THE /555 GUIDE

555ベンチマークガイド: CISO向け

クラウド環境でのより高度でより迅速な脅威検知を実現

sysdig.jp/555

sysdig SECURE EVERY SECOND.

Sysdigは、クラウドを安全に運用するための基準として「**クラウドの検知と対応における5/5/5ベンチマーク**」を設定しています。クラウド攻撃にかかる平均時間は、最初のネットワークアクセスからビジネスに悪影響を及ぼすまでにわずか10分であることが分かっています。Sysdigが設定した555ベンチマークとは、5秒以内に脅威を検知し、5分以内にデータの相互関連付けとトリアージを行い、そして5分以内に対応することを推奨しています　。

このベンチマークは、Sysdig脅威リサーチチーム（以下「TRT」）が「**2023年度版グローバルクラウド脅威レポート**」で提示した証拠により裏付けられています。TRTは、自動化手法やAI機能の悪用により、クラウド攻撃のスピードと巧妙さが増していることを明らかにしました。たとえば、TRTが2023年7月に発見した**SCARLETEEL**クラウド攻に関する報告によれば、攻撃者が被害者からプロプライエタリなデータを盗むのにかかった時間は、わずか4分でした。

レガシーなセキュリティツールは後れを取らないよう努力してはいますが、それらがサポートできるのは今日のクラウド環境で発生するセキュリティ問題のほんの一部のみにすぎません。これらのツールは、攻撃者がキルチェーン（攻撃連鎖）を通過するのに数日から数週間を要するような、オンプレミス環境を保護するために構築されています。今や企業や組織は、クラウドネイティブ環境の動的な性質に合わせて設計されたツールとプロセスが必要です。最適なクラウドセキュリティプログラムは、適切な人材、プロセス、ツールのオーケストレーションによって構築されます。**ビジネス戦略やイニシアティブに沿って組織の回復力を推進するようなセキュリティチームを作る事は、非常に大きなビジネス価値があるのです。**

目次

組織の経営幹部にとって、大きな痛手となる情報漏洩は、自社のSOCを10分で対応できるレベルまで成熟させれば、その可能性は低くないでしょう。本ガイドは「**555ベンチマークガイド：クラウドセキュリティ実務担当者向け**」と対になるものであり、クラウドセキュリティ実務担当者向けガイドには、規範的なガイダンスと次に取るべき実行可能なステップを提供しています。**本ガイドにより、クラウドセキュリティ運用を成熟させるために必要となる分野と方法を理解できるようになるでしょう。そして、共通の言語と運用の方向性をご理解いただくことで組織の実務担当者と同じ見解を持っていただけるでしょう。**同時に、組織の持つ運用上のレジリエンスを向上させ、セキュリティチーム全体のインシデント対応の負担、ストレス、疲労を軽減できるようになります。

多くのツール、プラットフォーム、ダッシュボードが企業や組織の抱えているセキュリティ上の問題を解決すると謳っていますが、実際に攻撃を受けた場合に役立つのは、結局のところ組織内のセキュリティチームが持つ専門知識、能力、そして準備に他なりません。攻撃者がその手法をますます強化し改良している中、 Sysdigは、多くの企業や組織とコラボレーションを行うことで、レベルアップを図り、最新のクラウドセキュリティリスクと攻撃に対する準備を整えることができるようにしています。

このガイドは、革新的で適応力の高いツールと自動化を活用し、クラウドリスクへの積極的な対処の実現に役立ちます。

» 攻撃者が最初の10分を超えてネットワークにアクセスし続けた場合、それが1時間ごとまたは1日ごとに及ぼす重大な影響を想像してみてください。組織の規模や業種にもよりますが、**計画外のダウンタイムにかかるコストは、1時間あたり13万8000ドルから54万ドルの間で変動します。**つまり、平均的な1日の労働時間にわたって致命的なサービス停止が発生した場合、企業には、復旧時に500万ドル以上のコストがかかる可能性があります。

