THE /555 GUIDE

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

sysdig.jp/555

sysdig SECURE EVERY SECOND.

クラウド環境が進化し、アタックサーフェスが拡大するにつれて、堅牢でタイムリーなセキュリティ対策が不可欠になります。Sysdigの「**クラウドの検知と対応における555ベンチマーク**」とは、クラウドを安全に運用するための基準を設定するものであり、セキュリティチームが10分以内に攻撃を検知 、トリアージ、対応までを完了するものです。なぜなら、攻撃者が攻撃を遂行するのにかかる平均時間が10分だからです。

Sysdig脅威リサーチチーム（TRT）が作成した「**2023年度版グローバルクラウド脅威レポート**」は、クラウド環境における攻撃のスピードと巧妙さがエスカレートしていること、そして悪意あるAIと自動化の利用により攻撃がさらに強化されていることを強調しています。今やクラウドネイティブ環境の動的な性質に特化して設計されたツールとプロセスを必要としているのです。

本ガイドでは、Sysdigが提唱する555ベンチマークがなぜ重要であるのかを説明しています。本ガイドの目的は、共通した言語と運用の方向性を通じて企業や組織による555ベンチマークの達成を支援し、クラウド脅威の迅速な検知を可能にすることです。

目次

ユーザーがプロセスを作成し、ツールを利用する

従来のSOCモデルの時代は、最新の攻撃の多さと速度には対抗できないため、終わりを告げました。アナリストが受信イベントの画面を監視し、手作業でトリアージし、チケットをエスカレーションまたはクローズアウトするという階層モデルは、クラウド攻撃に対応するには時間がかかりすぎ、かつ煩雑すぎます。SOCアナリストが活用、理解、対処するよう期待されるデータの量は、すでに持続不可能なものとなっています。.

この時点で、SOCは、どの活動や機能を自動化すべきで、どれが手作業による裁量や介入を必要とするかを見極めなければなりません。これは、SOCの個々の構造や優先事項によって異なるかもしれませんが、セキュリティプロセスの少なくとも一部に自動化を組み込まないことの言い訳にはなりません。

自動操縦で飛行機を操縦するパイロットを例に考えてみましょう。飛行機は自動操縦の助けを借りて、リアルタイムで数千タスクもの調整を行っています。パイロットは時折テレメトリーを検証し、着陸時や何か問題が発生した場合に手動操縦に切り替えます。このような飛行機の例と同様に、攻撃者より速く対応するには、組織の持つSOCは可能な限り自動化されていなければなりません。

クラウドへの攻撃者を検知してから阻止できる時間はわずか数分しかありません。このため、まずは初期対応プロセスを自動化する必要があります。そうすれば、データやイベントをフォローアップ、分析、理解する時間が増え、適切な対応や修正を見極めることができます。クラウドセキュリティの調査では、複数のサービスプロバイダー、環境、エンドポイントなどからイベントログを取得することがあります。これらのログはすべて関連している可能性がありますが、一見するとその関連性は不明確です。

クラウドへの攻撃者を検知してから阻止できる時間はわずか数分しかありません。このため、まずは初期対応プロセスを自動化する必要があります。そうすれば、データやイベントをフォローアップ、分析、理解する時間が増え、適切な対応や修正を見極めることができます。

SOCとDevOpsの専門知識を統合し、クラウドセキュリティ運用を加速する

ある意味、SOCの守備範囲をクラウドへと拡大することは痛みを生じますが、DevOpsはその任も担っています。なぜなら、DevOpsの持つ専門知識とスキルセットが、視野を拡げ、自動化を通じて、レガシー、モダン、そしてハイブリッドの運用環境におけるSOCの効率性の向上に最も貢献する可能性があるからです。

