翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。

GuardDuty IAM 検出結果タイプ

PDF (guardduty-ug.pdf#guardduty_finding-types-iam) | **RSS (amazon-guardduty-doc-history.rss)**

次の検出結果は、IAM エンティティとアクセスキーに特有であり、常に AccessKey の **[Resource Type]** (リソースタイプ) です。検出結果の重要度と詳細は、検出結果タイプによって異なります。

ここにリストされている検出結果には、検出結果タイプの生成に使用されるデータソースとモデルが含まれます。詳細については、「基礎データソース (./guardduty_data-sources.html) 」を参照してください。

すべての IAM 関連の検出結果について、問題のエンティティを検証し、その許可が最小特権のベストプラクティスに従っていることを確認することをお勧めします。このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。検出結果の修正についての詳細は、「侵害された可能性のある AWS 認証情報の修正 (./compromised-creds.html) 」を参照してください。

トピック

- Impact:IAMUser/AnomalousBehavior (#impact-iam-anomalousbehavior)
- InitialAccess:IAMUser/AnomalousBehavior (#initialaccess-iam-anomalousbehavior)
- PenTest:IAMUser/KaliLinux (#pentest-iam-kalilinux)
- PenTest:IAMUser/ParrotLinux (#pentest-iam-parrotlinux)
- PenTest:IAMUser/PentooLinux (#pentest-iam-pentoolinux)
- Persistence:IAMUser/AnomalousBehavior (#persistence-iam-anomalousbehavior)
- Policy:IAMUser/RootCredentialUsage (#policy-iam-rootcredentialusage)
- PrivilegeEscalation:IAMUser/AnomalousBehavior (#privilegeescalation-iam-anomalousbehavior)
- Recon:IAMUser/MaliciousIPCaller (#recon-iam-maliciousipcaller)
- Recon:IAMUser/MaliciousIPCaller.Custom (#recon-iam-maliciousipcallercustom)
- Recon:IAMUser/TorIPCaller (#recon-iam-toripcaller)
- Stealth:IAMUser/CloudTrailLoggingDisabled (#stealth-iam-cloudtrailloggingdisabled)
- Stealth:IAMUser/PasswordPolicyChange (#stealth-iam-passwordpolicychange)
- UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B (#unauthorizedaccess-iam-consoleloginsuccessb)
- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS (#unauthorizedaccess-iam-instancecredentialexfiltrationinsideaws)
- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS (#unauthorizedaccess-iam-instancecredentialexfiltrationoutsideaws)
- UnauthorizedAccess:IAMUser/MaliciousIPCaller (#unauthorizedaccess-iam-maliciousipcaller)
- UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom (#unauthorizedaccess-iam-maliciousipcallercustom)
- UnauthorizedAccess:IAMUser/TorIPCaller (#unauthorizedaccess-iam-toripcaller)

CredentialAccess:IAMUser/AnomalousBehavior

AWS 環境へのアクセスに使用される API が異常な方法で呼び出されました。

デフォルトの重要度: [Medium] (中)

- **データソース:** CloudTrail 管理イベント

この検出結果は、アカウント内で異常な API リクエストが観察されたことを知らせるものです。この検出結果には、単一の API、または単一のユーザーアイデンティティ (https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-event-reference-user-identity.html) で近似の一連の関連 API リクエストが含まれる場合があります。観察される API は、攻撃者がユーザーの環境のパスワード、ユーザー名、およびアクセスキーを収集しようとすると、攻撃の認証情報アクセスステージに一般的に関連しています。このカテゴリの API は、`GetPasswordData`、`GetSecretValue`、`GenerateDbAuthToken` です。

