



このコンテンツは公開から3年以上経過しており内容が古い可能性があります
最新情報については[サービス別資料](#)もしくはサービスのドキュメントをご確認ください

[AWS Black Belt Online Seminar]

Amazon Detective

サービスカットシリーズ

Solutions Architect 中島 章博
2020/07/15

AWS 公式 Webinar
<https://amzn.to/JPWebinar>



過去資料
<https://amzn.to/JPArchive>



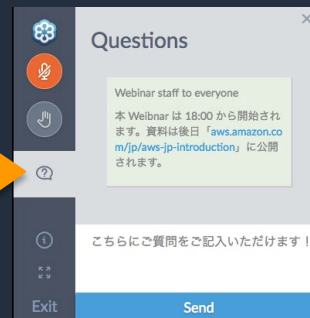
AWS Black Belt Online Seminar とは

「サービス別」「ソリューション別」「業種別」のそれぞれのテーマに分かれて、アマゾンウェブ サービス ジャパン株式会社が主催するオンラインセミナーシリーズです。

質問を投げることができます！

- 書き込んだ質問は、主催者にしか見えません
- 今後のロードマップに関するご質問は
お答えできませんのでご了承下さい

- ① 吹き出しをクリック
- ② 質問を入力
- ③ Sendをクリック



Twitter ハッシュタグは以下をご利用ください
#awsblackbelt

内容についての注意点

- 本資料では2020年7月15日現在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おります。日本居住者のお客様には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.

自己紹介

中島 章博 (なかじま あきひろ)

所属

アマゾン ウェブ サービス ジャパン株式会社
セキュリティ ソリューション アーキテクト



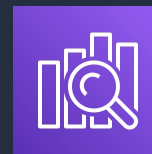
好きなサービス



Amazon Detective



Amazon GuardDuty



Amazon Elasticsearch
Service

本日のアジェンダ

- セキュリティインシデントの対応と課題
- Amazon Detective
 - 概要
 - ユースケース
 - ご利用方法とセキュリティ調査例
 - 内部の分析プロセス詳細
 - マルチアカウント環境への対応等
 - 料金体系
- まとめ

コンピューターセキュリティインシデントとは？

組織が定めるセキュリティポリシーやコンピューターの利用規定に対する違反行為または差し迫った脅威、あるいは、標準的なセキュリティ活動に対する違反行為または差し迫った脅威を示す



サービス不能



悪意のコード



不正アクセス



不適切な使用

※引用：[NIST SP 800-61 rev.1 「コンピュータインシデント対応ガイド」\(IPA日本語翻訳版\)](#)

セキュリティインシデント対応が重要な理由

攻撃により個人データや業務データが頻繁に損なわれている

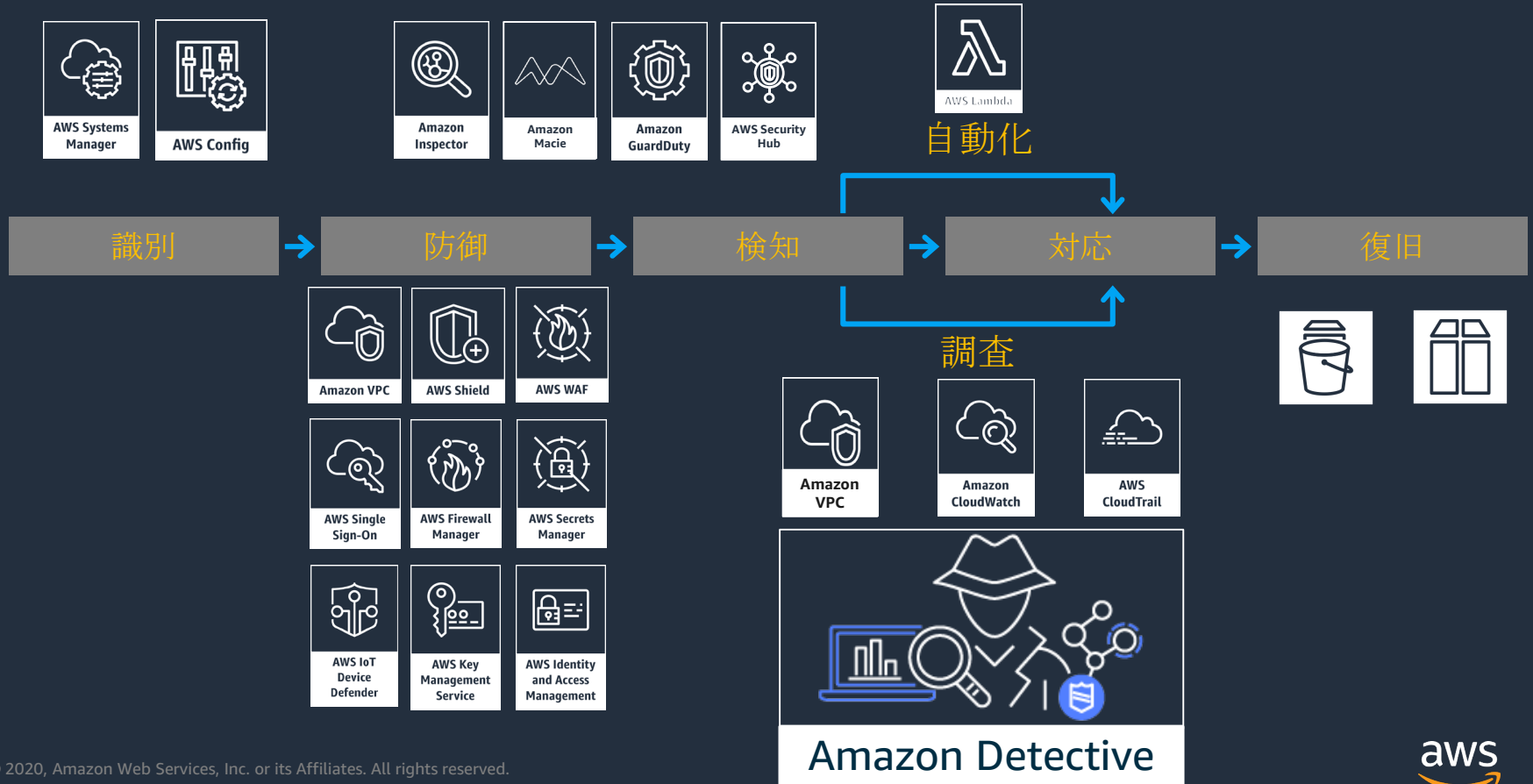


インシデント対応を適切に実施すると

- 迅速かつ効率的にセキュリティインシデントから復旧するのを助ける
- 情報の損失や盗難、サービスの中断を最小限に抑えることができる
- 事件処理の際に得た情報を使って、将来の事件に備え、システムとデータを強力に防護できる
- 事件に伴って発生する可能性がある法的な問題を正しく扱える

※引用：[NIST SP 800-61 rev.1「コンピュータインシデント対応ガイド」\(IPA日本語翻訳版\)](#)

AWS サービスとセキュリティインシデント対応



セキュリティ調査プロセス



インシデントに関連したテラバイト規模のログを収集



ETL ツールやカスタムスクリプトで、ログを分析できる状態に変換



ツール等を利用してデータを視覚化して分析



クエリ文を作成して詳細に事象を解析後、結論づけ

セキュリティ調査の課題



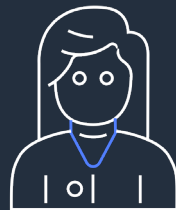
大量のノイズ

アラートの大部分はインシデントとは関係ないデータ



複雑さ

システムの拡大と変化が早いため、情報を最新化し、全てを理解しインシデントを適切に判断することが困難



人材と スキル不足

熟練した技術力のあるセキュリティエンジニアの不足

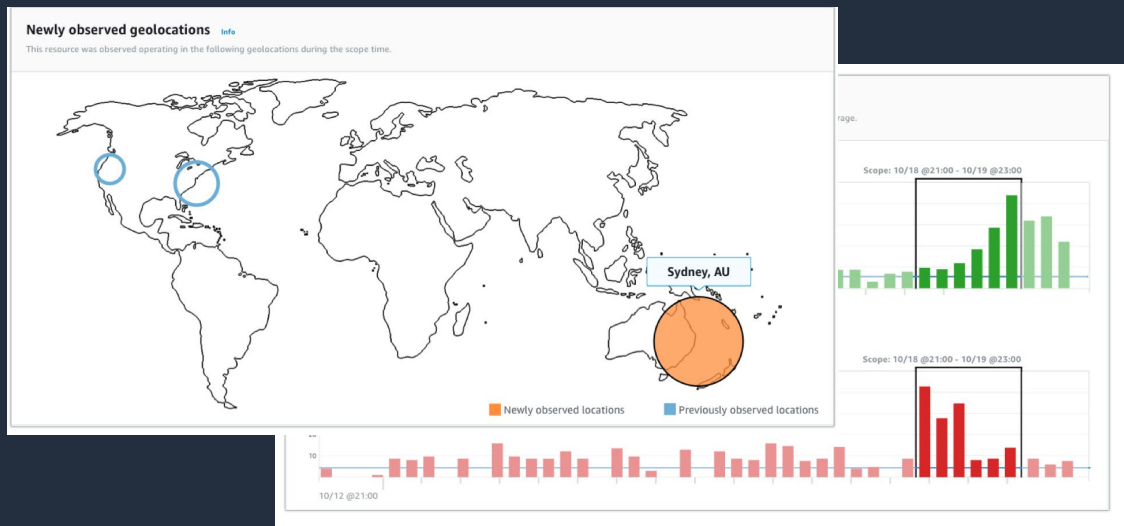


セキュリティ 対策コスト

外部のサービス利用、または内部で体制作りがあるが、どちらもコストが高い

Amazon Detective とは

2020年3月31日に一般提供開始(GA)
セキュリティデータの分析、視覚化をして、
潜在的なセキュリティ問題の根本原因を迅速に特定



Amazon Detective の特徴



ログの自動収集

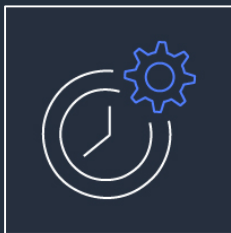


分析の自動化



視覚化

お客様にとってのメリット



より迅速で効果的な調査

情報を一ヶ所に集めて、統一的な画面からインタラクティブに調査。通常値と異常値の表示、時系列の変化、影響を受けたリソースや関連する情報へのドリルダウン等で迅速に調査可能です



継続的なデータ更新で時間と労力を節約

テラバイト規模の通信ログ、AWSの操作履歴、脅威の検出結果を継続的に自動で収集して、グラフモデルにまとめます。お客様のデータ収集・管理する時間を節約できます



使いやすい視覚化

機械学習、統計分析、グラフ理論を利用したインタラクティブな視覚化を提供します。お客様がデータを整理したり、独自のクエリやコード、アルゴリズムを開発、構成、調整する必要はありません

Amazon Detective の主要なユースケース



アラートの
トリアージ

脅威検出結果の分析

インシデント
調査

影響範囲の特定

スレット
ハンティング

侵害痕跡の調査

ユースケース(アラートのトリアージ)



アラートの
トリアージ

脅威検出結果の分析

- アラートがお客様環境にとって True Positive (正しい検出)か False Positive (誤った検出)かを素早く分析
- 分析例
 - 送信データのサイズは？
 - この通信は常時発生しているのか？
 - インシデントの前に何が起きたか？
 - API コールの失敗は異常なことか？
- False Positive なら不要な調査を回避
- True Positive と判断、または False Positive の判断ができない場合は、優先順位をつけて、インシデント調査へ

ユースケース(インシデント調査)



影響範囲の特定

- インシデントの根本原因や、被害の影響を特定するための本格調査
- 他のデータと関連させた深い調査
- 関連するリソースにも拡大して実施
- 分析例
 - この IP アドレスがコールした API は？
 - この API コールは偵察活動か？
 - 他に悪用された Principal ID はあるか？
 - この IP と通信している EC2 インスタンスはあるか？

ユースケース(スレットハンティング)



侵害痕跡の調査

- 内外の Indicator of Compromise(侵害の痕跡)を元に自組織にも影響があるか調査
- 分析例
 - 脅威レポートで報告された IP アドレスが過去1年間に EC2 インスタンスと通信をしたか？
 - 疑わしい User Agent がした 全ての API コールを確認

ご利用方法：Amazon Detective の有効化



前提サービス：Amazon GuardDuty

GuardDuty 有効化の48時間経過後に Amazon Detective のコンソールに移動



ご利用方法：Amazon Detective の有効化



aws サービス リソースグループ

Security, Identity, & Compliance

Amazon Detective

Investigate potential security issues

Amazon Detective makes it easy to investigate, analyze, and quickly identify the root cause of potential security issues or suspicious activities. Amazon Detective automatically collects log data from your AWS resources and uses machine learning, statistical analysis, and graph theory to help you visualize and conduct faster and more efficient security investigations.