DevOpsの専門知識をSOCに取り入れることは、ことは、いくつかのメリットがあります。クラウド、SaaS、および開発プロセスに関する知識は、これらの環境に関わるイベントやインシデントに対処するために不可欠です。この別の視点によって、攻撃につながる可能性のあるテレメトリーやその他の未確認のリスクを浮き彫りにすることもできます。従来のSOCアナリストにとって、クラウドで何が通常で、何が期待されるかを特定し理解することは難しいかもしれません。なぜなら、クラウド環境では、慣れ親しんでいるものとはまったく異なる技術スタックやプロセスが必要とされるからです。Jenkinsのようなビルドソフトウェアの正常な機能を理解しているSOCアナリストがどれだけいるでしょうか？また、SOCアナリストは、異常な動作を発見する方法を知っているでしょうか？これらの質問に対する答えが「いいえ」だとしたら、どうやってSOCアナリストに学習を開始させればよいでしょうか？

2020年に発生したSolarWinds社のインシデントは、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、脅威アクター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のアナリストは、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

既存のセキュリティプロセスを高度化する

今日セキュリティ分野の専門家になることの最も困難な側面の1つとして、企業や組織が使用している環境やテクノロジーの数が非常に多く、新しいテクノロジーが採用されるペースが速いことが挙げられます。セキュリティアナリスト（ひいては組織全体）を成功に導くためには、セキュリティ部門以外のチームの専門家を、意思決定プロセスやオンボーディングプロセスに参加させる必要があります。これには、新しいデータソースをSOCに追加することも含まれます。

たとえば、Kubernetesの保護と監視を適切に行うには、実装プロセスにDevOpsチームとアプリケーションチームを含める必要があります。彼らのインプットがなければ、SOCはKubernetesとそれがホスティングするアプリケーションから発生するイベントを理解し適切に対処するのに苦労することになるでしょう。一方、開発者はこれらの技術を熟知しています。そのようなクラウドとワークロードのセキュリティプロセスの開発に特定分野の専門家を参加させることで、共通の理解が生まれます。つまり、セキュリティアナリストだけでなく、DevOpsやアプリケーション開発者も、SOCが必要とするものとその理由を理解できるようになるのです。これらのチームが新しいシステムやソフトウェアを導入する際のチェックリストや共通基準を確定することで、このようなコラボレーションを形式化できます。

そして、このコラボレーションにより、SOCチームは自分たちが何を調べているのかをより深く理解できるようになるため、イベントやインシデントにより迅速に対応できるようになり、また誰が何を所有しているのかを把握できるようになります。調査やインシデント対応では、何が問題なのか、そして誰に助けを求める必要があるのかを判断するのに多くの時間が浪費されます。たとえば、Kubernetesワークロードの保護と監視においては、ネームスペースの整理とタグ付けを通じた明確な識別が、調査と対応の簡素化と迅速化に役立ちます。

たとえば、Kubernetesの保護と監視を適切に行うには、実装プロセスにDevOpsチームとアプリケーションチームを含める必要があります。彼らのインプットがなければ、SOCはKubernetesとそれがホスティングするアプリケーションから発生するイベントを理解し適切に対処するのに苦労することになるでしょう。

包括的な対応をあらかじめ決めておく

従来、インシデントが発生した場合の最初の対応は、イーサネットケーブルを抜くことでした。この解決策はオンプレミスでは効果的ですが、クラウド環境に導入されている新しいテクノロジーやサービスでは、そのような簡単な解決策が存在することは稀です。今や、戦略的にすべてをシャットダウンするのではなく、より戦術的なアプローチが標準となっています。クラウド環境では隔離手法を自動化することが可能であるため、セキュリティチームにとっては、隔離が自動的に実施される際の基準をあらかじめ定義しておくことが重要です。

事前に定義された基準を設定し、それに従うことで、承認されていないプロセスを実行しているマシンや不明なIPと通信しているマシンなど、特定のリスクの高いアクティビティをインシデント対応のために自動的に隔離できます。たとえば、Kubernetesノードやクラスター全体を強制終了する代わりに、単一のコンテナを自動的に強制終了または一時停止することで対応を開始し、インシデントを隔離できます。このような戦術的な対応策を講じることで、企業はある程度通常通りビジネスを継続できる可能性があります。ただし、実装する前に、アクションの広範な影響に関する新たな 知識と先見性も必要となります。また、利用可能なオプションが多すぎることが理由で、経験の浅いチームメンバーにとっては、適切な対応が分かりにくくなる可能性もあります。