この API リクエストは、 の異常検出機械学習 (ML) GuardDutyモデルによって異常として識別されました。機械学習モデルは、アカウント内のすべての API リクエストを評価し、攻撃者が使用するテクニックに関連する異常なイベントを特定します。機械学習モデルは、リクエストを行ったユーザー、リクエストが行われた場所、リクエストされた特定の API など、API リクエストのさまざまな要因を追跡します。リクエストしたユーザーアイデンティティにおいて API リクエストのどの要因が異常なのかという詳細については、「検出結果の詳細 (https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_findings-summary.html#finding-anomalous) 」を参照してください。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正 (./compromised-creds.html) 」を参照してください。

DefenseEvasion:IAMUser/AnomalousBehavior

防御対策を回避するために使用された API が異常な方法で呼び出されました。

デフォルトの重要度: [Medium] (中)

- **データソース:** CloudTrail 管理イベント

この検出結果は、アカウント内で異常な API リクエストが観察されたことを知らせるものです。この検出結果には、単一の API、または単一のユーザーアイデンティティ (https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-event-reference-user-identity.html) で近似の一連の関連 API リクエストが含まれる場合があります。観察された API は、攻撃者が自分のトラックをカバーし、検出を回避しようとしている防御回避戦術に一般的に関連しています。このカテゴリの API は通常、削除、無効化、停止オペレーションです (`DeleteFlowLogs`、`DisableAlarmActions`、`StopLogging` など)。

この API リクエストは、 の異常検出機械学習 (ML) GuardDutyモデルによって異常として識別されました。機械学習モデルは、アカウント内のすべての API リクエストを評価し、攻撃者が使用するテクニックに関連する異常なイベントを特定します。機械学習モデルは、リクエストを行ったユーザー、リクエストが行われた場所、リクエストされた特定の API など、API リクエストのさまざまな要因を追跡します。リクエストしたユーザーアイデンティティにおいて API リクエストのどの要因が異常なのかという詳細については、「検出結果の詳細 (https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_findings-summary.html#finding-anomalous)」を参照してください。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正 (./compromised-creds.html)」を参照してください。

Discovery:IAMUser/AnomalousBehavior

リソースの検出に一般的に使用される API が、異常な方法で呼び出されました。

デフォルトの重要度: [Low] (低)

- **データソース:** CloudTrail 管理イベント

この検出結果は、アカウント内で異常な API リクエストが観察されたことを知らせるものです。この検出結果には、単一の API、または単一のユーザーアイデンティティ (https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-event-reference-user-identity.html) で近似の一連の関連 API リクエストが含まれる場合があります。観察される API は、攻撃者が情報を収集して AWS 、環境がより広範な攻撃の影響を受けやすいかどうかを判断する場合に、攻撃の検出段階に一般的に関連します。このカテゴリの API は、get、describe、または list オペレーションです (`DescribeInstances`、 `GetRolePolicy`、または `ListAccessKeys` など)。

この API リクエストは、 の異常検出機械学習 (ML) GuardDutyモデルによって異常として識別されました。機械学習モデルは、アカウント内のすべての API リクエストを評価し、攻撃者が使用するテクニックに関連する異常なイベントを特定します。機械学習モデルは、リクエストを行ったユーザー、リクエストが行われた場所、リクエストされた特定の API など、API リクエストのさまざまな要因を追跡します。リクエストしたユーザーアイデンティティにおいて API リクエストのどの要因が異常なのかという詳細については、「検出結果の詳細 (https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_findings-summary.html#finding-anomalous) 」を参照してください。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正 (./compromised-creds.html) 」を参照してください。

Exfiltration:IAMUser/AnomalousBehavior

AWS 環境からデータを収集するために一般的に使用される API が異常な方法で呼び出されました。

デフォルトの重要度: [High] (高)

- **データソース:** CloudTrail 管理イベント

この検出結果は、アカウント内で異常な API リクエストが観察されたことを知らせるものです。この検出結果には、単一の API、または単一のユーザーアイデンティティ (https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-event-

reference-user-identity.html) で近似の一連の関連 API リクエストが含まれる場合があります。観測された API は、侵入戦術に一般的に関連していて、そこでは攻撃者がネットワークからデータを収集しようとしています。この検出結果タイプの API は管理 (コントロールプレーン)オペレーションのみであり、通常は、S3、スナップショット、およびデータベースに関連しています (`PutBucketReplication`、`CreateSnapshot`、`RestoreDBInstanceFromDBSnapshot` など)。

