【AWS Black Belt Online Seminar】

Amazon GuardDuty

Intelligent Threat Detection in the AWS Cloud

Tomoaki Sakatoku, Partner Solutions Architect
Amazon Web Services Japan

Who I am…

酒徳 知明 (Tomoaki Sakatoku)

Partner Solutions Architect

- Ecosystem
- DevSecOps

内容についての注意点

- 本資料では2018年5月9日時点のサービス内容および価格についてご説明しています。最新の情報はAWS公式ウェブサイト(http://aws.amazon.com)にてご確認ください。
- 資料作成には十分注意しておりますが、資料内の価格とAWS公式ウェブサイト記載の価格に相違があった場合、AWS公式ウェブサイトの価格を優先とさせていただきます。
- 価格は税抜表記となっています。日本居住者のお客様が東京リージョンを使用する場合、別途消費税をご請求させていただきます。
- AWS does not offer binding price quotes. AWS pricing is publicly available and is subject to change in accordance with the AWS Customer Agreement available at http://aws.amazon.com/agreement/. Any pricing information included in this document is provided only as an estimate of usage charges for AWS services based on certain information that you have provided. Monthly charges will be based on your actual use of AWS services, and may vary from the estimates provided.

Amazon GuardDuty

Intelligent protection of your
AWS accounts and workloads

Generally available
today

AWSセキュリティサービスの整理

発見的統制 - Detective Control

CloudWatch

- AWSサービスのリソース モニタリング
- ログモニタリング (CloudWatch Logs)
- プロアクティブ モニタリング (CloudWatch Events)

CloudTrail

- 呼び出されたAPIに関するイベントを継続的にロギング
- コンプライアンスの簡素化
- セキュリティの自動化

NEW!

GuardDuty

- セキュリティ脅威リスクを検知・可視化
- 悪意のあるIPアドレス、異常検出、機械学習などの統合脅威インテリジェンスを使用した脅威検知

What is Amazon GuardDuty ?

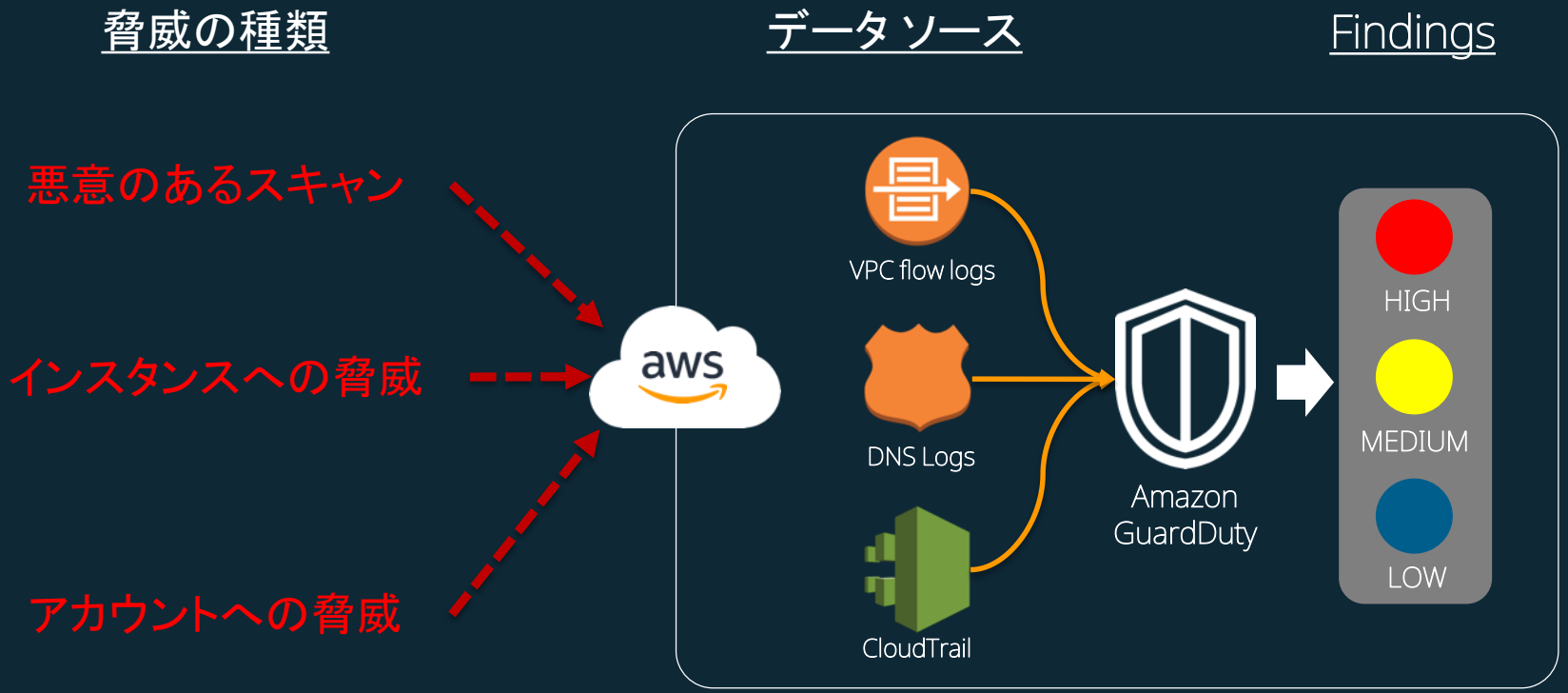
Amazon GuardDuty

- セキュリティの観点から脅威リスクを検知するAWSマネージド・サービス
- 分析のソースには下記を利用し、メタデータの連続ストリームを分析
  - VPC Flow Logs
  - AWS CloudTrail Event Logs
  - DNS Logs
- 悪意のあるIPアドレス、異常検出、機械学習などの統合脅威インテリジェンスを使用して脅威を認識

Amazon GuardDuty

- AWS環境における、脅威検出を目的としたマネージドサービス
- 機械学習による、異常検知の仕組み
- 東京含む、15のリージョンで利用可能
- エージェント、センサー、ネットワーク アプライアンス等は不要
- EC2またはIAMにおける脅威を検出
- エコシステムの充実
- シンプルなコスト体系と30日間の無料枠