新しい視点を取り入れる

開発者のマインドセットとセキュリティチームのマインドセットをシームレスに統合することで、セキュリティギャップを埋め、リスクを低減できます。そのための理想的な方法は、DevOpsのスキルセットをSOCとより広範な組織全体のセキュリティ業務の両方に導入することです。DevOps、開発者、インフラストラクチャー担当の各チームは、多くの場合、継続的に自社環境に身を置いているため、セキュリティチームに比べて環境に対するより精度の高いな可視性を持ち、環境をより深く理解しています。一方、SOCチームは、その定義上、異常に対して対応する人々です。開発者は、クラウド、SaaS、および開発プロセスに関する異なる視点を提供できるため、これらの環境に関わるインシデントに対処する上で重要となります。開発者をセキュリティに関与させることで、運営上のレジリエンスにおいて恩恵を受けることができます。

従来のSOCアナリストにとって、クラウド環境では何が標準であり何が期待されるかを特定し理解することが困難な場合があります。なぜなら、クラウド環境では、オブジェクトストレージ、サーバーレスコンピューティング、コンテナオーケストレーション、ランタイムイメージスキャンなど、従来のSOCアナリストが慣れ親しんできたものとは全く異なるテクノロジースタックやプロセスが必要となるためです。DevOpsチームとSOCチームのコラボレーションは、テレメトリーの欠落や、攻撃につながる可能性のあるその他の未知のリスクを浮き彫りにすることでしょう。

2020年に発生したSolarWinds社のインシデントは、わずか9カ月間で**4,000万ドルの損失**を出し、同社のCISOに対する訴訟が起きるという結果を招きましたが、これは、セキュリティチームと開発チームの間にしばしば存在する知識のギャップを示す興味深い事例だと言えます。このケースでは、攻撃者が当該ベンダーのビルドパイプラインをハッキングしてそこに悪意あるコードを仕込んだ結果、そのコードが知らぬ間に顧客に渡されてしまったのです。SOCアナリストは、ビルドパイプラインが通常どのように機能するのかに精通しておらず、オペレーティングシステム層の上にあるビルドサーバーからどのようなデータを収集する必要があるのかさえ知りませんでした。**DevOpsの知識を持つ誰かが、このようなケースでSOCをサポートできていたならば、よりダメージの少ない結果につながった可能性があります。**

SOCアナリストは、通常、次のような専門知識を持っています。

- 攻撃者の動機と手法に関する知識
- ネットワークトラフィックやシステムログの監視、および検知エンジニアリングにおけるスキル
- 脆弱性、マルウェア、侵入に関する深い理解
- サイバーセキュリティに関するベストプラクティス、セキュリティコンプライアンス要件、組織が抱えるセキュリティポリシーおよび手順などの分野における経験
- 最新のサイバーセキュリティ脅威とトレンドに対する認識

DevOpsエンジニアは、次のようなスキルをSOCにもたらすことができます。

- クラウドインフラストラクチャーに関する深い理解と、関連するCSPに特化した専門知識
- セキュアなソフトウェアデリバリーライフサイクル（SSDLC）に関する豊富な知識
- 一貫性、再現性、スケーラビリティを実現するようなITインフラストラクチャーの導入および管理の自動化に関する専門知識
- 導入と管理を合理化するための、コンテナ化技術およびコンテナオーケストレーションプラットフォームに関する理解
- ソフトウェアアプリケーションのビルド、テスト、デプロイを自動化するためのCI/CDパイプラインの実装に関するスキル

人がプロセスを強化し、セキュリティギャップを低減

セキュリティチームが、正式なインシデント対応プロセスチームだけではなく、それ以外の多くのチームと連携し、知識、能力、ツールを共有できるようにします。これにより、セキュリティチームは、自社のビジネスや運営をはじめ、攻撃者が侵入、移動、潜伏する可能性のある場所をよりよく理解できるようになり、ひいてはセキュリティチーム自身のプロセスを改善できるようになります。

職能上の垣根を超えた複数のチーム間で、会議の場を設けましょう。あるいはSOCアナリストをDevOpsチームやインフラチームに一定期間配属すること（またはDevOpsチームやインフラチームのメンバーをセキュリティチームに一定期間配属すること）。なお、これらの提案は、先を見越して管理する必要があり、きちんとした管理が行えないと成果が上がらない可能性があります。他のチームとのコラボレーションは、本質的に、データの相互関連付けやコンテキスト化を改善するための「シフトレフト」であり、インシデント対応の苦労を少しでも軽減することを目指すものです。