この API リクエストは、 の異常検出機械学習 (ML) GuardDutyモデルによって異常として識別されました。機械学習モデルは、アカウント内のすべての API リクエストを評価し、攻撃者が使用するテクニックに関連する異常なイベントを特定します。機械学習モデルは、リクエストを行ったユーザー、リクエストが行われた場所、リクエストされた特定の API など、API リクエストのさまざまな要因を追跡します。リクエストしたユーザーアイデンティティにおいて API リクエストのどの要因が異常なのかという詳細については、「検出結果の詳細 (https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_findings-summary.html#finding-anomalous) 」を参照してください。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正 (./compromised-creds.html) 」を参照してください。

Impact:IAMUser/AnomalousBehavior

AWS 環境内のデータまたはプロセスを改ざんするために一般的に使用される API が異常な方法で呼び出されました。

デフォルトの重要度: [High] (高)

- **データソース:** CloudTrail 管理イベント

この検出結果は、アカウント内で異常な API リクエストが観察されたことを知らせるものです。この検出結果には、単一の API、または単一のユーザーアイデンティティ (https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-event-reference-user-identity.html) で近似の一連の関連 API リクエストが含まれる場合があります。観察される API は、攻撃者がオペレーションを中断し、ユーザー

のアカウント内のデータを操作、中断、または破壊しようとするインパクト戦術に一般的に関連しています。この検出結果タイプの API は、通常、delete、update、または put オペレーションです (`DeleteSecurityGroup`、`UpdateUser`、`PutBucketPolicy` など)。

この API リクエストは、 の異常検出機械学習 (ML) GuardDutyモデルによって異常として識別されました。機械学習モデルは、アカウント内のすべての API リクエストを評価し、攻撃者が使用するテクニックに関連する異常なイベントを特定します。機械学習モデルは、リクエストを行ったユーザー、リクエストが行われた場所、リクエストされた特定の API など、API リクエストのさまざまな要因を追跡します。リクエストしたユーザーアイデンティティにおいて API リクエストのどの要因が異常なのかという詳細については、「検出結果の詳細 (https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_findings-summary.html#finding-anomalous) 」を参照してください。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正 (./compromised-creds.html) 」を参照してください。

InitialAccess:IAMUser/AnomalousBehavior

AWS 環境への不正アクセスを得るために一般的に使用される API が異常な方法で呼び出されました。

デフォルトの重要度: [Medium] (中)

- **データソース:** CloudTrail 管理イベント

この検出結果は、アカウント内で異常な API リクエストが観察されたことを知らせるものです。この検出結果には、単一の API、または単一のユーザーアイデンティティ (https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-event-reference-user-identity.html) で近似の一連の関連 API リクエストが含まれる場合があります。攻撃者がユーザーの環境へのアクセスを確立しようとすると、観察される API は、攻撃の初期アクセス段階に一般的に関連しています。このカテゴリの API は、通常 get トークン、またはセッションオペレーションです (`GetFederationToken`、`StartSession`、`GetAuthorizationToken` など)。

この API リクエストは、 の異常検出機械学習 (ML) GuardDutyモデルによって異常として識別されました。機械学習モデルは、アカウント内のすべての API リクエストを評価し、攻撃者が使用するテクニックに関連する異常なイベントを特定します。機械学習モデルは、リクエストを行ったユーザー、リクエストが行われた場所、リクエストされた特定の API など、API リクエストのさまざまな要因を追跡します。リクエストしたユーザーアイデンティティにおいて API リクエストのどの要因が異常なのかという詳細については、「検出結果の詳細 (https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_findings-summary.html#finding-anomalous) 」を参照してください。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正 (./compromised-creds.html) 」を参照してください。

