Gérer l'application de sécurité cloud pour IBM QRadar

Table des matières

Introduction

Ce document décrit comment gérer l'application Cisco Cloud Security pour IBM QRadar.

Aperçu

QRadar d'IBM est un SIEM populaire pour l'analyse des journaux. Il fournit une interface puissante pour analyser de grandes quantités de données, telles que les journaux fournis par Cisco Umbrella pour le trafic DNS de votre entreprise. Les informations affichées dans l'application de sécurité cloud Cisco pour IBM QRadar proviennent des API de Cisco Umbrella, CloudLock, Investigate et Enforcement.

Lorsque vous configurez l'application Cisco Cloud Security pour QRadar, elle intègre toutes les données de la plate-forme Cisco Cloud Security et vous permet de visualiser les données sous forme graphique dans la console QRadar. À partir de l'application, les analystes peuvent :

- Étudier les domaines, les adresses IP et les adresses e-mail
- Bloquer et débloquer des domaines (application)
- Affichez les informations de tous les incidents du réseau.

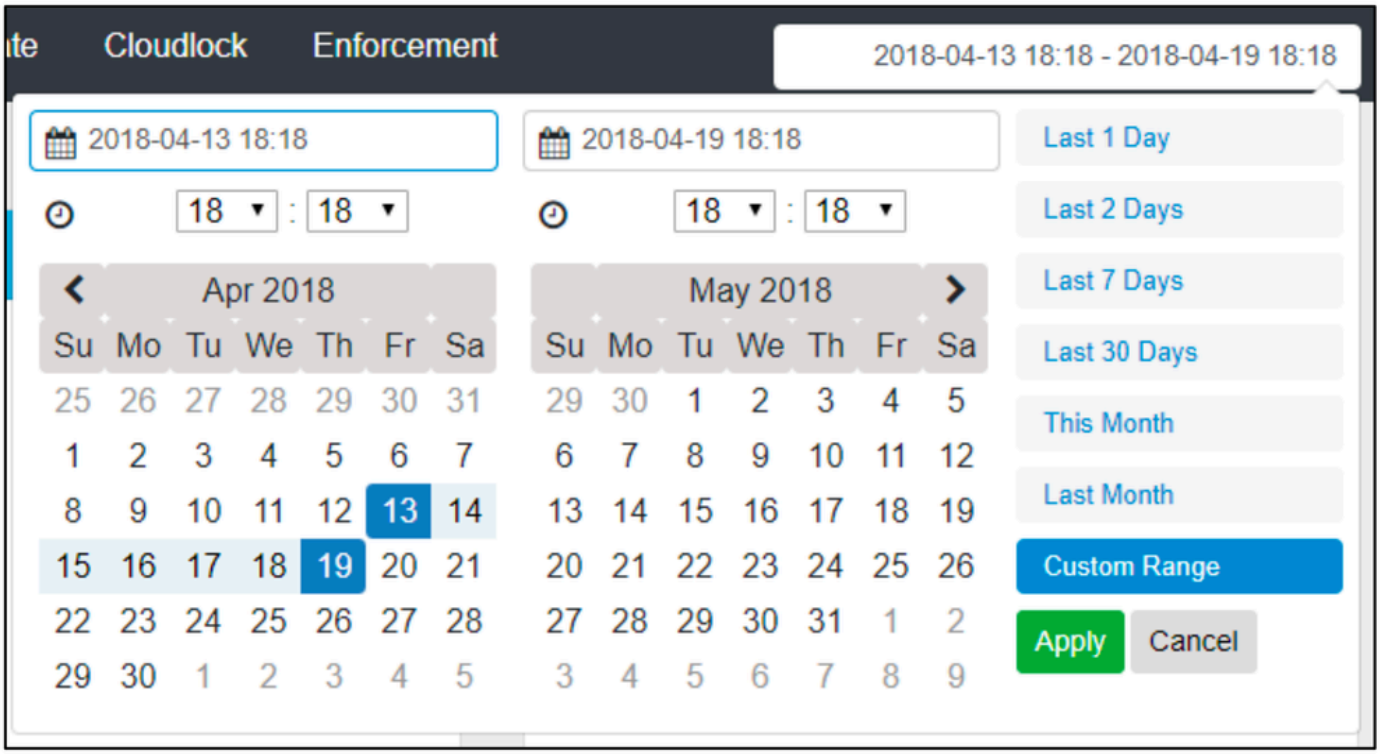
Cet article vous explique comment naviguer dans l'application Cisco Cloud Security. Les instructions relatives à la configuration de l'application sont disponibles ici : Configuration de l'application de sécurité cloud Cisco pour IBM QRadar

Accès à l'application Cisco Cloud Security

Pour accéder à l'application Cisco Cloud Security dans IBM QRadar, accédez à la page d'accueil

et cliquez sur l'onglet Cisco Cloud Security. L'onglet Cloud Overview et le tableau de bord s'affichent. Vous pouvez ensuite accéder aux onglets Umbrella, Investigate, CloudLock et Enforcement pour afficher vos journaux.

