クラウドネイティブに潜むセキュリティ上の脅威を可視化！安心のクラウドネイティブセキュリティと万全のSoC運用を「Sysdig」と「Splunk」の連携で実現

講演のポイント

講演の概要

- Sysdig社公開「2022年版クラウドネイティブセキュリティと利用状況レポート」から「Sysdig」と「Splunk」の連携運用による安全性を担保する概要を紹介

講演のまとめ

- コンテナ/Kubernetesといった新しい技術要素において、従来型の境界型防御やシグネチャ型のマルウェアスキャンだけでは安全性は担保できず、毎日数万件の深刻度の脆弱性が顧客システム環境で発見されており、設定ミスも多く存在する
- WireSharkの創作者が開発した「Sysdig」がコンテナに潜む脆弱性の発見、不正アクセスやサイバー攻撃などの異常検知、コンテナ制御でフルフォレンジックも実現
- あらゆるログの統合管理と相関分析を実現する「Splunk」と「Sysdig」を連携利用することで、コンテナを含めシステム全体のセキュリティ課題を可視化して対応可

紹介製品

sysdig コンテナ向けSaaSセキュリティ

splunk> あらゆるログの相関分析で脅威対策

SCSK株式会社は、2022年10月4日（火）にJPタワーカンファレンスで開催された「SecurityDays Tokyo Fall 2022」において、Sysdig社が公開した「2022年版クラウドネイティブセキュリティと利用状況レポート」による、クラウドネイティブアプリケーションに潜む脅威概要と適切な対策について説明を行った。

本番環境にそのまま放置される脆弱性

Sysdig社では毎日数万件の脆弱性がお客様のクラウドネイティブアプリケーション環境において発見できており、実環境で動作するイメージの85%で、すでに対策用のパッチがリリースされていながらも、なんら適用されずにそのままの状態にされていることが確認できている。
特にその脆弱性の75%のイメージには、深刻度、「高」または「重大」といったレベルの脆弱性も含まれており、Sysdig社は「非常に由々しき事態である」と指摘をした上で 深刻度「高」または「重大」といったレベルの問題だけに限定しても、「すべてを修正することは不可能である」と言及している。

「リスクを見極めながらこの問題にしっかり優先順位をつけて対処するべきだ」と警告されている。

rootのまま実行されるコンテナ権限

コンテナイメージの76%が実はrootのまま実行されており、特権的なコンテナとして実行されていることからセキュリティ上の脅威にさらされている状況になっている。
この点について一般には脆弱性スキャンはその必要性は理解されているが、脆弱性スキャンではrootのまま実行といった設定ミスは把握できないことから、脅威がいつまでも内包されている状況が続き、非常に危険であるということが言える。
この原因はコンテナイメージを本番環境にプッシュする

sysdig splunk>

講演者プロフィール

SCSK

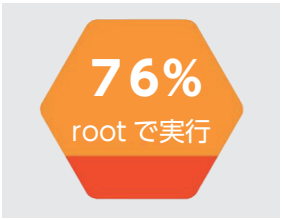
社　　名：SCSK株式会社
（コード番号 9719 東証プライム市場）
本社所在地：東京都江東区豊洲3-2-20
設　　立：1969（昭和44年）年10月25日
資 本 金：21,285百万円
従業員数：14,938名（2022年3月現在）
事業概要：コンサルティングからシステム開発、検証サービス、ITインフラ構築、ITマネジメント、ITハード・ソフト販売、BPOまで、ビジネスに必要なすべてのITサービスをフルラインアップでご提供
U　R　L：https://www.scsk.jp/

SCSK株式会社
ITエンジニアリング事業本部
ミドルウェア営業部 第一課
姜 来誠

SCSK株式会社
ITエンジニアリング事業本部
ミドルウェアソリューション部 第一課
川杉 喜彦

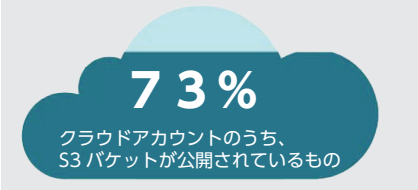
SCSK株式会社
ITエンジニアリング事業本部
ミドルウェアソリューション部 第四課
大竹 雄樹

前に、開発者がパーミッションを正しく設定することを忘れていることが主な原因といえ、このような設定問題に起因する脅威は全く減っておらず、逆に昨年度より31%も増加している状況になっている。



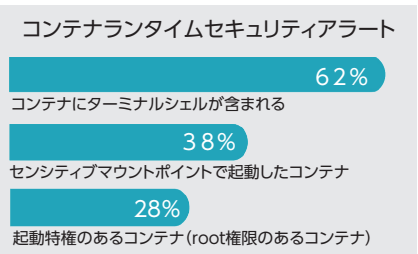
設定ミスはコンテナだけでない。クラウドアカウントにもある

クラウド・アカウントの73%にデータを危険にさらす可能性があるS3バケットが公開されているということが判明している。
この原因として、例えばAWSの場合はデフォルトではパブリックアクセスを無効にした状態でバケットが作成されるが、一時的なテストや長期的な使い勝手の良さからこの設定を変更することがあるため、変更したままの状態で放置されたりしているケースがあるのではないかとSysdig社は指摘している。