Get started with Detective

- Automatically collects log data from your AWS resources
- Assists in visualizing and conducting faster and more efficient security investigations

[Get started](#)

[Learn about our 30-day free trial](#)

ご利用方法：Amazon Detective の有効化



Amazon Detective の有効化後は
24時間程度お待ちください
データの収集とグラフモデルへの
変換が行われます

Enable Amazon Detective

Align master accounts (recommended)

Master account alignment allows an account to select a finding in Amazon GuardDuty or AWS Security Hub and pivot seamlessly into Detective. Once in the Detective console, a master account can archive GuardDuty findings.

To enable this capability, we recommend using the same account as the master across GuardDuty, Security Hub, and Detective. If this is not possible, you can set up a cross-account role to allow multiple accounts to act as the master across these services. [Learn more](#)

Attach IAM policy

Before you enable Detective, you must have the following IAM policy attached to your user or role. This policy is intended for master accounts only. After you enable Detective, you can view this policy from the General page.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "detective:CreateGraph",
        "detective:CreateMembers",
        "detective>DeleteGraph",
        "detective>DeleteMembers",
      ]
    }
  ]
}
```

Copy IAM policy

Cancel

Enable Amazon Detective

ご利用方法：Amazon Detective の有効化の確認



Detective のサーチコンソールにて自身のグローバルアドレスを検索

The screenshot shows the Amazon Detective Search console interface. On the left is a navigation sidebar with a 'Detective' header and a close button. Below it are sections for 'Getting started' and 'Settings'. The 'Search' option is highlighted in orange, with a large orange arrow labeled '1' pointing to it. Under 'Settings', 'Account management' is selected, and 'IP address' is highlighted in orange, with a large orange arrow labeled '2' pointing to it. The main content area is titled 'Search' and contains the instruction 'Search for a finding or resource.' Below this is a search input field with a dropdown menu for 'Select type'. The dropdown menu is open, showing options: 'GuardDuty finding', 'AWS account', 'EC2 instance', 'IP address', 'AWS role', 'AWS user', and 'User agent'. The 'IP address' option is highlighted in orange, with a large orange arrow labeled '3' pointing to it. The search input field contains the placeholder text 'Select the entity ID for the entity ID' and a 'Search' button.

セキュリティ分析の調査例

事象

Amazon GuardDuty で CryptoCurrency:EC2/BitcoinTool.B を検出
EC2 インスタンスが仮想通貨(暗号資産)マイニングに悪用された疑い

調査プロセス

① Amazon GuardDuty または AWS Security Hub から脅威を確認

② トリアージ

このインシデントは False Positive(誤検知)か True Positive(真の検知)か？
本当にマイニングか？いつから発生か？まだ続いているのか？

③ インシデント調査

どのユーザーがいつ EC2 インスタンスを起動したのか？

マイニングをしている EC2 インスタンス は他の不正を行っていないか？

調査例：Amazon GuardDuty から調査開始

GuardDuty × 結果

表示中: 2 / 2 1 0 1

結果

無料トライアル

アクション ▼ 結果の抑制

保存済みのルール 保存済みのルールがありません

最近 ▼ フィルタの追加

<input type="checkbox"/>	▼ 検出タイプ	▼ リソース	▼ 最終アクセス	▼ カウント
<input type="checkbox"/>	△ CryptoCurrency:EC2/BitcoinTool.B	Instance: i-08a8e40be65425909	10分前	966
<input type="checkbox"/>	○ Stealth:IAMUser/CloudTrailLoggingDisabled	DetectiveDemo-AdminUser-1FJ4B2YNDYPYG: AKIAT4OQX3HXV6NI6YXX	8日前	1

検出結果を確認するために検出タイプを選択

調査例 : Amazon GuardDuty から調査開始

GuardDuty ×

結果 ☾

表示中: 2 / 2 1 0 1

CryptoCurrency:EC2/BitcoinTool.B 🔍

結果 ID: c2b98b95c5440025c05b405065ed3bb9 フィードバック

無料トライアル

結果の抑制

保存済みのルール

最近 ▼ フィルタの追加

<input type="checkbox"/>	検索タイプ	リソース	最...	カウ...
<input type="checkbox"/>	△	CryptoCurrency:EC2/BitcoinTool.B	Instance: i-08a8e40be65425909	10分前 966
<input type="checkbox"/>	○	Stealth:IAMUser/CloudTrailLoggingDisabled	DetectiveDemo-AdminUser-1FJ4B2YNDYPY	8日前 1

作成時刻、更新時刻、通信先 IP アドレス、EC2 インスタンス ID 等を確認

次の疑問
本当に仮想通貨(暗号資産)マイニングの通信か？
定常的に続いているのか？

重要度 高い 🔍

リージョン us-east-1

アカウント 966

アカウント ID 267...99 🔍

リソース ID i-08a8e40be65425909 🔍

作成時刻 2020-07-04 09:13:16 (8日前)

更新時刻 2020-07-12 10:13:17 (10分前)

▼ 影響を受けるリソース

Resource role TARGET 🔍	Resource type Instance 🔍
Instance ID i-08a8e40be65425909 🔍	Port 49738
Port name Unknown	Instance type t2.micro
Instance state running	Availability zone us-east-1a
Image ID ami-09d95fab7fff3776c 🔍	Image description Amazon Linux 2 AMI 2.0.20200520.1 x...

調査例：Amazon GuardDuty から調査開始

GuardDuty ×

結果

表示中: 2 / 2 1 0 1

CryptoCurrency:EC2/BitcoinTool.B 🔍

結果 ID: c2b98b95c5440025c05b405065ed3bb9 [フィードバック](#)

🚨 EC2 instance i-08a8e40be65425909 is communicating outbound with a known Bitcoin-related IP address 104. [redacted].42. [Learn More](#)

アクション ▲	結果の抑制	保存済みのルール	保存済みのルールがありません
アーカイブ	フィルタの追加		
エクスポート...			
元に戻す			
調査			

タイプ	リソース	最...	カウ...
<input checked="" type="checkbox"/>	🚨 CryptoCurrency:EC2/BitcoinTool.B Instance: i-08a8e40be65425909	10分前	966
<input type="checkbox"/>	🔵 Stealth:IAMUser/CloudTrailLoggingDisabled DetectiveDemo-AdminUser-1FJ4B2YNDYPY	8日前	1

Amazon Detective で調査を開始する方法

- ① 該当の検出タイプにチェックを入れる
- ② プルダウンメニューの「調査」を選択

⇒ Detective のコンソールへ

重要度	リージョン
高い 🔍	us-east-1
カウント	アカウント ID
966	267 [redacted] 99 🔍
リソース ID	作成時刻
i-08a8e40be65425909 🔍	2020-07-04 09:13:16 (8日前)
更新時刻	
2020-07-12 10:13:17 (10分前)	
▼ 影響を受けるリソース	
Resource role	Resource type
TARGET 🔍	Instance 🔍
Instance ID	Port
i-08a8e40be65425909 🔍	49738
Port name	Instance type
Unknown	t2.micro
Instance state	Availability zone
running	us-east-1a
Image ID	Image description
ami-09d95fab7ff3776c 🔍	Amazon Linux 2 AMI 2.0.20200520.1 x...

調査例 : AWS Security Hub から調査開始

Security Hub

Security Hub > 検出結果

検出結果

検出結果は、セキュリティ上の問題か、失敗したセキュリティチェックです。

アクション

ワークフローステータスを変更

インサイトを作成する

ワークフローのステータス EQUALS NEW

ワークフローのステータス EQUALS NOTIFIED

レコードの状態 EQUALS ACTIVE

フィルターの追加

重要度	ワークフローのステータス	会社	製品	タイトル	リソ
MEDIUM	NEW	Amazon	GuardDuty	EC2 instance i-08a8e40be65425909 communicating with a known Bitcoin-related IP Address.	arn:a-east-1:267262613999:detector/i-08a8e40be65425909
MEDIUM	NEW	AWS	Security Hub	S3.4 S3 buckets should have server-side encryption enabled	AWS 267262613999
				EC2.2 The VPC default subnets should have IAM attached to them	AWS 267262613999

Amazon Detective で調査を開始する方法

- ① 該当の検出タイプを選択する
- ② 詳細情報の「結果の調査」を選択
⇒ Detective のコンソールへ

EC2 instance i-08a8e40be65425909 communicating with a known Bitcoin-related IP Address.

Finding ID: arn:aws:guardduty:us-east-1:267262613999:detector/i-08a8e40be65425909/finding/c2b98b95c5440025c05b405065ed3bb9

MEDIUM

EC2 instance i-08a8e40be65425909 is communicating outbound with a known Bitcoin-related IP address 104.24.1.42.

ワークフローのステータス

新規

レコードの状態

ACTIVE

検出結果プロバイダーによって設定

AWS アカウント ID

267262613999

重要度 (オリジナル)

8

重要度 (正規化済み)

60

作成時刻

2020-07-04T00:13:16.296Z

更新日時

2020-07-12T01:13:17.885Z

製品名

GuardDuty

重要度ラベル

MEDIUM

会社名

Amazon

種類および関連検出結果

リソース

Amazon Detective の調査

結果の調査

調査例：プロファイル (GuardDuty)

Detective

Getting started
Search

Settings
Account management
General
Preferences
Usage

⚠ Detective is baselining member account data
The data and analytics within Detective will improve as we ingest and baseline member account data. Baselining typically takes two weeks. Your estimated date is 07/16/2020.

Detective > Search > GuardDuty/c2b98b95c5440025c05b405065ed3bb9



EC2 instance i-08a8e40be65425909 communicating with a known Bitcoin-related IP Address. [情報](#)

CryptoCurrency:EC2-BitcoinTool.B

Scope time [情報](#)
07/04, 00:00 - 07/12, 02:00

Lock

Detective の開始後2週間はトレーニング期間

GuardDuty finding details