PenTest:IAMUser/KaliLinux

API が Kali Linux マシンから呼び出されました。

デフォルトの重要度: [Medium] (中)

- **データソース:** CloudTrail 管理イベント

この検出結果は、Kali Linux を実行しているマシンが、 環境のリストされた AWS アカウントに属する認証情報を使用して API コールを行っていることを知らせるものです。Kali Linux は、セキュリティプロフェッショナルが EC2 インスタンスの脆弱性を特定してパッチを適用するために使う一般的な侵入テストツールです。また、攻撃者はこのツールを使用して EC2 設定の弱点を見つけ、 AWS 環境への不正アクセスを行います。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正 (./compromised-creds.html) 」を参照してください。

PenTest:IAMUser/ParrotLinux

API が Parrot Security Linux マシンから呼び出されました。

デフォルトの重要度: [Medium] (中)

- **データソース:** CloudTrail 管理イベント

この検出結果は、Parrot Security Linux を実行しているマシンが、 環境のリストされた AWS アカウントに属する認証情報を使用して API コールを行っていることを知らせるものです。Parrot Security Linux は、セキュリティプロフェッショナルが EC2 インスタンスの脆弱性を特定してパッチを適用するために使う一般的な侵入テストツールです。また、攻撃者はこのツールを使用して EC2 設定の弱点を見つけ、 AWS 環境への不正アクセスを行います。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正 (./compromised-creds.html) 」を参照してください。

PenTest:IAMUser/PentooLinux

API が Pentoo Linux マシンから呼び出されました。

デフォルトの重要度: [Medium] (中)

- **データソース:** CloudTrail 管理イベント

この検出結果は、Pentoo Linux を実行しているマシンが、環境内のリストされている AWS アカウントに属する認証情報を使用して API コールを行っていることを知らせるものです。Pentoo Linux は、セキュリティプロフェッショナルが EC2 インスタンスの脆弱性を特定してパッチを適用するために使う一般的な侵入テストツールです。また、攻撃者はこのツールを使用して EC2 設定の弱点を見つけ、 AWS 環境への不正アクセスを行います。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正 (./compromised-creds.html) 」を参照してください。

Persistence:IAMUser/AnomalousBehavior

AWS 環境への不正アクセスを維持するために一般的に使用される API が異常な方法で呼び出されました。

デフォルトの重要度: [Medium] (中)

- **データソース:** CloudTrail 管理イベント

この検出結果は、アカウント内で異常な API リクエストが観察されたことを知らせるものです。この検出結果には、単一の API、または単一のユーザーアイデンティティ (https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-event-reference-user-identity.html) で近似の一連の関連 API リクエストが含まれる場合があります。観察される API は、攻撃者がユーザーの環境へのアクセスを獲得し、そのアクセスを維持しようとするパーシスタンス戦術に一般的に関連しています。このカテゴリの API は、通常、create、インimport、または modify オペレーションです (`CreateAccessKey`、 `ImportKeyPair`、 `ModifyInstanceAttribute` など)。

この API リクエストは、 の異常検出機械学習 (ML) GuardDutyモデルによって異常として識別されました。機械学習モデルは、アカウント内のすべての API リクエストを評価し、攻撃者が使用するテクニックに関連する異常なイベントを特定します。機械学習モデルは、リクエストを行ったユーザー、リクエストが行われた場所、リクエストされた特定の API など、API リクエストのさまざまな要因を追跡します。リクエストしたユーザーアイデンティティにおいて API リクエストのどの要因が異常なのかという詳細については、「検出結果の詳細 (https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_findings-summary.html#finding-anomalous) 」を参照してください。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正 (./compromised-creds.html) 」を参照してください。

Policy:IAMUser/RootCredentialUsage

API がルートユーザーサインイン認証情報を使用して呼び出されました。

デフォルトの重要度: [Low] (低)

