

SONY

マネージドクラウド
新バージョンリリースのお知らせ
Version 2.6.0

2024年6月27日

ソニービズネットワークス株式会社

- マネージドクラウド with AWS
 - AI管理機能
 - アラート通知管理
 - 利用環境評価
 - マネージドサポート管理

マネージドクラウド with AWS

AI管理機能

- Amazon GuardDuty のアラートを生成AIによって要約して通知する機能を追加しました。

※ご利用にあたってお客様環境にAmazon Bedrockや関連リソースがデプロイされます。

通知先のメールアドレスと通知する
閾値の設定のみで各リソースを展開
可能

セキュリティアラート通知 リソース展開

セキュリティアラート通知を利用するための各種AWSリソースを展開します。
また、アラート通知先のメールアドレスを指定して下さい。

通知先メールアドレス

通知の閾値設定 重大度(Severity)が CRITICAL: 緊急 以上の場合

キャンセル

作成

セキュリティアラート通知

☐ お気に入りに登録

リソース状況

[更新](#)

リージョン選択 アジアパシフィック (東京)

AWSサービス		ステータス
 Amazon GuardDuty		有効 重大度設定
 AWS Security Hub		有効
 Amazon EventBridge	ルール名: PortalSecurityAlertRule-20240611172628221	有効
 Amazon SNS	トピック名: PortalTopic-ToSecurityAlert-20240611_172626 Email通知先	有効
 AWS Lambda	関数名: portal-security-alert	有効
 AWS Step Functions	ステートマシン名: SecurityAlertState20240611_172627	有効
リージョン固定: オレゴン		
 Amazon Bedrock	モデル名: Claude 3 Sonnet	リソース展開済み

[リソース展開](#)

アラート通知管理

- ジョブ実行ログ通知、カスタマイズAPI実行結果通知を指定した電話番号に架電する機能を追加しました。
※ご利用いただくには、別途“自動音声オプション”の契約が必要になります。

クラウドポータル 通知管理

通知方法を
プルダウン【自動音声】を選択

通知名	通知方法	送信設定	設定内容	設定
ジョブ実行ログ通知	自動音声	送信しない	-	<button>設定</button>
カスタマイズAPI実行結果通知	自動音声	送信しない	-	<button>設定</button>

設定内容

電話転送ポリシー ☒ 送信しない ☐ 警告時のみ送信 ☐ エラー時のみ送信 ☐ エラー時・警告時に送信

発信元電話番号 +81

発信先電話番号 +81

弊社基盤の電話番号
より通知されます

戻る 設定

アラート通知管理

- AWS SNS Topic管理で指定した電話番号に架電するTopicを作成できる機能を追加しました。
システムステータスやインスタンスステータスの監視でのアラート通知先として利用いただけます。
※ご利用いただくには、別途“自動音声オプション”の契約が必要になります。

AWS SNS Topic管理

リージョン選択: アジアパシフィック (東京) Protocol: https

Protocolを
プルダウン【https】を選択

Topic名	Protocol	エンドポイント	設定	削除
PortalTopic-Https-test_20240611_101141	https	通知タイプ: 自動音声 発信元電話番号: +81 発信先電話番号: +81	設定	削除
PortalTopic-SQATest_20230523_104148	https	メール転送で使用中です。	-	-
PortalTopic-Test0526_20230526_101413	https	メール転送で使用中です。	-	-
PortalTopic-usage-alert_20230626_215232	https	メール転送で使用中です。	-	-

Topic新規作成

基本設定

設定内容
リージョン: 東京
Topic名: PortalTopic-Https- [] _yyyymmdd_HHMMSS
プロトコル: https
通知タイプ: 自動音声
発信元電話番号: +81 []
発信先電話番号: +81 9001234567 (ハイフン無し)

弊社基盤の電話番号
より通知されます

戻る 設定

アラート通知管理

- AWSからの通知転送設定で不正利用通知で指定した電話番号に架電する機能を追加しました。

※本機能はオプション契約なくご利用いただけます。

AWSからの通知転送設定

通知転送設定	通知翻訳設定	電話転送設定	転送元, 転送先	設定
転送しない	翻訳しない	転送なし	メールアドレス:	<button>設定</button>

基本設定	設定内容
通知転送設定	通知転送ポリシー ☒ 転送しない ☐ 転送する
	転送先メールアドレス
通知翻訳設定	通知翻訳ポリシー ☒ 翻訳しない ☐ 翻訳する
電話転送設定	電話転送ポリシー 不正使用通知: ☒ 転送しない ☐ 転送する
	発信元電話番号 +81
	発信先電話番号 +81

