Qualys TotalCloud v2.x
リリースノート

Version 2.6.0
October 04, 2023

新着情報

Amazon Web Services

Cloud Detection and Response にウィジェットを導入

インベントリでの Cloud Detection and Response の検出結果の強化

TotalCloud Inventory に TruRisk Insights のサポートを導入

新しいトークン

共通機能

新しい義務付けの導入

コントロールの変更

Qualys TotalCloud 2.6.0 は、改善とアップデートをもたらします。 詳細情報

TotalCloud API の更新については、TotalCloud API リリースノートを参照してください

コネクタ・アプリケーションの更新については、コネクタ・ リリース・ノートを参照してください

Copyright 2023 by Qualys, Inc. All Rights Reserved.

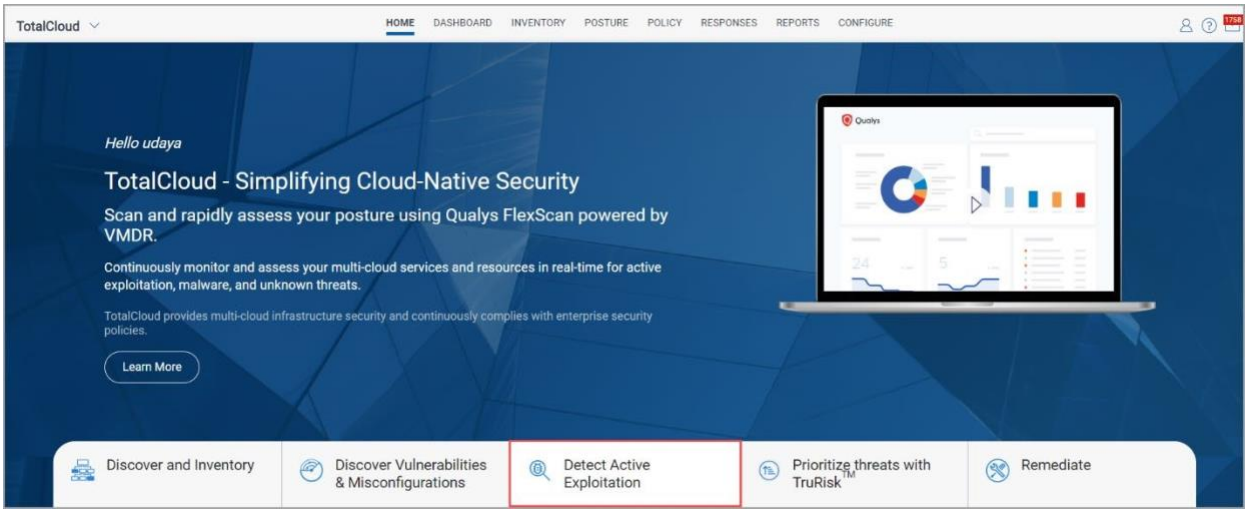
Amazon Web Services

このリリースで Amazon Web Services に導入された機能。

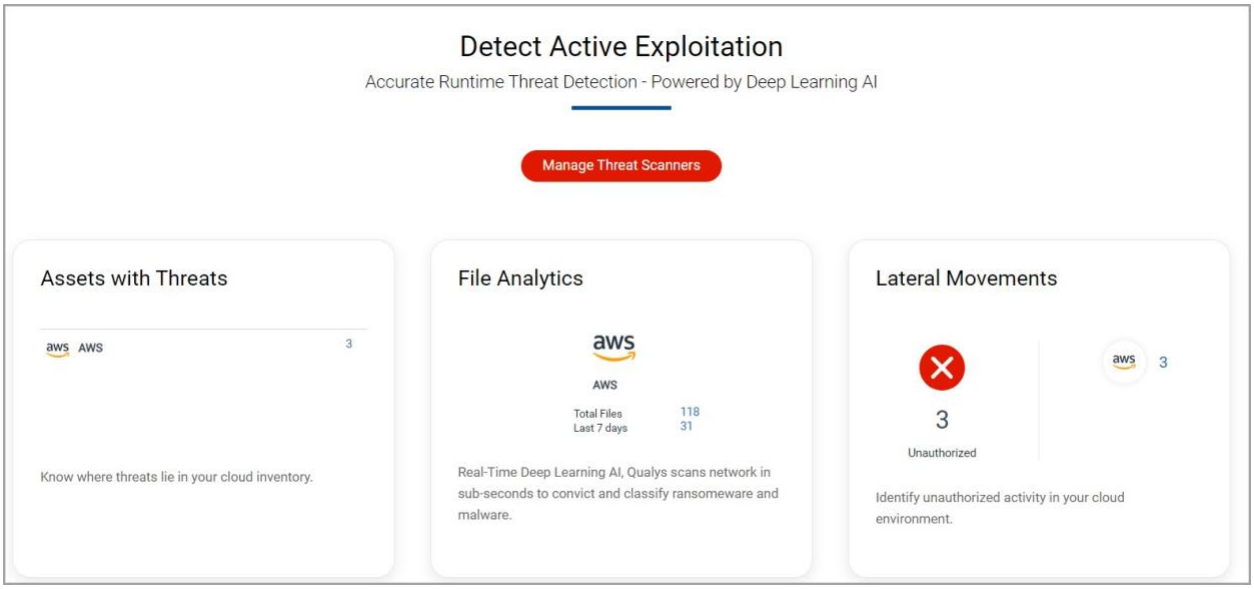
