



【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.

NEW
!



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



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

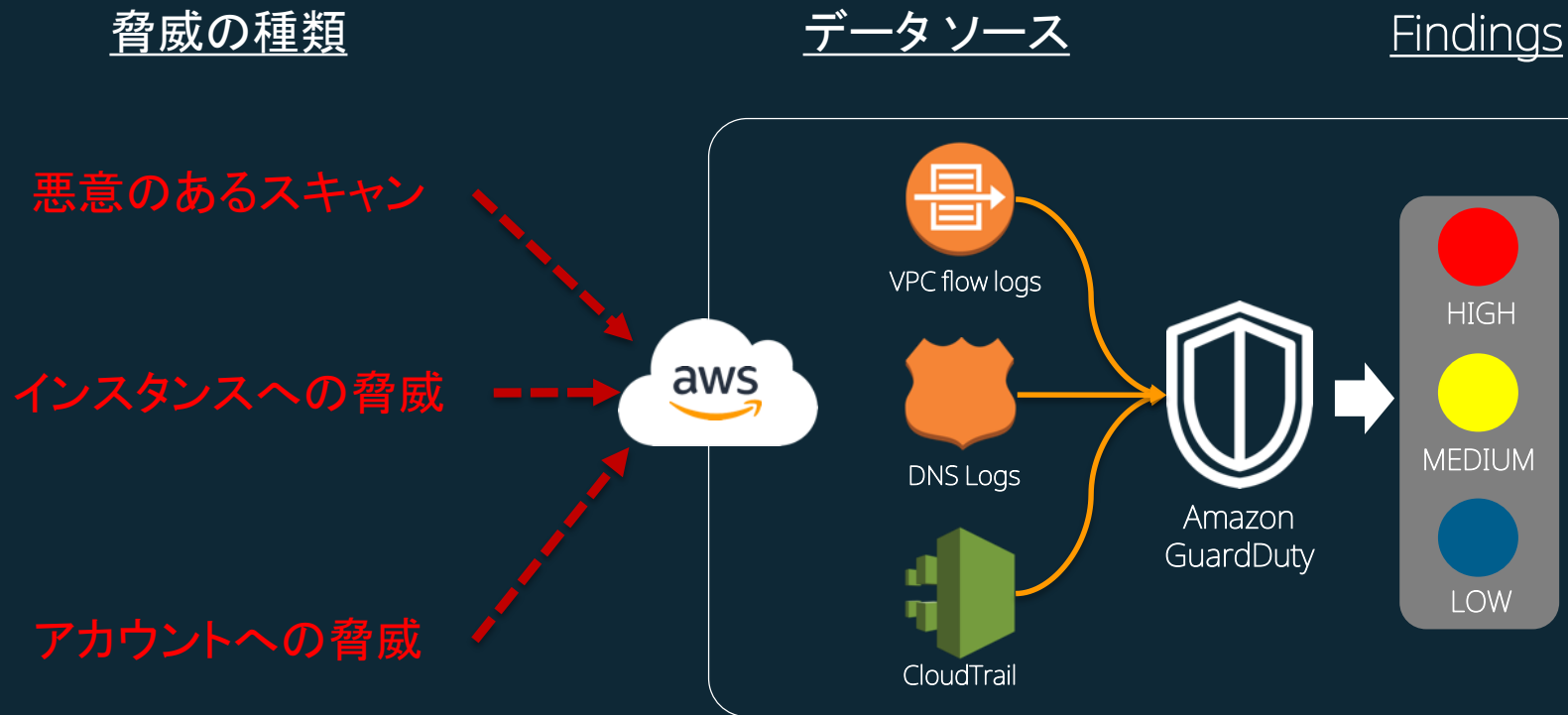


Amazon GuardDuty

- 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**



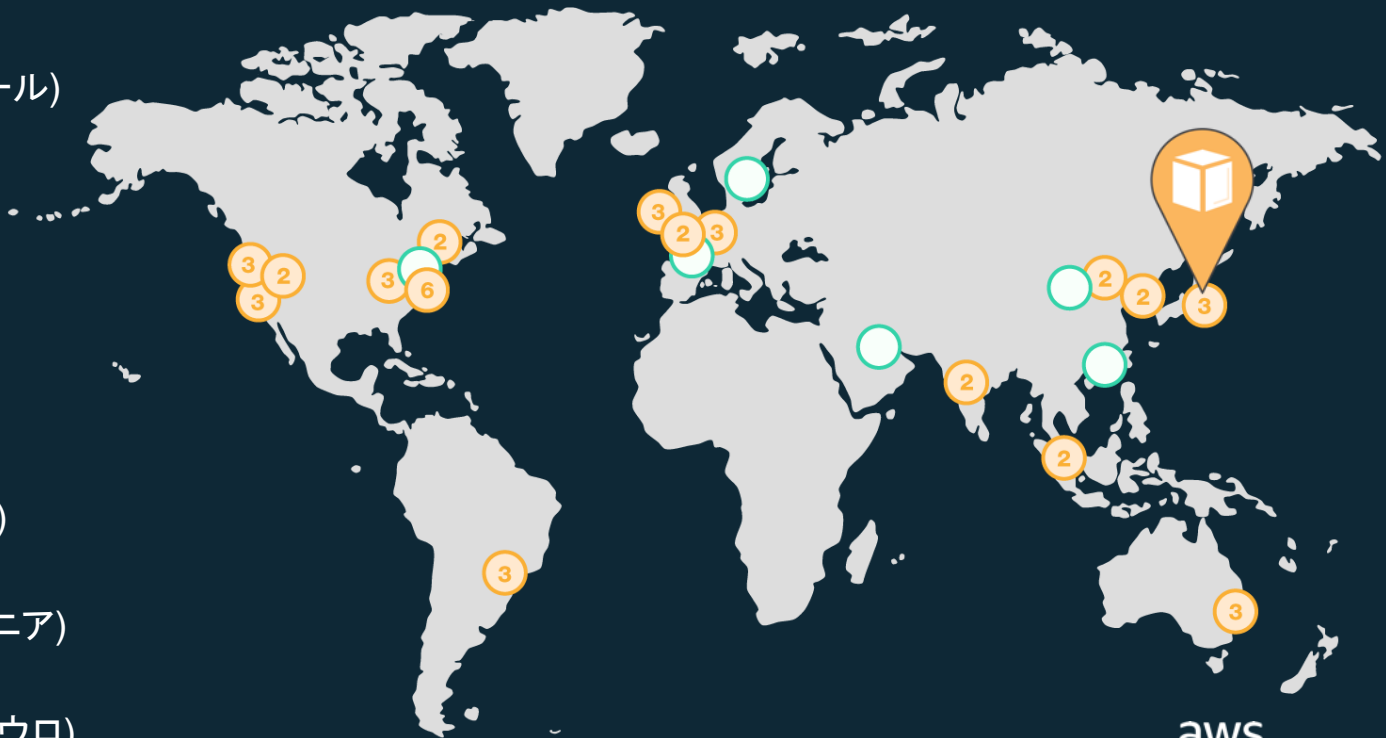
GuardDuty による脅威の検知



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



Amazon GuardDuty

Amazon GuardDuty は、継続的なセキュリティのモニタリングおよび分析サービスで、AWS 環境に対する潜在的な脅威を検出します。

[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](#)



Setting Up Amazon GuardDuty

GuardDuty

GuardDuty の有効化

Partners 

GuardDuty によるこそ

30 day free trial

サービスのアクセス権限

GuardDuty を有効にすると、AWS CloudTrail ログ、VPC フローログ、および DNS クエリログを分析してセキュリティに関する分析結果を生成するための GuardDuty のアクセス許可を付与することになります。 [詳細はこちら](#)

サービスロールのアクセス権限の表示

注意: GuardDuty では AWS CloudTrail ログ、VPC フローログ、DNS クエリログを管理したり、イベントやログを使用可能にすることはしません。これらのデータソースはそれぞれのコンソールまたは API で設定できます。GuardDuty はいつでも停止または無効にして、イベントおよびログの処理や分析が行われないようにすることができます。 [詳細はこちら](#)

When you enable GuardDuty for the first time, your AWS account is automatically enrolled in a 30 day [GuardDuty free trial](#). Learn more about [GuardDuty pricing](#).