[Archive finding](#)

EC2 instance i-08a8e40be65425909 is communicating outbound with a known Bitcoin-related IP address 104. [redacted] 42.

Finding details

GuardDuty finding ID
c2b98b95c5440025c05b405065ed3bb9

Finding time
07/04/2020, 00:12 UTC - 07/12/2020, 01:12 UTC

Finding severity
60

Finding direction
Outbound

Involved AWS resources

AWS account
267. [redacted] 99

EC2 instance
i-08a8e40be65425909

Overall VPC flow volume [情報](#)

Summarizes the overall volume of VPC flow data into and out of the EC2 instance, compared to baseline averages from the prior 45 days.

調査例：時間範囲の固定

Detective ×

Getting started
Search

▼ Settings

Account management
General
Preferences
Usage

Detective > Search > GuardDuty/c2b98b95c5440025c05b405065ed3bb9



EC2 instance i-08a8e40be65425909 communicating with a known Bitcoin-related IP Address. [情報](#)

CryptoCurrency:EC2-BitcoinTool.B

Scope time [情報](#)
07/04, 00:00 - 07/12, 02:00
 Lock

Overview VPC flow details

GuardDuty finding details

EC2 instance i-08a8e40be65425909 is communicating outbound with a known Bitcoin-related IP address 104. 42.

[Archive finding](#)

Finding details

GuardDuty finding ID
c2b98b95c5440025c05b405065ed3bb9

Finding time
07/04/2020, 00:12 UTC - 07/12/2020, 01:12 UTC

Finding severity
60

Finding direction
Outbound

Involved AWS resources

AWS account
267. 99

EC2 instance
i-08a8e40be65425909

Overall VPC flow volume [情報](#)

Summarizes the overall volume of VPC flow data into and out of the EC2 instance, compared to baseline averages from the prior 45 days.

[Linear](#) [Log](#)

Inbound traffic

Scope start: 07/04, 00:00

Scope end: 07/12, 02:00

調査例：時間範囲の固定

Detective ×

Getting started
Search

▼ Settings

Account management
General
Preferences
Usage

Detective > Search > GuardDuty/c2b98b95c5440025c05b405065ed3bb9



EC2 instance i-08a8e40be65425909 communicating with a known Bitcoin-related IP Address. [情報](#)

CryptoCurrency:EC2-BitcoinTool.B

Scope time [情報](#)

07/04, 00:00 - 07/12, 02:00

Lock

Overview **VPC flow details**

GuardDuty finding details

EC2 instance i-08a8e40be65425909 is communicating outbound with a known Bitcoin-related IP address 104. 42.

[Archive finding](#)

Finding details

GuardDuty finding ID
c2b98b95c5440025c05b405065ed3bb9

Finding time
07/04/2020, 00:12 UTC - 07/12/2020, 01:12 UTC

Finding severity
60

Finding direction
Outbound

Involved AWS resources

AWS account
267. 99

EC2 instance
i-08a8e40be65425909

Overall VPC flow volume [情報](#)

Summarizes the overall volume of VPC flow data into and out of the EC2 instance, compared to baseline averages from the prior 45 days.

Inbound traffic

Scope start: 07/04, 00:00

Scope end: 07/12, 02:00

調査例：時間範囲の固定

Edit scope time ✕

Editing the scope time updates the content of the profile.

Start: 2020/07/03 00 :00 UTC End: 2020/07/11 02 :00 UTC

Historical [6H](#) [24H](#) [3D](#) [7D](#) [14D](#) [30D](#) [Default](#) ⓘ

Lock
Locking the scope time maintains the same time window across profiles.

[Cancel](#) [Update scope time](#)

EC2 instance
known Bitcoin
Cryptocurrency:EC2-Bit

GuardDuty finding details
EC2 instance: i-08a8e40be5425908 in com

GuardDuty finding ID	Finding time	Finding severity
c2b98b95c5440025c05b405065ed5bb9	07/04/2020, 00:12 UTC - 07/12/2020, 01:12 UTC	60

Involved AWS resources

AWS account	EC2 instance
267-██████-99	i-08a8e40be5425908

Overall VPC flow volume 📊
Summarizes the overall volume of VPC flow data into and out of the EC2 instance, compared to baseline volumes from the prior 15 days.

Inbound traffic

Scope time: 07/04, 00:00 - 07/12, 02:00
[Lock](#) [Edit](#)

[Archive finding](#)

[Linear](#) [Log](#)

調査例：プロファイルタブ (Overview)

Detective

Getting started
Search

▼ Settings

Account management
General
Preferences
Usage

Detective > Search > GuardDuty/c2b98b95c5440025c05b405065ed3bb9



EC2 instance i-08a8e40be65425909 communicating with a known Bitcoin-related IP Address. [情報](#)

CryptoCurrency:EC2-BitcoinTool.B

Scope time [情報](#)
07/04, 00:00 - 07/12, 02:00

Lock

Overview [VPC flow details](#)

GuardDuty finding details

EC2 instance i-08a8e40be65425909 is communicating outbound with a known Bitcoin-related IP address 104. 42.

[Archive finding](#)

Finding details

GuardDuty finding ID
c2b98b95c5440025c05b405065ed3bb9

Finding time
07/04/2020, 00:12 UTC - 07/12/2020, 01:12 UTC

Finding severity
60

Finding direction
Outbound

Involved AWS resources

AWS account
267. 99

EC2 instance
i-08a8e40be65425909

Overall VPC flow volume [情報](#)

Summarizes the overall volume of VPC flow data into and out of the EC2 instance, compared to baseline averages from the prior 45 days.

Inbound traffic

Scope start: 07/04, 00:00

Scope end: 07/12, 02:00

調査例：プロファイルパネル

Detective

Getting started
Search

Settings

Account management
General
Preferences
Usage

Detective > Search > GuardDuty/c2b98b95c5440025c05b405065ed3bb9



EC2 instance i-08a8e40be65425909 communicating with a known Bitcoin-related IP Address. [情報](#)

CryptoCurrency:EC2-BitcoinTool.B

Scope time [情報](#)

07/04, 00:00 - 07/12, 02:00

Lock

Overview VPC flow details

GuardDuty finding details

EC2 instance i-08a8e40be65425909 is communicating outbound with a known Bitcoin-related IP address 104. [redacted] 42. [Archive finding](#)

Finding details

GuardDuty finding ID
c2b98b95c5440025c05b405065ed3bb9

Finding time
07/04/2020, 00:12 UTC - 07/12/2020, 01:12 UTC

Finding severity
60

Finding direction
Outbound

Involved AWS resources

AWS account
267. [redacted] 99

EC2 instance
i-08a8e40be65425909

Overall VPC flow volume [情報](#)

Summarizes the overall volume of VPC flow data into and out of the EC2 instance, compared to baseline averages from the prior 45 days.

Inbound traffic

Scope start: 07/04, 00:00

Scope end: 07/12, 02:00

調査例：プロファイルパネル(GuardDuty finding details)

Detective X

Detective > Search > GuardDuty/c2b98b95c5440025c05b405065ed3bb9



EC2 instance i-08a8e40be65425909 communicating with a known Bitcoin-related IP Address. [情報](#)

CryptoCurrency:EC2-BitcoinTool.B

Scope time [情報](#)
07/04, 00:00 - 07/12, 02:00

Lock

Overview VPC flow details

GuardDuty finding details

EC2 instance i-08a8e40be65425909 is communicating outbound with a known Bitcoin-related IP address 104. [redacted] 42.

[Archive finding](#)

Finding details

GuardDuty finding ID
c2b98b95c5440025c05b405065ed3bb9

Finding time
07/04/2020, 00:12 UTC - 07/12/2020, 01:12 UTC

Finding severity
60

Finding direction
Outbound

Detective から調査が完了した検出結果について GuardDuty のアーカイブ処理が可能

Involved AWS resources

AWS account
267. [redacted] 99

EC2 instance
i-08a8e40be65425909

Overall VPC flow volume [情報](#)

Summarizes the overall volume of VPC flow data into and out of the EC2 instance, compared to baseline averages from the prior 45 days.

Inbound traffic

Scope start: 07/04, 00:00

Scope end: 07/12, 02:00

下にスクロール

調査例：プロファイルパネル

Detective X

Finding direction

Outbound

Involved AWS resources

AWS account

267. [redacted] 99

EC2 instance

i-08a8e40be65425909

Getting started
Search

Settings

Account management
General
Preferences
Usage

Overall VPC flow volume 情報

Summarizes the overall volume of VPC flow data into and out of the EC2 instance, compared to baseline averages from the prior 45 days.

過去45日間のベースライン

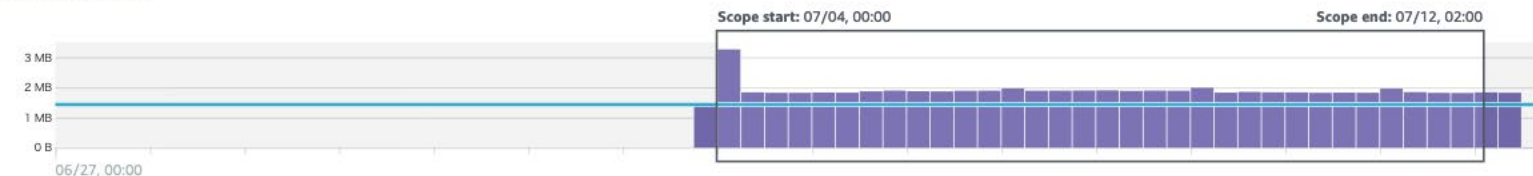
Linear

Log

Inbound traffic



Outbound traffic



調査例：プロファイルパネルガイド