よく練られた対応計画は、インシデント対応に直接関与する人々によって組織化され、調整されるでしょう。インシデント対応計画には、セキュリティ担当者、開発者、シニアリーダー、およびその他の関連部門間のコミュニケーションチャネルとコラボレーションを含めなければなりません。すでに計画が策定されている場合であっても、今こそ計画を見直し、必要に応じて改善すべき時です。まずは最新のクラウド攻撃への対応に必要なスピードに対応できるかどうかを判断するための演習から開始し、対応できない場合は、プロアクティブな軽減策が取れるように計画を調整する必要があります。また、555ベンチマークによると、標準化された報告テンプレートをはじめ、すぐに利用できるコミュニケーションチャネル、さらにはインシデント対応プロセスを合理化するための自動化も含める必要があります。

まずは最新のクラウド攻撃への対応に必要なスピードに対応できるかどうかを判断するための演習から開始し、対応できない場合は、プロアクティブな軽減策が取れるように計画を調整するようにしましょう。

そして、対応プロセスには、環境問題をよりよく理解するために、DevOpsのような開発の専門知識を持つチームメンバーも含める必要があります。対応の意思決定において彼らを含めるのは現実的ではないかもしれませんが、プロセスの開発には彼らもチームとして参加させるべきです。

セキュリティチームは、インシデントに即座に対応できるように準備しておく必要がありますが、インシデント発生後の組織全体での情報共有も同様に重要です。開発者とエンジニアが関与するインシデント発生後のワークフローによって、環境全体にわたる徹底的な修正のための包括的なデータ共有が保証されます。

クラウド攻撃者はすでにプロセスを自動化している

SCARLETEELはランタイム環境とクラウド環境をまたいで行われた攻撃であり、わずか数分（正確には3分42秒）で発生し、プロプライエタリなデータが失われる結果となりました。この攻撃を検知し、阻止できた可能性のあるポイントは複数ありますが、攻撃は各ポイントで非常に速く発生しました。たとえばランタイム環境では、攻撃者はEC2のIMDSエンドポイントから認証情報を盗むためにcurlを使用しました。これはかなり一般的な行為ですが、盗まれた認証情報は、クラウドアカウント全体への読み取り専用アクセスを提供する過剰なアクセス許可ポリシーを持っていました。堅牢な検知ツールであれば、コンテキストにおいて、これを「危険な」ポリシーとして理解し、SOCアナリストに対してアラートを発行するはずです。そして、アラートを受け取ったSOCアナリストは、危険性を即座に理解し、それを軽減するための作業が行えたでしょう。

クラウドはスピードとシンプルさを追求するために構築されたものであるため、攻撃者が自動化に大きく依存しているのは理にかなっています。SCARLETEELの攻撃者はクラウドにアクセスすると、自動化されたスクリプトを実行して偵察を行いました。偵察はしばしば非常にノイズの多いプロセスですが、この例が特に奇妙だったのは、使用されたIDがEC2インスタンスに属していたことです。攻撃者は、過剰な権限を持つ認証情報を悪用することで、環境内でラテラルムーブメントを実施しました。あなたの会社でお使いの検知テクノロジーは、この動きを理解し、2つのイベントを相互に関連付けることができるでしょうか？もしそれができない場合、迅速で効果的な対応は不可能になります。なぜなら、これらの情報がすべて手動で収集されるまでに、攻撃は完了してしまうからです。

上記の例を読んで、攻撃を時間内に止めることは不可能だと思われるかもしれません。しかし、攻撃者が活用する同じテクノロジーは、私たちに迅速効果的な対応アクションをもたらす可能性があります。クラウドのスピードとシンプルさをスケールメリットとして活用できるのは攻撃者だけではありません。攻撃者が最初に過剰な権限を持つ認証情報を窃取した際に、アナリスト（または最先端のテクノロジーがお好きな場合は「自動化されたプロセス」）を使ってポリシーにおける権限を引き下げることができたならば、その結果として、効果的な隔離を実施することで、攻撃全体を防ぐことができたはずです。また、攻撃者の偵察段階でも、同じことが可能だったはずです。あるいは、影響を受けたEC2インスタンスにセキュリティグループポリシーを割り当てることで、すべてのネットワークアクセスを遮断することも可能だったはずです。クラウド対応アクションで防御者が利用できるオプションは、従来のEDRツールが提供するものよりもはるかに広範でありかつ的確です。