- **データソース:** CloudTrail 管理イベントまたは CloudTrail データイベント

この検出結果は、ユーザーの環境のリスト化された AWS アカウント のルートユーザーサインイン認証情報が AWS サービスへのリクエストに使用されていることを知らせるものです。ユーザーは、ルートユーザーのサインイン認証情報を使用して AWS サービスにアクセスしないことをお勧めします。代わりに、 AWS Security Token Service (STS) からの最小特権の一時的な認証情報を使用して AWS サービスにアクセスする必要があります。 AWS STS がサポートされていない状況では、IAM ユーザー認証情報をお勧めします。詳細については、「IAM ベストプラクティス (https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html) 」を参照してください。

> **注記**
>
> アカウントで S3 脅威検出が有効になっている場合、この検出結果は、 AWS アカウントアのルートユーザーサインイン認証情報を使用して S3 リソースで S3 データプレーンオペレーションを実行しようとした場合に応答して生成される可能性があります。使用された API コールは、検出結果の詳細でリスト化されます。S3 脅威検出が有効になっていない場合、この検出結果はイベントログ API によってのみトリガーされます。S3 脅威検出の詳細については、「S3 Protection (s3-protection.html) 」を参照してください。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正 (./compromised-creds.html) 」を参照してください。

PrivilegeEscalation:IAMUser/AnomalousBehavior

AWS 環境への高レベルのアクセス許可を取得するために一般的に使用される API が異常な方法で呼び出されました。

デフォルトの重要度: [Medium] (中)

- **データソース:** CloudTrail 管理イベント

この検出結果は、アカウント内で異常な API リクエストが観察されたことを知らせるものです。この検出結果には、単一の API、または単一のユーザーアイデンティティ (https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-event-reference-user-identity.html) で近似の一連の関連 API リクエストが含まれる場合があります。観察される API は、攻撃者が環境へのより高いレベルの許可を取得しようとする特権エスカレーション戦術に一般的に関連しています。このカテゴリの API は、通常、IAM ポリシー、ロール、ユーザーを変更するオペレーションを含みます (`AssociateIamInstanceProfile`、`AddUserToGroup`、`PutUserPolicy` など)。

この API リクエストは、 の異常検出機械学習 (ML) GuardDutyモデルによって異常として識別されました。機械学習モデルは、アカウント内のすべての API リクエストを評価し、攻撃者が使用するテクニックに関連する異常なイベントを特定します。機械学習モデルは、リクエストを行ったユーザー、リクエストが行われた場所、リクエストされた特定の API など、API リクエストのさまざまな要因を追跡します。リクエストしたユーザーアイデンティティにおいて API リクエストのどの要因が異常なのかという詳細については、「検出結果の詳細 (https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_findings-summary.html#finding-anomalous) 」を参照してください。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正 (./compromised-creds.html) 」を参照してください。

Recon:IAMUser/MaliciousIPCaller

API が悪意のある既知の IP アドレスから呼び出されました。

デフォルトの重要度: [Medium] (中)

- **データソース:** CloudTrail 管理イベント

この検出結果は、ユーザーの環境内のアカウントの AWS リソースをリスト化または記述できる API オペレーションが、脅威リストの IP アドレスから呼び出されたことを知らせるものです。攻撃者は、盗まれた認証情報を使用して、より貴重な認証情報を見つけたり、既に持っている認証情報の機能を特定したりするために、 AWS リソースのこの種の偵察を実行する場合があります。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正 (./compromised-creds.html) 」を参照してください。

Recon:IAMUser/MaliciousIPCaller.Custom

API が悪意のある既知の IP アドレスから呼び出されました。

デフォルトの重要度: [Medium] (中)