Detective

Getting started
Search

▼ Settings

Account management
General
Preferences
Usage

Finding direction

Outbound

Involved AWS resources

AWS account
267. [redacted] 99

EC2 instance
i-08a8e40be65425909

Overall VPC flow volume [情報](#)

Summarizes the overall volume of VPC flow data in this instance, compared to baseline averages from the prior 45 days.

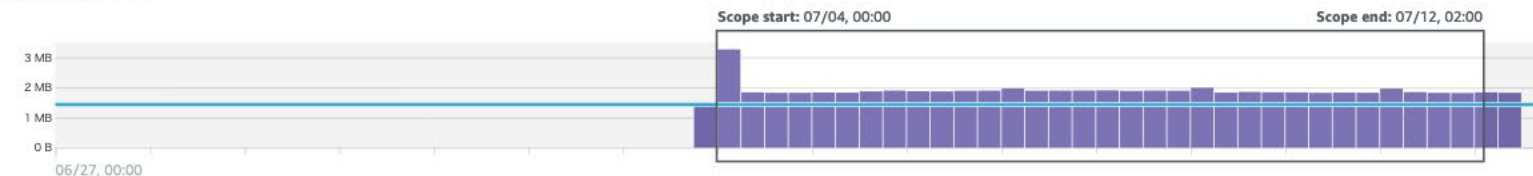


Linear Log

Inbound traffic



Outbound traffic



調査例：プロフィールパネルガイド

Detective X

Getting started
Search

▼ Settings

Account management
General
Preferences
Usage

Finding direction

Outbound

Involved AWS resources

AWS account
267. [redacted] 99

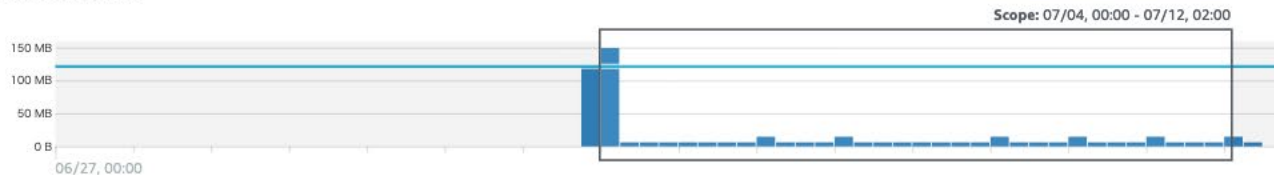
EC2 instance
i-08a8e40be65425909

Overall VPC flow volume 情報

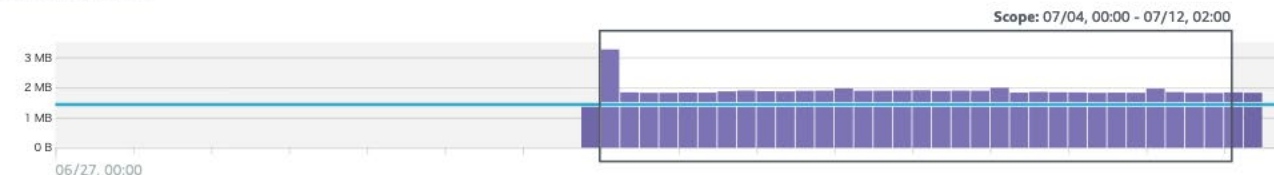
Summarizes the overall volume of VPC flow data into and out of the EC2 instance, compared to baseline averages from the prior 45 days.

Linear Log

Inbound traffic



Outbound traffic



Overall VPC flow volume X

This profile panel displays the overall volume of bytes into and out of the EC2 instance for all destination IP addresses.

A question to consider:

- Is the volume regular (flat or periodic), or are there any unexpected increases or decreases in either direction?

How to use this profile panel

The highlighted portion of the timeline is the scope time.

The baseline value shows the average flow volume per time interval during the previous 45 days, ignoring time intervals without activity.

Learn more [↗](#)

[Viewing and interacting with profile panels](#)

上にスクロール

調査例：プロファイルタブ

Detective

Getting started
Search

Settings

Account management
General
Preferences
Usage

Detective > Search > GuardDuty/c2b98b95c5440025c05b405065ed3bb9



EC2 instance i-08a8e40be65425909 communicating with a known Bitcoin-related IP Address. [情報](#)

CryptoCurrency:EC2-BitcoinTool

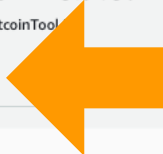
Scope time [情報](#)

07/04, 00:00 - 07/12, 02:00

Lock

Overview

VPC flow details



GuardDuty finding details

EC2 instance i-08a8e40be65425909 is communicating outbound with a known Bitcoin-related IP address 104.██████████42.

[Archive finding](#)

Finding details

GuardDuty finding ID
c2b98b95c5440025c05b405065ed3bb9

Finding time
07/04/2020, 00:12 UTC - 07/12/2020, 01:12 UTC

Finding severity
60

Finding direction
Outbound

Involved AWS resources

AWS account
267.██████████99

EC2 instance
i-08a8e40be65425909

Overall VPC flow volume [情報](#)

Summarizes the overall volume of VPC flow data into and out of the EC2 instance, compared to baseline averages from the prior 45 days.

Inbound traffic

Scope start: 07/04, 00:00

Scope end: 07/12, 02:00

調査例：プロファイルタブ (VPC Flow details)

Detective

Getting started
Search

Settings

Account management
General
Preferences
Usage

Detective > Search > GuardDuty/c2b98b95c5440025c05b405065ed3bb9



EC2 instance i-08a8e40be65425909 communicating with a known Bitcoin-related IP Address. [情報](#)

CryptoCurrency:EC2-BitcoinTool.B

Scope time [情報](#)
07/04, 00:00 - 07/12, 02:00

Lock

Overview **VPC flow details**

VPC traffic between the finding EC2 instance and 104. [REDACTED] 42 [情報](#)

Shows the average flow volume between the EC2 instance and the remote IP addresses involved in this finding. Expand each row to see a timeline of that communication.

Remote IP address ▾

Average inbound volume (scope time) ▾

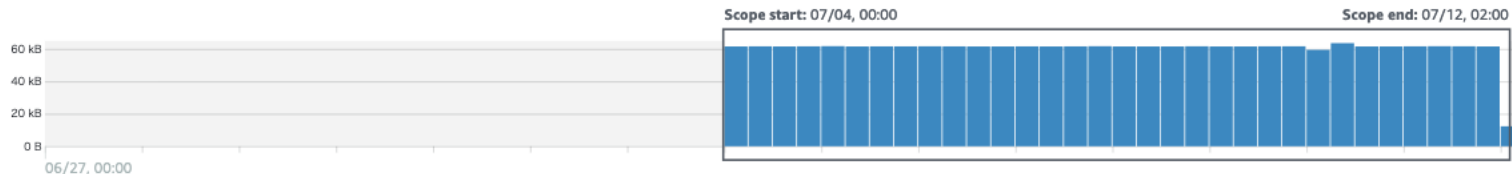
Average outbound volume (scope time) ▾

▾ 104. [REDACTED] 42

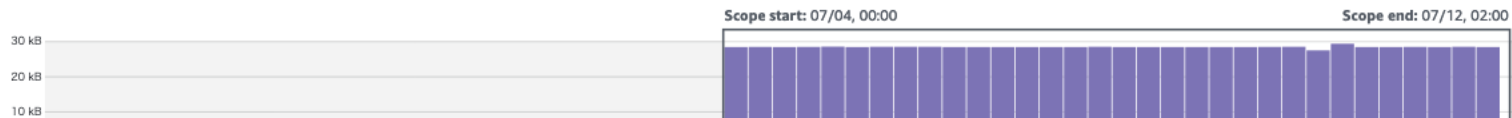
10.2 kB/hour

4.7 kB/hour

Inbound traffic



Outbound traffic



調査例：IP アドレスごとの時系列グラフ

Detective

Getting started
Search

Settings

Account management
General
Preferences
Usage

Detective > Search > GuardDuty/c2b98b95c5440025c05b405065ed3bb9



EC2 instance i-08a8e40be65425909 communicating with a known Bitcoin-related IP Address. [情報](#)

CryptoCurrency:EC2-BitcoinTool.B

Scope time [情報](#)

07/04, 00:00 - 07/12, 02:00

Lock

Overview **VPC flow details**

VPC traffic between the finding EC2 instance and 104. [情報](#)

Shows the average flow volume between the EC2 instance and the remote IP addresses involved in this finding. Expand each row to see

Remote IP address ▾

▾ 104. [情報](#)

通信トラフィックの時系列から、ビットコイン特有の通信が続いておりインシデントと判断
⇒ 本格調査へ

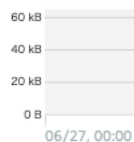
Average inbound volume (scope time) ▾

10.2 kB/hour

Average outbound volume (scope time) ▾

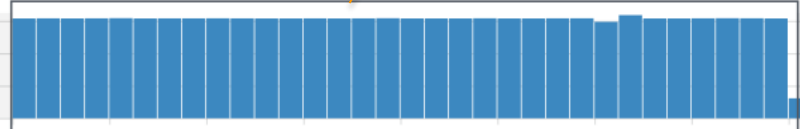
4.7 kB/hour

Inbound traffic



Scope start: 07/04, 00:00

Scope end: 07/12, 02:00



Outbound traffic



Scope start: 07/04, 00:00

Scope end: 07/12, 02:00



調査例：IP アドレスのプロファイルヘッドリルダウン

Detective

Getting started

Search

Settings

Account management

General

Preferences

Usage

Detective > Search > GuardDuty/c2b98b95c5440025c05b405065ed3bb9



EC2 instance i-08a8e40be65425909 communicating with a known Bitcoin-related IP Address. [情報](#)

CryptoCurrency:EC2-BitcoinTool.B

Scope time [情報](#)

07/04, 00:00 - 07/12, 02:00

Lock

Overview

VPC flow details

VPC traffic between the finding EC2 instance and 104. [REDACTED].42 [情報](#)

Shows the average flow volume between the EC2 instance and the remote IP addresses involved in this finding. Expand each row to see a timeline of that communication.

Remote IP address ▾

Average inbound volume (scope time) ▾

Average outbound volume (scope time) ▾

104. [REDACTED].42

10.2 kB/hour

4.7 kB/hour

Inbound traffic

60 kB

40 kB

20 kB

0 B

06/27,

Outbound traffic

30 kB

20 kB

10 kB

Scope start: 07/04, 00:00

Scope end: 07/12, 02:00

Scope start: 07/04, 00:00

Scope end: 07/12, 02:00

- リンクを新しいタブで開く
- リンクを新しいウィンドウで開く
- リンクを新しいプライベートウィンドウで開く
- このリンクをブックマーク
- 名前を付けてリンク先を保存...
- リンクの URL をコピー
- Google で検索: "104. [REDACTED].42"
- 要素を調査

調査例：プロフィール (IP アドレス)

Detective X

Getting started
Search

▼ Settings

Account management
General
Preferences
Usage

Detective > Search > IpAddress/104.1[redacted].42



104.[redacted].42 情報

IP address

Scope time 情報

07/04, 00:00 - 07/12, 02:00

Lock Edit

Overview New behavior Resource interaction

IP address details 情報

High-level descriptive data for the given IP address.

First observed

07/03/2020, 15:59 UTC

Last observed

07/12/2020, 01:24 UTC

Total times observed

-

Distinct AWS users and roles

-

Count of related user agents

-

Findings associated with IP address 104.[redacted].42 情報

The following findings occurred on this resource around the scope time.

Filter by title and type

Title	Finding type	First observed	Last observed	Finding severity
EC2 instance i-074af3e48bb2bbd77 communicating with a known Bitcoin-related IP Address.	TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B	07/05/2020, 12:47 UTC	07/12/2020, 01:24 UTC	60
EC2 instance i-08a8e40be65425909 communicating with a known Bitcoin-related IP Address.	TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B	07/04/2020, 00:12 UTC	07/12/2020, 01:12 UTC	60
EC2 instance i-074af3e48bb2bbd77 communicating with a known Bitcoin-related IP Address.	TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B	07/03/2020, 15:59 UTC	07/05/2020, 12:36 UTC	60

調査例：プロフィール (IP アドレス)

Detective

Getting started
Search

Settings

Account management
General
Preferences
Usage

Detective > Search > IpAddress/104.1[redacted].42



104.[redacted].42 情報

IP address

Scope time 情報

07/04, 00:00 - 07/12, 02:00