Par défaut, l'application de sécurité du cloud est configurée pour afficher les données des 7 derniers jours. Vous pouvez modifier la période en cliquant sur la plage de dates en haut à droite :

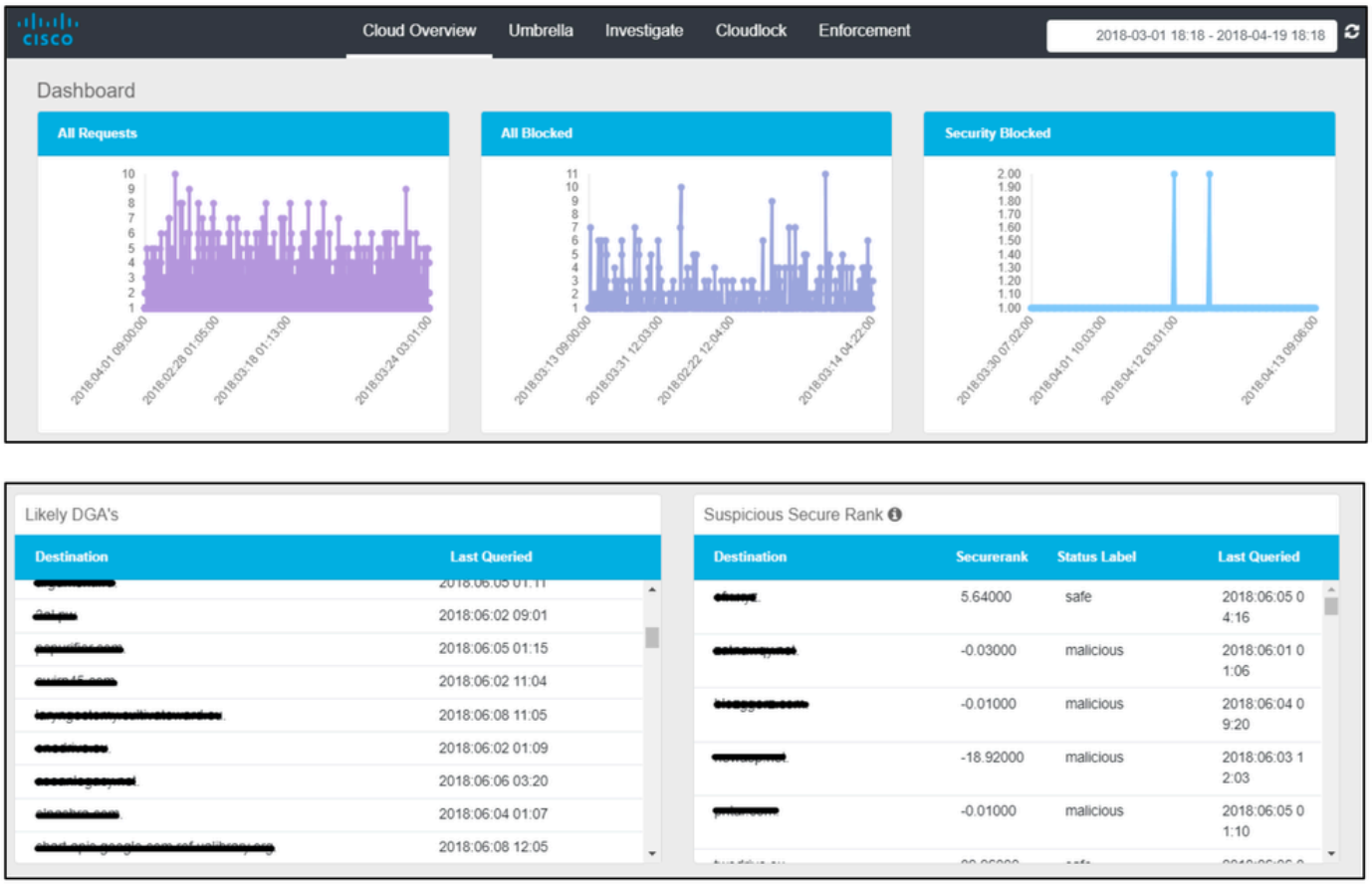


360072030052

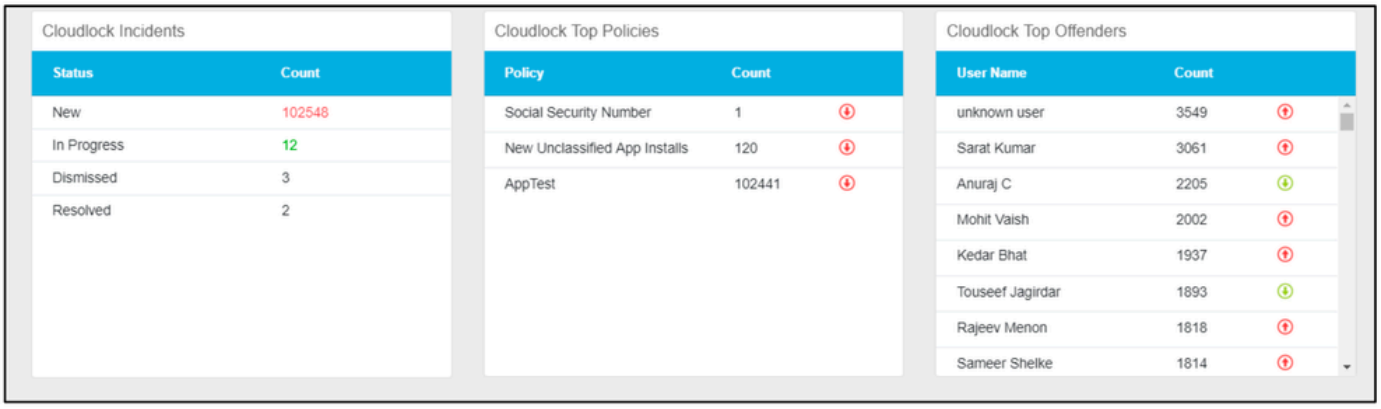
Composants de l'application Cisco Cloud Security

Présentation du cloud

L'onglet Cloud Overview affiche des informations telles que All Requests, All Blocked, Security Blocked, Likely DGA's, Suspicious Secure Rank, Cloudlock Incidents, CloudLock Overall, Top Policies et Top Offenders dans une représentation visuelle basée sur un tableau.