GuardDuty の有効化



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

Current findings

Showing 37 of 37 4 31 2

Actions ▼ Saved filters No saved filters

▼ Include and exclude filter options are available on certain finding attributes in the details

<input type="checkbox"/>	Finding	Last seen	Count
<input type="checkbox"/>	Unprotected port on EC2 instance i-... 188.212.100.78 is performing SSH brute force attacks again...	2017-11-27 16:55:46 (an hour ...)	301
<input type="checkbox"/>	202.107.104.119 is performing SSH brute force attacks again...	2017-11-26 12:11:00 (a day ago)	1
<input type="checkbox"/>	103.27.239.2 is performing SSH brute force attacks against ...	2017-11-23 19:41:01 (4 days a...)	1
<input type="checkbox"/>	[SAMPLE] Credentials for instance role GeneratedFindingUs...	2017-11-23 19:25:27 (4 days a...)	1
<input type="checkbox"/>	[SAMPLE] Reconnaissance API GeneratedFindingAPIName ...	2017-11-23 19:25:27 (4 days a...)	1
<input type="checkbox"/>	[SAMPLE] Unusually large amount of network traffic from E...	2017-11-23 19:25:27 (4 days a...)	1
<input type="checkbox"/>	[SAMPLE] EC2 instance i-99999999 communicating with kn...	2017-11-23 19:25:27 (4 days a...)	1
<input type="checkbox"/>	[SAMPLE] EC2 instance involved in SSH brute force attacks.	2017-11-23 19:25:27 (4 days a...)	1
<input type="checkbox"/>	[SAMPLE] Unusual outbound communication seen from EC...	2017-11-23 19:25:27 (4 days a...)	1
<input type="checkbox"/>	[SAMPLE] IAM User GeneratedFindingUserName logged int...	2017-11-23 19:25:27 (4 days a...)	1
<input type="checkbox"/>	[SAMPLE] Drop Point domain name queried by EC2 instanc...	2017-11-23 19:25:27 (4 days a...)	1
<input type="checkbox"/>	[SAMPLE] API GeneratedFindingAPIName was invoked fro...	2017-11-23 19:25:27 (4 days a...)	1
<input type="checkbox"/>	[SAMPLE] Reconnaissance API GeneratedFindingAPIName ...	2017-11-23 19:25:27 (4 days a...)	1
<input type="checkbox"/>	[SAMPLE] Drive-by source domain name queried by EC2 in...	2017-11-23 19:25:27 (4 days a...)	1

Useful?

[Close](#)

Recon:EC2/PortProbeUnprotectedPort

EC2 instance has an unprotected port which is being probed by a known malicious host. [↗](#)

Severity	Region	Count
Low	ap-northeast-1	301

Account ID	Resource ID	Threat list name
	i-	ProofPoint

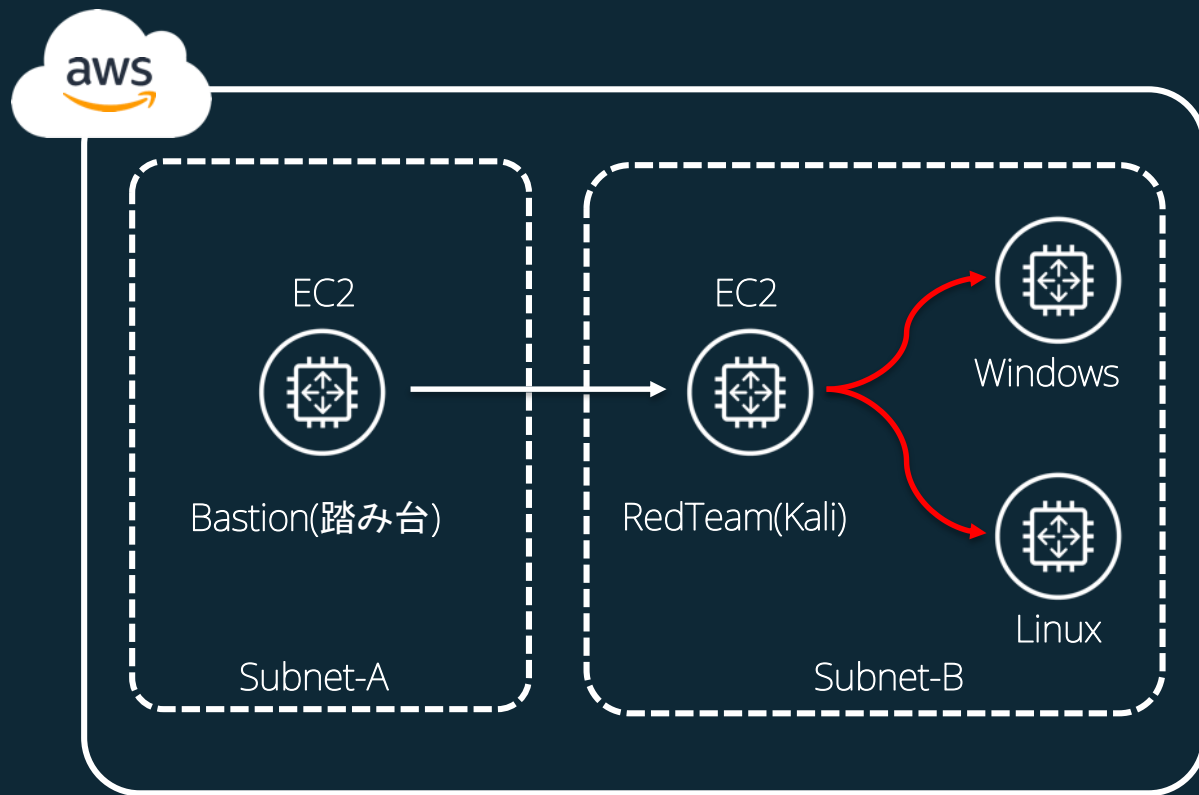
Last seen
2017-11-27 16:55:46 (an hour ago)