Lock Edit

Overview New behavior Resource interaction

IP address details 情報

High-level descriptive data for the given IP address.

First observed

07/03/2020, 15:59 UTC

Last observed

07/12/2020, 01:24 UTC

Total times observed

-

Distinct AWS users and roles

-

Count of related user agents

-

Findings associated with IP address 104.[redacted].42 情報

The following findings occurred on this resource around the scope time.

Filter by title and type

Title	Finding type	First observed	Last observed	Finding severity
EC2 instance i-074af3e48bb2bbd77 communicating with a known Bitcoin-related IP Address.	TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B	07/05/2020, 12:47 UTC	07/12/2020, 01:24 UTC	60
EC2 instance i-08a8e40be65425909 communicating with a known Bitcoin-related IP Address.	TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B	07/04/2020, 00:12 UTC	07/12/2020, 01:12 UTC	60
EC2 instance i-074af3e48bb2bbd77 communicating with a known Bitcoin-related IP Address.	TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B	07/03/2020, 15:59 UTC	07/05/2020, 12:36 UTC	60

調査例：プロフィール (IP アドレス)

Detective

Detective > Search > IpAddress/104.1...42

Getting started
Search



104. ... 42 情報
IP address

Scope time 情報

07/04, 00:00 - 07/12, 02:00

Lock Edit

Overview New behavior Resource interaction

IP address details 情報

High-level descriptive data for the given IP address.

First observed
07/03/2020, 15:59 UTC

別のインスタンスも侵害されている可能性あり

Distinct AWS users and roles

Findings associated with IP address 104. ... 42 情報

The following findings occurred on this resource around the scope time.

Filter by title and type

Title	Finding type	First observed	Last observed	Finding severity
EC2 instance i-074af3e48bb2bbd77 communicating with a known Bitcoin-related IP Address.	TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B	07/05/2020, 12:47 UTC	07/12/2020, 01:24 UTC	60
EC2 instance i-08a8e40be65425909 communicating with a known Bitcoin-related IP Address.	TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B	07/04/2020, 00:12 UTC	07/12/2020, 01:12 UTC	60
EC2 instance i-074af3e48bb2bbd77 communicating with a known Bitcoin-related IP Address.	TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B	07/03/2020, 15:59 UTC	07/05/2020, 12:36 UTC	60

下にスクロール

調査例：プロフィール (IP アドレス)

Detective X

Getting started
Search

▼ Settings
Account management
General
Preferences
Usage

Findings associated with IP address 104. [REDACTED].42 情報

The following findings occurred on this resource around the scope time.

Q Filter by title and type

Title	Finding type	First observed	Last observed	Finding severity
EC2 instance i-08a8e40be65425909 communicating with a known Bitcoin-related IP Address.	TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B	07/04/2020, 00:12 UTC	07/12/2020, 01:12 UTC	60
EC2 instance i-074af3e48bb2bbd77 communicating with a known Bitcoin-related IP Address.	TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B	07/03/2020, 15:59 UTC	07/05/2020, 12:36 UTC	60

Overall API call volume 情報

Overall volume of API calls issued by this resource around the scope time.

Successful calls - of scope time call volume

時間範囲内での API コール数
⇒ 成功も失敗もない

Linear Log

No successful API calls observed

Failed calls - of scope time call volume

No failed API calls observed

上にスクロール

調査例：プロファイルタブ

Detective

Getting started
Search

▼ Settings

Account management
General
Preferences
Usage

Detective > Search > ipAddress/104.1[redacted].42



104.[redacted].42 情報

IP address

Scope time 情報

07/04, 00:00 - 07/12, 02:00

Lock Edit

Overview

New behavior

Resource interaction



IP address details 情報

High-level descriptive data for the given IP address.

First observed

07/03/2020, 15:59 UTC

Last observed

07/12/2020, 01:24 UTC

Total times observed

-

Distinct AWS users and roles

-

Count of related user agents

-

Findings associated with IP address 104.[redacted].42 情報

The following findings occurred on this resource around the scope time.

Filter by title and type

Title	Finding type	First observed	Last observed	Finding severity
EC2 instance i-074af3e48bb2bbd77 communicating with a known Bitcoin-related IP Address.	TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B	07/05/2020, 12:47 UTC	07/12/2020, 01:24 UTC	60
EC2 instance i-08a8e40be65425909 communicating with a known Bitcoin-related IP Address.	TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B	07/04/2020, 00:12 UTC	07/12/2020, 01:12 UTC	60
EC2 instance i-074af3e48bb2bbd77 communicating with a known Bitcoin-related IP Address.	TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B	07/03/2020, 15:59 UTC	07/05/2020, 12:36 UTC	60

調査例：プロファイルタブ (Resource Interaction)

Detective

⚠ Detective is baselining member account data
The data and analytics within Detective will improve as we ingest and baseline member account data. Baselining typically takes two weeks. Your estimated date is 07/16/2020.

Getting started
Search

Settings
Account management
General
Preferences
Usage

Detective > Search > IPAddress/104. .42



104. .42 情報
IP address

Scope time 情報

07/04, 00:00 - 07/12, 02:00

Lock Edit

Overview New behavior **Resource interaction**

Resource interaction 情報

This IP address interacted with the following AWS roles, users, and accounts during the scope time.

Name	Resource type	AWS account	First observed	Last observed
------	---------------	-------------	----------------	---------------

No results to display

EC2 instances communicating with IP address 情報

EC2 instance	First observed	Last observed	Inbound traffic	Outbound traffic
i-074af3e48bb2bbd77	07/03/2020, 15:00 UTC	07/12/2020, 01:00 UTC	1.99 MB	915 kB
i-08a8e40be65425909	07/04/2020, 00:00 UTC	07/12/2020, 01:00 UTC	1.99 MB	914 kB

調査例：EC2 インスタンスのプロファイルヘッドリルダウン

Detective

⚠ Detective is baselining member account data
The data and analytics within Detective will improve as we ingest and baseline member account data. Baselining typically takes two weeks. Your estimated date is 07/16/2020.

Getting started

Search

Settings

Account management

General

Preferences

Usage

Detective > Search > IPAddress/104. [redacted] .42



104. [redacted] .42 情報

IP address

Scope time 情報

07/04, 00:00 - 07/12, 02:00

Lock Edit

Overview New behavior Resource interaction

Resource interaction 情報

This IP address interacted with the following AWS roles, users, and accounts during the scope time.

🔍

Name	Resource type	AWS account	First observed	Last observed
No results to display				

EC2 instances communicating with IP address 情報

EC2 instance	Last observed	Inbound traffic	Outbound traffic
i-074af3e48bb2bbd	07/12/2020, 04:00 UTC	1.99 MB	918 kB
i-08a8e40be654259	07/12/2020, 04:00 UTC	1.99 MB	916 kB

リンクを新しいタブで開く
リンクを新しいウィンドウで開く
リンクを新しいプライベートウィンドウで開く

このリンクをブックマーク
名前を付けてリンク先を保存...
リンクの URL をコピー
Google で検索: "i-08a8e40be6542..."

要素を調査

調査例：プロフィール (EC2 インスタンス)

Detective X

Getting started
Search

▼ Settings

Account management
General
Preferences
Usage

Detective > Search > Ec2Instance/i-08a8e40be65425909



i-08a8e40be65425909 情報

EC2 instance

Scope time 情報

07/04, 00:00 - 07/12, 02:00

Lock Edit

Overview

EC2 instance details 情報

High-level descriptive data for the given EC2 instance

EC2 creation date

07/03/2020, 23:56 UTC

ARN

-

Created by

DetectiveDemo-AdminUser-1FJ482YN...

Associated VPC

vpc-0c755a714886152a3