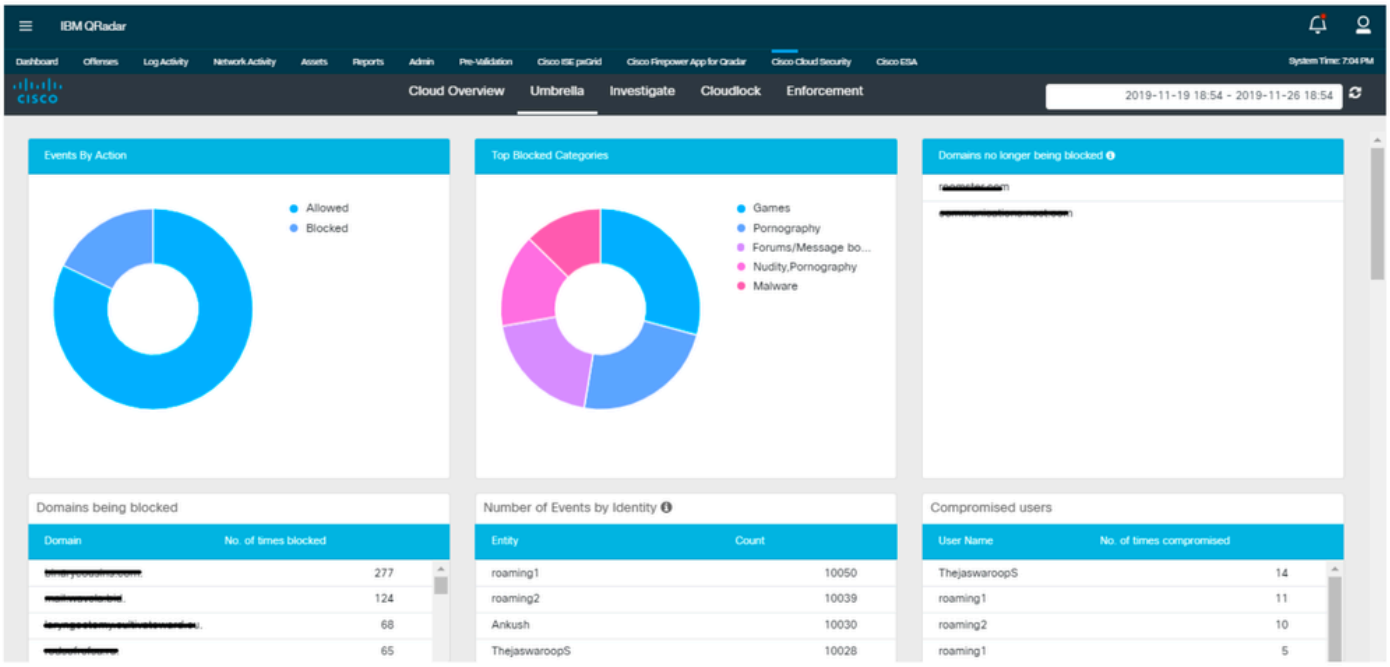
360072257631



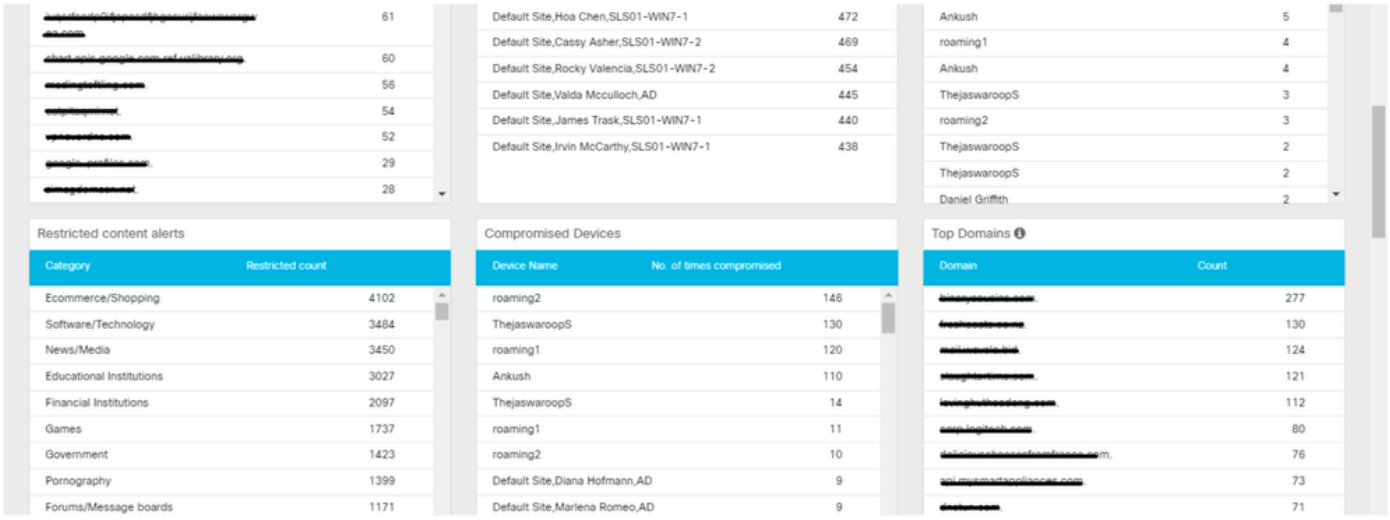
360072257611

Umbrella

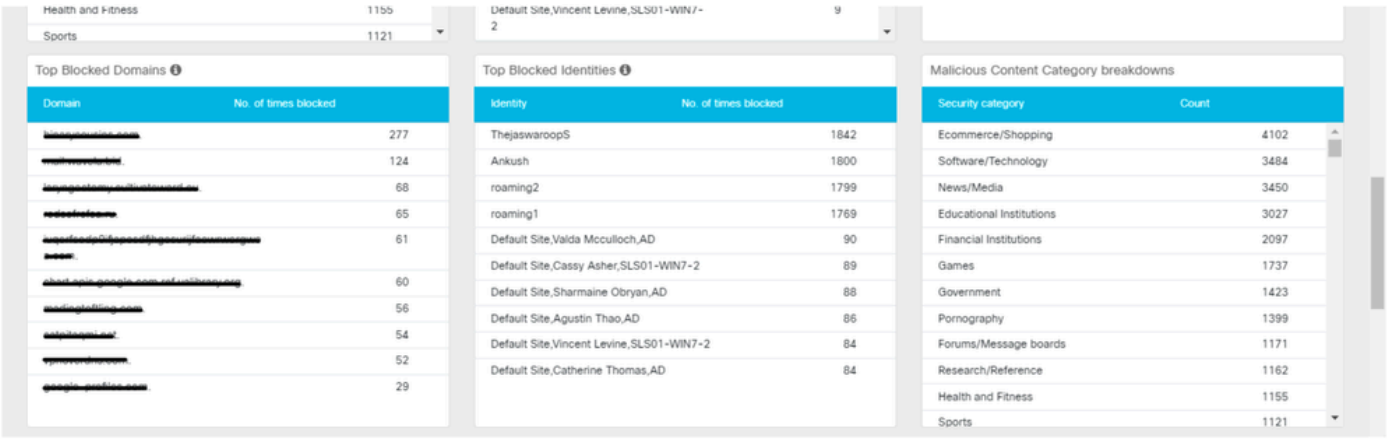
L'onglet Umbrella affiche des informations telles que Événements par action, Principales catégories bloquées, Nombre d'événements par identité, Domaines bloqués, Domaines qui ne sont plus bloqués, Utilisateurs compromis, Alertes de contenu limité, Périphériques compromis, Principaux domaines, Principaux domaines bloqués, Principales identités bloquées, Ventilations des catégories de contenu malveillant, Principales catégories, Tendance de l'activité et de l'accès utilisateur dans une représentation visuelle basée sur un graphique.