▼ Resource affected

Resource role TARGET	Resource type Instance
Instance ID i-	Port 22
	Image ID ami-bbf2f9dc
Launch time 2017-06-20 23:15:32	
Tags Owner: sakatoku PrincipalId:	
Public IP 	Public dns name ec2-.ap-northeast-1....
Private IP address 	Private dns name ip-.ap-northeast-1.com...
Subnet ID subnet-	VPC ID
Security groups 22ssh-only-open: sg-44dac821	



Demo 😊



amazon-guardduty-tester

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



awslabs / amazon-guardduty-tester

Watch 2 Star 20 Fork 2

Code Issues 0 Pull requests 0 Projects 0 Insights

This script is used to generate some basic detections of the GuardDuty service

27 commits 1 branch 0 releases 2 contributors Apache-2.0

Branch: master New pull request Create new file Upload files Find file Clone or download

Stickle improved results formatting Latest commit 0144198 on Mar 31

.github	Creating initial file from template	3 months ago
artifacts	Fixed hydra parameters to properly use password list	3 months ago
CODE_OF_CONDUCT.md	Creating initial file from template	3 months ago
CONTRIBUTING.md	Creating initial file from template	3 months ago
LICENSE	Creating initial file from template	3 months ago
NOTICE	Creating initial file from template	3 months ago
README.md	Update README.md	3 months ago
bastion_bootstrap.sh	Fixed issues with bastion_bootstrap on newer instances	3 months ago
guardduty-tester.template	Changed main script to guardduty_tester.sh for consistency	3 months ago
guardduty_tester.sh	improved results formatting	a month ago

※ 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

結果

設定

リスト

アカウント

使用状況

パートナー

リスト管理

信頼されている IP リスト

信頼されている IP リストは、AWS 環境で安全に通信できることがわかっている、ホワイトリストは、信頼されている IP リストに含まれている IP アドレスの結果を生成しません。 [詳細はこちら](#)

+ 信頼されている IP リストの追加

リスト名	リストファイルの URL
------	--------------

i **信頼されている IP リスト**

信頼されている IP リストは、AWS 環境で安全に通信できることがわかっている、ホワイトリストは、信頼されている IP リストに含まれている IP アドレスの結果を生成しません。 GuardDuty では、信頼されている IP リストに含まれている IP アドレスの結果を生成しません。

脅威リスト

脅威リストは、既知の悪意のある IP アドレスで構成されています。 GuardDuty では、脅威リストは、既知の悪意のある IP アドレスで構成されています。 GuardDuty では、脅威リストに含まれている IP アドレスの結果を生成しません。 [詳細はこちら](#)