Overall VPC flow volume 情報

Summarizes the overall volume of VPC flow data into and out of the EC2 instance, compared to baseline averages from the prior 45 days.

Linear Log

Inbound traffic

150 MB
100 MB
50 MB
0 B

06/27, 00:00

Scope start: 07/04, 00:00

Scope end: 07/12, 02:00

下にスクロール

調査例：プロフィール (EC2 インスタンス)

Detective X

Getting started
Search

▼ Settings

Account management
General
Preferences
Usage

Overall VPC flow volume 情報

Summarizes the overall volume of VPC flow data into and out of the EC2 instance, compared to baseline averages from the prior 45 days.



Findings associated with EC2 instance i-08a8e40be65425909 情報

The following findings occurred on this resource around the scope time.

Q Filter by title and type

Title	Finding type	First observed	Last observed	Finding severity
EC2 instance i-08a8e40be65425909 communicating with a known Bitcoin-related IP Address.	TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B	07/04/2020, 00:12 UTC	07/12/2020, 01:12 UTC	60

下にスクロール

調査例：プロフィール (EC2 インスタンス)

Detective

Getting started
Search

▼ Settings

Account management
General
Preferences
Usage

Findings associated with EC2 instance i-08a8e40be65425909 [情報](#)

The following findings occurred on this resource around the scope time.

🔍 Filter by title and type

Title	Finding type	First observed	Last observed	Finding severity
EC2 instance i-08a8e40be65425909 communicating with a known Bitcoin-related IP Address.	TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B	07/04/2020, 00:12 UTC	07/12/2020, 04:48 UTC	60

Distinct count of ports over time [情報](#)

Timeline showing the count of distinct local and remote ports observed for this EC2 instance.

Linear Log

Local ports



Remote ports



調査例：プロフィール (EC2 インスタンス)

Detective

Getting started
Search

Settings

Account management
General
Preferences
Usage

Findings associated with EC2 instance i-08a8e40be65425909

The following findings occurred on this resource around the scope time.

Filter by title and type

Title	Finding type	First observed	Last observed	Finding severity
EC2 instance i-08a8e40be65425909 communicating with a known Bitcoin-related IP Address.	TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B	07/04/2020, 00:12 UTC	07/12/2020, 04:48 UTC	60

Distinct count of ports over time

Timeline showing the count of distinct local and remote ports observed for this EC2 instance.

時間範囲内でのポート数

Linear Log

Local ports



Remote ports



下にスクロール

調査例：プロフィール (EC2 インスタンス)

Detective

Getting started

Search

▼ Settings

Account management

General

Preferences

Usage

Remote ports



Distinct IP addresses over time 情報

時間範囲内での IPアドレス数

Linear Log

Inbound connections



Outbound connections



上にスクロール

調査例：プロフィール (EC2 インスタンス)

Detective

Getting started
Search

Settings

Account management
General
Preferences
Usage

Detective > Search > Ec2Instance/i-08a8e40be65425909



i-08a8e40be65425909 情報

EC2 instance

Scope time 情報

07/04, 00:00 - 07/12, 02:00

Lock Edit

Overview

EC2 instance details 情報

High-level descriptive data for the given EC2 instance

EC2 creation date

07/03/2020, 23:56 UTC

ARN

-

Created by

DetectiveDemo-AdminUser-1FJ482YN...

Associated VPC

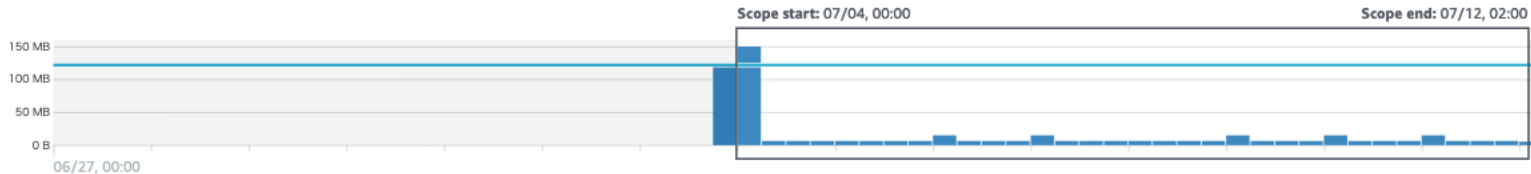
vpc-0c755a714886152a3

Overall VPC flow volume 情報

Summarizes the overall volume of VPC flow data into and out of the EC2 instance, compared to baseline averages from the p

マイニングをしている EC2 インスタンスを
作成した IAM ユーザー

Inbound traffic



調査例：AWSユーザーのプロファイルヘッドリルダウン

Detective

Detective > Search > Ec2Instance/i-08a8e40be65425909



i-08a8e40be65425909 情報

EC2 instance

Scope time 情報

07/04, 00:00 - 07/12, 02:00

Lock Edit

Overview

EC2 instance details 情報

High-level descriptive data for the given EC2 instance

EC2 creation date

07/03/2020, 23:56 UTC

ARN

-

Created by

[DetectiveDemo-AdminUser-1FJ4B2Y...](#)

Associated VPC

vpc-0c755a714886152a3

リンクを新しいタブで開く
リンクを新しいウィンドウで開く
リンクを新しいプライベートウィンドウで開く

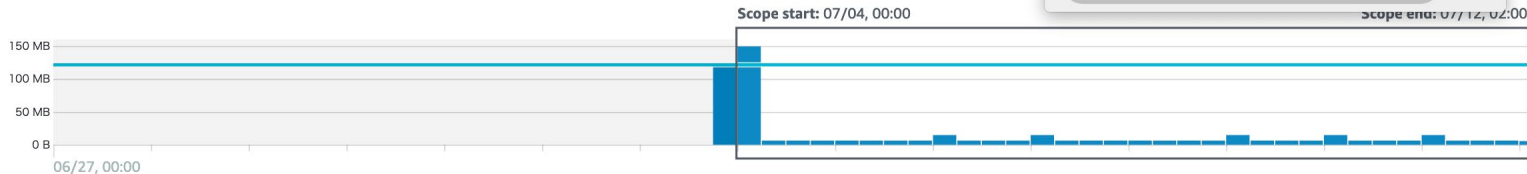
このリンクをブックマーク
名前を付けてリンク先を保存...
リンクの URL をコピー
Google で検索: "DetectiveDemo-A..."

要素を調査

Overall VPC flow volume 情報

Summarizes the overall volume of VPC flow data into and out of the EC2 instance, compared to baseline averages from the prior 45 days.

Inbound traffic



調査例：プロフィール (AWS ユーザー)

Detective X

Getting started
Search

▼ Settings

Account management
General
Preferences
Usage

Detective > Search > AwsUser/AIDAT4OQX3HXVHJD7UIUR



DetectiveDemo-AdminUser-1FJ4B2YNDYPYG 情報

AWS user

Scope time 情報

07/04, 00:00 - 07/12, 02:00

Lock

Overview New behavior

AWS user details 情報

High-level descriptive data for the given user.

Principal ID

AIDAT4OQX3HXVHJD7UIUR

AWS account

267-99

Created by

admin

Created date

07/03/2020, 23:23 UTC

Last observed

07/04/2020, 00:16 UTC

Findings associated with AWS user DetectiveDemo-AdminUser-1FJ4B2YNDYPYG 情報

The following findings occurred on this resource around the scope time.

🔍 Filter by title and type

Title	Finding type	First observed	Last observed	Finding severity
AWS CloudTrail trail DetectiveDemo-CloudTrail-71A56FFY2JCX was disabled.	TTPs/Defense Evasion/Stealth:IAMUser-CloudTrailLoggingDisabled	07/04/2020, 00:00 UTC	07/04/2020, 00:00 UTC	40

Overall API call volume 情報

Overall volume of API calls issued by this resource around the scope time.

Linear Log

調査例：プロフィール (AWS ユーザー)

Detective X

Detective > Search > AwsUser/AIDAT4OQX3HXVHJD7UIUR



DetectiveDemo-AdminUser-1FJ4B2YNDYPYG 情報

AWS user

Scope time 情報

07/04, 00:00 - 07/12, 02:00

Lock Edit

Overview

New behavior

AWS user details 情報

High-level descriptive data for the given user.

Principal ID

AIDAT4OQX3HXVHJD7UIUR

Created date

07/03/2020, 23:23 UTC

AWS account

267-99

Last observed

07/04/2020, 00:16 UTC

Created by

admin

Findings associated with AWS user DetectiveDemo-AdminUser-1FJ4B2YNDYPYG 情報

The following findings occurred on this resource around the scope time.

Filter by title and type

Title	Finding type	First observed	Last observed	Finding severity
AWS CloudTrail trail DetectiveDemo-CloudTrail-71A56FFY2JCX was disabled.	TTPs/Defense Evasion/Stealth:IAMUser-CloudTrailLoggingDisabled	07/04/2020, 00:00 UTC	07/04/2020, 00:00 UTC	40

Overall API call volume 情報

Overall volume of API calls issued by this resource around the scope time.

侵害されている可能性あり

Linear Log

調査例：プロフィール (AWS ユーザー)

Detective

Detective > Search > AwsUser/AIDAT4OQX3HXVHJD7UIUR



DetectiveDemo-AdminUser-1FJ4B2YNDYPYG

AWS user

Scope time 情報

07/04, 00:00 - 07/12, 02:00

Lock Edit

Overview

New behavior

AWS user details 情報

High-level descriptive data for the given user.

Principal ID

AIDAT4OQX3HXVHJD7UIUR

Created date

07/03/2020, 23:23 UTC

AWS account

267-99

Last observed

07/04/2020, 00:16 UTC

Created by

admin

CloudTrail 証跡取得の停止を検知
Detective は AWS 内部で CloudTrail の証跡を
収集しているので調査に影響しない

Findings associated with AWS user DetectiveDemo-AdminUser-1FJ4B2YNDYPYG 情報

The following findings occurred on this resource around the scope time.

Filter by title and type

Title	Finding type	First observed	Last observed	Finding severity
AWS CloudTrail trail DetectiveDemo-CloudTrail-71A56FFY2JCX was disabled.	TTPs/Defense Evasion/Stealth:IAMUser-CloudTrailLoggingDisabled	07/04/2020, 00:00 UTC	07/04/2020, 00:00 UTC	40

Overall API call volume 情報

Overall volume of API calls issued by this resource around the scope time.

Linear Log