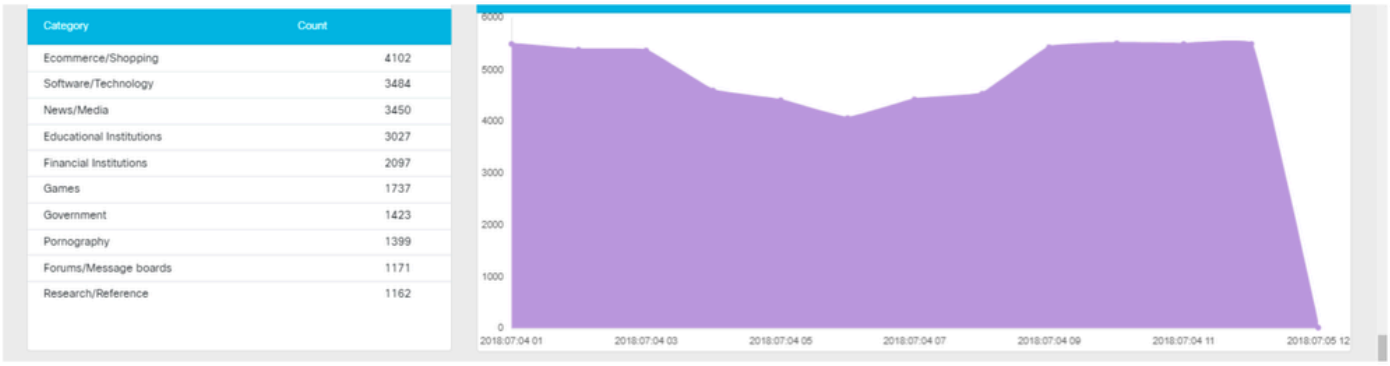
360072263411



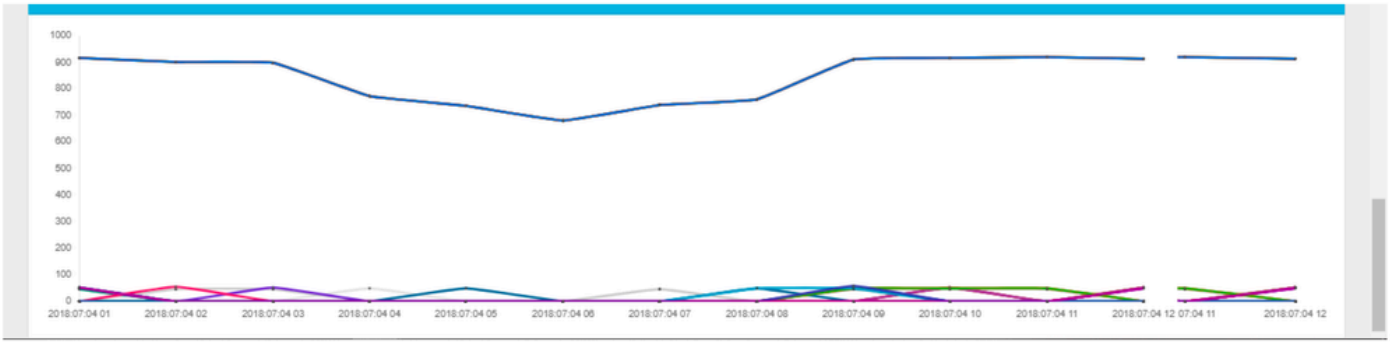
360072263391



360072037372



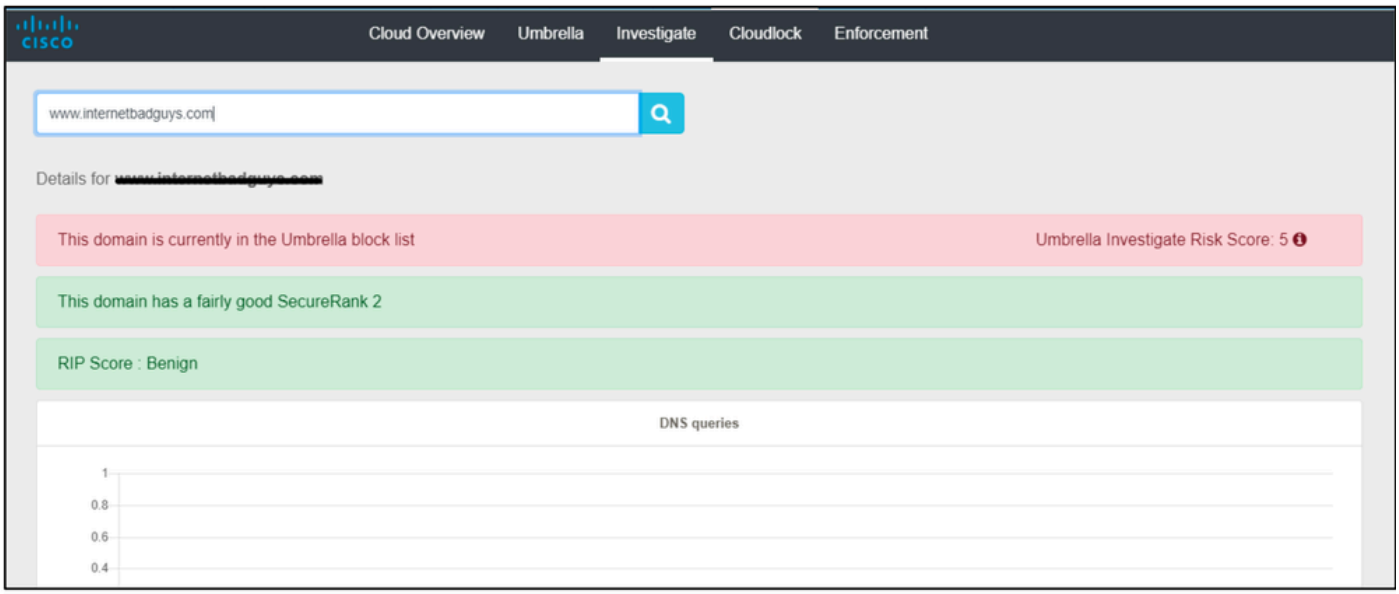
360072263331



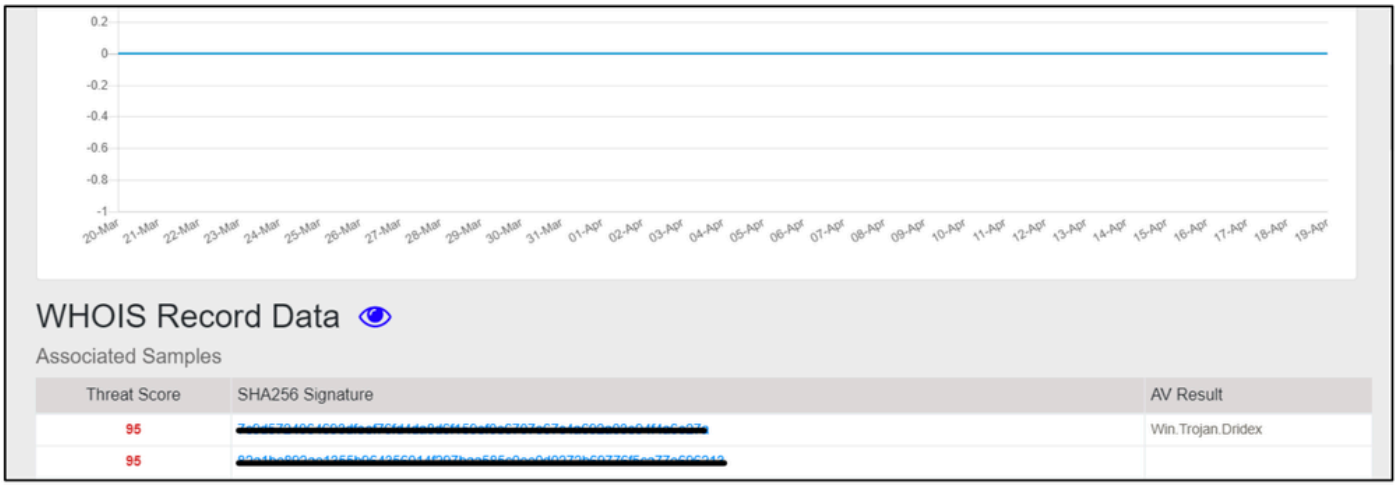
360072263351

Enquêter

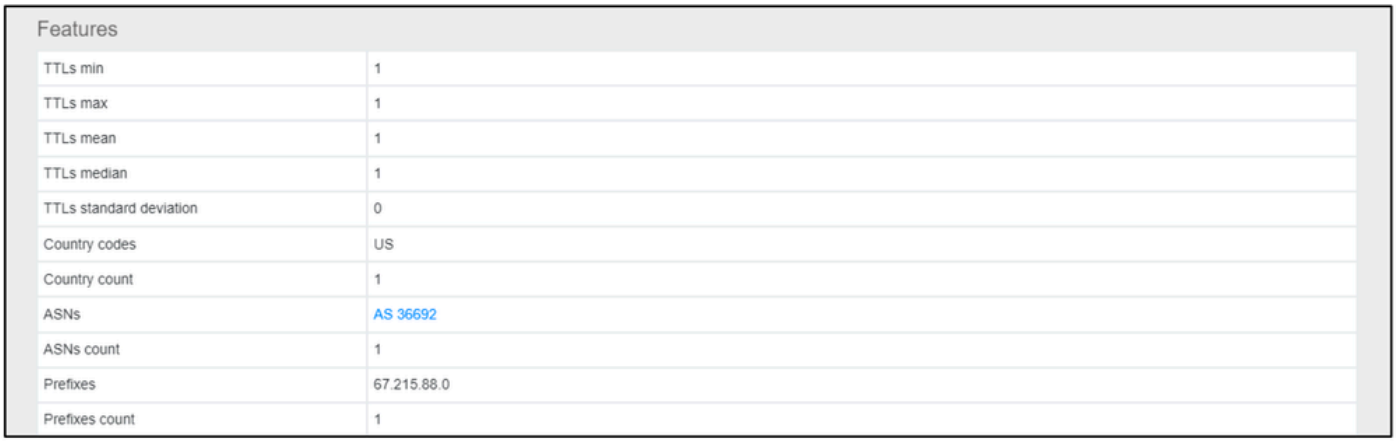
L'onglet Enquêter permet à l'utilisateur d'effectuer une recherche dans les informations relatives au nom d'hôte, à l'URL, au numéro de système autonome, à l'IP, au hachage ou à l'adresse électronique. Il contient également des informations telles que les enregistrements WHOIS, les informations DGA, etc.



