GuardDutyによる コンテナランタイム脅威検知のすべて

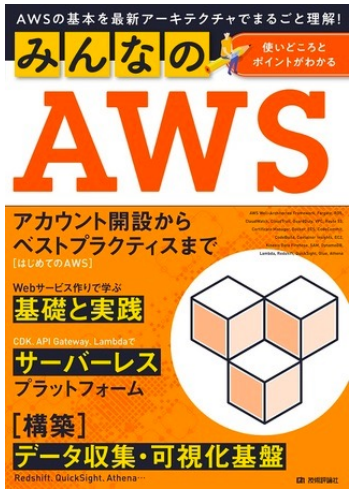
～その凄さと設定注意点と検知の様子をまるっとお届け～

濱田孝治（ハマコー）

About me

濱田孝治（ハマコー）

- @hamako9999
- 最近の流行
  - ランニング
    - フロストバイトロードレース（ハーフ）
    - さいたまマラソン（フル）
  - サイバーパンク2077 仮初めの自由
  - Cities Skylines2
    - このゲームめっちゃ重いので、誰かGeForce RTX 4070下さい



みなさんあの日の
感動と興奮を覚えていますか？

NEW

Container runtime threat detection for GuardDuty

COMING SOON


これはre:Invent
2022
の出来事です

遥かなる時を経て2023年11月26日リリース！！

AWS News Blog

Detect runtime security threats in Amazon ECS and AWS Fargate, new in Amazon GuardDuty

by Sébastien Stormacq | on 26 NOV 2023 | in Amazon Detective, Amazon Elastic Container Service, Amazon GuardDuty, Announcements, AWS Fargate, AWS re:Invent, Launch, News | Permalink | Comments | Share

0:00 / 0:00

Voiced by Amazon Polly

Today, we're announcing Amazon GuardDuty **ECS Runtime Monitoring** to help detect potential runtime security issues in Amazon Elastic Container Service (Amazon ECS) clusters running on both AWS Fargate and Amazon Elastic Compute Cloud (Amazon EC2).

GuardDuty combines machine learning (ML), anomaly detection, network monitoring, and malicious file discovery against various AWS data sources. When threats are detected, GuardDuty generates security findings and automatically sends them to AWS Security Hub, Amazon EventBridge, and Amazon Detective. These integrations help centralize monitoring for AWS and partner services, initiate automated responses, and launch security investigations.

ref: https://aws.amazon.com/jp/blogs/aws/introducing-amazon-guardduty-ecs-runtime-monitoring-including-aws-fargate/

世界が注目、そして待望していた
コンテナランタイム脅威検知を
皆さんにお届け

Agenda

- Container runtime threat detectionとは
- 動作イメージ
- 設定方法と設定上の注意点
- 実際に脅威を検出してみた
- まとめ

Container runtime threat detectionとは

Container runtime threat detectionとは

GuardDutyの新機能としてECS Runtime Monitoringが提供

- 実行中のECSタスクにおいて、ランタイムの脅威を示す可能性のあるイベントを検出
- GuadDutyに集約されるので、他のセキュリティ脅威と合わせて包括的に脅威情報を集約し管理可能
- ECS on FargateはGA（今日の話は全部こちら）
- ECS on EC2はPreview

実際になにが検出されるのか？

GuadDuty:Runtime Monitoring finding types

- 通常ではないネットワークトラフィック
コンテナからの予期しないアウトバウンド接続。
- ポートスキャン活動
コンテナが他のシステムやサービスのポートをスキャン。
- 既知の悪意のあるIPまたはドメインへのアクセス
コンテナが既知の悪意あるIPやドメインと通信。
- 予期せぬデータ量やパターン
データ転送量やパターンの大幅な変化。
- 疑わしいファイルやプロセスの活動
コンテナ内での通常ではないファイルの変更やプロセスの実行。
- 異常なユーザー行動
コンテナ内からの通常ではないログインパターンや特権昇格試み。
- 侵害されたコンテナイメージ
既知の脆弱性がある、または悪意のあるコンテナイメージの使用。
- 暗号通貨マイニング
CPUまたはGPU使用率の予期しない急増。
- コマンド＆コントロール（C&C）通信
既知のC&C通信プロトコルに一致するトラフィックパターン。
- リバースシェルまたは不正なリモートアクセス

