティングされており、北南米、オーストラリア、EU、英国、アジアの多国籍企業をカバーしています。

結論

Sysdigの『2024年度版クラウドネイティブセキュリティおよび利用状況レポート』は、クラウド環境および組織における進化を続けるセキュリティ状況に関する包括的なビューを提供するものです。本レポートは、実行時の脅威の優先順位付けが大幅に進歩したにもかかわらず、シフトレフトという概念との格闘が今もなお続いていることを浮き彫りにしています。特にID管理における困難に直面している場合、堅牢なクラウド脅威の検知と対応メカニズムの緊急性は明らかです。

本レポートは、実行時の脆弱性の減少を取り上げていますが、同時に、ヒューマンIDとマシンIDに付与された過剰な権限に関連するリスクを受け入れることが、セキュリティ環境に重大な脅威をもたらしているという懸念も強調しています。リソース消費の傾向は、攻撃者がアクセス制御のギャップを通じて悪用できる経済的および物質的な影響を強調しており、事前対策の必要性を浮き彫りにしています。企業や組織はセキュリティのベストプラクティスを無視してクラウドへの移行を急速に進めていますが、AIの実装に関してはまだ自信を持てないようです。

今年の年次レポートの主なトレンドとしては、現実的なセキュリティ実務では、迅速なクラウド革新に歩調を合わせるためにセキュリティのベストプラクティスよりも利便性を優先しているが、AIパッケージの導入にはためらいがあることが浮き彫りになっています。

私たちは、来年に向けてセキュリティの進歩を皆様に報告できることを楽しみにしています。それでは、またお会いしましょう。

sysdig

Sysdigが発行した過去の『クラウドネイティブセキュリティィおよび使用状況レポート』（英語原文）はこちらのリンクからご覧になれます。

日本語訳された2023年度レポートはこちら

2024年度版クラウドネイティブセキュリティおよび利用状況レポート

RP-009-JA REV. A 1/24