360072263511



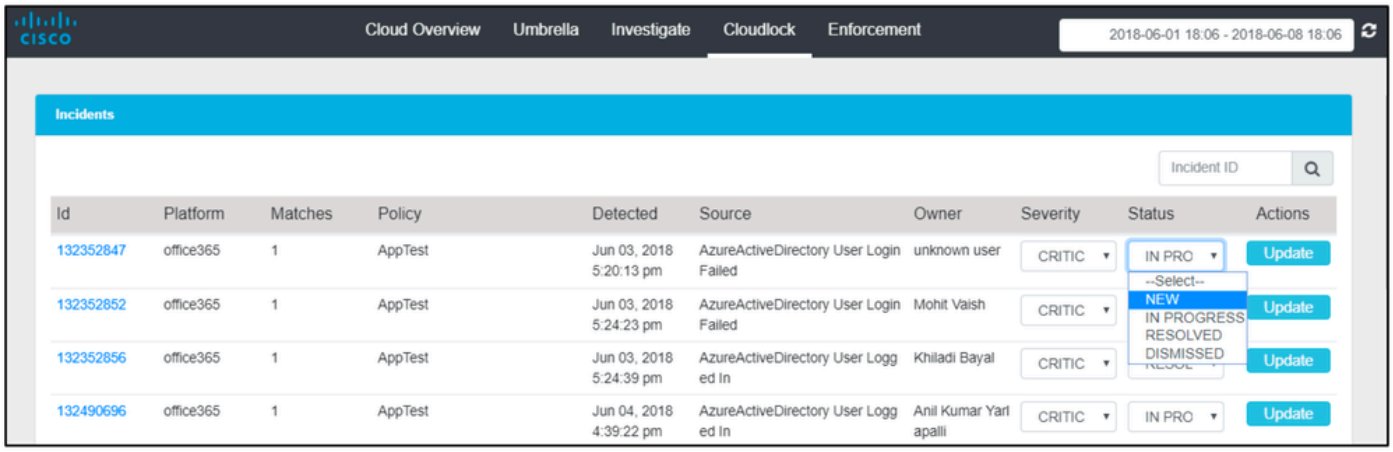
360072037472



360072037452

CloudLock

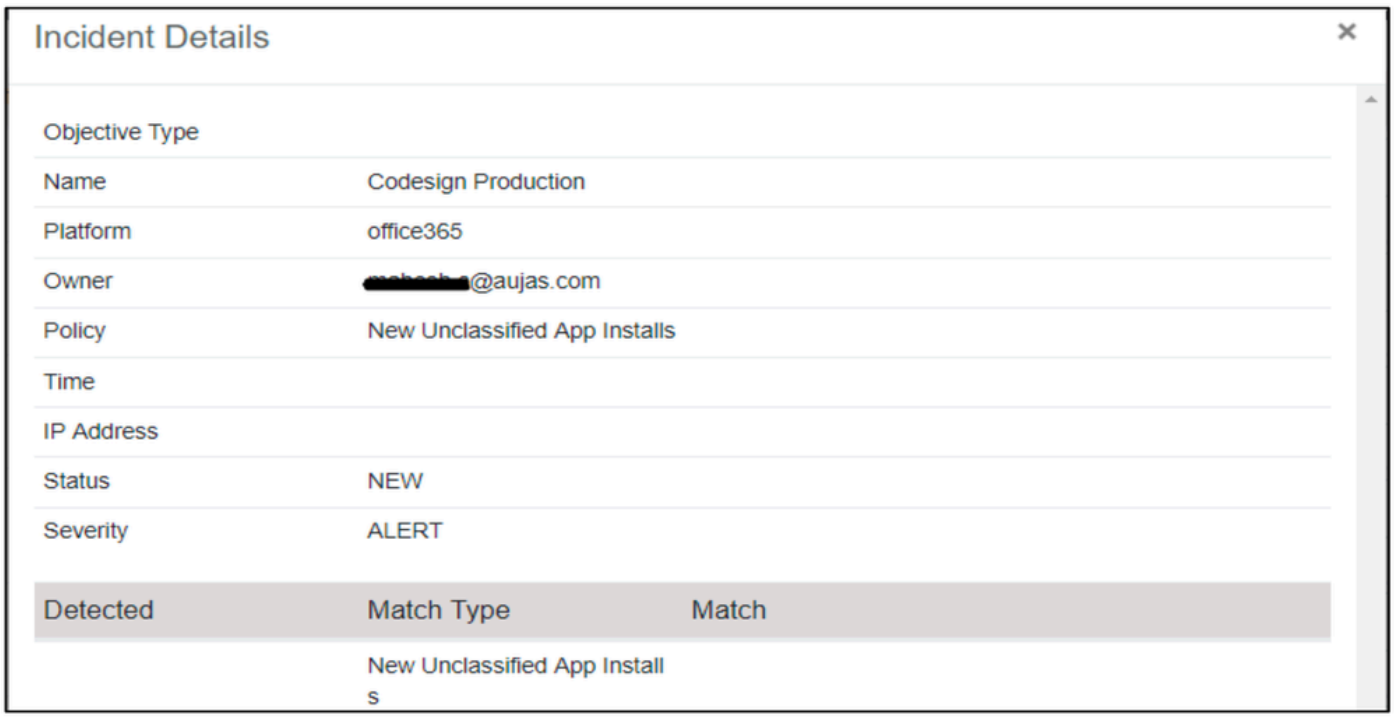
L'onglet CloudLock permet aux utilisateurs d'afficher des informations sur tous les incidents détectés. Les utilisateurs peuvent également mettre à jour la gravité et l'état de l'incident en sélectionnant les valeurs dans le menu déroulant et en cliquant sur « Mettre à jour ».



360072268311

Les utilisateurs peuvent surveiller n'importe quel événement pour afficher plus de détails sur

l'incident.



360072042332

Onglet Application

L'onglet Application affiche des informations sur les domaines bloqués. Les utilisateurs peuvent également sélectionner des domaines bloqués et les débloquer de cette interface.

360072038472

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.