+ 脅威リストの追加

リスト名	リストファイルの URL	形式	アクティブ
------	--------------	----	-------

i **脅威リスト**

脅威リストは、既知の悪意のある IP アドレスで構成されています。 GuardDuty では、脅威リストに含まれている IP アドレスの結果を生成しません。 [詳細はこちら](#)

脅威リストの追加

GuardDuty では、脅威リストに基づいて結果を生成します。 [詳細はこちら](#)

リスト名 **i**

場所 **i**

形式

このリストを追加することにより、サードパーティーの脅威のインテリジェンスに関連するものを含む、GuardDuty のサービス条項に同意し、このリソースからデータを読み取るように GuardDuty を設定するものとします。

同意します

[キャンセル](#) [リストの追加](#)

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

GuardDuty Service Components



Findings

AWS Management Console

EC2 Instance `i-e2f5f524`
performing outbound port scans.

Recon:EC2/Portscan

Actions

This finding was:

EC2 Instance `i-e2f5f524` is performing outbound port scans against remote host `10.0.0.158`.

Severity	Region	Count
Medium	us-west-2	1

Account ID	Resource ID
1851063622...	<code>i-e2f5f524</code>

Last seen
2017-11-01 15:53:28 (an hour ago)

Resource Affected

Resource role	Resource type
ACTOR	Instance

Instance ID	Port
<code>i-e2f5f524</code>	38128

Image ID	Launch time
<code>ami-494e7279</code>	2015-10-14 23:57:18

Tags

Name: `tester`
Inspector: Enabled

Private IP address	Private dns name
<code>10.0.1.224</code>	<code>ip-10-0-1-224.us-west-2...</code>

Subnet ID	VPC ID
<code>subnet-d44ca8bc</code>	<code>vpc-d64ca8b6</code>

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

```
...
  "type": "Recon:EC2/Portscan",
  "resource": {
    "resourceType": "Instance",
    "instanceDetails": {
      "imageId": "ami-494e7279",
      "instanceId": "i-e2f5f524",
...
  "service": {
    "serviceName": "guardduty",
    "detectorId": "6caf9da04f873e4",
    "action": {
      "actionType": "NETWORK_CONN",
      "networkConnectionAction": {
        "connectionDirection": "OU",
        "remoteIpDetails": {
          "ipAddressV4": "10.0.0.158",
...
  "resourceRole": "ACTOR",
  "additionalInfo": {
    "portsScannedSample": [
      146,
      83,
      110,
...
  "eventFirstSeen": "2017-11-01T15:53:28.000Z",
  "eventLastSeen": "2017-11-01T15:53:28.000Z",
...
  "severity": 5,
  "createdAt": "2017-11-01T23:00:10.179Z",
  "updatedAt": "2017-11-01T23:00:10.179Z",
  "title": "EC2 Instance i-e2f5f524 performing outbound port scans.",
  "description": "EC2 Instance i-e2f5f524 is performing outbound port scans against remote host 10.0.0.158."
}
```

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** : 既知のペント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

<p>Added the following three threat intelligence detections (finding types):</p> <ul style="list-style-type: none">• Trojan:EC2/PhishingDomainRequest!DNS• Trojan:EC2/BlackholeTraffic!DNS• Trojan:EC2/DGADomainRequest.C!DNS	<p>These new finding types are automatically enabled in GuardDuty in all supported regions. For more information, see Amazon GuardDuty Finding Types.</p>	<p>February 5, 2018</p>
<p>Added the following nine CloudTrail-based anomaly detections (finding types):</p> <ul style="list-style-type: none">• 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	<p>These new finding types are automatically enabled in GuardDuty in all supported regions. For more information, see Amazon GuardDuty Finding Types.</p>	<p>February 28, 2018</p>

<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ビティ



Finding 検出時のアクション

aws サービス リソースグループ

CloudWatch
ダッシュボード
アラーム
アラーム
不足
OK
請求
イベント
ルール
イベントバス
ログ
メトリクス
お気に入り

ステップ 1: ルールの作成

AWS 環境で発生するイベントに基づいてターゲットを呼び出すためのルールを作成します。

イベントソース

イベントパターンを構築またはカスタマイズするか、スケジュールを設定してターゲットを呼び出します。

イベントパターン スケジュール

サービス別のイベントに一致するイベントパターンの構築

サービス名: GuardDuty
イベントタイプ: GuardDuty Finding

イベントパターンのプレビュー [クリップボードにコピー](#) [編集](#)

```
{
  "detail-type": [
    "GuardDuty Finding"
  ],
  "source": [
    "aws.guardduty"
  ]
}
```