弊社基盤の電話番号より通知されます

戻る 設定

<AWSからの通知転送設定について>
・本機能はAWSからの通知を転送する機能です。
・翻訳についてはAWS Translateを用いています。

利用環境評価

- Amazon Inspector V2 の管理画面を追加し、EC2、ECR、Lambda関数の脆弱性検出を行える機能を追加しました。

TOP > AWS > 利用環境評価 > Amazon Inspector v2 > 基本設定

基本設定

設定一覧

脆弱性検出を行いたいリージョンで Amazon Inspector V2を有効化

お気に入り登録

一括有効化設定

リージョン	有効化 / 無効化
 アジアパシフィック (東京)	状態: DISABLED  有効化
 アジアパシフィック (大阪)	状態: DISABLED  有効化
 アジアパシフィック (ムンバイ)	状態: DISABLED  有効化
 欧州 (ストックホルム)	状態: DISABLED  有効化
 欧州 (パリ)	状態: DISABLED  有効化
 欧州 (ロンドン)	状態: DISABLED  有効化
 欧州 (アイルランド)	状態: DISABLED  有効化
 アジアパシフィック (ソウル)	状態: DISABLED  有効化

Amazon Inspector v2の有効化 / 無効化

アジアパシフィック (東京)リージョンの Inspector v2 を有効にします。よろしいですか？

利用環境評価

検出結果表示例

TOP > AWS > 利用環境評価 > Amazon Inspector v2 > 検出結果

検出結果

検出結果を表示したいリソースを絞り込み

お気に入り登録

リージョン指定および絞り込み検索

リージョン選択: アジアパシフィック (東京)

リソース選択: EC2インスタンス

絞り込み: EC2インスタンスID

が から始まる

検索

結果一覧: EC2インスタンス別

脆弱性が検出されたリソースを一覧で表示

1ページの表示件数: 10

EC2インスタンス	AWSアカウント	Operating System	AMI ID	緊急	高	全て
		AMAZON_LINUX_2023		0	7	38

<EC2インスタンスの脆弱性検出について>

- EC2インスタンスの脆弱性検出を行うには、検出対象のインスタンスをマネージドインスタンスに登録する必要があります。サーバ管理>リモート管理より、マネージドインスタンス登録を実行してください。
- マネージドインスタンス未登録の場合、EBSに対して脆弱性検出が行われます。詳細は以下をご参照ください。
https://docs.aws.amazon.com/ja_jp/inspector/latest/user/scanning-ec2.html
- InspectorV2のサポート対象となるOSについては以下をご参照ください。
<https://docs.aws.amazon.com/inspector/latest/user/inspector-supported.html#inspector-supported-os>

利用環境評価

- GuardDuty の指摘事項を英語から日本語に翻訳して表示する機能を追加しました。

旧表示例

Behavior:EC2/TrafficVolumeUnusual			
Medium The EC2 instance i-99999999 is generating unusually large amounts of network traffic to remote host 198.51.100.0.			
概要			
重要度	0	リージョン	ap-northeast-1
カウント	1	アカウントID	
リソースID	i-99999999		
作成時刻	2024/06/06 13:51:19	更新時刻	2024/06/06 13:51:19
影響を受けるリソース			
Resource Role	TARGET	Resource Type	Instance
Instance Id	i-99999999	Instance Type	m3.xlarge
Outpost Arn	arn:aws:outposts:us-west-2:123456789000:outpost/op-0fbc006e9abb73c3	Instance State	running
Availability Zone	GeneratedFindingInstanceAvailabilityZone	Image Id	ami-99999999
Image Description	GeneratedFindingInstanceImageDescription	Launch Time	2016/08/02 11:05:06
アクション			
Action Type	NETWORK_CONNECTION	Protocol	TCP
Blocked	false		
First Seen	2024/06/06 13:51:19	Last Seen	2024/06/06 13:51:19

新表示例

Behavior:EC2/TrafficVolumeUnusual			
Medium EC2 インスタンス i-99999999 は、リモートホスト 198.51.100.0 に異常に大量のネットワークトラフィックを生成しています。			
概要			
重要度	0	リージョン	ap-northeast-1
カウント	3	アカウントID	
リソースID	i-99999999		
作成時刻	2024/06/06 15:56:24	更新時刻	2024/06/06 17:21:28
影響を受けるリソース			
リソースロール	TARGET	リソースタイプ	Instance
インスタンスID	i-99999999	インスタンスタイプ	m3.xlarge
Outpost ARN	arn:aws:outposts:us-west-2:123456789000:outpost/op-0fbc006e9abb73c3	インスタンスの状態	running
アベイラビリティゾーン	GeneratedFindingInstanceAvailabilityZone	イメージID	ami-99999999
イメージの説明	GeneratedFindingInstanceImageDescription	起動時間	2016/08/02 11:05:06
アクション			
アクションタイプ	NETWORK_CONNECTION	プロトコル	TCP
ブロック	false		
初回表示	2024/06/06 15:56:24	最終表示	2024/06/06 17:21:28