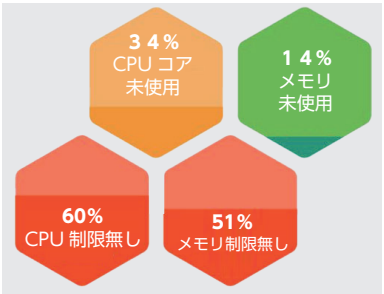
ルールセットに違反するコンテナアクティビティ、コンテナ・ランタイム

後述するSysdig製品では、振る舞い検知ソフトウェアに『Falco(ファルコ)』が利用可能であり、このFalcoでセキュリティ・アラートが定期的に受け取れる。このFalcoで最も多い62%のアラートが、コンテナ内にターミナルシェルを検出をしていることで、これは改ざんのリスクが非常に高まっているということを示すものである。更に検出で38%と2番目に多いのが、機密性の高いマウントポイントで起動されたコンテナが検出されているという点で、これはコンテナ自体がホスト上の重要なファイルを変更できるということを意味している。
さらに28%と3番目に検出されているのが、お客様の環境においてホストマシンへのルート権限を持ったコンテナが存在しているといった状況がある。



Kubernetesの不適切なキャパシティプランニング

約60%のコンテナでCPUの制限が定義されていない。そして51%でメモリー制限も無いことが判明している。さらにはCPUに制限があったクラスターでも、平均34%のCPUコアが未使用であったという報告がなされている。
これらの情報から、Kubernetesのようなダイナミックな環境において、キャパシティマネジメント、キャパシティプランニングが困難であるという点が挙げられる。



2022年版クラウドネイティブセキュリティと利用状況レポートのまとめ

本レポートにおいては、今後のコンテナ利用における重要なポイントを以下3点で締めくくっている。

『権限管理の重要性の認識』
クラウド、コンテナの導入が進むと、コンテナがrootとして実行されたり、クラウド・アカウントに過剰な権限が与えられたりということが発生している。これは安全性に欠ける行動が多く発生してしまうことであり、権限管理は極めて重要であるということが言える。よってデータの機密性と特定のユースケースに基づいてアクセスを管理するとともに最小特権の原則の遵守が必要である。

『ランタイムの脅威検知の重要性』
如何に堅牢なプログラムであってもすべての脆弱性や設定ミスの対処はできない。よってクラウドやコンテナのセキュリティを確保する上で、『ランタイムの脅威検知』は重要なポイントであり、クラウドネイティブな機能を成熟させるにつれ、安全でないビヘイビアを排除、または削減するようにすることが必要である。

『Kubernetes環境ではキャパシティ・プランニングは難しい』
適切なコンテナリソース制限、そして継続的なモニタリングの仕組みがあって、初めてクラウド事業者への過剰なペイメントの防止や、アプリケーションのパフォーマンス問題といったものを回避できるということが言える。よって必要に応じてコンテナへのリミットを設けたり、Kubernetesリソースを注意深く管理しなければならない。

レポートのまとめから言える、解決に最適な「Sysdig」

コンテナ環境の統合モニタリング&セキュリティプラットフォームである「Sysdig」は、前項のコンテナ利用における重要なポイントの解決に繋がる製品である。
「Sysdig」はネットワークアナライザの筆頭であるWiresharkの創作者によって開発された製品で、「Sysdig」の特長としてコンテナのモニタリングに長けており、数十、数百、数千と言ったコンテナの内部のアプリケーションやKubernetesやOpenShiftといったコンテナプラットフォーム、AWSといったマネージドKubernetesの利用状況やコンテナ間通信も可視化も可能である。更にセキュリティへの対応としてコンテナに潜む脆弱性の発見、不正アクセスやサイバー攻撃の検知、異常の検知を実現できるほか、Kubernetesのログを全て完全な形で保存が可能なため、フルフォレンジックもサポートする。

「Sysdig」と「Splunk」の統合利用でセキュリティの課題を完全に払拭

ログを統合管理するためのプラットフォーム「Splunk」は、多種多様のログデータを集約、蓄積してシステムを横断した相関分析を実現する。
「Splunk」の特長としてログの正規化が不要でどんなログもすぐに取り込み可能な点や標準搭載のコマンドで簡単に分析が可能な点、インフラを拡張することで容易なスケールアップが可能な点である。

この「Splunk」は前述の「Sysdig」と統合利用が可能であり、「Sysdig」と「Splunk」を利用することでコンテナを含めシステム全体のセキュリティの課題を可視化する。ゆえにクラウドネイティブセキュリティへの対応を容易に実現する。

製品および記載内容に関するお問い合わせ

SCSK株式会社
https://www.scsk.jp/

ITエンジニアリング事業本部 ミドルウェア営業部
〒135-8110 東京都江東区豊洲3-2-20 豊洲フロント

Sysdigお問い合わせ：sysdig-sales@ml.scsk.jp
Sysdig製品情報 https://www.scsk.jp/sp/sysdig/
Splunkお問合わせ：splunk-sales@ml.scsk.jp
Splunk製品情報 https://www.scsk.jp/sp/splunk/

Sysdig 製品情報

Splunk 製品情報