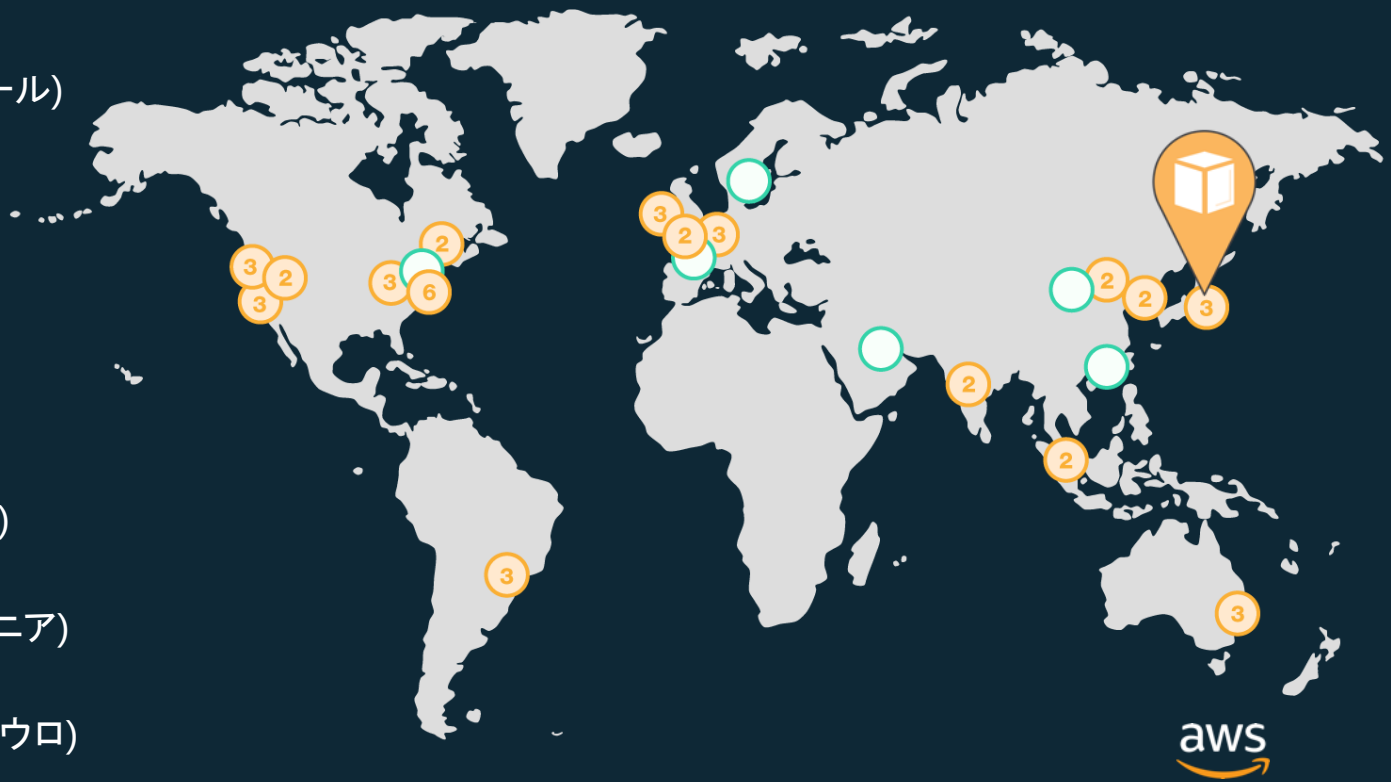
GuardDuty による脅威の検知



Amazon GuardDuty - 利用可能なリージョン

東京リージョンでもご利用頂けます！

- Asia Pacific (ムンバイ)
- Asia Pacific (ソウル)
- Asia Pacific (シンガポール)
- Asia Pacific (シドニー)
- **Asia Pacific (東京)**
- Canada (セントラル)
- EU (フランクフルト)
- EU (アイルランド)
- EU (ロンドン)
- EU (パリ)
- US East (北バージニア)
- US East (オハイオ)
- US West (北カリフォルニア)
- US West (オレゴン)
- South America (サンパウロ)



Amazon GuardDuty の利用

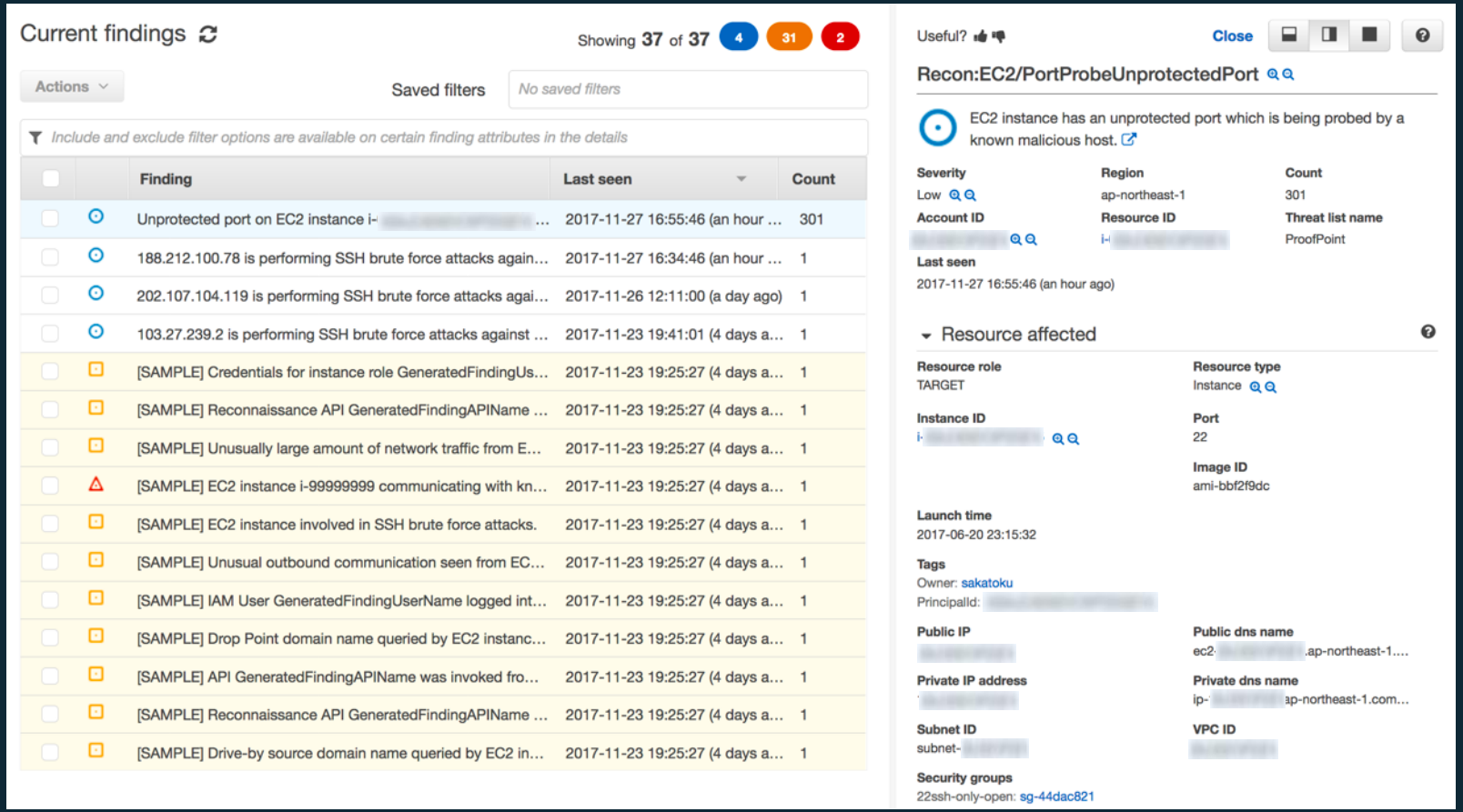
Setting Up Amazon GuardDuty

Amazon GuardDuty Service-Linked Role

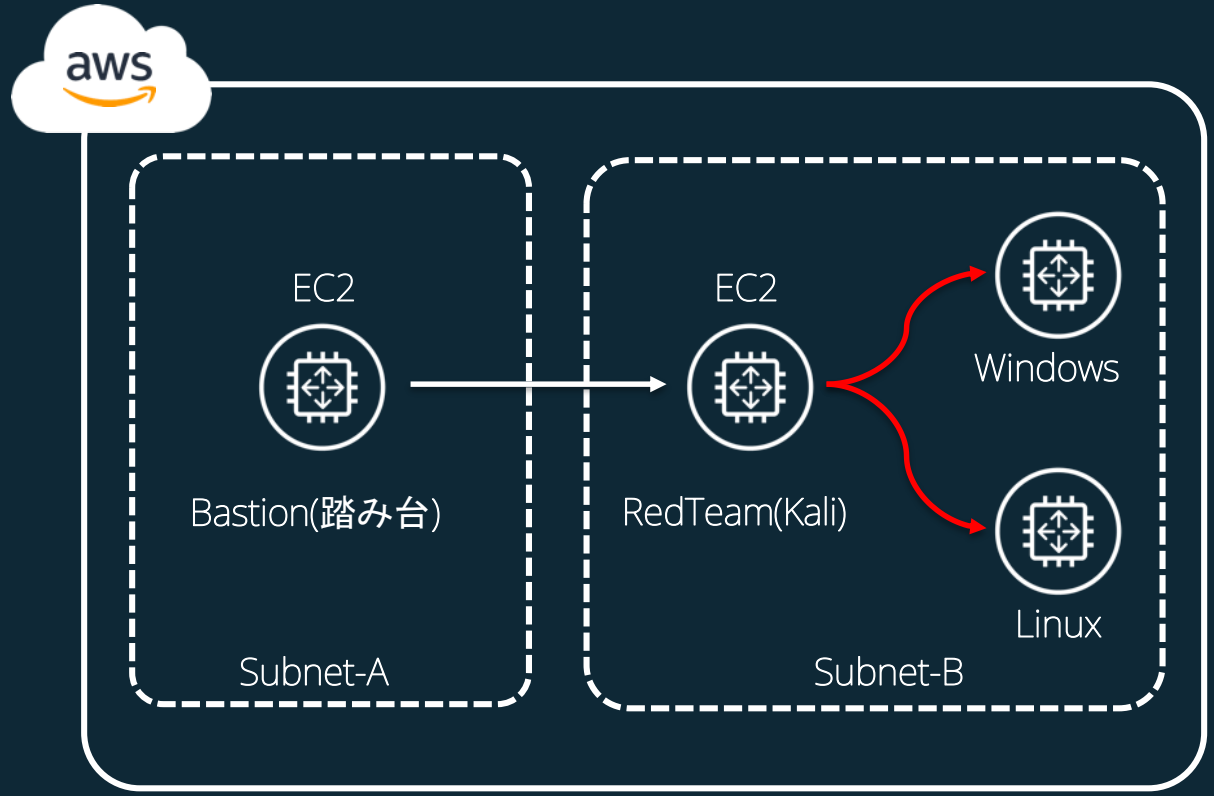
- GuardDutyを有効にすると、サービスにリンクされたロールとして AWSServiceRoleForAmazonGuardDutyが自動的に作成されます