▶ サンプルイベントの表示

* 必須

ターゲット

イベントがイベントパターンに一致するか、スケジュールがトリガーされたときに呼び出すターゲットを選択します。

Lambda 関数

機能: msp-lambda-slack

▶ バージョン/エイリアスの設定
▶ 入力の設定

ターゲットの追加*

```
graph LR
  A[GuardDuty Findings] --> B[CloudWatch Events]
  B --> C[AWS Lambda]
```

キャンセル [設定の詳細](#)

amazon-guardduty-to-slack



aws-samples / amazon-guardduty-to-slack

Watch 3 Star 25 Fork 9

<> Code Issues 2 Pull requests 1 Projects 0 Insights

Demonstrates integrating Amazon GuardDuty with your Slack Channel

13 commits 1 branch 0 releases 3 contributors

Branch: master New pull request Create new file Upload files Find file Clone or download

tomstickle Merge pull request #6 from thamizarasu/master Latest commit 4c874cd 13 days ago

.github	Creating initial file from template	4 months ago
images	Initial check-in of cloudformation template, readme and logo	4 months ago
CONTRIBUTING.md	Creating initial file from template	4 months ago
LICENSE	Creating initial file from template	4 months ago
NOTICE	Creating initial file from template	4 months ago
README.md	Initial check-in of cloudformation template, readme and logo	4 months ago
gd2slack.template	To Fix correct AccountID to be shown in Slack	17 days ago

<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

You are on day 4 of your 30 day trial.

28
November



28
December

Current Charges	\$0.00
-----------------	--------

Estimated daily cost after free trial ends	\$0.01*
--	---------

based on the events processed since November 28:

CloudTrail logs	5.6 k events
VPC Flow logs	3.46 MB
DNS queries log	802.35 KB

*This is an estimate of your daily average GuardDuty charges based on logs analyzed during the free trial. Actual metering of the service will not begin until the free trial has ended. See the [GuardDuty pricing](#) for full pricing details.



GuardDuty Service Components





ONE AWS ACCOUNT

vs.




MULTIPLE ACCOUNTS




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

Accounts

Member accounts 

Member accounts share their findings with you. Members must first accept your invitation. [Learn more](#)

Actions  [+ Add accounts](#)

<input type="checkbox"/>	Account ID	Email	Status	Date Invited	Date Updated	
<input type="checkbox"/>	[REDACTED]	[REDACTED]	Monitored	2017-11-30 19:31:30	2017-11-30 19:39:29	
<input type="checkbox"/>	[REDACTED]	[REDACTED]	Monitored	2017-11-30 19:31:30	2017-11-30 19:39:29	
<input type="checkbox"/>	[REDACTED]	[REDACTED]	Monitored	2017-11-30 19:31:30	2017-11-30 19:39:29	
<input type="checkbox"/>	[REDACTED]	[REDACTED]	Monitored	2017-11-30 19:31:30	2017-11-30 19:39:29	