下にスクロール

調査例：プロフィール (AWS ユーザー)

Detective X

Filter by title and type

Title Finding type First observed Last observed Finding severity

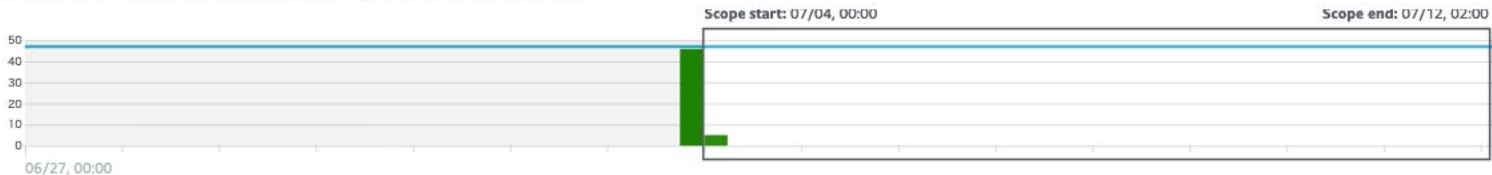
Overall API call volume 情報

Overall volume of API calls issued by this resource around the scope time.

時間範囲内での API コール数

Linear Log

Successful calls 83.33% of scope time call volume (14.58% less than typical activity)



Failed calls 16.67% of scope time call volume (14.58% more than typical activity)



Select a bar to see more details about that time window

調査例：プロフィール (AWS ユーザー)

Detective X

Getting started
Search

Settings

Account management
General
Preferences
Usage

Filter by title and type

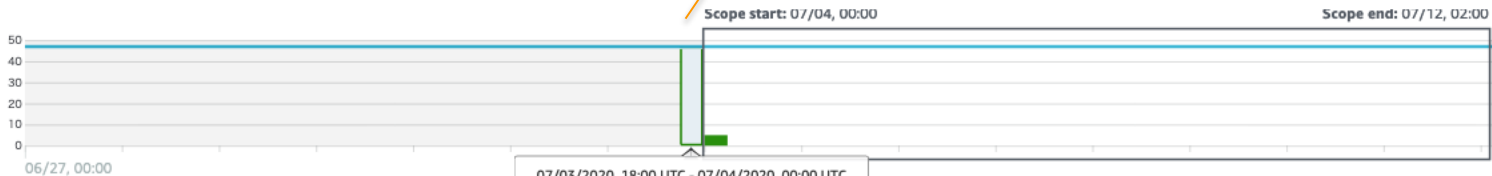
Title Finding type First observed Last observed Finding severity

Overall API call volume 情報

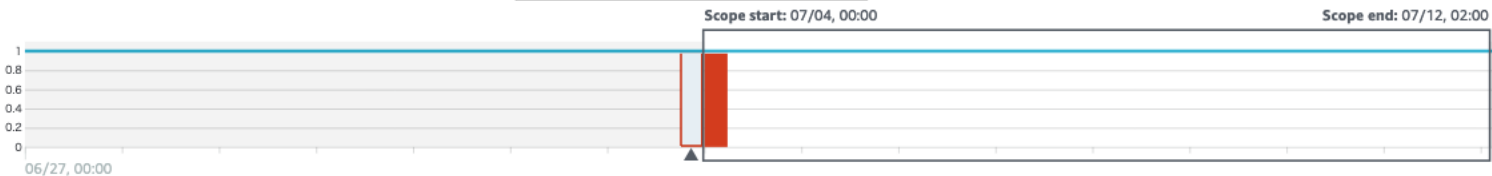
Overall volume of API calls issued by this resource around the scope time.

API コールの詳細をドリルダウン

Successful calls 83.33% of scope time call volume (14.58% less than typical activity)



Failed calls 16.67% of scope time call volume (14.58% more than typical activity)



Showing activity for selected bar: 07/03/2020, 18:00 UTC - 07/04/2020, 00:00 UTC

Observed IP addresses API method Access Key ID

Filter by IP CIDR, API Method name, or AKID string

下にスクロール

調査例：プロフィール (AWS ユーザー)

Detective X

Getting started

Search

▼ Settings

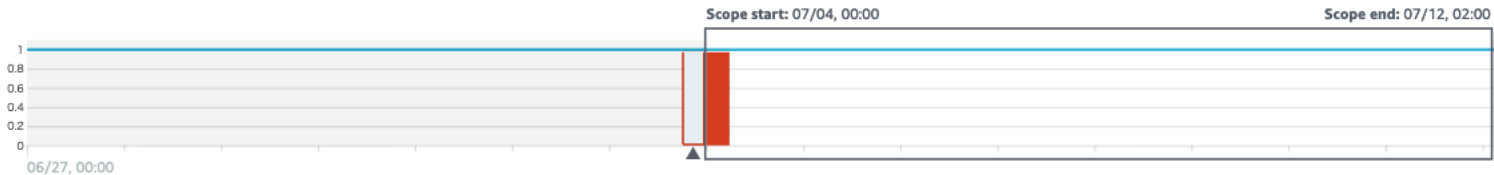
Account management

General

Preferences

Usage

Failed calls 16.67% of scope time call volume (14.58% more than typical activity)



Showing activity for selected bar: 07/03/2020, 18:00 UTC - 07/04/2020, 00:00 UTC

Observed IP addresses API method Access Key ID

Filter by IP CIDR, API Method name, or AKID string

IP address ▼	Successful calls ▼	Failed calls ▼	Location ▼
▼ 3. [redacted] 37	46	1	-
▶ DescribeSnapshots	41	0	
▶ RunInstances	1	0	
▶ RemoveRoleFromInstanceProfile	1	0	
▶ DescribeVolumes	1	0	
▶ DescribeDBInstances	1	0	
▶ CreateSecret	1	0	
▶ DescribeDBSecurityGroups	0	1	
▶ 10.71.68.1	1	0	-

上にスクロール


調査例：何が通常で何が異常か？

Detective ×

Getting started
Search


▼ Settings
Account management
General
Preferences
Usage

Detective > Search > AwsUser/AIDAT4OQX3HXVHJD7UIUR

 **DetectiveDemo-AdminUser-1FJ4B2YNDYPYG** 情報
AWS user

Scope time 情報
07/04, 00:00 - 07/12, 02:00

Lock

Overview New behavior 

AWS user details 情報
High-level descriptive data for the given user.

Principal ID	AWS account	Created by
AIDAT4OQX3HXV		
Created date		
07/03/2020, 23:2		

Findings associated with this user
The following findings are associated with this user.

Title	Finding type	First observed	Last observed	Finding severity
AWS CloudTrail trail DetectiveDemo-CloudTrail-71A56FFY2JCX was disabled.	TTPs/Defense Evasion/Stealth:IAMUser-CloudTrailLoggingDisabled	07/04/2020, 00:00 UTC	07/04/2020, 00:00 UTC	40

Overall API call volume 情報
Overall volume of API calls issued by this resource around the scope time.

疑問

このユーザーが EC2 インスタンスを作成することは通常業務か？
CloudTrail を停止することは通常業務か？
攻撃者が実行した API コールは何か(調査対象はどこまで拡大)？

調査例：プロファイルタブ (New Behavior)

Detective X

Detective > Search > AwsUser/AIDAT4OQX3HXVHJD7UIUR



DetectiveDemo-AdminUser-1FJ4B2YNDYPYG 情報

AWS user

Scope time 情報

07/04, 00:00 - 07/12, 02:00

Lock Edit

ベースライン期間の動作から外れた観測はあるか？

Overview

New behavior

Newly observed geolocations 情報

This resource was observed operating in the following geolocations during the scope time. Select a location to see more details.



■ Newly observed ■ Previously observed

調査例：プロファイルタブ (New Behavior)

Detective X

Getting started
Search

▼ Settings

Account management
General
Preferences
Usage

Newly observed geolocations 情報

This resource was observed operating in the following geolocations during the scope time. Select a location to see more details.



ベースライン期間中にも
観測されたロケーション

Observed	Geolocation	Number of times observed	Percentage of total API calls	Annotations
■ Previously observed	Tokyo, JP	55	50.13%	Details >
■ Newly observed	Ashburn, US	53	49.07%	Details >

調査例：プロファイルタブ (New Behavior)

Detective

Getting started
Search

Settings

Account management
General
Preferences
Usage

Newly observed geolocations 情報

This resource was observed operating in the following geolocations during the scope time. Select a location to see more details.



Newly observed Previously observed

Q

Observed	Geolocation	Number of times observed	Percentage of total API calls	Annotations
Previously observed	Tokyo, JP	55	50.13%	Details >
Newly observed	Ashburn, US	53	49.07%	Details >

下にスクロール

ドリルダウン

調査例：プロファイルタブ (New Behavior)

Detective X

Getting started
Search

▼ Settings

Account management
General
Preferences
Usage

■ Newly observed ■ Previously observed

[Return to all results](#)

Ashburn, US from 07/04/2020 - 07/12/2020

Observed IP addresses Resource

Filter by IP CIDR, API Method name, or AKID string

< 1 2 3 4 5 6 7 ... 17 >

IP address ▾

▶ 10	7.162
▶ 10	7.62
▶ 10	.205
▶ 10	6.92
▶ 10	1.231
▶ 17	2.131
▶ 18	9.91
▶ 18	92
▶ 18	9.130
▶ 18	32

Successful calls ▾

Failed calls ▾

新しく観測されたロケーションの
IP アドレスの一覧

調査例：プロファイルタブ (New Behavior)

Detective X

Getting started
Search

▼ Settings

Account management
General
Preferences
Usage

■ Newly observed ■ Previously observed

[← Return to all results](#)

Ashburn, US from 07/04/2020 - 07/12/2020

Observed IP addresses **Resource**

Q Filter by IP CIDR, API Method name, or AKID string

Resource ▾

Successful calls ▾

Failed calls ▾

Account ID ▾

- ▶ DetectiveDemo-InspectorLambdaRol...
- ▶ DetectiveDemo-InspectorLambdaRol...
- ▶ DetectiveDemo-MaliciousInstanceR...
- ▶ DetectiveDemo-MaliciousInstanceR...
- ▶ DetectiveDemo-WebInstanceRole-18...
- ▶ DetectiveDemo-AdminUser-1FJ4B2YN...
- ▶ admin

新しく観測されたロケーションから
リクエストしたリソースの一覧

admin 以外は不明なリソース
不正に作成され、悪用された可能性あり

Newly observed API calls 情報

The following API methods were newly observed during the scope time.

Q

調査例：プロファイルタブ (New Behavior)

Detective X

Getting started
Search

▼ Settings

Account management
General
Preferences
Usage

■ Newly observed ■ Previously observed

[Return to all results](#)

Ashburn, US from 07/04/2020 - 07/12/2020

Observed IP addresses Resource

Q Filter by IP CIDR, API Method name, or AKID string

Resource ▾	Successful calls ▾	Failed calls ▾	Account ID ▾
▶ DetectiveDemo-InspectorLambdaRo...	-	-	-
▶ DetectiveDemo-InspectorLambdaRo...	-	-	-
▶ DetectiveDemo-MaliciousInstanceR...	-	-	-
▶ DetectiveDemo-MaliciousInstanceR...	-	-	-
▼ DetectiveDemo-WebInstanceRole-18...	-	-	-
▼ ListInstanceAssociations	-	-	-
3.1.1.1/32	-	-	-
▶ UpdateInstanceInformation	-	-	-
▶ DetectiveDemo-AdminUser-1FJ4B2YN...	-	-	-
▶ admin	-	-	-

下にスクロール

詳細表示し、さらなるドリルダウンも可能

調査例：プロファイルタブ (New Behavior)

Detective X

Getting started
Search

▼ Settings

Account management
General
Preferences
Usage

Newly observed API calls 情報

The following API methods were newly observed during the scope time.

新しく観測されたAPI コール

API call	Count	Success rate
▼ StopLogging	2	50.00%



Scope start: 07/04, 00:00

Scope end: 07/12, 02:00

▶ CreateUser	1	100.00%
▶ DeleteAccessKey	1	100.00%
▶ GenerateCredentialReport	1	100.00%

API calls with increased volume 情報

The following API methods were observed at a substantially higher rate during the scope time.

API call	Rate increase ▼	Internal call count	External call count
----------	-----------------	---------------------	---------------------

No results found