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeImages"
            ],
            "Resource": "*"
        }
    ]
}
```

Amazon GuardDuty による検知

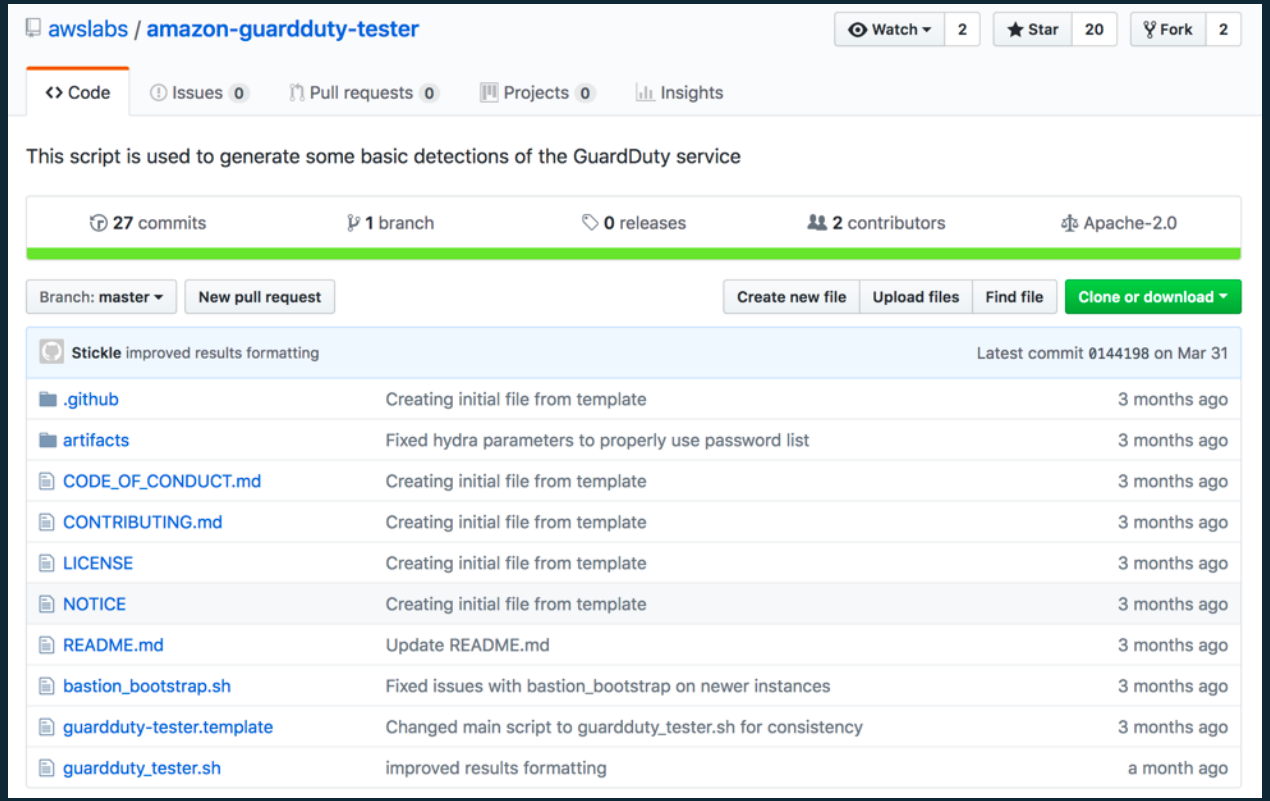


Demo ☺



amazon-guardduty-tester

https://github.com/awslabs/amazon-guardduty-tester



※AWS環境における侵入テスト、脆弱性テスト、その他シミュレートされたイベントには事前申請が必要です
https://aws.amazon.com/jp/security/penetration-testing/

Amazon GuardDuty

AWS アカウントとワークロードを守るインテリジェントな脅威検出

今すぐ始める

入門ガイド

Continuous

AWS 環境に疑わしいアクティビティが発生していないかどうかを継続的に監視し、結果を生成します。

詳細はこちら

包括的な

AWS CloudTrail イベントや VPC フローログを含む複数のデータソースを分析します。

詳細はこちら

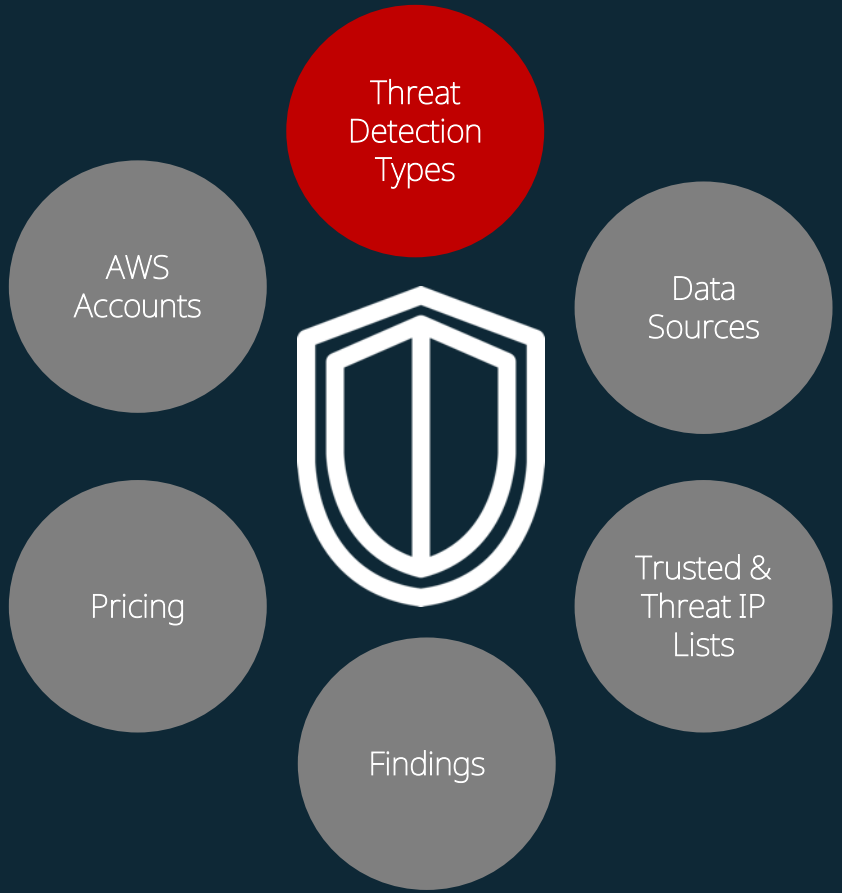
カスタマイズ可能

独自の脅威リストや信頼されている IP リストを追加して GuardDuty をカスタマイズします。

詳細はこちら

検知の仕組み

GuardDuty Service Components



Threat Detection Types

悪意のあるスキャン

Instance Recon:
- Port Probe/Accepted Comm
- Port Scan (intra-VPC)
- Brute Force Attack (IP)
- Drop Point (IP)
- Tor Communications

Account Recon:
- Tor API Call (failed)

インスタンスへの脅威

- C&C Activity
- Malicious Domain Request
- EC2 on Threat List
- Drop Point IP
- Malicious Comms (ASIS)
- Bitcoin Mining
- Outbound DDoS
- Spambot Activity
- Outbound SSH Brute Force
- Unusual Network Port
- Unusual Traffic Volume/Direction
- Unusual DNS Requests
- Domain Generated Algorithms

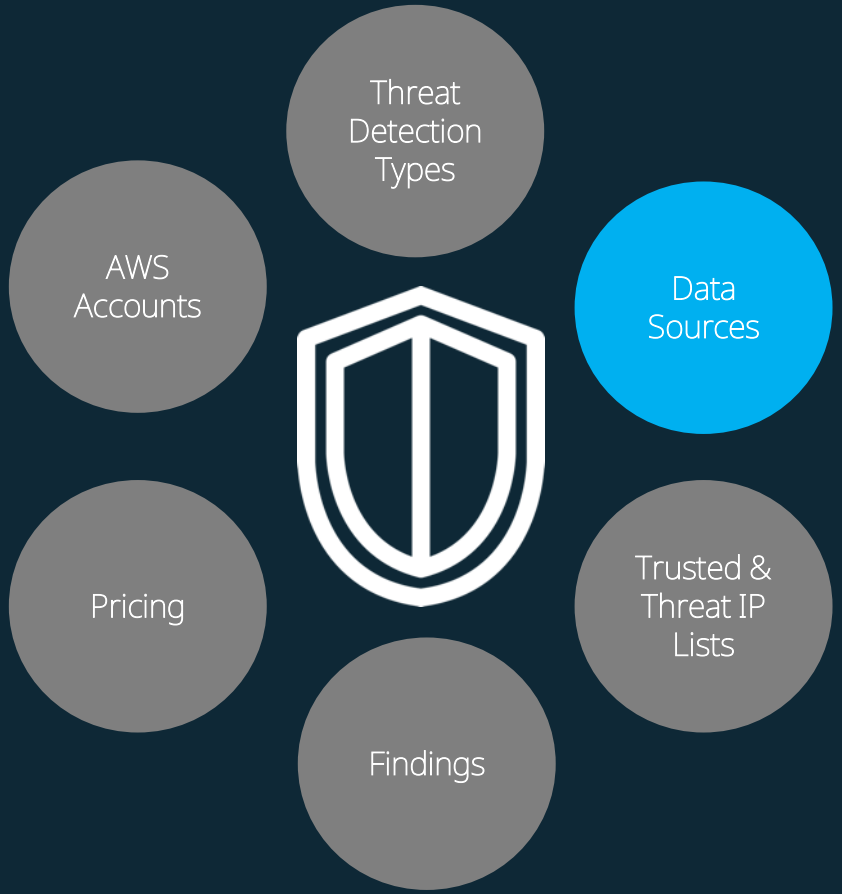
アカウントへの脅威

- Malicious API Call (bad IP)
- Tor API Call (accepted)
- CloudTrail Disabled
- Password Policy Change
- Instance Launch Unusual
- Region Activity Unusual