セキュリティアナリストや脅威アナリストに、分析で一番好きなことは何かと尋ねると、彼らはおそらく、パズルを掘り下げ、ストーリーの全貌を明らかにすることだと答えるでしょう。しかし、残念ながら、クラウド脅威の検知と対応プロセスでは、本来の目的から逸れた作業を行っている暇はありません。レガシーなツールで複数のエンドポイント、ワークロード、環境などからのデータを手作業で相互に関連付けるには多くの時間がかかり、その一方で、クラウド攻撃者はすでに攻撃プロセスを自動化しています。**手作業での相互関連付け作業に費やす時間は、敵に利益をもたらすだけです。インシデント対応時におけるデータ相互関連付けは、精度が高く、かつ自動化されていなければなりません。**

» 攻撃経路を可視化することで、セキュリティチームは、初期アクセス、パーミッション、ラテラルムーブメント、そしてデータの収集と流出のすべてがどのようにつながっているかを確認できます。

相互関連付けとトリアージを5分で行うには、合理化されたプロセスが必要となります。これにはダッシュボードの統合も含まれます。相互関連付けを行う際には、**攻撃経路を可視化すること**が理想的です。セキュリティチームは、最初のアクセス設定ミスや脆弱性、使用されたIDパーミッション、複数のワークロードや環境をまたがる移動、データの収集や流出がどのようにつながっているかを、ほぼリアルタイムで確認する必要があります。さらに、これらの詳細情報は、事後対応レビューや根本原因分析に不可欠なものです。企業や組織が情報漏洩に対応するために必要なセキュリティインフラをすべて備えている可能性は高いのですが、セキュリティチームがこれらのツールをすべて使用して対応するためには、おそらく10分以上の時間がかかるでしょう。

適切なツールで検知効率を最大化し、リスク管理を改善

リアルタイムの脅威検知は、平均修復時間（MTTR）を短縮するための重要なステップです。リアルタイムでの検知は、「エフェメラル型の資産」を可視化するために必要となります。エフェメラル型の資産とは、コンテナ、仮想マシン、クラウドインスタンスのような、一時的なまたは短命のリソースのことです。エフェメラル型の資産は、最新のコンピューティング環境の一部として動的に作成され、スピンダウンされることが多いため、レガシーなセキュリティツールやプロセスではこれらの資産の監視や保護が行えません。

リアルタイム検知により、セキュリティチームはエフェメラル型の資産がプロビジョニングされ、デコミッショニングされるのを継続的に監視し、セキュリティの脆弱性や不審な行動が見つかった場合には、即座にアラートを発行できます。これは、進化するクラウドの脅威に対する早期警告システムであり、多くの業界や連邦政府のコンプライアンス要件によって義務付けられています。コンプライアンス規制が理由で、企業や組織がリアルタイム検知機能を備えている可能性は高いのですが、真にクラウドネイティブなツールを使用することで、スピード、コスト、スケーラビリティ、革新性において飛躍的な向上を実現できます。

» CNAPPは、クラウド特有の運用の複雑さを軽減し、個々のCSPでは実現できない包括的なカバレッジを提供します。

クラウドツールの複雑さを簡素化

まずはクラウドサービスプロバイダー（CSP）から始めましょう。すでにCSPと契約しているのですから、それを利用しない手はありません。強力なクラウドセキュリティプログラムを構築するには、CSPのネイティブデータと機能が不可欠です。しかし、「クラウド生まれ」の組織でない限り、クラウドネイティブアプリケーションとクラウドに移行したレガシーアプリケーションを組み合わせたハイブリッド環境になっている可能性が高いでしょう。このような場合、複数のCSP間での一貫した相互関連付けが必要となるため、特定のクラウドに依存しないツールが必須となります。このような横方向のギャップを放置しておくことはできません。

CNAPP（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）ツールは、リアルタイム検知の問題を解決するためのクラウドネイティブソリューションです。これは、必要となる複数のクラウドネイティブ機能をまとめて1つのソリューションにしたものです。CNAPPは、クラウド特有の運用の複雑さを軽減し、個々のCSPでは実現できない包括的なカバレッジを提供します。