利用環境評価

- Security Hub のセキュリティ基準・指摘事項タイトル・結果詳細タイトルを英語から日本語に翻訳して表示するよう機能を追加しました。

旧表示例

結果一覧						
			選択した結果を無効化する		結果CSV出力	1ページの表示件数: 10 ▼
ステータス	重要度	ID	タイトル	不合格のチェック	詳細	無効化
FAILED	MEDIUM	ACM.1	Imported and ACM-issued certificates should be renewed after a specified time period	19/25	詳細	☐
PASSED	HIGH	ACM.2	RSA certificates managed by ACM should use a key length of at least 2,048 bits	0/8	詳細	☐
FAILED	MEDIUM	APIGateway.1	API Gateway REST and WebSocket API execution logging should be enabled	11/13	詳細	☐
PASSED	MEDIUM	APIGateway.2	API Gateway REST API stages should be configured to use SSL certificates for backend authentication	0/1	詳細	☐
FAILED	LOW	APIGateway.3	API Gateway REST API stages should have AWS X-Ray tracing enabled	11/13	詳細	☐
FAILED	MEDIUM	APIGateway.4	API Gateway should be associated with a WAF Web ACL	13/13	詳細	☐
PASSED	MEDIUM	APIGateway.5	API Gateway REST API cache data should be encrypted at rest	0/1	詳細	☐
FAILED	MEDIUM	APIGateway.8	API Gateway routes should specify an authorization type	3/5	詳細	☐
FAILED	MEDIUM	APIGateway.9	Access logging should be configured for API Gateway V2 Stages	3/5	詳細	☐
PASSED	MEDIUM	Account.1	Security contact information should be provided for an AWS account.	0/1	詳細	☐

セキュリティ基準一覧

セキュリティ基準	セキュリティスコア	有効化/無効化	結果表示
AWS基礎セキュリティのベストプラクティス v1.0.0 The AWS Foundational Security Best Practices standard is a set of automated security checks that detect when AWS accounts and deployed resources do not align to security best practices. The standard is defined by AWS security experts. This curated set of controls helps improve your security posture in AWS, and cover AWS's most popular and foundational services.	62%	有効	設定 表示
AWS リソースタグ付け標準 v1.0.0 The AWS Resource Tagging standard is a set of automated security checks that detect when AWS resources are not tagged.	データなし	無効	設定 表示
CIS AWS Foundations Benchmark v1.2.0 The Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0 is a set of security configuration best practices for AWS. This Security Hub standard automatically checks for your compliance readiness against a subset of CIS requirements.	データなし	無効	設定 表示
CIS AWS Foundations Benchmark v1.4.0 The Center for Internet Security (CIS) AWS Foundations Benchmark v1.4.0 is a set of security configuration best practices for AWS. This Security Hub standard automatically checks for your compliance readiness against a subset of CIS requirements.	データなし	無効	設定 表示
CIS AWS Foundations Benchmark v3.0.0 The Center for Internet Security (CIS) AWS Foundations Benchmark v3.0.0 is a set of security configuration best practices for AWS. This Security Hub standard automatically checks for your compliance readiness against a subset of CIS requirements.	データなし	無効	設定 表示