- Suspicious Console Login
- Unusual ISP Caller
- Mutating API Calls (create, update, delete)
- High Volume of Describe calls
- Unusual IAM User Added

● Signature Based Stateless Findings

● Behavioral Stateful Findings and Anomaly Detections

GuardDuty Service Components



Data Sources

VPC Flow Logs

VPC flow logs

- VPC Flow Logs が有効でなくても GuardDuty Findings を生成
- 一方で、中長期的なログ分析において、VPC Flow Logs を有効にすることは推奨

DNS Logs

DNS Logs

- EC2 インスタンス上から実行されたクエリログがDNS Logs 解析対象

CloudTrail Events

CloudTrail Events

- AWS Management Console, SDKs, CLI から実行されるAPIコール含む CloudTrail イベントログを利用

GuardDuty Service Components

Trusted and Threat IP Lists

- GuardDuty の提供する脅威インテリジェンス
  - 攻撃者が使用することがわかっている IP アドレスとドメインで構成
    - CrowdStrike
    - Proofpoint
    - AWS Security

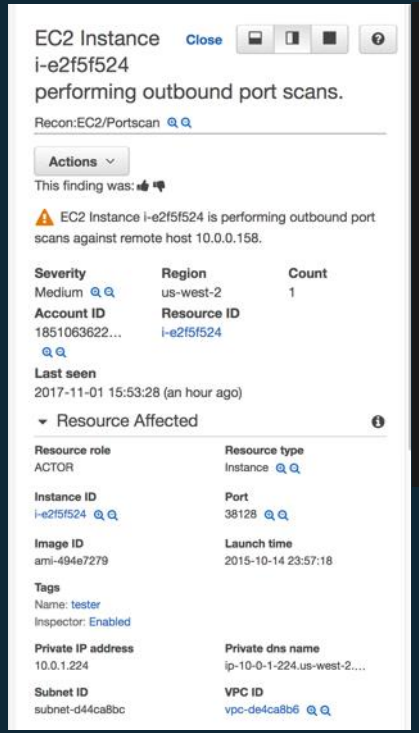
- カスタムリストを作成することで、既知の脅威リストをカスタマイズ
  - Trusted IP List(ホワイトリスト)
    - 登録されたIPリストはホワイトリストされ、登録IPに対するアクティビティは、GuardDutyはFindingとして検知しない
  - Threat IP List(ブラックリスト)
    - 既知の悪意のあるIPリストを登録可能。登録した脅威リストに基づき GuardDuty Findings として通知

Trusted IP Lists and Threat Lists

GuardDuty Service Components

Findings

AWS Management Console



脅威に関する情報:

- 重要度
- 頻度
- リージョン
- 国
- 脅威タイプ
- 影響範囲
- 攻撃元情報

API / JSON Format

脅威情報の活用:

- SIEM 連携
- データ活用
- 自動アクション
- それ以外の情報
  - ARN
  - 時間
  - リソース情報

Findings Purpose:

脅威または潜在的な攻撃リスクの主な目的

- Backdoor : AWS リソースが攻撃を受けていることを検出
- Behavior : ベースラインとは異なるアクティビティやアクティビティパターンを検出
- Crypto Currency : ビットコインやイーサリアムなどの暗号通貨に関連付けられたソフトウェアを検出