Cloud Detection and Response にウィジェットを導入

TotalCloud ホームページに CDR 用の 3 つの新しいウィジェットを導入しました。ウィジェットは、脅威のある資産のリアルタイム数、マルウェア/ランサムウェアの分析、ネットワーク内の疑わしい動作など、重要な資産情報を強調表示します。

新しい CDR ウィジェットにアクセスするには、**TotalCloud> HOME>Detect Active Exploitation** タブに移動します。



ウィジェットは、環境に CDR を設定するために脅威スキャナーを展開すると表示されます。脅威スキャナーをまだ設定していない場合は、TotalCloud オンラインヘルプで詳細を確認してください。



脅威のあるアセット – クラウドアカウント内の脅威にさらされている資産の数を特定します。CDR のリアルタイムの調査結果により、常に攻撃者の一歩先を行くことができ、迅速な更新が可能です。

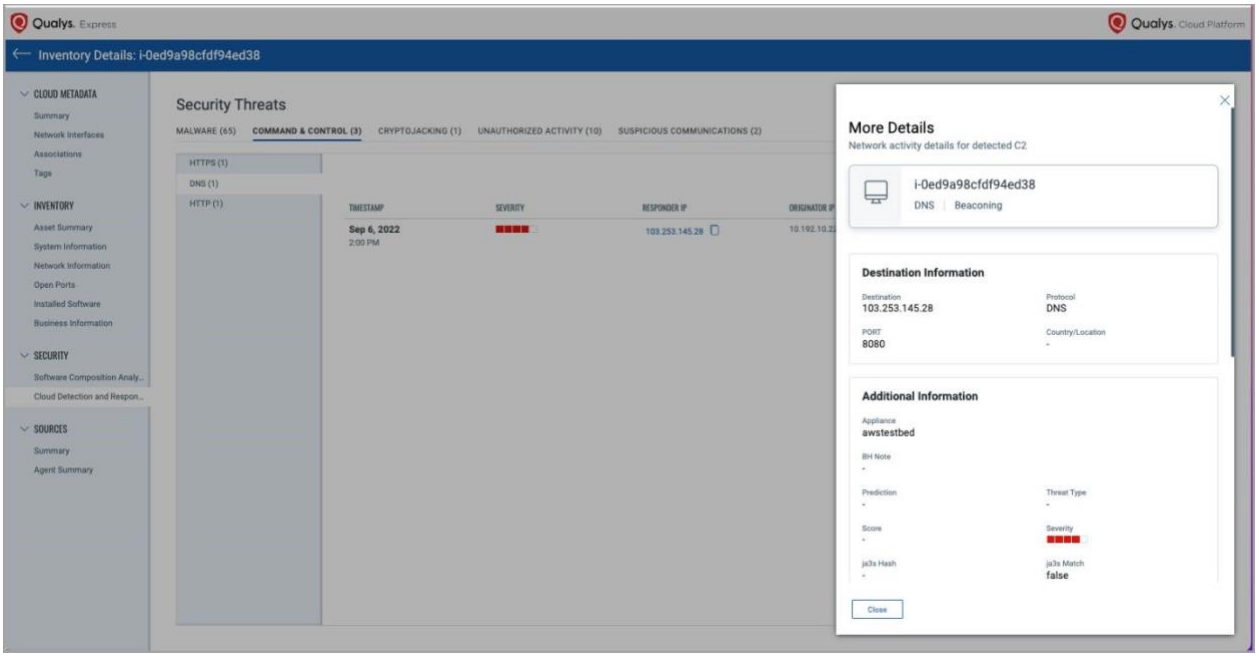
ファイル分析 – Qualys CDR は、ネットワークをスキャンして、導入されたファイルを識別し、悪意のあるエンティティを分類します。ウィジェットには、ネットワーク内の悪意のあるファイルの合計数と、過去 7 日間に検出された悪意のあるファイルの数が表示されます。

ラテラルムーブメント - アカウント内の不審なアクティビティを追跡します。不正な動き、RDP ブルートフォース攻撃などを嗅ぎ分けます。ウィジェットには、未承認のアクティビティの数が表示されます。

CDR ウィジェットの活用の詳細については、TotalCloud オンラインヘルプの「Cloud Detection and Response」セクションを参照してください。

インベントリでの Cloud Detection and Response の検出結果の強化

TotalCloud Inventory のアセットサマリーにリストされている CDR の調査結果を強化しました。CDR の調査結果は、5 つの形態のネットワーク攻撃すべてについて、より詳細なことを浮き彫りにしています。



マルウェア – ネットワークに対する潜在的なマルウェア攻撃の詳細について説明します。検出された脅威は、バックドア攻撃、トロイの木馬、ランサムウェアなどのマルウェアの種類に分類されます。

コマンド&コントロール – ネットワークプロトコルに対するコマンド&コントロール攻撃の発生についての詳細をご覧ください。暗号化された通信とネットワークプローブの送信元と宛先を理解します。

クリプトジャッキング – 攻撃者によるネットワーク内のクリプトマイニングの詳細をご覧ください。どのコインが採掘され、どのように採掘されるかについての直接的な情報を受け取ることができます。

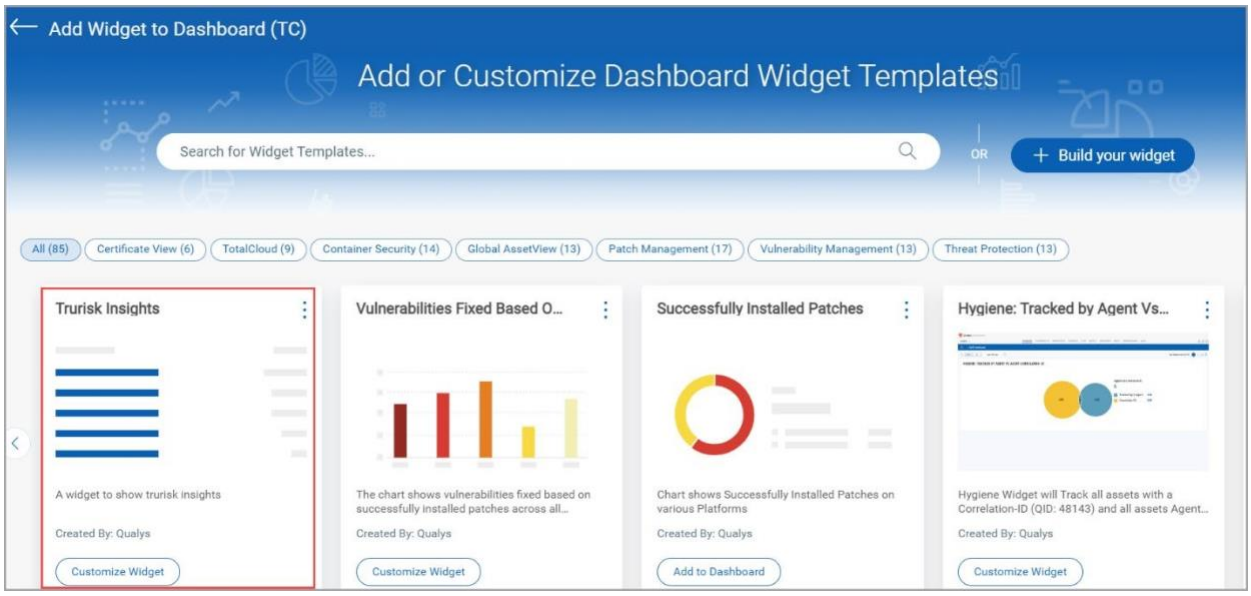
Unauthorized Activity (未承認のアクティビティ) – ネットワーク内のすべての未承認のアクティビティの詳細を確認します。アクティビティの種類、ブルートフォース攻撃、ポートスキャンなどに関する情報を受け取ります。

不審な通信 – 内部または外部を問わず、疑わしいネットワーク通信の詳細について説明します。

TotalCloud Inventory に TruRisk Insights のサポートを導入

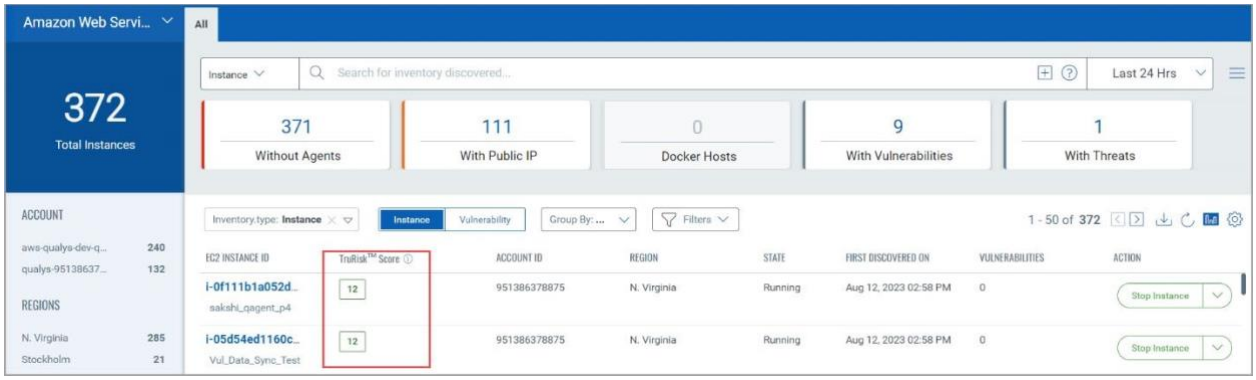
このリリースでは、TotalCloud ダッシュボードで TruRisk insights をリリースしました。TruRisk Insights は、お客様が TotalCloud の調査結果に基づいて脆弱性に優先順位を付けるのを支援するために導入されました。TruRisk Insights for TotalCloud は、CSPM、FlexScan、CDR、CWP の調査結果を活用して、関連するすべてのリソースデータを含む単一のウィジェットを表示します。

TotalCloud > Dashboard に移動します。「+」アイコンをクリックしてウィジェットを追加します。 TruRisk Insights ウィジェットが一覧表示されます。



また、TotalCloud Inventory に **TruRisk Score** 列を導入しました。この追加により、外部のセキュリティ、設定ミス、脆弱性スコアリングを TotalCloud エコシステムに導入することで、お客様に力を与えることができます。

TruRisk Score 列は、**[Inventory]タブ**に移動すると確認できます。リソース名の横に新しい列が表示されます。デフォルトでは、**TruRisk** スコアのリストは、最も重要なスコアがリストの一番上に表示されるように設定されています。検出結果をさらに並べ替えることもできます。



TruRisk **スコアは、** FlexScan の結果のみを使用してスコアを計算します。

新しいトークン

このリリースでは、新しいトークンのサポートが導入されました。

TruRisk トークン
この TruRisk Score のトークンは、TotalCloud の Inventory タブで確認できます。これらのトークンを使用して、提供された TruRisk スコアに基づいてリソースを検索します。

「インベントリ」>「任意のリソース・タイプ」に移動します。

Name	Description
instance.riskScore	Use an integer value (0-1000) to search for all the EC2 instances with the specified risk score.

レポートトークン

TotalCloud の[レポート]タブに新しいトークンを導入しました。以下のトークンを使用して、レポート ID に基づいてレポートを検索します。

Name	Description
report.id	Use a text value ##### to show reports based on the report ID.

共通機能

このリリースで TotalCloud アプリケーション全体に導入された機能。

新しい義務付けの導入

このリリースでは、新しい必須要件のサポートが導入されました。

Doc ID	Document Name	Publisher	Version
6281	Payment Card Industry Data Security Standard (PCI-DSS) v4.0	PCI Security Standards Council	Ver. 4.0

コントロールの変更

TotalCloud 2.6.0 のコントロールとポリシーに導入された変更。

Amazon Web Services

アマゾン ウェブ サービスの変更を制御します。

CIS Amazon Web Services Foundations Benchmark の新しいコントロール

CIS Amazon Web Services Foundations Benchmark の新しいコントロールが導入されました。

Platform	CID	Title
AWS	253	Ensure AWS Security Hub is enabled in all regions.

CIS Amazon Web Services Foundations Benchmark から Amazon Web に制御を移行サービスのベスト・プラクティス・ポリシー

CIS Amazon Web Services Foundations Benchmark の新しいコントロールを Amazon Web Services Best Practices Policy に移行しました。

Platform	CID	Title
AWS	67	Ensure all S3 buckets employ encryption-at-rest.

AWS CIS 2.0 のタイトル変更

CIS Amazon Web Services Foundations Benchmark 2.0 の次のコントロールのタイトルが変更されました。

Platform	CID	Old Title	New Title
AWS	67	Ensure a log metric filter and alarm exist for unauthorized API calls	Ensure unauthorized API calls are monitored.
AWS	28	Ensure a log metric filter and alarm exist for Management Console sign-in without MFA	Ensure management console sign-in without MFA is monitored
AWS	29	Ensure a log metric filter and alarm exist for usage of the root account	Ensure usage of the 'root' account is monitored
Platform	**CID**	**Old Title**	**New Title**
AWS	30	Ensure a log metric filter and alarm exist for IAM policy changes	Ensure IAM policy changes are monitored
AWS	31	Ensure a log metric filter and alarm exist for CloudTrail configuration changes	Ensure CloudTrail configuration changes are monitored
AWS	32	Ensure a log metric filter and alarm exist for AWS Management Console authentication failures	Ensure AWS Management Console authentication failures are monitored
AWS	33	Ensure a log metric filter and alarm exist for disabling or scheduled deletion of customer-created CMKs	Ensure disabling or scheduled deletion of customer-created CMKs is monitored
AWS	34	Ensure a log metric filter and alarm exist for S3 bucket policy changes	Ensure S3 bucket policy changes are monitored
AWS	35	Ensure a log metric filter and alarm exist for AWS Config configuration changes	Ensure AWS Config configuration changes are monitored
AWS	36	Ensure a log metric filter and alarm exist for security group changes	Ensure security group changes are monitored
AWS	37	Ensure a log metric filter and alarm exist for changes to Network Access Control Lists (NACL)	Ensure Network Access Control Lists (NACL) changes are monitored
AWS	38	Ensure a log metric filter and alarm exist for changes to network gateways	Ensure changes to network gateways are monitored
AWS	39	Ensure a log metric filter and alarm exist for route table changes	Ensure route table changes are monitored
AWS	40	Ensure a log metric filter and alarm exist for VPC changes	Ensure VPC changes are monitored
AWS	53	Ensure Encryption is enabled for the RDS database Instance	Ensure that encryption-at-rest is enabled for RDS Instances

AWS	172	Ensure a log metric filter and alarm exists for AWS Organizations changes	Ensure AWS Organizations changes are monitored

Microsoft Azure
Microsoft Azure の変更を制御します。
Microsoft Azure ベスト プラクティス ポリシーで非推奨のコントロール
Microsoft Azure ベスト プラクティス ポリシーのコントロールは非推奨になりました。

Platform	CID	Title
Azure	50172	Ensure that public network access is disabled for Azure Key Vaults.

対処された問題

- CID-52043 と CID 50070 で誤検出が生成される問題を修正しました。

- 評価レポート API が拡張され、レポート ID に基づくレポートが意図したとおりに生成されるようになりました。

- パブリックアクセスがあるにもかかわらず、S3 バケットにパブリックアクセスタイプが表示されていないとお客様から報告された問題を修正しました。アクセスタイプが正しく表示されるように、新しいパラメーターが導入されました。

- レポート作成ウィザードにメモを追加しました。このメモでは、検索クエリで resource.result トークンを使用する場合、コントロールの概要結果は、選択したリソース評価フィルターにのみ一致することを顧客に通知します。