Newly observed autonomous system organizations (ASOs) 情報

This resource issued API calls from the following ASOs during the scope time, but not during the previous 45 days.

下にスクロール

調査例：プロファイルタブ (New Behavior)

Detective X

- Getting started
- Search
- ▼ Settings
 - Account management
 - General
 - Preferences
 - Usage

API calls with increased volume 情報

The following API methods were observed at a substantially higher rate during the scope time.

検索

API call	Rate increase ▼	Internal call count	External call count
No results found			

増加した API コール

Newly observed autonomous system organizations (ASOs) 情報

This resource issued API calls from the following ASOs during the scope time, but not during the previous 45 days.

検索

AS organization	API call count	Annotations
No results found		

新しく観測された AS 組織

Newly observed user agents 情報

This resource used the following user agents to issue API calls during the scope time, but not during the previous 45 days.

検索

User agent	Internal call count	External call count
aws-cli/1.16.300 Python/2.7.18 Linux/4.14.177-139.254.amzn2.x86_64 botocore/1.13...	0	6

新しく観測されたユーザーエージェント

Scope start: 07/04, 00:00 Scope end: 07/12, 02:00

インシデント調査例のまとめ

仮想通貨(暗号資産)マイニングのインシデントに関する調査

調査の起点は Detective と統合された GuardDuty または Security Hub
インタラクティブに視覚化

関連する検出結果、IP アドレス、インスタンス、IAM ユーザをドリルダウンして調査
通常とは違う行動を視覚化された時系列グラフ、リスト、世界地図から判断

ここまでの調査結果

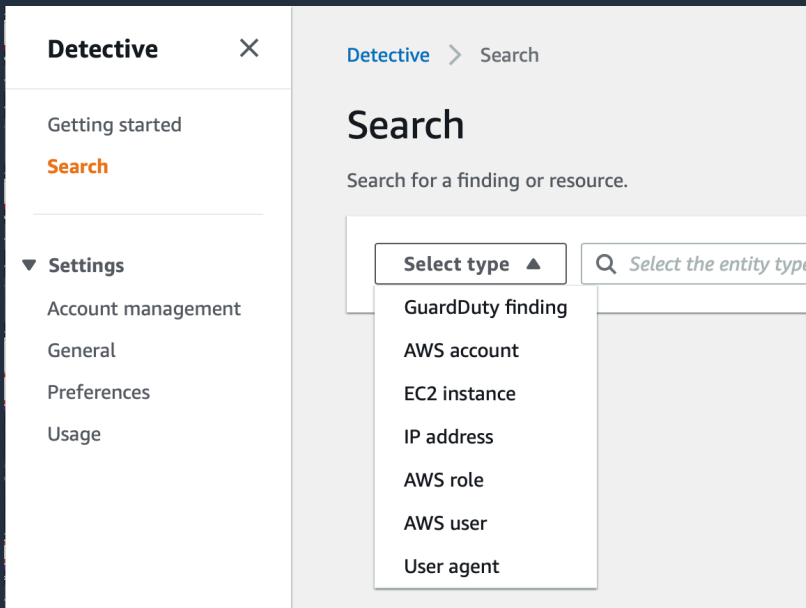
不正なインスタンスの作成とマイニングが実行された。インスタンス作成者は特定済
攻撃者は CloudTrail を停止(ただし Detective の調査には影響なし)

不正なリソース作成の疑いを GuardDuty では検知していないが Detective では特定
当初の予想より侵害範囲が広い

次のアクション

同じ方法で関連するリソースをドリルダウンして根本原因を特定

スレットハンティングの例

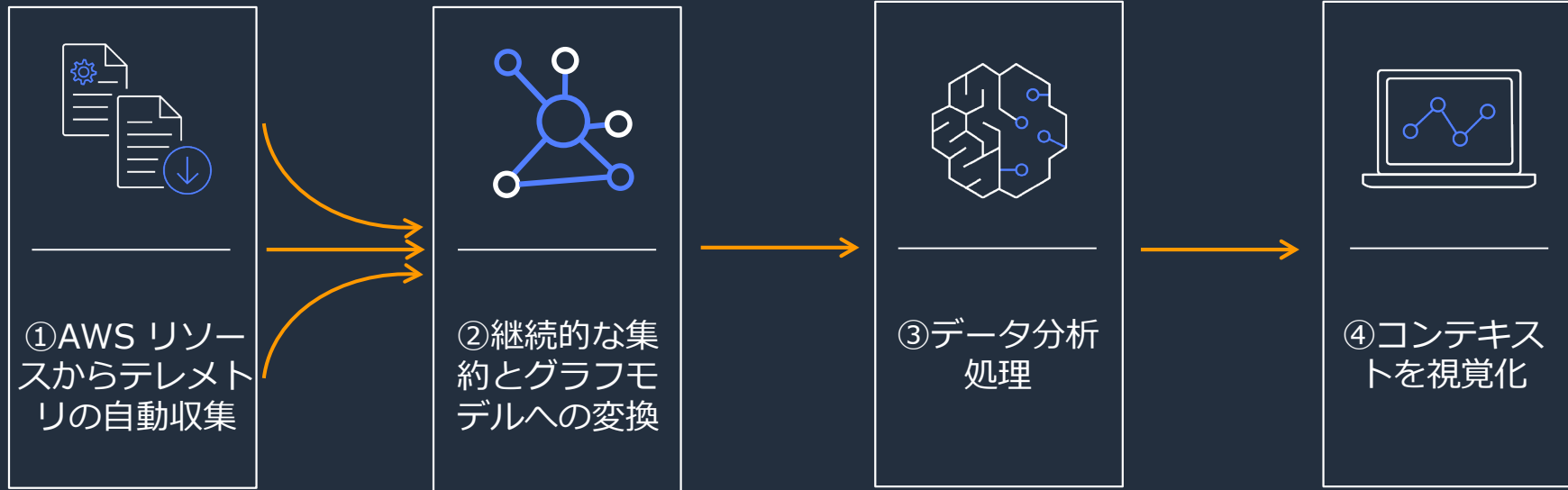


Indicator of Compromise (侵害の痕跡)を元に、Detective のプロファイルを呼び出して分析

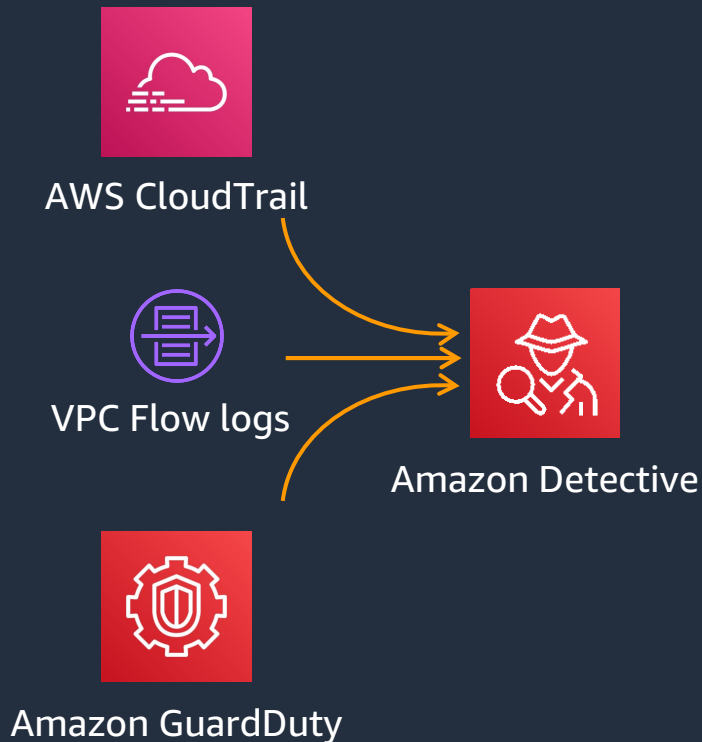
トリガーの例

- 内外のセキュリティ侵害レポート
 - IP address
 - User agent
- CPU 使用率が突然上昇した EC2 インスタンス
- 月次の定期分析

Detective 内部の分析プロセス詳細



① AWS リソースからテレメトリの自動収集



- Detective を有効化するとデータを自動収集
- 収集のために特別な設定は必要ありません
- 開始後2週間は機械学習のトレーニング期間
- GuardDuty から取り込まれる検出結果は一部の結果タイプ。全てではありません
- 取り込まれる結果タイプのリストは[こちら](#)をご参照ください

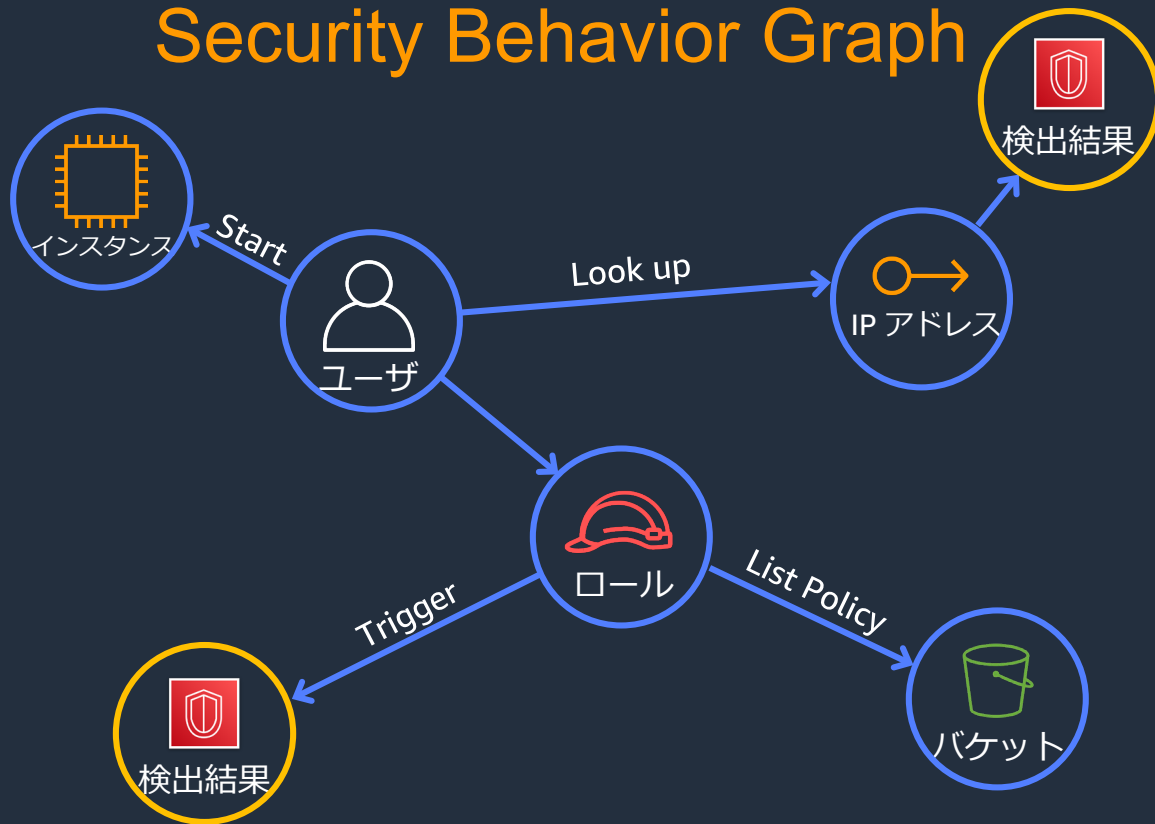
■ 推奨設定

Amazon GuardDuty は、繰り返す検出結果のエクスポートするタイミングを変更可能
初期設定6時間ごとから15分ごとへ変更を推奨

② 継続的な集約とグラフモデルへの変換



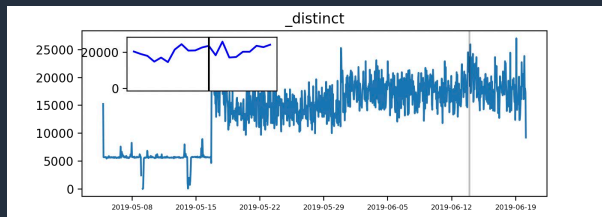
Security Behavior Graph



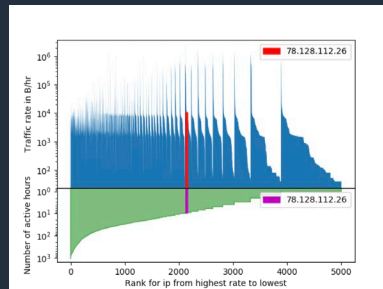
③ データ分析処理



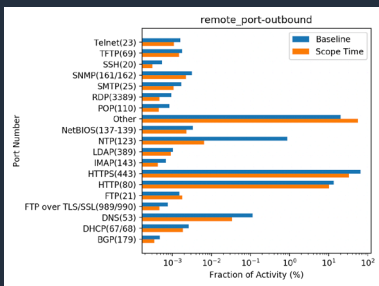
データサイエンティストによる開発



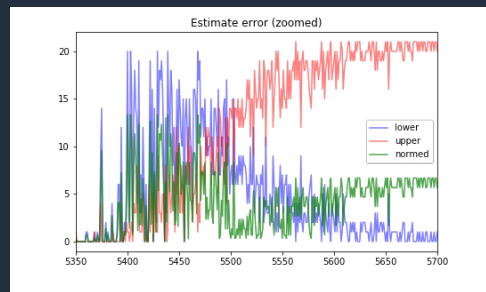
ビヘビアベースライン



分布

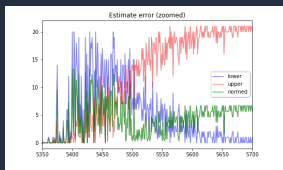
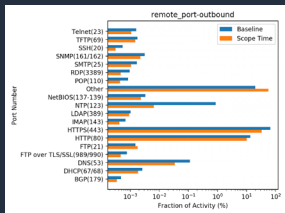
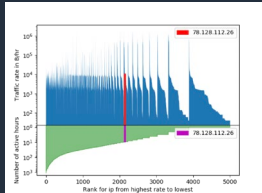
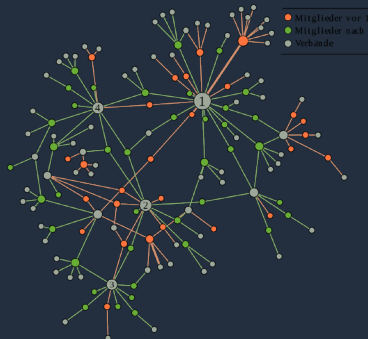


時系列分析

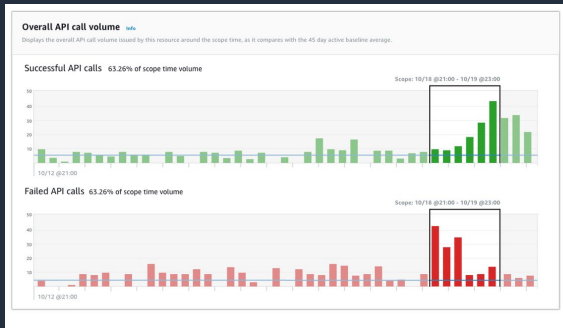
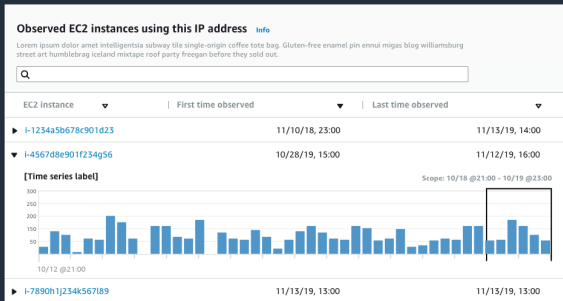


データストリーム分析

④ コンテキストの視覚化



効率的な調査のための インタラクティブな視覚化



収集したデータと分析結果は最大 1 年間保持



マルチアカウント対応



他の AWS アカウントを Detective のメンバーとして招待すると、招待元のアカウントがマスターアカウントとなり、アカウントを横断してセキュリティ調査が可能



Amazon Detective

マスターアカウント

Detective
メンバー1

Detective
メンバー2

Detective
メンバー3

Detective Account management

Getting started
Search

▼ Settings
Account management
General
Preferences
Usage

Account management Info

My member accounts (3) Info

Manage accounts | Invite accounts from .csv | **Invite individual accounts**

Filter by Account ID, Email address, or Status

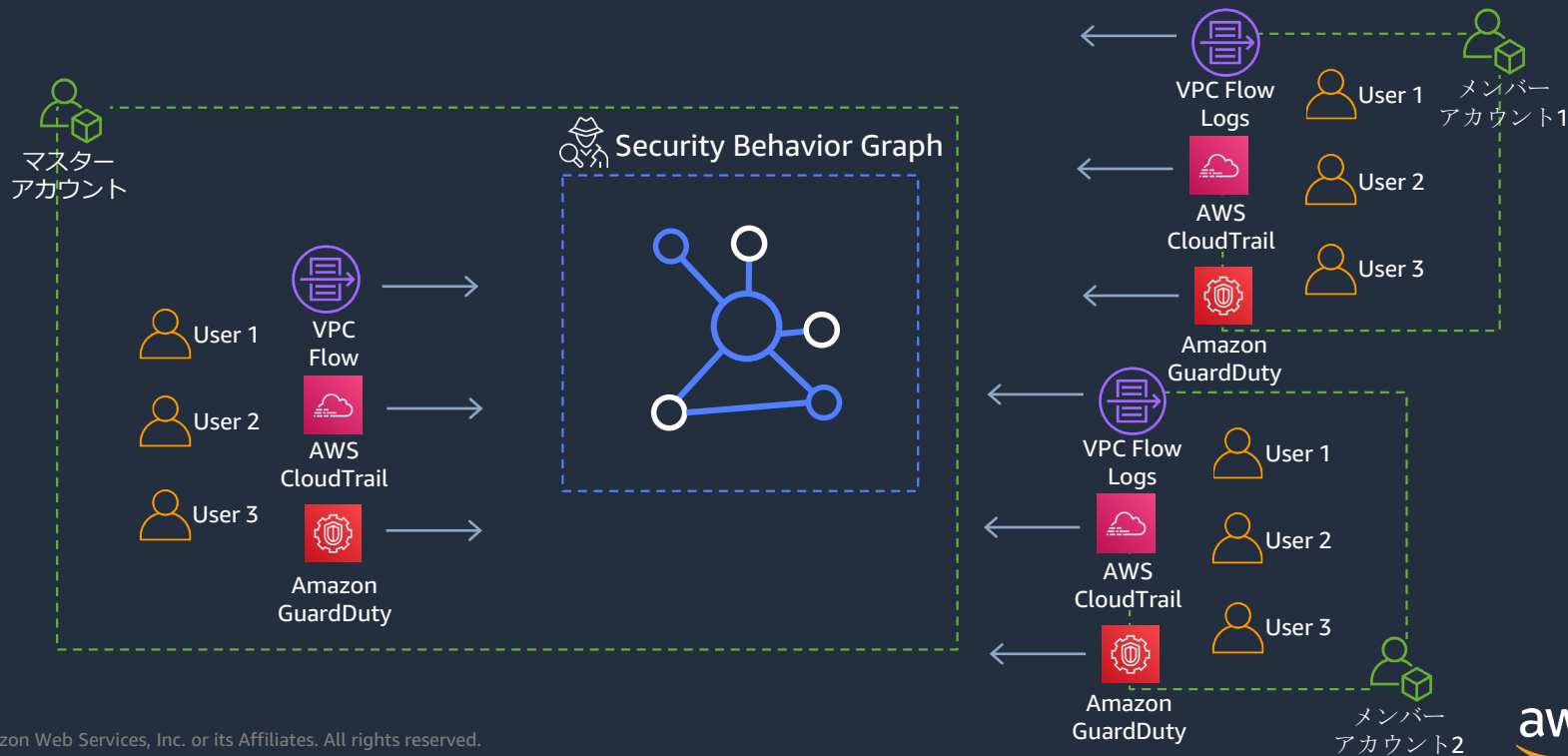
<input type="checkbox"/>	Account ID	Email address	Date updated	Volume	Status
<input checked="" type="checkbox"/>	796-571 (Master account)	-	04/24/2020, 08:44 UTC	0%	Accepted (Enabled)
<input type="checkbox"/>	195-034	na...log@... co.jp	05/27/2020, 12:29 UTC	0%	Accepted (Enabled)
<input type="checkbox"/>	945-475	na...amaz	05/27/2020, 09:08 UTC	0%	Accepted (Enabled)

※ Detective のマスターアカウントとメンバーアカウントは、AWS Organizations とは別の管理です

マルチアカウントのテレメトリの収集



- ・ マスターアカウントのグラフモデルに、メンバーアカウントはテレメトリを提供
- ・ マルチアカウントから収集すると分析精度が高まる



スクリプトによるマルチアカウント一括有効化



マルチアカウント有効化のスクリプトを Github で公開

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

機能： 複数リージョンで Detective のマスターアカウントを有効化
マスターからメンバーへの招待、メンバーの承認を一括実施

The screenshot shows the GitHub repository page for `aws-samples / amazon-detective-multiaccount-scripts`. The repository has 4 watches, 7 stars, and 5 forks. The main navigation bar includes links for Code, Issues, Pull requests, Actions, Projects, Wiki, Security, and Insights. The repository is currently on the `master` branch. A commit history table is visible, showing a commit by `...` on May 23, 2020, with 12 commits, 1 branch, and 0 tags. The file list includes a `tests` folder and `CODE_OF_CONDUCT.md` and `CONTRIBUTING.md` files. The right sidebar contains an `About` section with the description: "interact with Amazon Detective in multiple accounts and regions", a `Readme` link, and the `Apache-2.0 License`.

File/Folder	Commit Message	Time
tests	Enable Amazon Detective in regions where no gra...	last month
CODE_OF_CONDUCT.md	Initial commit	6 months ago
CONTRIBUTING.md	Initial commit	6 months ago

マルチアカウント時の GuardDuty / Security Hub との統合

- マルチアカウントでも GuardDuty および Security Hub と統合可能
- GuardDuty および Security Hub のマスターアカウントと Detective のマスターアカウントを同一にすることを推奨
- マスターアカウントはメンバーアカウントが検知した脅威を迅速に調査可能
- 同一にできない場合：クロスアカウントロールを設定して、Detective のマスターアカウントが GuardDuty または Security Hub のマスターアカウントにアクセス



プロフィールへの URL リンク



Amazon Detective のエンティティまたは検出結果のプロファイルについて、直接参照するための URL リンクを生成可能

フォーマット

<https://console.aws.amazon.com/detective/home?region=Region#type/namespace/instanceID?parameters>

パラメータ	説明	例
Region	利用したい Detective のリージョン	ap-northeast-1
type	エンティティ(entities)または検出結果(findings)	entities
namespace	type の識別子	IpAddress
instanceID	namespace の識別子	198.51.100.1
parameters	オプション。Scope のロック有無など	scopeLocked

詳細 : <https://docs.aws.amazon.com/detective/latest/userguide/profile-navigate-url.html>

URLリンクによる他システムとの連携



SIEM /
アラートコンソール



リソースの調査

チケット調査

セキュリティ
オーケストレーション /
チケットシステム



検出結果の調査



Amazon Detective

料金



- 月ごとに取り込まれたデータの量に基づく GB 単位の従量課金
- インシデント調査等での Amazon Detective の利用や、取り込み済みデータには課金されません。データは1年間保持されます
- ご利用開始後、30日間は無料トライアルとなり、予測コストを確認できます
- マルチアカウントの場合はデータを提供している各メンバーアカウントに課金
- マルチリージョンでのご利用は、各リージョンごとに課金

例) 1ヶ月間で100 GBのデータを取り込み、GB ごとの料金が2.7ドルだった場合
 $100 \text{ GB} \times 2.7 \text{ ドル/GB} = 270 \text{ ドル}$

詳細は [AWS 公式ウェブサイトの料金ページ](#)をご参照ください

まとめ



- インシデント対応で調査を迅速に行うと被害を最小化できる
- 調査の課題はログの収集・加工・分析、熟練した人材の不足、コスト等

- Amazon Detective はこの調査の課題を解決するサービス
- 特徴
 - 調査に必要なログを自動的に収集
 - グラフモデル・機械学習による分析
 - インタラクティブな視覚化
- お客様が得られるメリット
 - お客様の調査プロセスが効率的になり簡素化
 - セキュリティ問題の根本原因を迅速に特定

Q&A

お答えできなかったご質問については

AWS Japan Blog 「<https://aws.amazon.com/jp/blogs/news/>」にて

後日掲載します。

AWS の日本語資料の場所「AWS 資料」で検索



日本担当チームへお問い合わせ サポート 日本語 ▾ アカウント ▾

コンソールにサインイン

製品 ソリューション 料金 ドキュメント 学習 パートナー AWS Marketplace その他 🔍

AWS クラウドサービス活用資料集トップ

アマゾン ウェブ サービス (AWS) は安全なクラウドサービスプラットフォームで、ビジネスのスケールと成長をサポートする処理能力、データベースストレージ、およびその他多種多様な機能を提供します。お客様は必要なサービスを選択し、必要な分だけご利用いただけます。それらを活用するために役立つ日本語資料、動画コンテンツを多数ご提供しております。(本サイトは主に、AWS Webinar で使用した資料およびオンデマンドセミナー情報を掲載しています。)

[AWS Webinar お申込 »](#)

[AWS 初心者向け »](#)

[業種・ソリューション別資料 »](#)

[サービス別資料 »](#)

<https://amzn.to/JPArchive>



AWS Well-Architected 個別技術相談会

毎週“W-A個別技術相談会”を実施中

- AWSのソリューションアーキテクト(SA)に
対策などを相談することも可能

• **申込みはイベント告知サイトから**

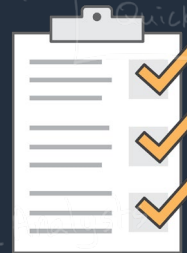
(<https://aws.amazon.com/jp/about-aws/events/>)

AWS イベント

で[検索]



AWS Well-Architected





ご視聴ありがとうございました

AWS 公式 Webinar
<https://amzn.to/JPWebinar>



過去資料
<https://amzn.to/JPArchive>