- Pentest : 既知のペンテストツールで生成されたアクティビティと類似するアクティビティを検出
- Recon : AWS 環境の脆弱性を探そうとしているアクティビティを検出
- Stealth : 攻撃アクションや形跡を隠そうとするアクティビティを検出
- Trojan : トロイの木馬プログラムが攻撃に使用されていることを検知
- Unauthorized Access : 不審なアクティビティまたアクティビティパターンの検出

Finding タイプ

- Backdoor:EC2/XORDDOS
- Backdoor:EC2/Spambot
- Backdoor:EC2/C&CActivity.B!DNS
- Behavior:IAMUser/InstanceLaunchUnusual
- Behavior:EC2/NetworkPortUnusual
- Behavior:EC2/TrafficVolumeUnusual
- CryptoCurrency:EC2/BitcoinTool.A
- CryptoCurrency:EC2/BitcoinTool.B!DNS
- PenTest:IAMUser/KaliLinux
- Recon:EC2/PortProbeUnprotectedPort
- Recon:IAMUser/TorIPCaller
- Recon:IAMUser/MaliciousIPCaller.Custom
- Recon:IAMUser/MaliciousIPCaller
- Recon:EC2/Portscan
- Stealth:IAMUser/PasswordPolicyChange
- Stealth:IAMUser/CloudTrailLoggingDisabled
- Trojan:EC2/BlackholeTraffic
- Trojan:EC2/DropPoint
- Trojan:EC2/BlackholeTraffic!DNS
- Trojan:EC2/DriveBySourceTraffic!DNS
- Trojan:EC2/DropPoint!DNS
- Trojan:EC2/DGADomainRequest.B
- Trojan:EC2/DNSDataExfiltration
- UnauthorizedAccess:IAMUser/TorIPCaller
- UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom
- UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B
- UnauthorizedAccess:IAMUser/MaliciousIPCaller
- UnauthorizedAccess:IAMUser/UnusualASNCaller
- UnauthorizedAccess:EC2/TorIPCaller
- UnauthorizedAccess:EC2/MaliciousIPCaller.Custom
- UnauthorizedAccess:EC2/SSHBruteForce
- UnauthorizedAccess:EC2/RDPBruteForce
- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration

http://docs.aws.amazon.com/ja_jp/guardduty/latest/ug/guardduty_finding-types.html

新しく追加された GuardDuty Findings

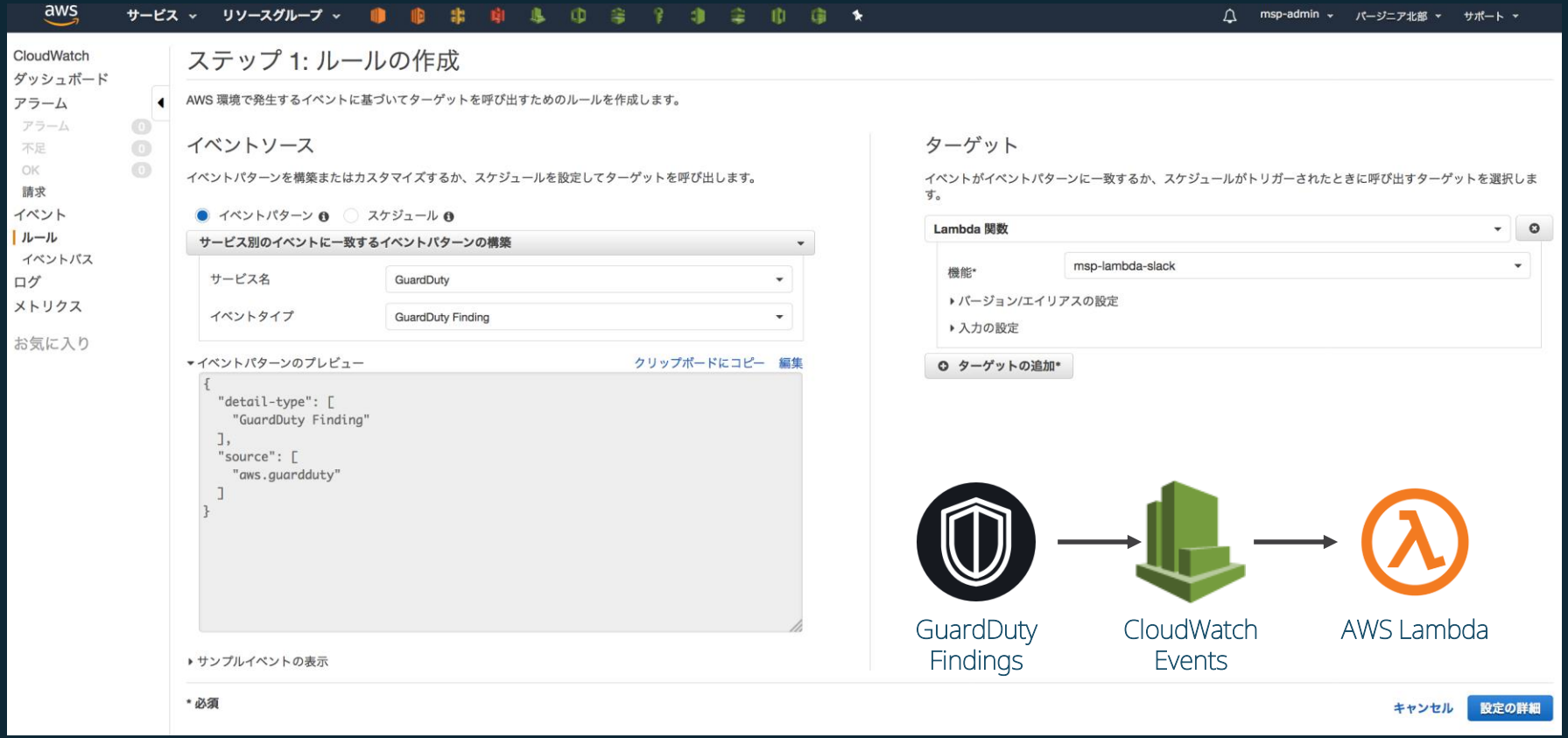
Added the following three threat intelligence detections (finding types): • Trojan:EC2/PhishingDomainRequest!DNS • Trojan:EC2/BlackholeTraffic!DNS • Trojan:EC2/DGADomainRequest.C!DNS	These new finding types are automatically enabled in GuardDuty in all supported regions. For more information, see Amazon GuardDuty Finding Types.	February 5, 2018
Added the following nine CloudTrail-based anomaly detections (finding types): • Recon:IAMUser/NetworkPermissions • Recon:IAMUser/ResourcePermissions • Recon:IAMUser/UserPermissions • Persistence:IAMUser/NetworkPermissions • Persistence:IAMUser/ResourcePermissions • Persistence:IAMUser/UserPermissions • ResourceConsumption:IAMUser/ComputeResources • Stealth:IAMUser/LoggingConfigurationModified • UnauthorizedAccess:IAMUser/ConsoleLogin	These new finding types are automatically enabled in GuardDuty in all supported regions. For more information, see Amazon GuardDuty Finding Types.	February 28, 2018

https://docs.aws.amazon.com/guardduty/latest/ug/doc-history.html

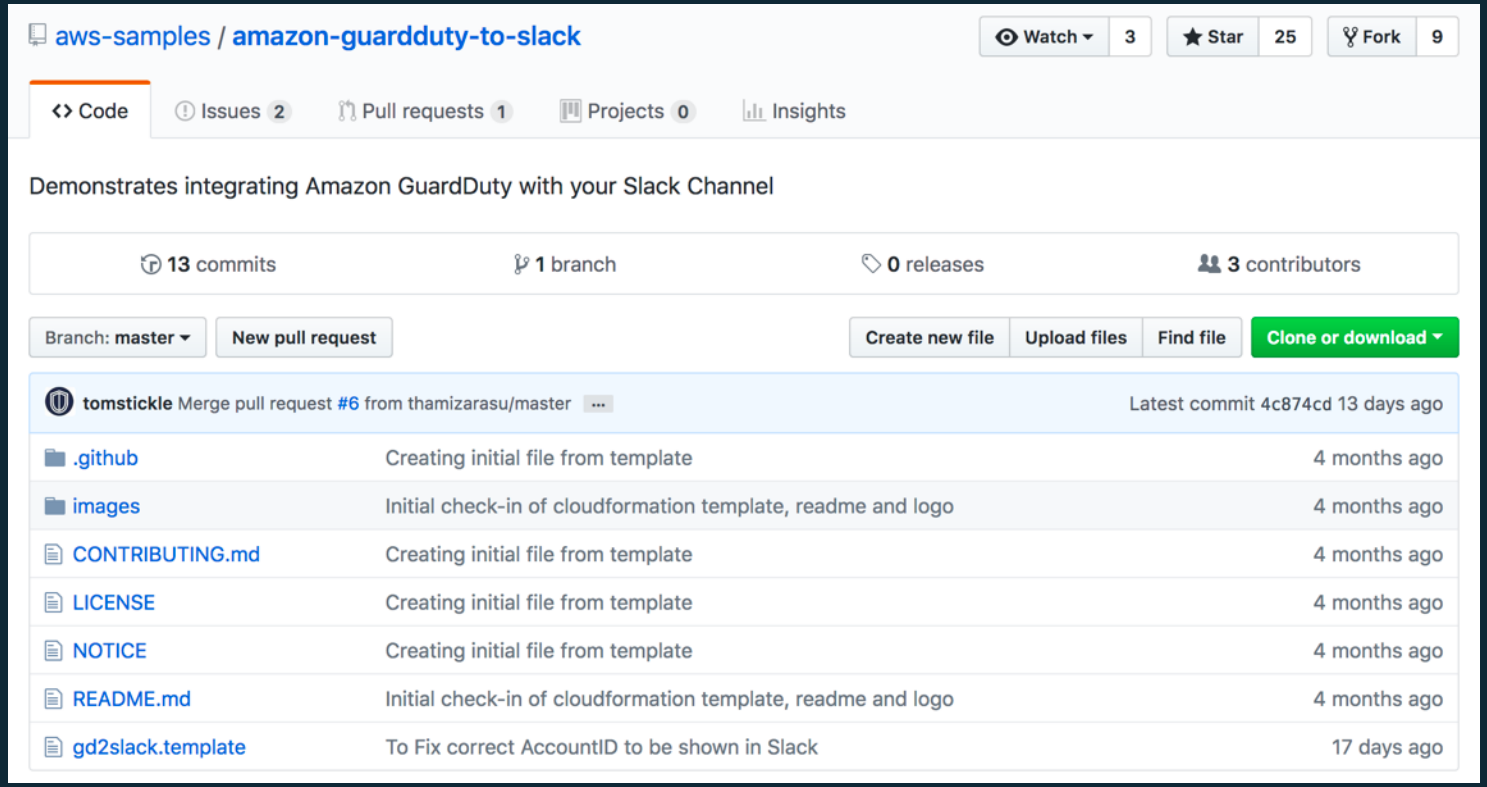
Severity Levels for GuardDuty Findings

- 検知するFindingsには重要度(Severity)を設定
- 重要度は、0.0 – 10.0 の範囲で設定
  - High (**重要度**: **高**) : Severity 7.0 – 8.9
    - 例) EC2 instance / IAM user credentials 関連
  - Medium (**重要度**: **中**) : Severity 4.0 – 6.9
    - 例) 大量トラフィック、通常アクティビティから外れる動き