なにが嬉しいのか？

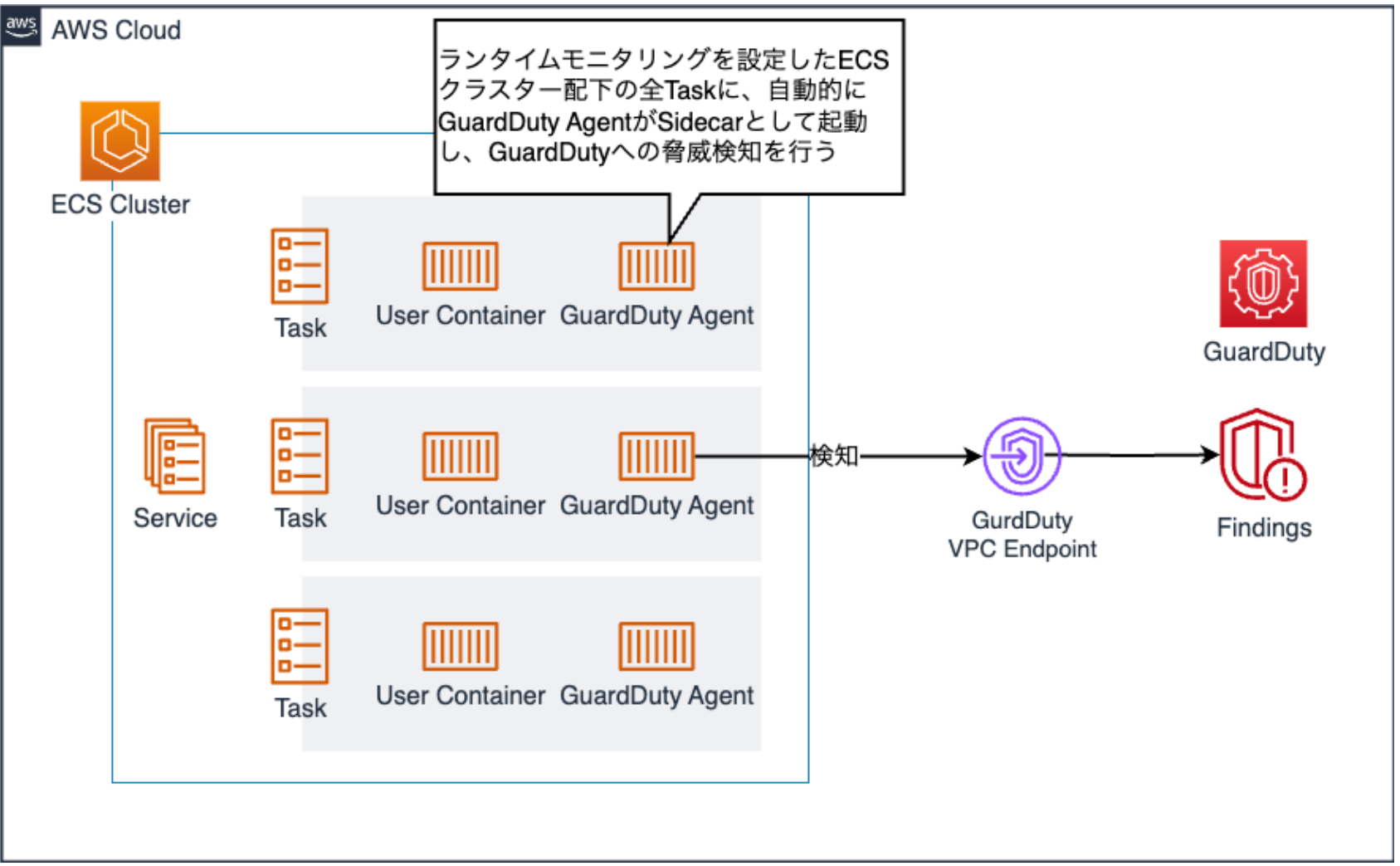
これまでは、実行中のECSタスクのランタイム脅威検知にはそれなりに高価な商用製品の導入が必須だった

- ex. Sysdig, aqua, dynatrace
- aquaは、脅威検知後のコンテナ保護機能などもあり

AWSマネージドな仕組みだけでこのランタイム検知ができるようになったのは素晴らしい進化！

動作イメージ

動作イメージ



- 設定はクラスター単位で実施（配下の全サービスが対象）
- タスク起動時にフルマネージドなGuardDutyサイドカーコンテナが自動的に起動し、検出した脅威のGuadDutyへの通知を実施