既存のツールを新しいツールで補完することで最大限の可視性と応答速度を実現

クラウド攻撃を迅速に検知してそれに対応するためには、環境全体にわたって完全に統合された協調的な技術スタックが必要です。検知の隙間や遅れは許されません。今や私たちは、常に新しい革新的なクラウドの戦術や手法から自らを守る必要があります。SOCがその防御ポスチャーにおいてより革新的であるべき時期はとうに過ぎています。

最先端のツール

最新の課題には最新のツールが必要です。リーダーは、既存のエコシステムと統合し、クラウドネイティブのワークロードとデータを安全に保つためのコンプライアンスと技術的要件を満たすツールとプラットフォームを検討しなければなりません。CNAPPやCDRツールは、コンプライアンス関連のチェックボックスを提供するだけでなく、従来の検知と対応を拡張する共通のプラットフォームを提供します。また、これらのツールを使うと、セキュリティチームと非セキュリティチーム（法務、人事、エンジニアなど）の両方を巻き込むことで、責任共有モデルを構築できます。これらのチームは、予期せぬリスクをより的確に把握し、新たな脅威に対処する準備を整えることができます。

現在、検知と対応は、組織が持つ環境との永遠の共進化状態にあります。オンプレミス環境では、脅威を効果的に検知し、調査し、それに対応するために、数ある専門ツールの中でも、SIEM（セキュリティ情報およびイベント管理）、IPS/IDS（侵入検知システム/侵入防御システム）、EDR（エンドポイント検知および対応）が必要でした。組織環境における次なる進化は、クラウドネイティブです。クラウドネイティブは、スピード、コスト、拡張性、イノベーションにおいて飛躍的な向上を組織にもたらします。しかし、こうした進化に伴い、セキュリティチームは、データ量の急激な増加、エフェメラル型のワークロード、攻撃の高速化、複雑なコンプライアンスシナリオといった課題に直面しています。

CNAPPやCDRツールは、従来の検知と対応を拡張する共通のプラットフォームを提供します。また、これらのツールを使うと、セキュリティチームと非セキュリティチーム（法務、人事、エンジニアなど）の双方を巻き込むことで、責任共有モデルを構築できます。

インシデント対応中にログインしなければならないダッシュボードの数は、より少ない方が好まれます。異なる機能にアクセスするために、複数のウィンドウで複数のツールにログインしなければならないのは、時間がかかりすぎて不便だからです。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）のようなワンストップショップを利用することで、組織のセキュリティプロセスと相互関連付け機能を合理化する必要があります。CNAPPはクラウドネイティブの必要性から生まれたプラットフォームであり、ランタイムセキュリティを標準としています。CNAPPは、複数のソース間でほぼリアルタイムにイベントを相互に関連付け、情報を理解しやすい形式に仕上げた後、すべてひとつの場所で提供します。攻撃経路を可視化することで、対応アクションを加速できるほか、ユーザーはクリックやスクリプトを実行することなく、ワークロードの設定と脆弱性のステータスを即座に確認できるようになります。

このため、セキュリティチームは本番環境に導入されている何百、何千ものコンテナやその他のワークロードを含む環境全体の可視性とコンテキストを必要としています。クラウド脅威検知は、ワークロードのランタイムセキュリティだけでなく、クラウドサービス、人間およびマシンのアイデンティティ、ソフトウェアのサプライチェーンをもカバーしています。CNAPPは、可視性を高めるだけでなく、セキュリティチームが自動化されたポリシー実施、リスク認識、コンプライアンスなどを利用できるようにすることで、より優れたセキュリティ制御を提供します。

古典的なツール

クラウド検知の技術スタックには、すでにおなじみの名前がいくつか含まれているでしょう。例としては、データ集約のためのSIEM、クラウドアイデンティティコンテキストのためのCIEM（Cloud Infrastructure Entitlement Management）、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のためのSOAR、コンテキスト、根本原因の分析、欠陥を発生源から修正する方法を理解するためのCSPM（Cloud Security Posture Management）機能などが挙げられます。