クラウド脅威検知・対応（CDR）ツールと同様に、CNAPPは、クラウドおよびハイブリッド環境のインフラとサービスに関する包括的なリアルタイム可視性と検知を提供し、設定ミス、脆弱性、コンプライアンス上の問題に対して即座にアラートを発行します。

また、CNAPPは、クラウドワークロードプロテクション（CWPP）、アイデンティティ管理（CIEM）、ポスチャー管理（CSPM）のすべてを1つのダッシュボードに集約することで、脅威の検知と対応を可能にします。CNAPPのような高度で包括的なツールを活用することで、クラウドで必要とされるプロアクティブな初期対応が可能になります。

さらに、CNAPPはセキュリティチーム以外のチームにも使用されることで、セキュリティを向上できます。今日の「セキュアファースト」式のハイテクビジネスの世界では、セキュリティに対する責任共有が必須となります。このような責任共有は、法務、人事、エンジニアリングなどのチームとのコラボレーティブなユースケースとして、CNAPP内でサポートされます。

セキュリティ技術スタックの統合

CNAPPは、お客様がお使いのセキュリティ技術スタック内にすでに存在している他のツールと上手く統合できます。これには、データ集約のためのSIEM（Security Information and Event Management）や、データの相互関連付け、情報のコンテキスト化、対応アクションの自動化を行うSOAR（Security Orchestration, Automation, and Response）などのソリューションが含まれます。これらのツールは、CNAPPと組み合わせることで、検知と対応の効率をさらに向上させます。クラウドネイティブの技術スタックを構築する際には、統合の簡素化を優先し、ツールがAPIベースであることを確認してください。統合はマシンスピードで行うべきであり、統合が煩雑な場合や実施するのが難しい場合は役に立ちません。なぜなら、それはセキュリティチームに、複数のダッシュボードにログインすることを強制してしまうことになるからです。

統合はマシンスピードで行うべきであり、統合が煩雑な場合や実施するのが難しい場合は役に立ちません。

統合されたSOARツールがあれば、クラウド脅威の検知と対応に必要なスピードで、ツール、プロセス、ワークフローのオーケストレーションを実施し、それらを調整できます。**プロアクティブな脅威モデリングを通じて、セキュリティチームは、事前に設定された攻撃経路に対する自動化された対応アクションを確立できます。**必要となるのは、「xが発生したならばyをトリガせよ」という「if then」文だけです。脅威モデリングを通じてxを予測し、かつyをプロアクティブに軽減するかまたは継続的に評価することにより、脅威がもたらす影響を取り除くことができます。

たとえば、Sysdigはこのコンセプトに基づいて、**ドリフト制御**と呼ばれる機能を提供しています。ドリフト制御を使うと、セキュリティチームは、本番環境でワークロードの変更が検知された場合の対応を自動化できます。たとえば、アラートを発行するか、ワークロードを一時停止するか、あるいは完全に停止するかを選択できます。このアイデアは他のイベントにも適用できるため、セキュリティチームは、状況を分析しながら、潜在的な問題を即座に隔離し、適切な対応を策定するための時間を確保できます。

しかし、作業負荷の自動停止を行う際には、予期せぬダウンタイムがビジネスに与える可能性がある財務的な影響を考慮する必要があります。すなわち、セキュリティチームと開発者チームの間における相互理解とコミュニケーションを通じて、業務への影響を回避する必要があります。

チームを信頼し訓練する

貴社の組織では、すでにインシデント対応計画を策定済みであるかもしれません。策定していない場合でも、今からセキュリティチームが計画を作成するのは遅すぎます。インシデント対応計画を策定済みである場合、今こそそれを見直した上で、インシデント対応ポリシーとプレイブックのすべての要素に、最新のクラウド攻撃が持つ時間的なプレッシャーに対する配慮が含まれているか、を確認してください。インシデント対応計画を確立するか、それとも現在策定済みの対応計画を更新するかは、マネージャーレベルが決めるのではなく、実務レベルの担当者が決められるようにすべきです。

CISOの方にお願いしたいのは企業のセキュリティチームが対応を行う際に、他の経営幹部や取締役会のメンバーに伝えなければならない重要な詳細情報（マテリアリティ、事業や運営への影響など）を常に把握しておくことです。攻撃の影響が重大であるかどうかを把握し、そして判断し、それについて報告する準備ができている必要があります。タイムリーに対応できれば、重大な影響が生じる可能性は低くなります。