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

`AWSTemplateFormatVersion: 2010-09-09`

`Description: Enable Amazon GuardDuty. This template enables Amazon GaurdDuty.`

`Resources:`

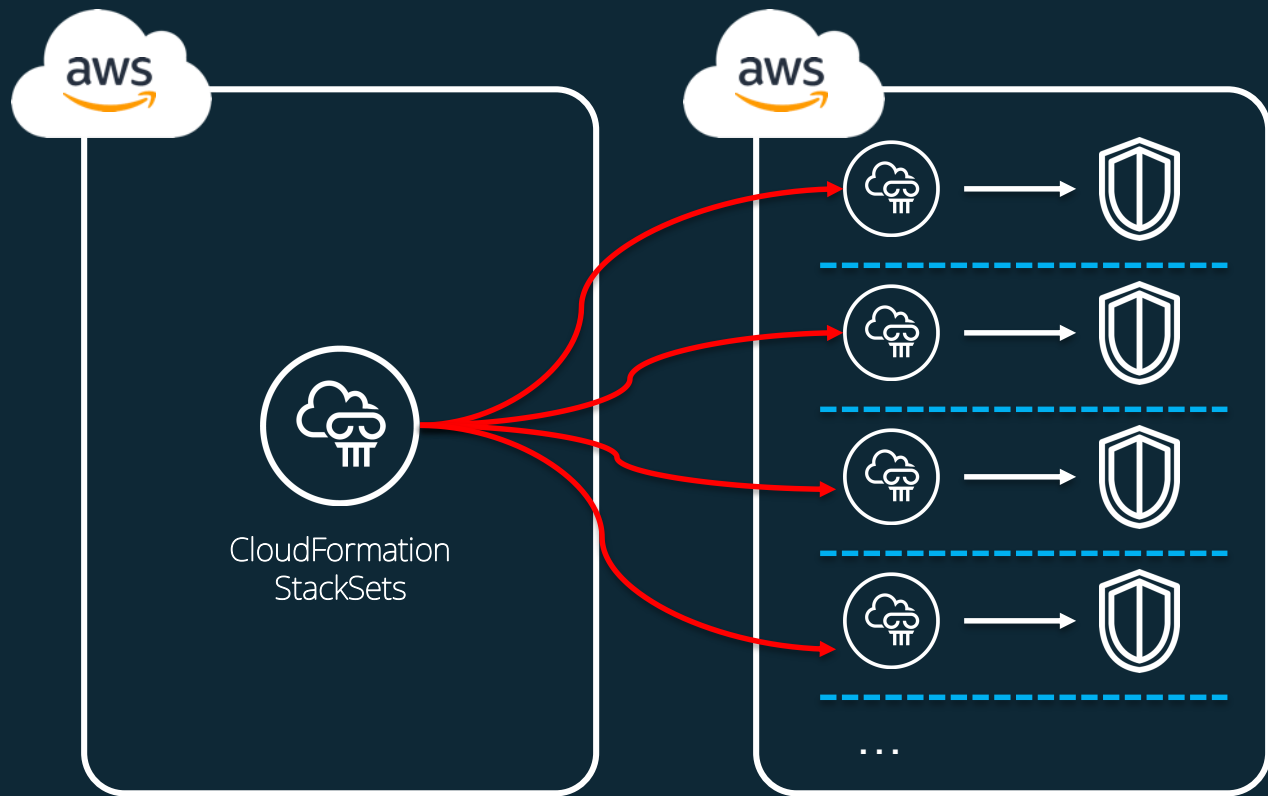
`GuardDutyDetector:`

`Type: "AWS::GuardDuty::Detector"`

`Properties:`

`Enable: true`

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 ▾



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=guardduty member@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



aws-samples / amazon-guardduty-multiaccount-scripts

Watch 7 Star 18 Fork 10

Code Issues 1 Pull requests 0 Projects 0 Insights

This script automates the process of running the GuardDuty multi-account workflow across a group of accounts that are in your control

11 commits 1 branch 0 releases 3 contributors Apache-2.0

Branch: master New pull request Create new file Upload files Find file Clone or download

Stickle Updated with fixes for issues Latest commit 845315a 26 days ago

.github	Creating initial file from template	4 months ago
CONTRIBUTING.md	Creating initial file from template	4 months ago
LICENSE	Creating initial file from template	4 months ago
NOTICE	Creating initial file from template	4 months ago
README.md	Update README.md	3 months ago
disableguardduty.py	Updated with fixes for issues	26 days ago
enableguardduty.py	Updated with fixes for issues	26 days ago

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



GuardDuty Partners

accenture

Deloitte.

RedLock



RAPID7



proofpoint



splunk



<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.gregmccannel.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



検索

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/>

お問い合わせ

日本担当チームへのお問い合わせ >

関連リンク

フォーラム

日本担当チームへのお問い合わせ

AWS クラウド導入に関するご質問、お見積り、資料請求をご希望のお客様は、以下のフォームよりお気軽にご相談ください。平日営業時間内に日本オフィス担当者よりご連絡させていただきます。

※ご請求金額またはアカウントに関する質問は[こちらからお問い合わせください](#)。
※Amazon.com または Kindle のサポートに問い合わせは[こちらからお問い合わせください](#)。

アスタリスク (*) は必須情報となります。

姓*

名*

※「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いただきます。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ポートでの相談も承ります。



下記のフォームよりお申込みください。

• 姓:

• 名:

