IBM QRadar向けクラウドセキュリティアプリの管理

内容

はじめに

このドキュメントでは、IBM QRadar向けCisco Cloud Securityアプリの管理方法について説明します。

概要

IBMのQRadarは、ログ分析用の一般的なSIEMです。Cisco Umbrellaが組織のDNSトラフィック用に提供するログなど、大量のデータを分析するための強力なインターフェイスを提供します。IBM QRadar向けCisco Cloud Security Appに表示される情報は、Cisco Umbrella、CloudLock、Investigate、およびEnforcementのAPIを通じて提供されます。

QRadar用のCisco Cloud Securityアプリをセットアップすると、Cisco Cloud Securityプラットフォームからのすべてのデータが統合され、QRadarコンソールにグラフィカルな形式でデータを表示できるようになります。アナリストはアプリケーションから次の操作を実行できます。

- ドメイン、IPアドレス、電子メールアドレスの調査
- ドメインのブロックとブロック解除（適用）
- ネットワークのすべてのインシデントに関する情報を表示します。

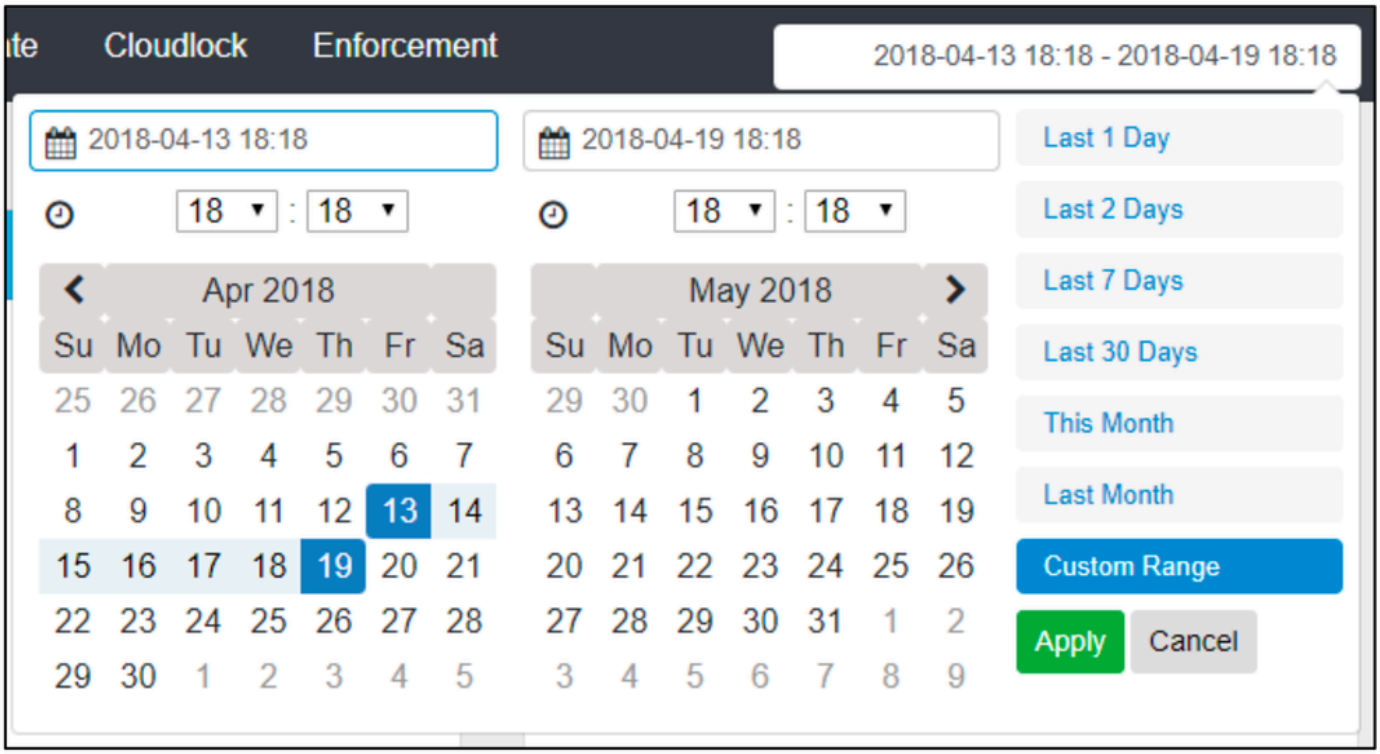
この記事では、Cisco Cloud Securityアプリケーションのナビゲート方法について説明します。アプリケーションをセットアップする方法については、次のサイトを参照してください。
Configuring the Cisco Cloud Security App for IBM QRadar

Cisco Cloud Securityアプリケーションへのアクセス

IBM QRadarでCisco Cloud Securityアプリケーションに移動するには、ホームページに移動して

Cisco Cloud Securityタブをクリックします。クラウドの概要タブとダッシュボードが表示されます。その後、Umbrella、Investigate、CloudLock、およびEnforcementの各タブにアクセスして、ログを表示できます。

デフォルトでは、クラウドセキュリティアプリケーションは過去7日間のデータを表示するように設定されています。時間枠を変更するには、右上の日付範囲をクリックします。

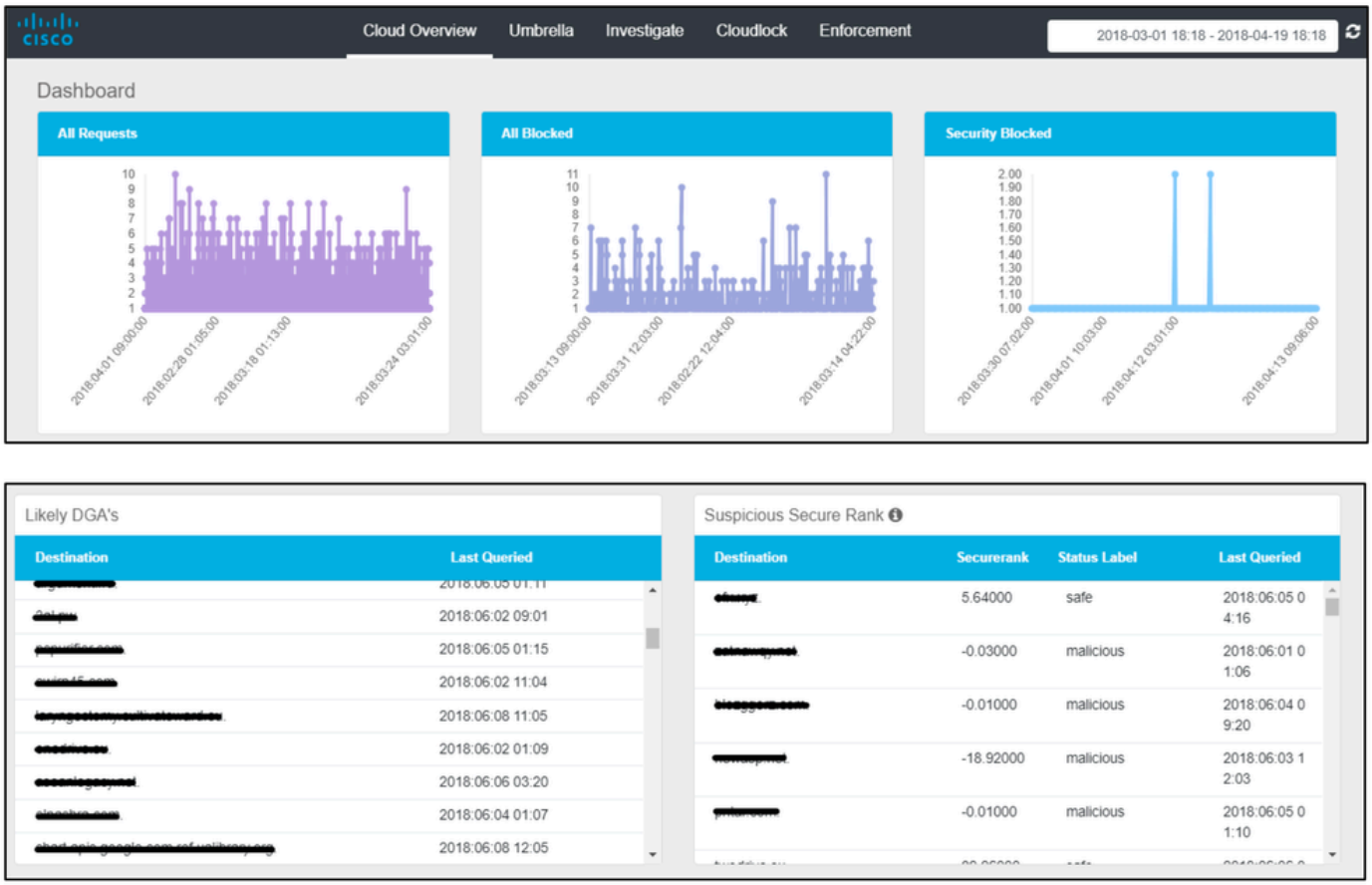


360072030052

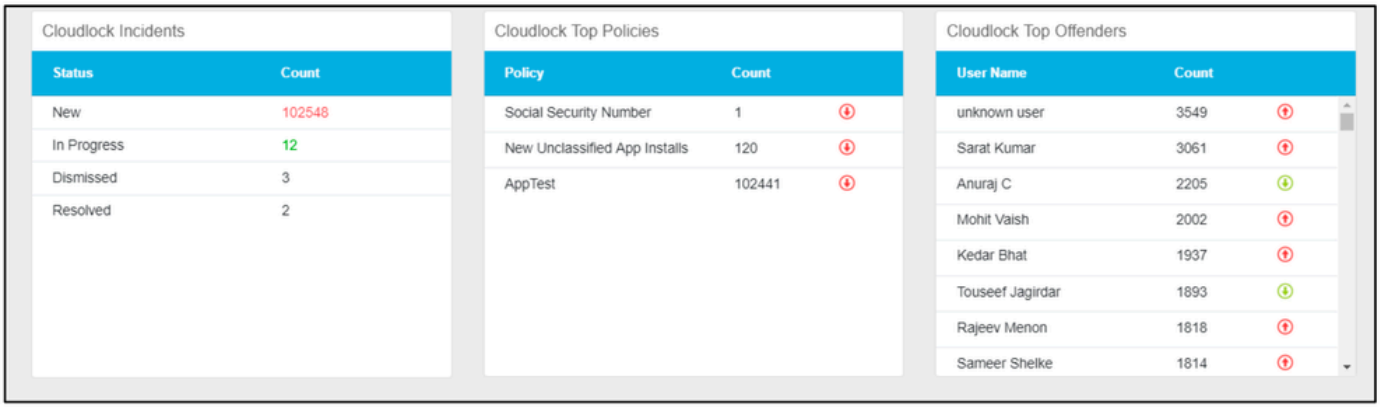
Cisco Cloud Securityアプリケーションコンポーネント

クラウドの概要

Cloud Overviewタブには、All Requests、All Blocked、Security Blocked、Possible DGA's、Suspicious Secure Rank、Cloudlock Incidents、CloudLock Overall、Top Policies、Top Severorなどの情報がグラフ形式で表示されます。



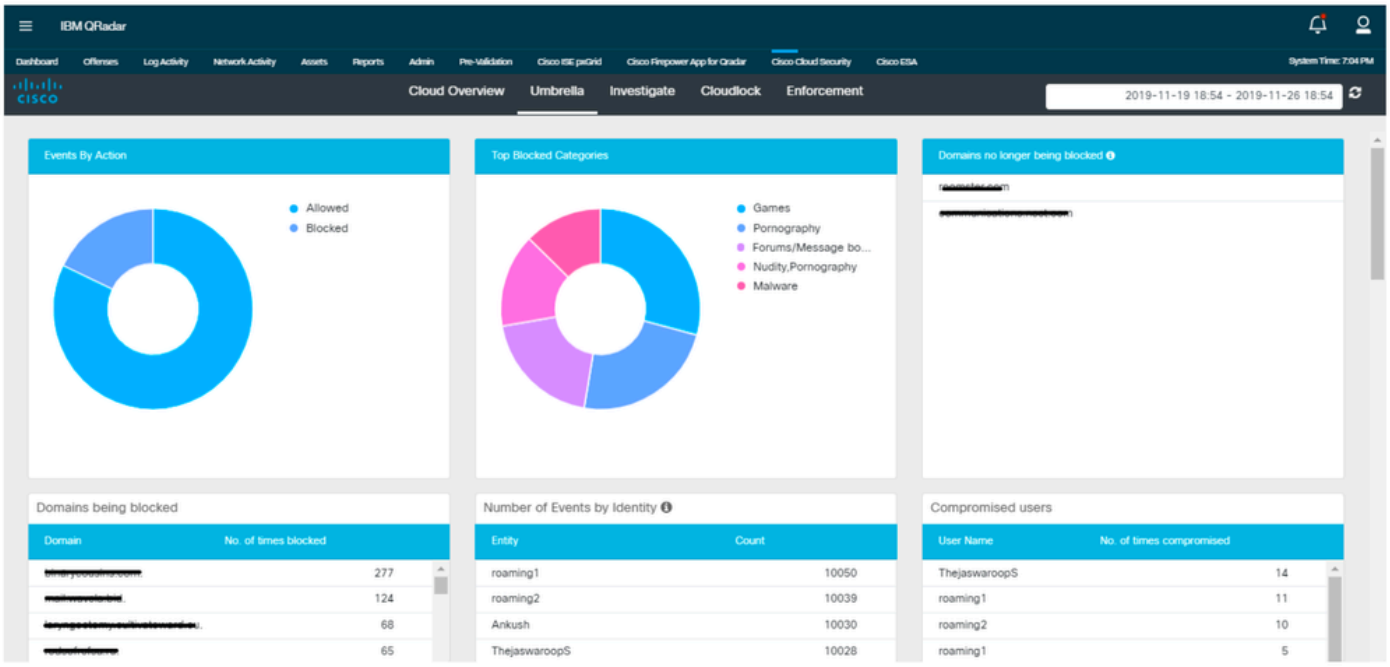
360072257631



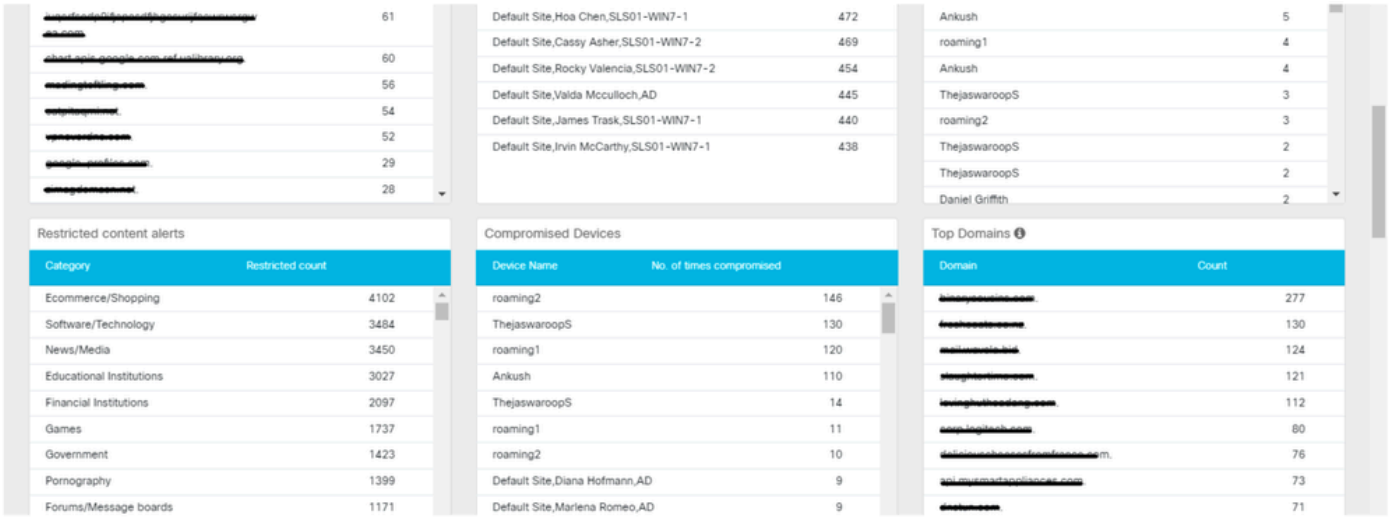
360072257611

Umbrella

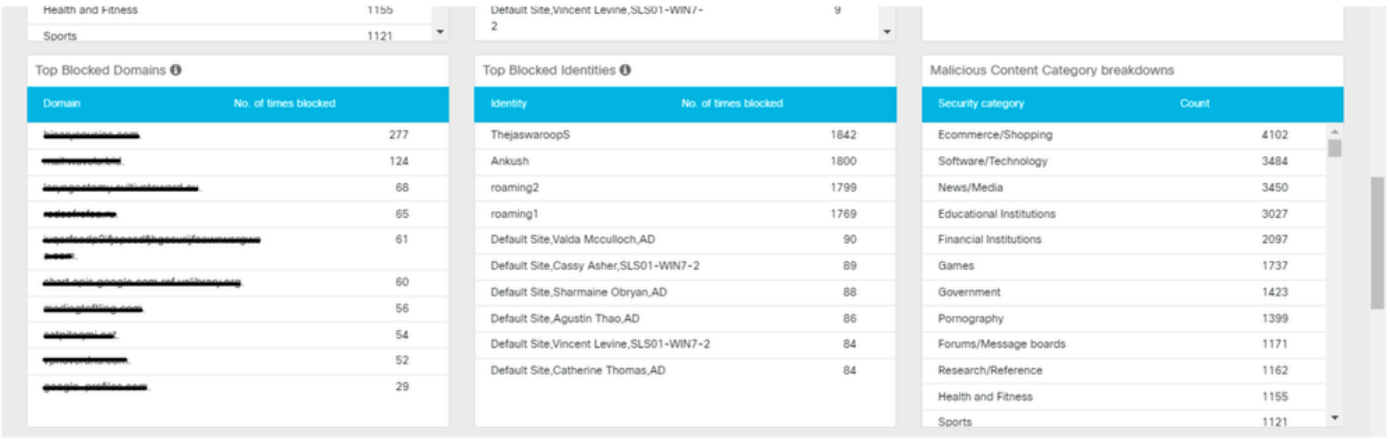
Umbrellaタブには、アクション別イベント、ブロックされた上位カテゴリ、ID別イベントの数、ブロックされているドメイン、ブロックされていないドメイン、侵害されたユーザ、制限されたコンテンツアラート、侵害されたデバイス、上位ドメイン、ブロックされた上位ドメイン、ブロックされた上位ID、悪意のあるコンテンツカテゴリの内訳、上位カテゴリ、アクティビティ、およびユーザアクセスの傾向などの情報が、グラフベースの視覚表現で表示されます。



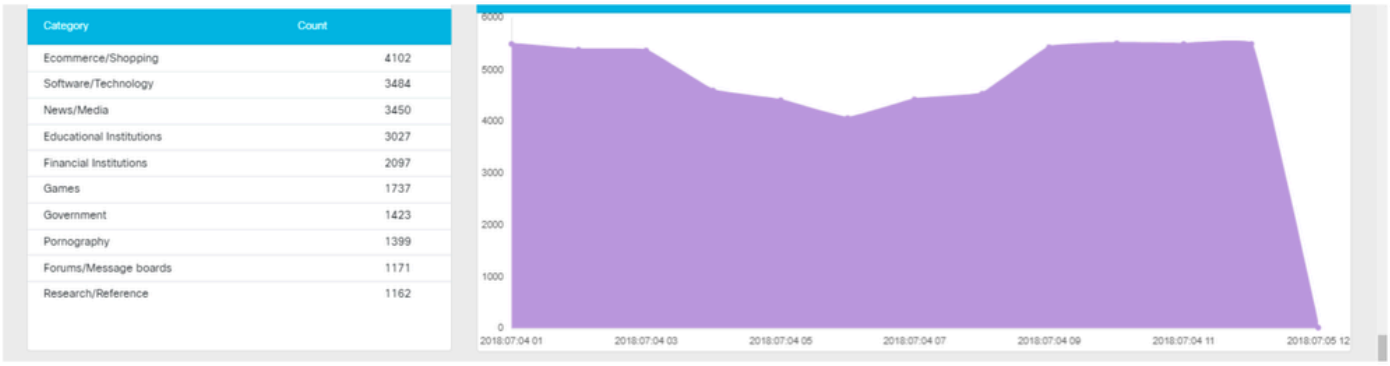
360072263411



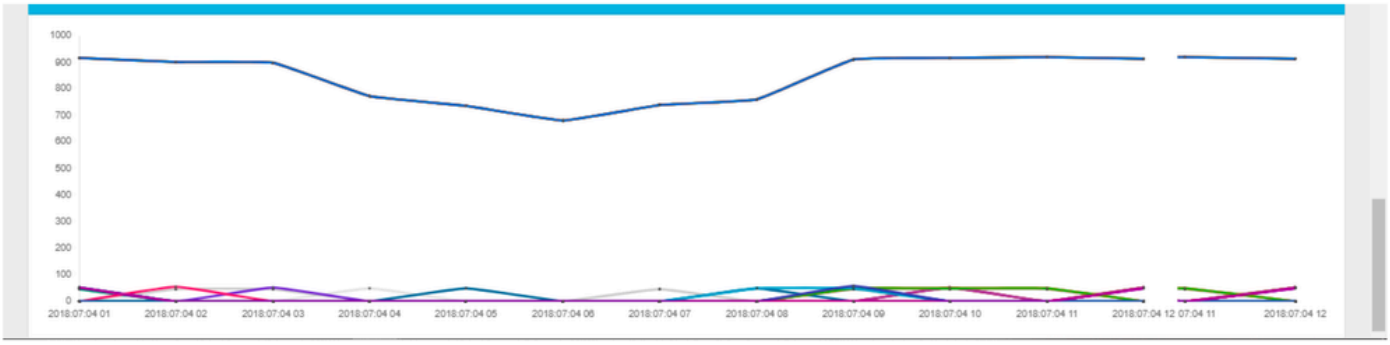
360072263391



360072037372



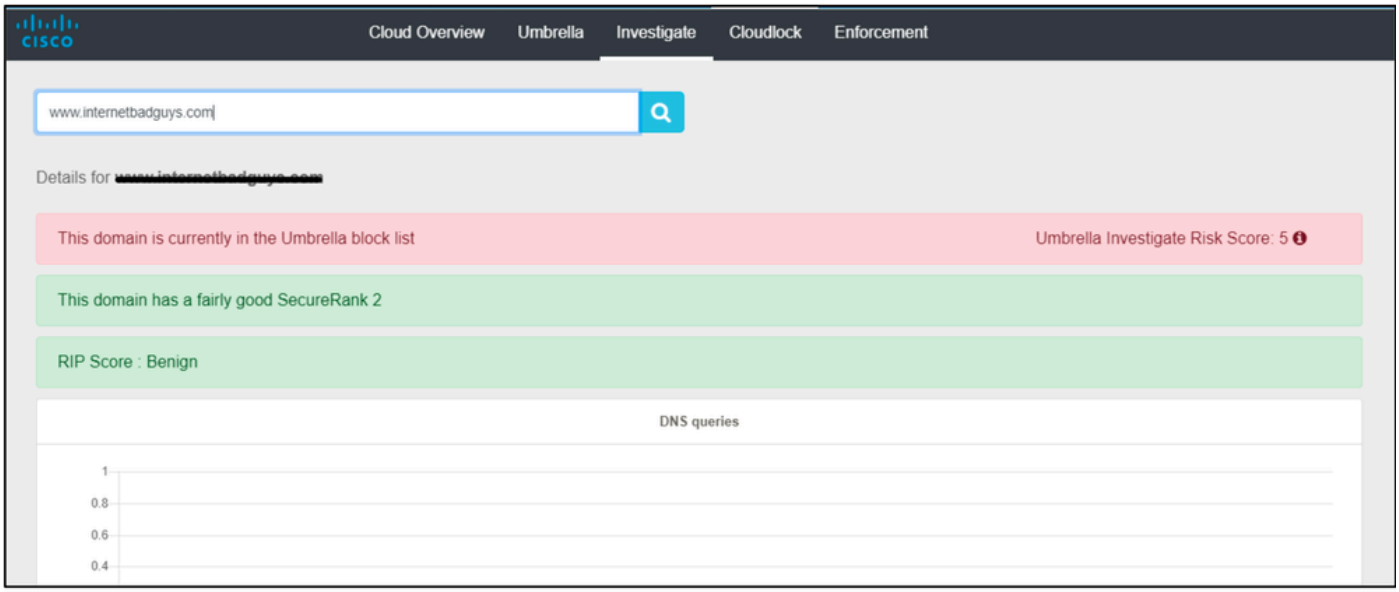
360072263331



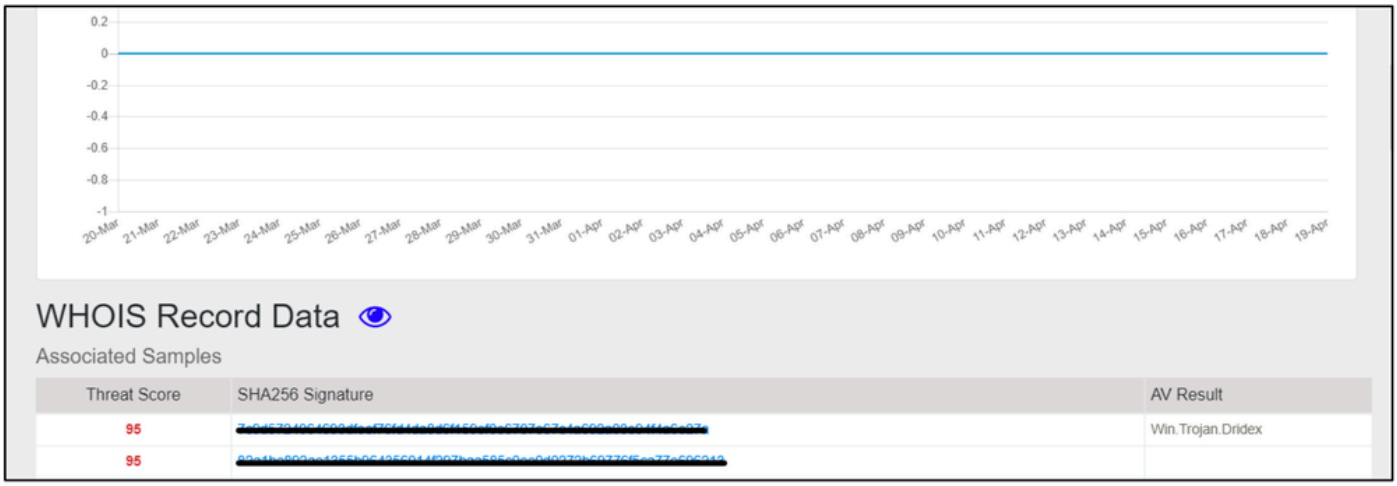
360072263351

調査

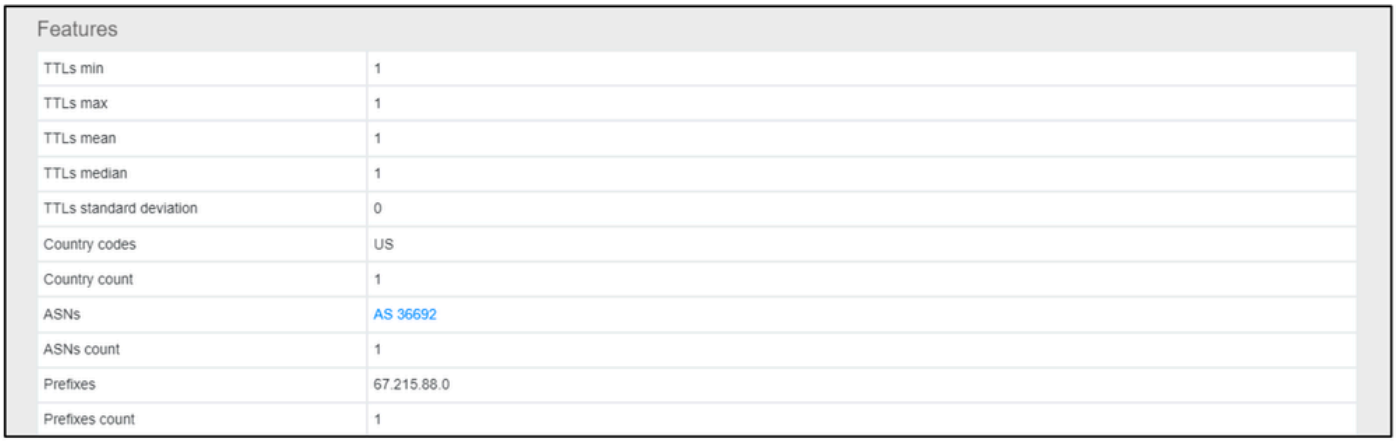
「Investigate」タブでは、ホスト名、URL、ASN、IP、ハッシュ、またはメール・アドレスに関連する情報を検索できます。また、WHOISレコード、DGA情報などの情報もあります。



360072263511



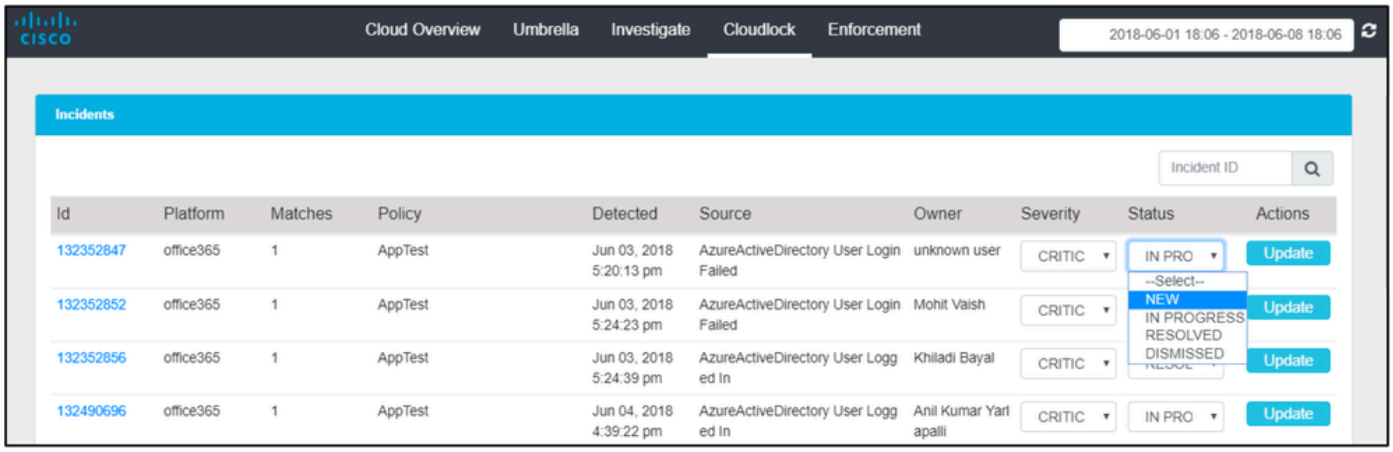
360072037472



360072037452

Cloudlock

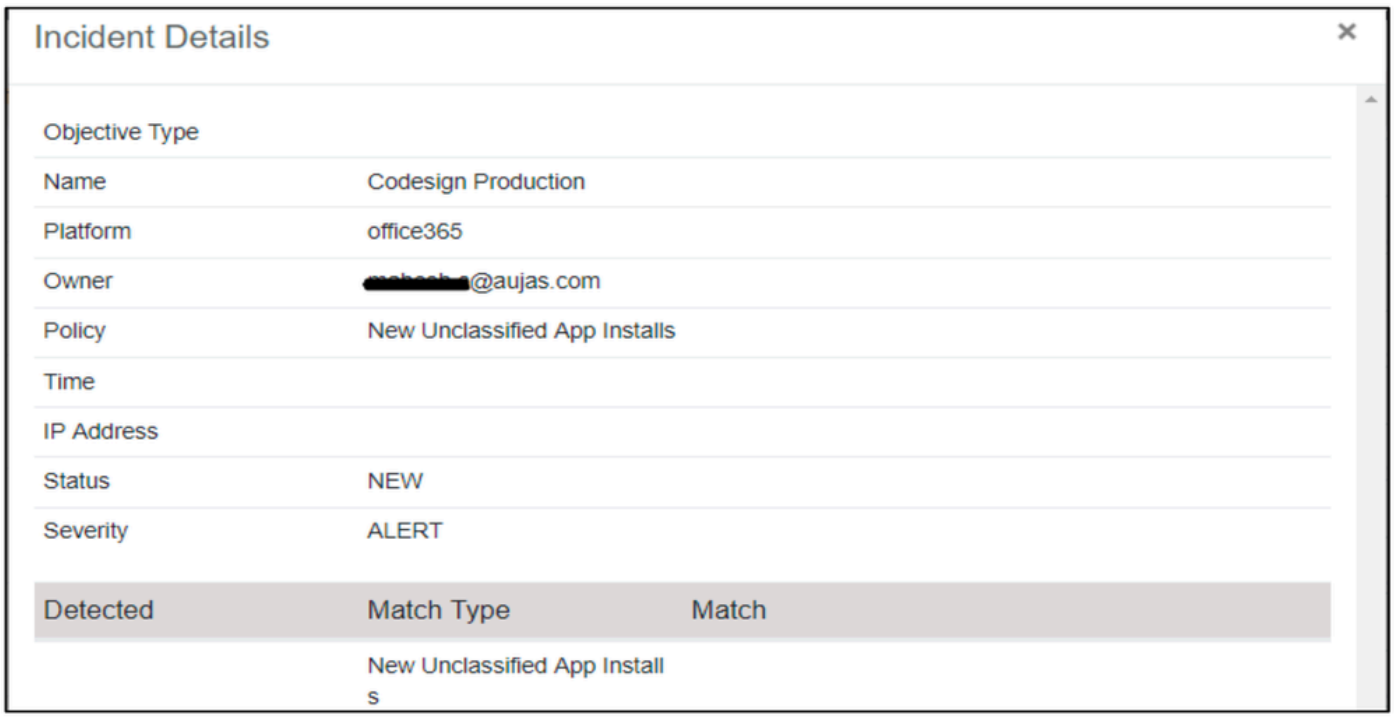
CloudLockタブでは、検出されたすべてのインシデントに関する情報を表示できます。また、ドロップダウンメニューから値を選択して[更新]をクリックすることで、インシデントの重大度とステータスを更新することもできます。



360072268311

ユーザは、インシデントに関する詳細を表示するために、任意のイベントにクロックを合わせる

ことができます。



360072042332

「強制」タブ

[強制]タブには、ブロックされているドメインに関する情報が表示されます。ユーザは、ブロックされたドメインを選択し、このインターフェイスからブロックを解除することもできます。

360072038472

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。