CISOの方にお願いしたいのは企業のセキュリティチームが対応を行う際に、他の経営幹部や取締役会のメンバーに伝えなければならない重要な詳細情報（マテリアリティ、事業や運営への影響など）を常に把握しておくことです。

協力と傾聴でセキュリティプロセスを設定する

セキュリティチームを率いて、自動化によるセキュリティプロセスの合理化と継続的な、改善を目標に、このような10分間におけるクラウド脅威の検知と対応の課題に取り組むことが必要です。また、検知、データの相互関連付け、そして対応の各ステップにおいて、自動化の統合を優先することも必要です。完全な実装には時間がかかるかもしれませんが、数分で脅威を検知、相関、修復できるようになれば、リスクを低減し、レジリエンスを向上させ、規制やマテリアリティルールへの準拠を維持できます。また、面倒な手作業のインシデント対応プロセスを自動化することで、セキュリティチームから大きな負担を取り除くことが可能となり、空いた時間で、検知やハンティングのようなプロアクティブなアクションに取り組めるようになります。

CISOの皆さんにお願いしたいのはは、セキュリティチームと開発者チームの間に強い関係の醸成と両者間での定期的なコミュニケーションの機会の設定です。これらの2つのチームが緊密に連携し、互いのプロセスを理解することで、可視性、理解度、検知、および対応を改善できるようになります。この実現には、次のことが必要になります。

- セキュリティリーダーやエンジニアリングリーダーとコミュニケーションを取りつつ、このコラボレーションを推進することで、組織変革のためのアクションを呼びかける定期的なチームミーティングを開始します。
- リスクを軽減し、プロセスを改善するためのコラボレーションと自動化の必要性についての議論をリードします。
- フォローアップを行い、より迅速な脅威の検知と対応の推進に関して積極的な声を上げ続けます。

» 数分間で脅威の検知、相互関連付け、対応が行えるならば、リスクを削減し、レジリエンスを高め、規制やマテリアリティルールへの準拠を維持できるようになります。

さらに、テストから始めてベースラインを確立し、自社のSOCの現状と改善すべき点を把握することも必要です。攻撃側を演じることができるようなセキュリティチームがある場合はそのチーム、サードパーティのベンダー、またはオープンソースの機能を使用し、実際のクラウド脅威に対して組織のセキュリティインシデント対応計画をテストします。クラウド攻撃は数分で終わるため、この演習と報告には数時間以上かからないはずです。その後、対応措置とタイムラインを見直し、過剰な時間が費やされた箇所や重要な情報が見落とされた箇所を強調します。Sysdigが提供する一連の555ベンチマークガイドを参考にして、取り組みを改善し、再挑戦してください。

結論

攻撃者がイノベーションと自動化を続ける中、クラウド攻撃は、今後も驚異的なスピードで発生し続けるでしょう。そして、私たちは、そのような攻撃を阻止するための準備を整える必要があります。実務担当者や組織のリーダー向けの555ガイドに倣うことで、チームは、組織全体のセキュリティポスチャーを改善し、重大な攻撃のリスクを軽減できます。**現時点で、多くのビジネスプロセスは自動化されています。今こそ、セキュリティプロセスを自動化すべき時です。**

Sysdig Secureについて

クラウドでは、1秒1秒が重要です。攻撃は瞬時に進行します。このような条件の下で、セキュリティチームはビジネスを減速させることなくクラウド環境を保護しなければなりません。Sysdigは、ランタイムインサイトとオープンソースのFalcoを通じて、リスクの変化を即座に検知し、クラウド攻撃をリアルタイムで阻止します。また、クラウドのワークロード、アイデンティティ、サービス全体におけるシグナルを相互に関連付けることで、隠れた攻撃経路を発見し、真のリスクに優先順位を付けます。予防から防御までをサポートすることで、Sysdigは、企業にとって重要なこと、すなわちイノベーションに集中できるよう支援します。

詳細は、**sysdig.jp**をご覧ください。

デモを依頼 →

WP-010-JA REV. A 7/24