  - Low (**重要度**: **低**) : Severity 0.1 – 3.9
    - 例) リソースに影響を及ぼす前にブロックされた悪意の疑いのあるアクティブティ

Finding 検出時のアクション



amazon-guardduty-to-slack



https://github.com/aws-samples/amazon-guardduty-to-slack

GuardDuty Service Components

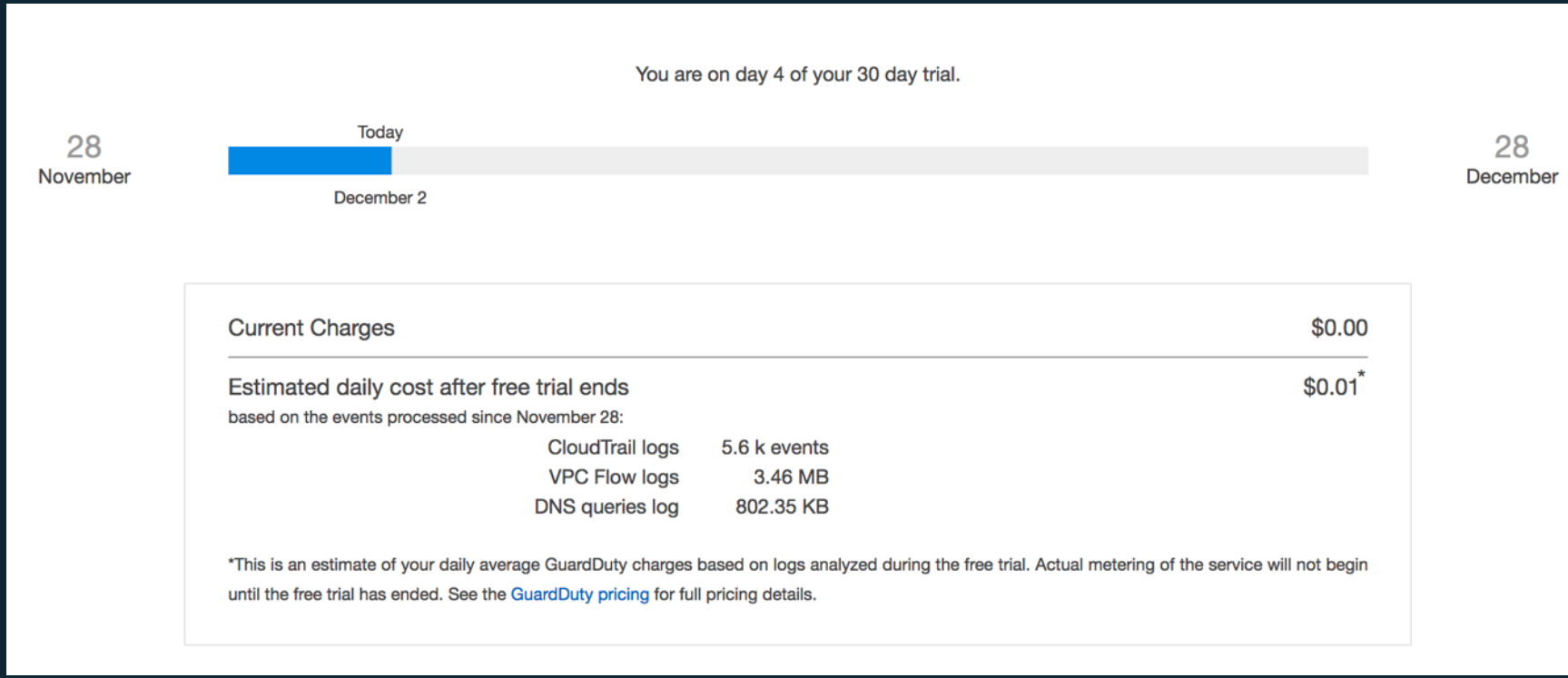
Pricing

- GuardDuty は2つのディメンジョンの合計金額が課金
  - CloudTrail Events: 分析されたAWS CloudTrailイベントの数量（1,000,000イベントあたり）と
  - VPC Flow Logs/DNS Logs: 分析されたAmazon VPC Flow LogおよびDNS Logデータの量（GBあたり）

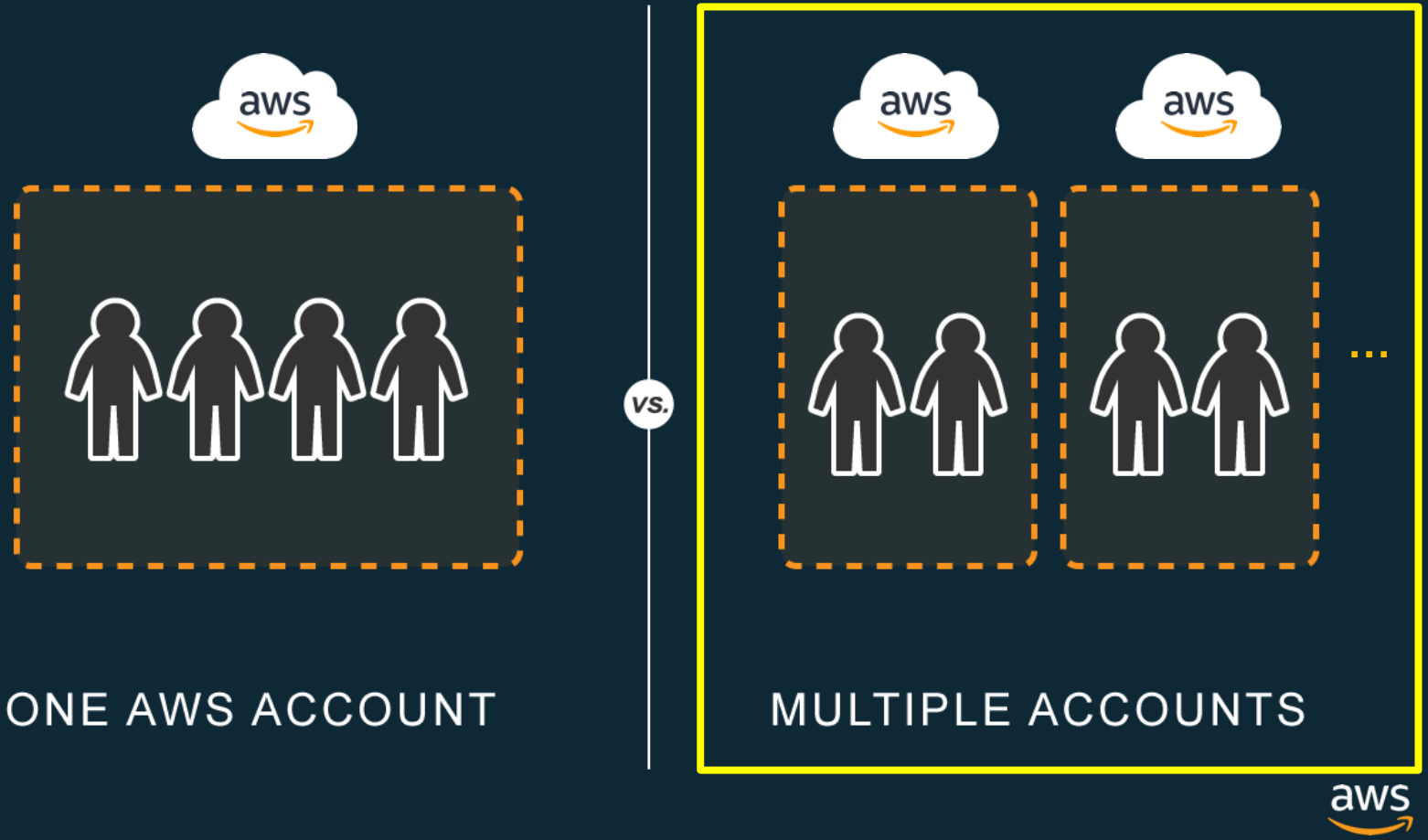
VPC Flow Log and DNS Log Analysis	
First 500 GB / month	$1.18 per GB
Next 2000 GB / month	$0.59 per GB
Over 2500 GB / month	$0.29 per GB
AWS CloudTrail Event Analysis	
Per 1,000,000 events / month	$4.72 per 1,000,000 events

https://aws.amazon.com/guardduty/pricing/

Amazon GuardDuty 30-day-Free-Trial

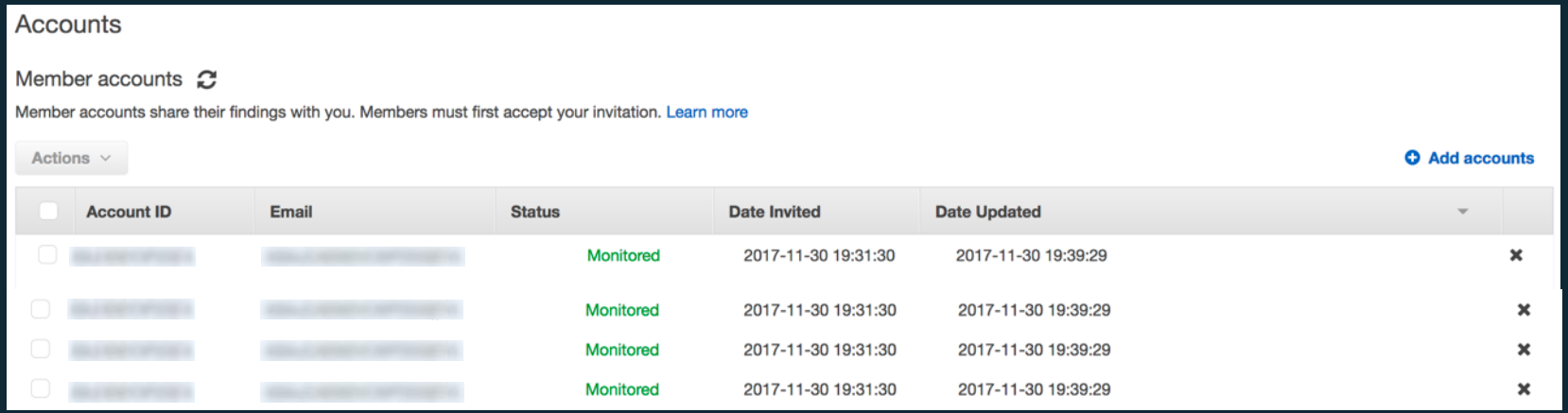


GuardDuty Service Components



Managing AWS Accounts in Amazon GuardDuty

- あるAWSアカウントで検知したFindingを、他AWSアカウントのGuardDutyに転送・統合管理することが可能
- 例えば、セキュリティ管理アカウントに他AWSアカウントのGuardDuty Findingsを集約し一元管理が可能



https://docs.aws.amazon.com/ja_jp/guardduty/latest/ug/guardduty_accounts.html

Amazon CloudFormation StackSets

CloudFormation

- Infrastructure as a code
- DevSecOpsを実現する主要サービス
- マルチアカウント、マルチリージョン対応
  - 管理者アカウント用IAMロール(Default): AWSCloudFormationStackSetAdministrationRole
  - ターゲットアカウント用IAMロール(Default): AWSCloudFormationStackSetExecutionRole

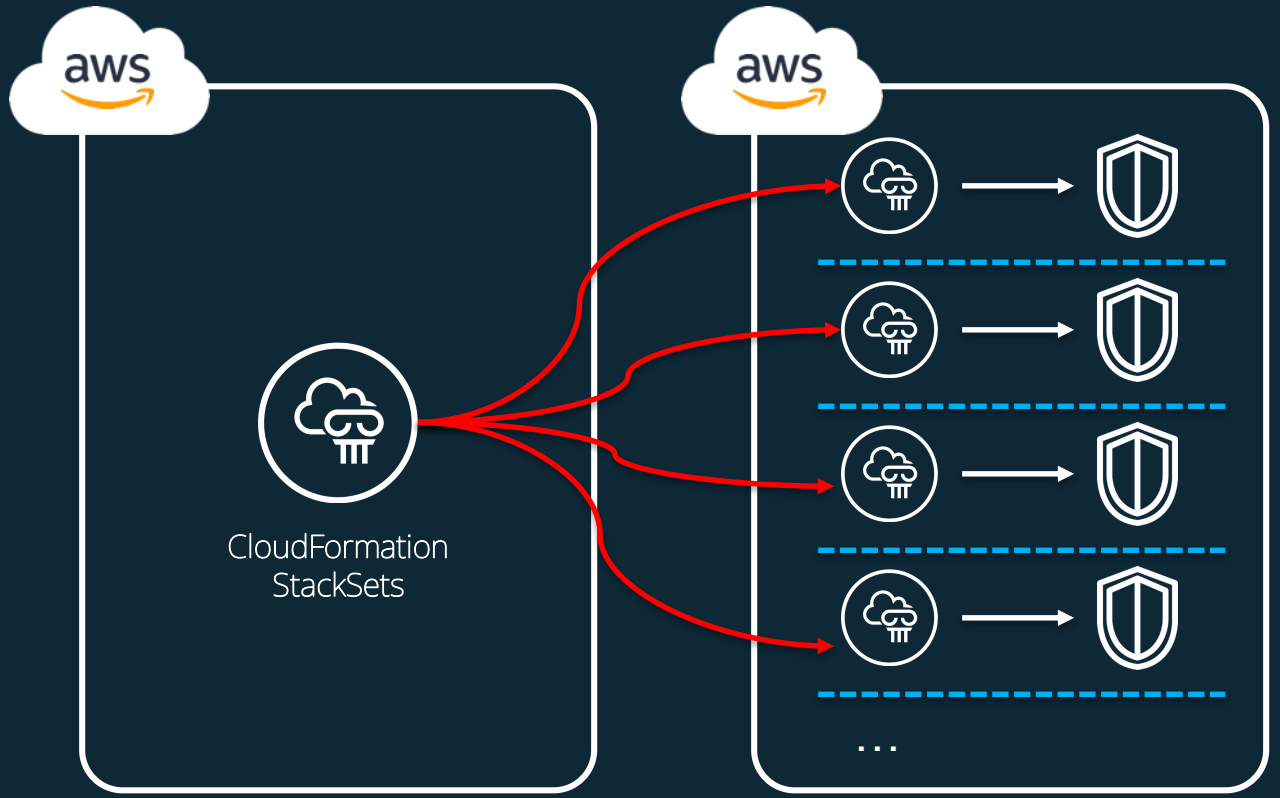
CloudFormation テンプレート