設定方法と設定上の注意点

設定はめちゃくちゃ簡単

安易にやるとめちゃくちゃ
影響範囲が大きくなります

設定時間30秒、影響範囲はリージョン全部

GuadDuty -> ランタイムモニタリングを開いて
「ランタイムモニタリング」を有効
「AWS Fargate」を有効
にするだけ

これだけで、設定したリージョンの全てのECSクラスターが検出対象になる

ランタイム脅威検知で利用するリソースと料金 19

検出対象になったクラスターで注意しておくべき代表点

- ECSタスクのリソース
  - ECSタスク定義はそのままの場合、設定したリソースを追加されるGuadDuty用のサイドカーコンテナが利用するので、注意が必要（CPU and memory limits）
- サイドカーコンテナの料金
  - 超ざっくりで4%ぐらいのコスト増
  - 参考：Intelligent Threat Detection – Amazon GuardDuty Pricing
- 一度設定すると、今後作成する全てのクラスターが上記の影響を受けることも注意

ECSクラスターを設定対象外にする方法

クラスターに事前に以下のタグを付与しておく

- Key:GuardDutyManaged
- Value:false

プロダクション環境などで設定する場合は、意図せぬところに影響が出ないように注意

実際に脅威を検出してみた

実際に検出してみないと
やっぱりねぇ、実感がわかないよねぇ

検出対象にしてみた脅威

GuadDuty:Runtime Monitoring finding types

- 通常ではないネットワークトラフィック
コンテナからの予期しないアウトバウンド接続。
- ポートスキャン活動
コンテナが他のシステムやサービスのポートをスキャン。
- 既知の悪意のあるIPまたはドメインへのアクセス
コンテナが既知の悪意あるIPやドメインと通信。
- 予期せぬデータ量やパターン
データ転送量やパターンの大幅な変化。
- 疑わしいファイルやプロセスの活動
コンテナ内での通常ではないファイルの変更やプロセスの実行。
- 異常なユーザー行動
コンテナ内からの通常ではないログインパターンや特権昇格試み。
- 侵害されたコンテナイメージ
既知の脆弱性がある、または悪意のあるコンテナイメージの使用。
- 暗号通貨マイニング
CPUまたはGPU使用率の予期しない急増。
- コマンド＆コントロール（C&C）通信
既知のC&C通信プロトコルに一致するトラフィックパターン。
- リバースシェルまたは不正なリモートアクセス

ECS ExecでFargateにログインして
コマンド実行

```
$ yum -y install bind-utils
$ dig pool.supportxmr.com +short
```

暗号通貨関連ドメイン pool.supportxmr.comへのDNSクエリ。これはほぼ確実に毎回出る。

他にも同じような挙動をするドメインがあるかどうかChatGPTに聞いてみたら、それは教えられないよ、と言われました。

参考にしたブログ

GuardDutyのEC2タイプFindingsを簡単に検知させる方法 – CryptoCurrency編

https://dev.classmethod.jp/articles/guardduty-findings-test-cryptocurrency/

Execution:Runtime/NewBinaryExecuted


```
$ dig example.com +short
93.184.216.34

$ yum install -y nmap

$ nmap -Pn -p 80,443 93.184.216.34
Starting Nmap 6.40 ( http://nmap.org ) at 2023-12-09 16:34 JST
Nmap scan report for 93.184.216.34
Host is up (0.11s latency).
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 0.57 seconds
```

インストールしたバイナリ実行の脅威が検知。

Nmapコマンド使っているので、ポートスキャン脅威がでるかと思いきや、ここでは、新バイナリの実行の脅威で検知されていた

実際の画面を見てみましょう

検出した後の運用をどうするか

設定したは良いが、実際に検出されたときの運用も考えておくのが大事

- Managing Amazon GuardDuty findings - Amazon GuardDuty
  - 公式ドキュメント。運用についての詳細が記載されてある
- [2021年版]Amazon GuardDutyによるAWSセキュリティ運用を考える | DevelopersIO
  - セキュリティHero、臼田の記事
- Amazon GuardDuty ECS Runtime Monitoringで脅威を検出したECSタスクを自動停止してみた | DevelopersIO
  - トクヤマシュンによる脅威検知対象ECSタスクの自動停止

まとめ

- ECSにおけるコンテナランタイム検知がマネージドな仕組みだけでできるようになったので大いに活用の余地あり！
- 設定は異常に簡単だが影響範囲が大きいため、事前の計画は必須
- コンテナセキュリティ全般は、ビルドプロセスにおけるイメージスキャンやIAMの最小権限の方策などと合わせて包括的に対処しましょう！

皆さんのECS環境
よりセキュアに安全に
使っていきましょう！