- **データソース:** CloudTrail 管理イベント

この検出結果は、ユーザーの環境のアカウントの AWS リソースをリスト化または説明できる API オペレーションがカスタム脅威リストの IP アドレスから呼び出されたことを知らせるものです。使用された脅威リストは、検出結果の詳細に表示されます。攻撃者は、盗まれた認証情報を使用して、より貴重な認証情報を見つけたり、既に持っている認証情報の機能を特定したりするために、 AWS リソースのこの種の偵察を実行する可能性があります。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正 (./compromised-creds.html) 」を参照してください。

Recon:IAMUser/TorIPCaller

API が Tor 出口ノードの IP アドレスから呼び出されました。

デフォルトの重要度: [Medium] (中)

- **データソース:** CloudTrail 管理イベント

この検出結果は、ユーザーの環境のアカウントの AWS リソースをリスト化または説明できる API オペレーションが Tor 出口ノードの IP アドレスから呼び出されたことを知らせるものです。Tor は匿名通信を有効化するソフトウェアです。通信を暗号化し、一連のネットワークノード間のリレー中にランダムに通信をバウンスさせます。最後の Tor ノードは出口ノードと呼ばれます。攻撃者は真のアイデンティティを隠すために Tor を使用します。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正 (./compromised-creds.html) 」を参照してください。

Stealth:IAMUser/CloudTrailLoggingDisabled

AWS CloudTrail ログ記録が無効になりました。

デフォルトの重要度: [Low] (低)

- **データソース:** CloudTrail 管理イベント

この検出結果は、 AWS 環境内の CloudTrail 証跡が無効になったことを知らせるものです。これにより、悪意ある目的でユーザーの AWS リソースへアクセスしている間、活動の痕跡を消してトラックを隠してログ記録を無効化しようとします。この検出結果は、証跡情報の削除または更新が成功することによってトリガーされる場合があります。この検出結果は、 に関連付けられている証跡からログを保存する S3 バケットが正常に削除されたことでトリガーすることもできます GuardDuty。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正 (./compromised-creds.html) 」を参照してください。

Stealth:IAMUser/PasswordPolicyChange

アカウントのパスワードポリシーが弱化されています。

デフォルトの重要度: [Low] (低)*

> **注記**
>
> この検出結果の重要度は、パスワードポリシーに加えられた変更の重要度に応じて、[Low] (低)、[Medium] (中)、[High] (高) になります。

- **データソース:** CloudTrail 管理イベント

AWS アカウントパスワードポリシーは、 AWS 環境内のリストされたアカウントで弱まりました。例えば、アカウントの削除、必要な文字数を減らすような更新、記号や数字を不要とする更新、パスワードの有効期限を延長するような更新が行われています。この検出結果は、 AWS アカウントのパスワードポリシーを更新または削除しようとしてトリガーすることもできます。 AWS アカウントパスワードポリシーは、IAM ユーザーに設定できるパスワードの種類を管理するルールを定義します。パスワードポリシーが弱化されると、覚えやすいパスワードや推測しやすいパスワードの作成が可能になり、セキュリティ上のリスクが生じます。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正 (./compromised-creds.html) 」を参照してください。

UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B

世界中でコンソールに対する複数の正常なログインが確認されました。

デフォルトの重要度: [Medium] (中)

- **データソース:** CloudTrail 管理イベント

この検出結果は、世界各地から同時に同じ IAM ユーザーによるコンソールへの複数の正常なログインが確認されたことを知らせるものです。このような異常でリスクの高いアクセス場所パターンは、 AWS リソースへの不正アクセスの可能性を示します。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正 (./compromised-creds.html) 」を参照してください。

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS

インスタンス起動ロールを通じて EC2 インスタンス専用に作成された認証情報は、 AWS内の別のアカウントから使用されています。

デフォルトの重要度: [High] (高)*

> **注記**
>
> この検出結果のデフォルトの重要度は [High] (高) です。ただし、API が AWS 環境に関連付けられたアカウントによって呼び出された場合、重要度は Medium になります。

- **データソース:** CloudTrail 管理イベントまたは S3 データイベント

この検出結果は、EC2 インスタンス認証情報を使用して、関連付けられた EC2 インスタンスが実行されているアカウントとは異なる AWS アカウントが所有する IP アドレスから APIs を呼び出すときに通知します。

AWS では、一時的な認証情報を作成したエンティティ (AWS アプリケーション、EC2、Lambda など) の外部に再配布することはお勧めしません。ただし、承認されたユーザーは EC2 インスタンスから認証情報をエクスポートして正当な API コールを行うことができます。
`remoteAccountDetails.Affiliated` フィールドが の場合 `True`、API は AWS 環境に関連付けられたアカウントから呼び出されました。攻撃の可能性

を排除してアクティビティが正当であることを確認するには、これらの認証情報を割り当てる先の IAM ユーザーに問い合わせてみます。

> **注記**
>
> がリモートアカウントからの継続的なアクティビティ GuardDuty を観察すると、その機械学習 (ML) モデルはこれを予想される動作として識別します。したがって、 GuardDuty は、そのリモートアカウントからのアクティビティに関するこの検出結果の生成を停止します。GuardDuty は、他のリモートアカウントからの新しい動作に関する検出結果を引き続き生成し、時間の経過とともに動作が変化するにつれて、学習したリモートアカウントを再評価します。

修復のレコメンデーション

この検出結果に応じて、次のワークフローを使用して、一連のアクションを決定できます。

1. `service.action.awsApiCallAction.remoteAccountDetails.accountId` フィールドから関係するリモートアカウントを特定します。
2. 次に、そのアカウントが `service.action.awsApiCallAction.remoteAccountDetails.affiliated` フィールドから環境 GuardDutyに関連付けられているかどうかを確認します。
3. アカウントが連携している場合は、リモートアカウントの所有者と EC2 インスタンスの認証情報の所有者に問い合わせて、調査してください。
4. アカウントが関連付けられていない場合、まず、アカウントが組織に関連付けられているがマルチアカウント設定の一部 GuardDutyではないか、アカウントで GuardDuty まだ有効になっていないかを評価します。それ以外の場合は、EC2 認証情報の所有者に問い合わせて、リモートアカウントがこれらの認証情報を使用するユースケースがあるかどうかを判断します。
5. 認証情報の所有者がリモートアカウントを認識しない場合は、 AWS内で動作する脅威アクターによって認証情報が侵害された可能性があります。ご利用の環境を保護するために、侵害された可能性のある Amazon EC2 インスタンスの修復 (./compromised-ec2.html) で推奨されているステップを実行する必要があります。

   さらに、 AWS Trust and Safety チームに不正使用レポートを送信 (https://support.aws.amazon.com/#/contacts/report-abuse) して、リモートア

カウントの調査を開始できます。 AWS Trust and Safety にレポートを送信するときは、検出結果の完全な JSON の詳細を含めます。

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS

インスタンス作成ロールで EC2 インスタンス専用に作成された認証情報が外部 IP アドレスから使用されています。

デフォルトの重要度: [High] (高)

- **データソース:** CloudTrail 管理イベントまたは S3 データイベント

この検出結果は、 以外のホスト AWS が AWS 、環境の EC2 インスタンスで作成された一時的な AWS 認証情報を使用して AWS API オペレーションを実行しようとしたことを知らせるものです。リストされている EC2 インスタンスが侵害されている可能性があり、このインスタンスの一時的な認証情報が の外部にあるリモートホストに流出した可能性があります AWS。 AWS は、一時的な認証情報を作成したエンティティ (AWS アプリケーション、EC2、Lambda など) の外部に再配布することはお勧めしません。ただし、承認されたユーザーは EC2 インスタンスから認証情報をエクスポートして正当な API コールを行うことができます。潜在的な攻撃を除外し、アクティビティの正当性を検証するには、検出結果においてリモート IP からのインスタンスの認証情報の使用が想定されるかどうかを検証します。

> **注記**
>
> がリモートアカウントからの継続的なアクティビティ GuardDuty を観察すると、その機械学習 (ML) モデルはこれを予想される動作として識別します。したがって、 GuardDuty は、そのリモートアカウントからのアクティビティに関するこの検出結果の生成を停止します。GuardDuty は、他のリモートアカウントからの新しい動作に関する検出結果を引き続き生成し、時間の経過とともに動作が変化するにつれて、学習したリモートアカウントを再評価します。

修復のレコメンデーション

この検出結果が生成されるのは、VPC インターネットゲートウェイ (IGW) からではなく、オンプレミスのゲートウェイから排出され、インターネットトラフィックがルーティングされるように、ネットワークが構成されている場合です。AWS Outposts (https://docs.aws.amazon.com/outposts/latest/userguide/) や VPC VPN 接続などの一般的な構成では、このようにトラフィックがルーティングされる可能性があります これが予期した動作である場合は、抑制ルールを使用して、2 つのフィルター条件で構成されるルールを作成することをお勧めします。1 つ目の条件では、**[finding type]** (結果タイプ) に `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS` を使用します。2 番目のフィルター条件は、オンプレミスインターネットゲートウェイの IP アドレスまたは CIDR 範囲を持つ **[API caller IPv4 Address]** (API 発信者の IPv4 アドレス) です。抑制ルールの作成の詳細については、「抑制ルール (./findings_suppression-rule.html) 」を参照してください。

> **注記**
>
> が外部ソースからの継続的なアクティビティ GuardDuty を観察した場合、その機械学習モデルはこれを予想される動作として識別し、そのソースからのアクティビティについてこの検出結果の生成を停止します。 GuardDuty は他のソースからの新しい動作の検出結果を引き続き生成し、時間の経過とともに動作が変化するにつれて学習したソースを再評価します。

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。「侵害された可能性のある AWS 認証情報の修正 (./compromised-creds.html) 」を参照してください。

UnauthorizedAccess:IAMUser/MaliciousIPCaller

API が悪意のある既知の IP アドレスから呼び出されました。

デフォルトの重要度: [Medium] (中)

- **データソース:** CloudTrail 管理イベント

この検出結果は、API オペレーション (EC2 インスタンスの起動、新しい IAM ユーザーの作成、 AWS 権限の変更など) が悪意のある既知の IP アドレスから

呼び出されたことを知らせるものです。これは、環境内の AWS リソースへの不正アクセスを示している可能性があります。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正 (./compromised-creds.html) 」を参照してください。

UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom

API がカスタム脅威リストにある IP アドレスから呼び出されました。

デフォルトの重要度: [Medium] (中)

- **データソース:** CloudTrail 管理イベント

この検出結果は、API オペレーション (EC2 インスタンスの起動、新しい IAM ユーザーの作成、 AWS 権限の変更など) が、アップロードした脅威リストに含まれている IP アドレスから呼び出されたことを知らせるものです。 では、脅威リストは悪意のある既知の IP アドレスで構成されます。これは、環境内の AWS リソースへの不正アクセスを示している可能性があります。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正 (./compromised-creds.html) 」を参照してください。

UnauthorizedAccess:IAMUser/TorIPCaller

API が Tor 出口ノードの IP アドレスから呼び出されました。

デフォルトの重要度: [Medium] (中)

- **データソース:** CloudTrail 管理イベント

この検出結果は、API オペレーション (EC2 インスタンスの起動、新しい IAM ユーザーの作成、 AWS 権限の変更などの試行など) が Tor 出口ノードの IP アドレスから呼び出されたことを知らせるものです。Tor は匿名通信を有効化するソフトウェアです。通信を暗号化し、一連のネットワークノード間のリレー中にランダムに通信をバウンスさせます。最後の Tor ノードは出口ノードと呼ばれます。これは、攻撃者が真のアイデンティティを隠しているという意図により、 AWS リソースへの未承認のアクセスを示している場合があります。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正 (./compromised-creds.html) 」を参照してください。