結果詳細

EBS snapshots should not be publicly restorable

ステータス	PASSED	失敗	0
重要度	CRITICAL	不和	0
すべてのチェック	1	成功	1
		処理済み	0

🔍 ステータス指定 および絞り込み結果

+ 閉く

結果詳細一覧

ステータス一括選択 結果CSV出力 1ページの表示件数: 10 ▼

ステータス	ワークフロー	アカウント	リソース	詳細	詳細読み	結果	ステータス表示
PASSED	RESOLVED			詳細	詳細説明	詳細	☐

※ 記載されている会社名、製品名、ブランド名、サービス名は、全て各社の商標または登録商標です。

Copyright 2024 Sony Biz Networks Corporation

利用環境評価

- Security Hub のセキュリティ基準・指摘事項タイトル・結果詳細タイトルを英語から日本語に翻訳して表示するよう機能を追加しました。

新表示例

結果一覧						
		選択した結果を無効化する		結果CSV出力	1ページの表示件数: 10	
ステータス	重要度	ID	タイトル	不合格のチェック	詳細	無効化
失敗	中	ACM.1	インポートされた証明書と ACM が発行した証明書は、指定された期間後に更新する必要があります	1/2	詳細	☐
成功	高	ACM.2	ACM が管理する RSA 証明書は、少なくとも 2,048 ビットのキー長を使用する必要があります	0/1	詳細	☐
成功	中	APIGateway.1	API ゲートウェイ REST と WebSocket API 実行ログを有効にする必要があります	0/1	詳細	☐
成功	中	APIGateway.2	API Gateway REST API ステージは、バックエンド認証に SSL 証明書を使用するように設定する必要があります	0/1	詳細	☐
成功	低	APIGateway.3	API ゲートウェイ REST API ステージでは AWS X-Ray トレースが有効になっている必要があります	0/1	詳細	☐
成功	中	APIGateway.4	API ゲートウェイは WAF ウェブ ACL に関連付ける必要があります	0/1	詳細	☐
成功	中	APIGateway.5	API ゲートウェイ REST API キャッシュデータは保存時に暗号化する必要があります	0/1	詳細	☐
成功	中	APIGateway.8	API Gateway ルートは認証タイプを指定する必要があります	0/1	詳細	☐
成功	中	APIGateway.9	アクセスログは API Gateway V2 ステージ用に設定する必要があります	0/1	詳細	☐
失敗	中	Account.1	AWS アカウントのセキュリティ連絡先情報を提供する必要があります。	1/1	詳細	☐

セキュリティ基準一覧

セキュリティ基準	セキュリティスコア	有効化/無効化	結果表示
AWS 基礎セキュリティのベストプラクティス v1.0.0 AWS Foundational Security Best Practices 標準は、AWS アカウントとデプロイされたリソースがセキュリティのベストプラクティスに合わない場合にそれを検出する一連の自動化されたチェックです。この標準は AWS のセキュリティ 専門知識に基づいて構築されています。この標準は一般的な規制は、AWS のセキュリティ 原則の改善に役立ち、AWS の最も一般的で基本的なサービスを対象としています。	84%	有効	設定 表示
AWS リソースタグ付け標準 v1.0.0 AWS リソースタグ付け標準は、AWS リソースがタグ付けされていないことを検出する一連の自動化されたセキュリティチェックです。	データなし	無効	設定 表示
CS AWS Foundations Benchmark v1.2.0 インターネットセキュリティセンター (CIS) の AWS 基礎ベンチマーク v1.2.0 は、AWS のセキュリティ 設定のベストプラクティスのセットです。この Security Hub 標準は、CIS 要件のサブセットに対するお客様のコンプライアンス準拠状況を自動的にチェックします。	19%	有効	設定 表示
CS AWS Foundations Benchmark v4.0 インターネットセキュリティセンター (CIS) の AWS 基礎ベンチマーク v4.0 は、AWS のセキュリティ 設定のベストプラクティスのセットです。この Security Hub 標準は、CIS 要件のサブセットに対するお客様のコンプライアンス準拠状況を自動的にチェックします。	26%	有効	設定 表示

結果詳細

EBS スナップショットは公開して復元できないようにすべきではない

ステータス	成功	失敗	0
重要度	高	中	0
すべてのチェック	1	成功	1
		無効化済み	0

Q ステータス指定および絞り込み結果

結果詳細一覧

ステータス	ラベル	イベント	リソース	発生	発生済み	結果	ステータス更新
成功	成功			詳細	2件発生	詳細	☐

※ 記載されている会社名、製品名、ブランド名、サービス名は、全て各社の商標または登録商標です。

Copyright 2024 Sony Biz Networks Corporation

マネージドサポート管理

- リソース監査ルールの基本監査ルールで指定した電話番号に架電する機能を追加しました。

※マネージドサポートサービスをご利用のお客様が対象となります

※ご利用いただくには、別途“自動音声オプション”の契約が必要になります。

基本監査ルール		
カテゴリ	検知内容	ログ記録
AWS Health Event	リスクになっているAWS Health Eventを検知する。	有効 設定
AWS Trusted Advisor	アクセスキーが公開状態の脅威を検知する。	無効 設定

弊社基盤の電話番号
より通知されます

×

ログ記録設定

ログ記録の設定を行います。
通知先を指定するとイベント検知時に指定したメールアドレスに通知されます。
電話番号を設定した場合指定した電話番号宛てにAmazonConnectより通知されます。

有効化 ☒ 有効 ☐ 無効

メールアドレス

発信元電話番号

発信先電話番号

SONY

SONYはソニー株式会社の登録商標または商標です。

各ソニー製品の商品名・サービス名はソニー株式会社またはグループ各社の登録商標または商標です。その他の製品および会社名は、各社の商号、登録商標または商標です。