第1に、SIEMがセキュリティの脅威や脆弱性が業務に支障をきたす前に検知するためには、SIEMは関連するデータにアクセスできなければなりません。しかし、ネット上に出回っている多くのミームによれば、それを可能にするためのコストが常に金銭的に支払い可能である額とは限らないことが分かります。第2に、SIEMは受信しているデータを理解する必要がありますが、新しいアプリケーションやサービスがオンラインになると、SIEMのデータ取り込みやパーシングが一定の水準に達していることが常に保証されるとは限りません。また、これはそもそも、必要なデータをSIEMに送信できることを前提としています。

クラウド環境では、開発者にとっても攻撃者にとっても、権限が何よりも重要となります。CIEMやCSPMのようなツールは、付与された権限、それらが利用される範囲、それらが実際にどれほどセキュアであるかに関するインサイトを提供できます。これらのツールは、SIEMとの相互作用に加えて、新しいデータ用に構築された検知の内容と、このデータを素早く適切に理解できるルールエンジンを備えている必要があります。これはすべて、「検知と対応」における「対応」の取り組みよりも前に実施される必要があります。

クラウド脅威の検知と対応を迅速に行うためには、自動化が鍵となります。この目標は、SOARを使用することで達成できます。SOARはCNAPPと同様に、2017年頃に出現したソリューションであり、一連のテクノロジーを単一のプラットフォームコンセプトへと統合したものです。SOARを使うと、セキュリティ脅威の自動検知、調査、軽減を通じて、セキュリティ運用の合理化を支援できます。クラウド攻撃のスピードを考慮するならば、今こそSOARをSOCに導入すべき時です。

俊敏性の向上

クラウド攻撃をリアルタイムで検知して対応するには、ツールだけでは不十分です。新しいスキル、最新の展望、洗練された手際の良さなど、セキュリティに関する新しい考え方を取り入れる必要もあります。

555ベンチマークは、クラウドセキュリティの俊敏性に関する新たな基準を設定しており、これは現時点でクラウドネイティブ環境と脅威が持つスピードと調和したものとなっています。企業や組織にプラクティショナーとして勤めている方には、クラウドセキュリティのコラボレーション、ツール、そしてプロセスを改善するための指針として、このベンチマークを採用することをお勧めします。

たとえば、潜在的なインシデントに関するアラートを受信した後、アナリストがアラームを発行するまでにどれくらいの時間がかかるでしょうか？また、セキュリティチームが、最初のイベントに関連する可能性のあるデータを見つけ、同データを相互に関連付け、何が起きているかを説明するのに、どれくらいの時間がかかるでしょうか？さらに、真陽性と判定された後、どのような対応策を、どれくらいの速さで実施できますか？誰に通知し、誰がインシデントをサポートするのでしょうか？これらの質問に対する答えが「数時間または数日間」である場合、あなたの会社が採用しているインシデント対応の取り組みには、徹底的な見直しが必要です。

555ベンチマークは、セキュリティの上層部との積極的なコラボレーションを通じて、クラウド脅威の検知と対応の課題に対応するために計画を策定する機会を提供します。まず、確立したプロセスとタイムラインを決定することからこの課題に取り組みましょう。模擬インシデントを発生させ、現在の対応計画に従って対応することで、これらのプロセスをテストし、評価します。社内のレッドチームや侵入テスターを利用できるか、あるいはサードパーティのレッドチームや侵入テスターを雇う能力がある場合は、それらを利用してこれらの攻撃を開始します。また、サンドボックス内で安全に攻撃を開始する方法を紹介したオープンソースのPoCもあります。テスト後に報告会を行い、参加者全員が足並みを揃えて、プロセスの改善とテストを継続できるようにします。得られた結果をセキュリティチームやCISOとレビューし、本稿で示したように修正と改善を行います。迅速性と俊敏性を備え、自動化にも対応し、かつ十分な情報を与えられたチームを作り上げることで、戦闘準備を整え、最終的に攻撃者の攻撃機会を事前に奪うことが可能となります。

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-011-JA REV. A 7/24