```yaml
AWSTemplateFormatVersion: 2010-09-09
Description: Enable Amazon GuardDuty. This template enables Amazon GaurdDuty.

Resources:
  GuardDutyDetector:
    Type: "AWS::GuardDuty::Detector"
    Properties:
      Enable: true
```

http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-resource-guardduty-detector.html

Demo ☺



スタックセットとは

スタックセットは、1 つの AWS CloudFormation テンプレートを使用して複数の AWS アカウントおよびリージョンにまたがってスタックをプロビジョニングできる、AWS CloudFormation スタックのコンテナです。

前提条件

StackSet の作成についての詳細はこちら

スタックセットの作成 | アクション

スタックセット名

表示可能なスタックセットはありません

スタックセットの作成

Amazon GuardDuty Cross Account

管理者アカウント

- **CreateMembers**

aws guardduty create-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-details AccountId=123456789012,Email=guarddutymember@amazon.com

- **InviteMembers**

aws guardduty invite-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 123456789012

管理対象アカウント

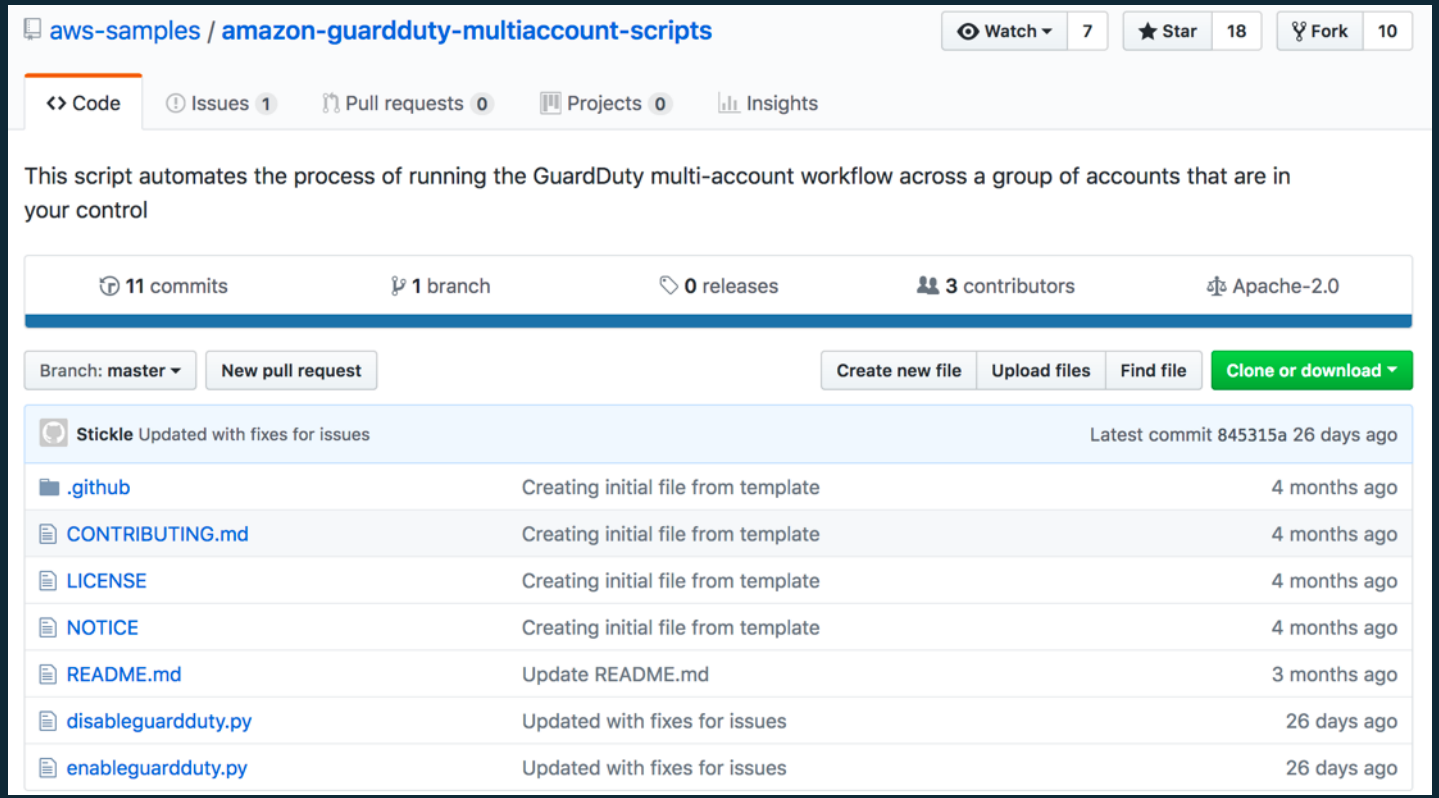
- **CreateDetector**

aws guardduty create-detector --enable

- **AcceptInvitation**

aws guardduty accept-invitation --detector-id 12abc34d567e8fa901bc2d34e56789f0 --master-id 012345678901 --invitation-id 84b097800250d17d1872b34c4daadcf5

amazon-guardduty-multiaccount-scripts



https://github.com/aws-samples/amazon-guardduty-multiaccount-scripts

GuardDuty Partners

https://aws.amazon.com/jp/guardduty/resources/partners/

まとめ – Amazon GuardDuty

- 機械学習を用いた脅威検知
- エージェント導入不要・既存環境に影響を与えずパフォーマンス劣化無し
- 初期費用不要・無料期間付きで導入が容易
- CloudWatch Events/Lambdaによる検知から対応までの自動化
- サードパーティ/エコシステム連携

参考資料

- Amazon GuardDuty

https://aws.amazon.com/jp/guardduty/

- Amazon GuardDuty - よくある質問

https://aws.amazon.com/jp/guardduty/faqs/

- Amazon GuardDuty Lab

http://lab.gregmcconnel.net/

https://www.slideshare.net/AmazonWebServices/sid304-threat-detection-and-remediation-with-amazon-guardduty?qid=7d6e2922-6a8b-4ab7-862e-0e057a7a2a5b&v=&b=&from_search=2

オンラインセミナー資料の配置場所

AWS クラウドサービス活用資料集

- https://aws.amazon.com/jp/aws-jp-introduction/

Amazon Web Services ブログ

- 最新の情報、セミナー中のQ&A等が掲載されています。
- https://aws.amazon.com/jp/blogs/news/

公式Twitter/Facebook
AWSの最新情報をお届けします

@awscloud_jp

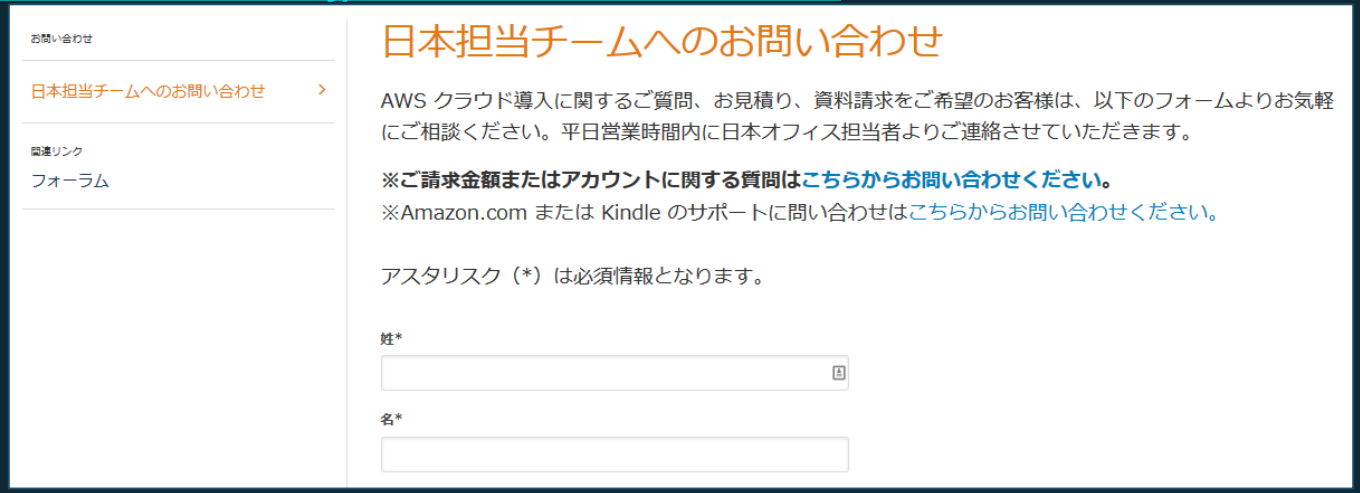
もしくは
http://on.fb.me/1vR8yWm

最新技術情報、イベント情報、お役立ち情報、
お得なキャンペーン情報などを日々更新しています！

AWSの導入、お問い合わせのご相談

AWSクラウド導入に関するご質問、お見積、資料請求をご希望のお客様は以下のリンクよりお気軽にご相談下さい。

https://aws.amazon.com/jp/contact-us/aws-sales/



※「AWS 問い合わせ」で検索して下さい。

AWS Well Architected 個別技術相談会お知らせ

- Well Architectedフレームワークに基づく数十個の質問項目を元に、お客様がAWS上で構築するシステムに潜むリスクやその回避方法をお伝えする個別相談会です。
  https://pages.awscloud.com/well-architected-consulting-jp.html
- 参加無料
- 毎週火曜・木曜開催

【毎週火、木曜開催】AWS Well-Architected 個別技術相談会

AWS 上で構築するシステムのリスクの把握・回避方法をご希望のお客様

この度 AWS をご活用頂いているお客様を対象に「AWS Well-Architected 個別技術相談会」を開催致します。

Well-Architected 個別技術相談会では、リスクの把握・回避を目的として、セキュリティ・信頼性・パフォーマンス・コスト・運用の５つの観点で、お客様の AWS 活用状況や構成についてお伺いします。AWS のベストプラクティスに基づき作成された Well-Architected フレームワークを元に、今までお客様がお気づきでなかったリスクやAWS活用の改善点を見つけることができます。例えば、自動車においては納車前点検、車検を定期的に行うのと同様に、本相談会はお客様の AWS 上のシステムをよりよく活用頂くことを目的にしております。

» 説明資料(PDF) [AWS Well-Architected Framework -クラウド設計・運用ベストプラクティスの活用-]

Well-Architected 個別技術相談会にご参加頂くには、本ページにてお申込み後、弊社担当者からお送りするヒアリングシートにご記入・担当者にご送付頂く必要があります。その内容を元に、当日の相談会では AWS のソリューションアーキテクトと共に技術的なディスカッションをさせて頂きます。また、遠方のお客様、アマゾン東京オフィスへのご来社が時間等の関係で難しいお客様は、Web のプレゼンテーションツールや、お電話を活用したリモートでのご相談も承ります。

下記のフォームよりお申込みください。

* 姓:

* 名: