# Gestione la aplicación Cloud Security App para IBM QRadar

## Contenido


Introducción

Overview

Acceso a la aplicación Cisco Cloud Security

Componentes de la aplicación Cisco Cloud Security

- Descripción general de nube
- Umbrella
- Investigar
- CloudLock
- Ficha Aplicación


## Introducción

Este documento describe cómo administrar la aplicación Cisco Cloud Security para IBM QRadar.

## Overview

QRadar de IBM es un popular SIEM para el análisis de registros. Proporciona una interfaz potente para analizar grandes fragmentos de datos, como los registros proporcionados por Cisco Umbrella para el tráfico DNS de su organización. La información que se muestra en la aplicación Cisco Cloud Security App para IBM QRadar proviene de las API de Cisco Umbrella, CloudLock, Investigate and Enforcement.

Al configurar la aplicación Cisco Cloud Security para QRadar, integra todos los datos de la plataforma Cisco Cloud Security y le permite ver los datos en forma gráfica en la consola de QRadar. Desde la aplicación, los analistas pueden:

- Investigue dominios, direcciones IP y direcciones de correo electrónico
- Bloquear y desbloquear dominios (aplicación)
- Ver la información de todos los incidentes de la red.

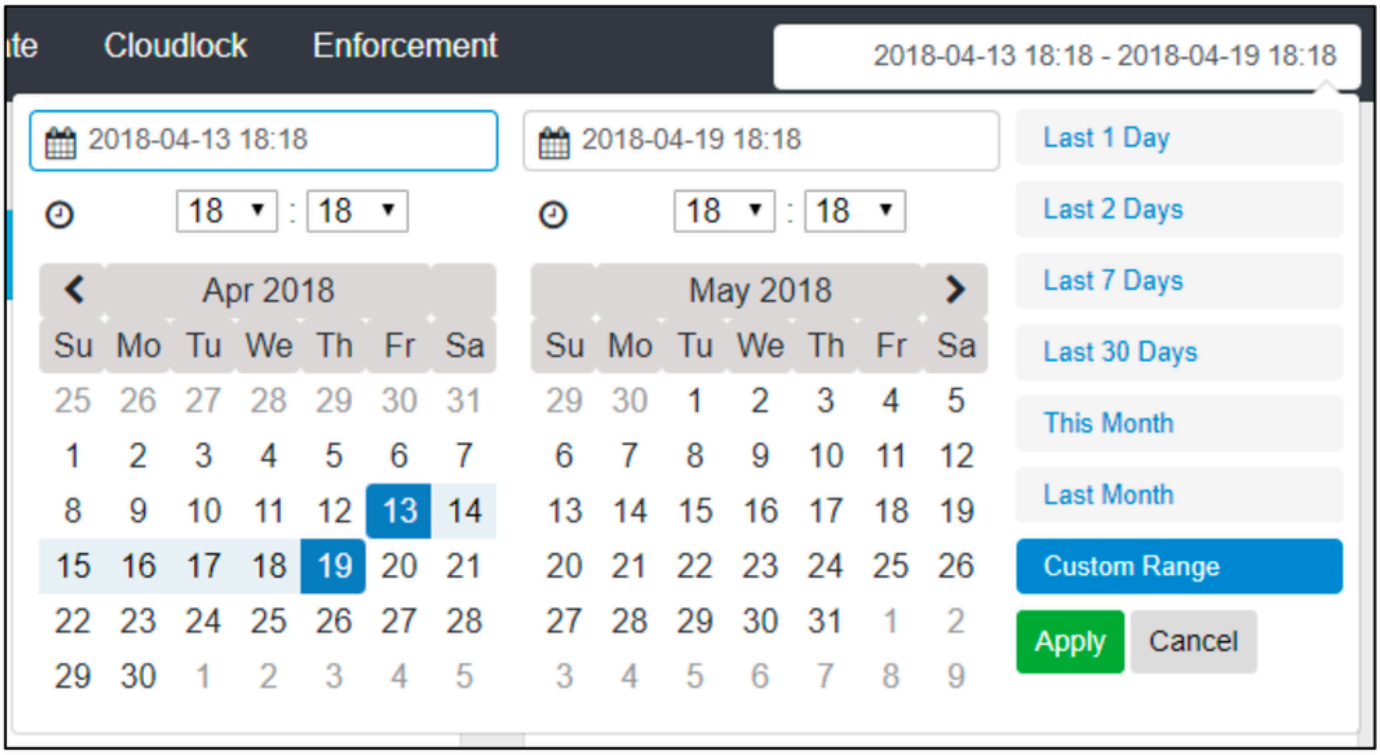
En este artículo se explica cómo navegar por la aplicación Cisco Cloud Security. Puede encontrar instrucciones sobre cómo configurar la aplicación aquí: Configuración de Cisco Cloud Security App para IBM QRadar

## Acceso a la aplicación Cisco Cloud Security

Para navegar hasta la aplicación Cisco Cloud Security en IBM QRadar, vaya a la página de inicio

y haga clic en la pestaña Cisco Cloud Security. Aparece la pestaña Descripción general de la nube y el panel. A continuación, puede acceder a las pestañas Umbrella, Investigate, CloudLock y Enforcement para ver sus registros.

La aplicación Cloud Security está configurada para mostrar los datos de los últimos 7 días de forma predeterminada. Puede cambiar el intervalo de tiempo haciendo clic en el intervalo de fechas de la parte superior derecha:

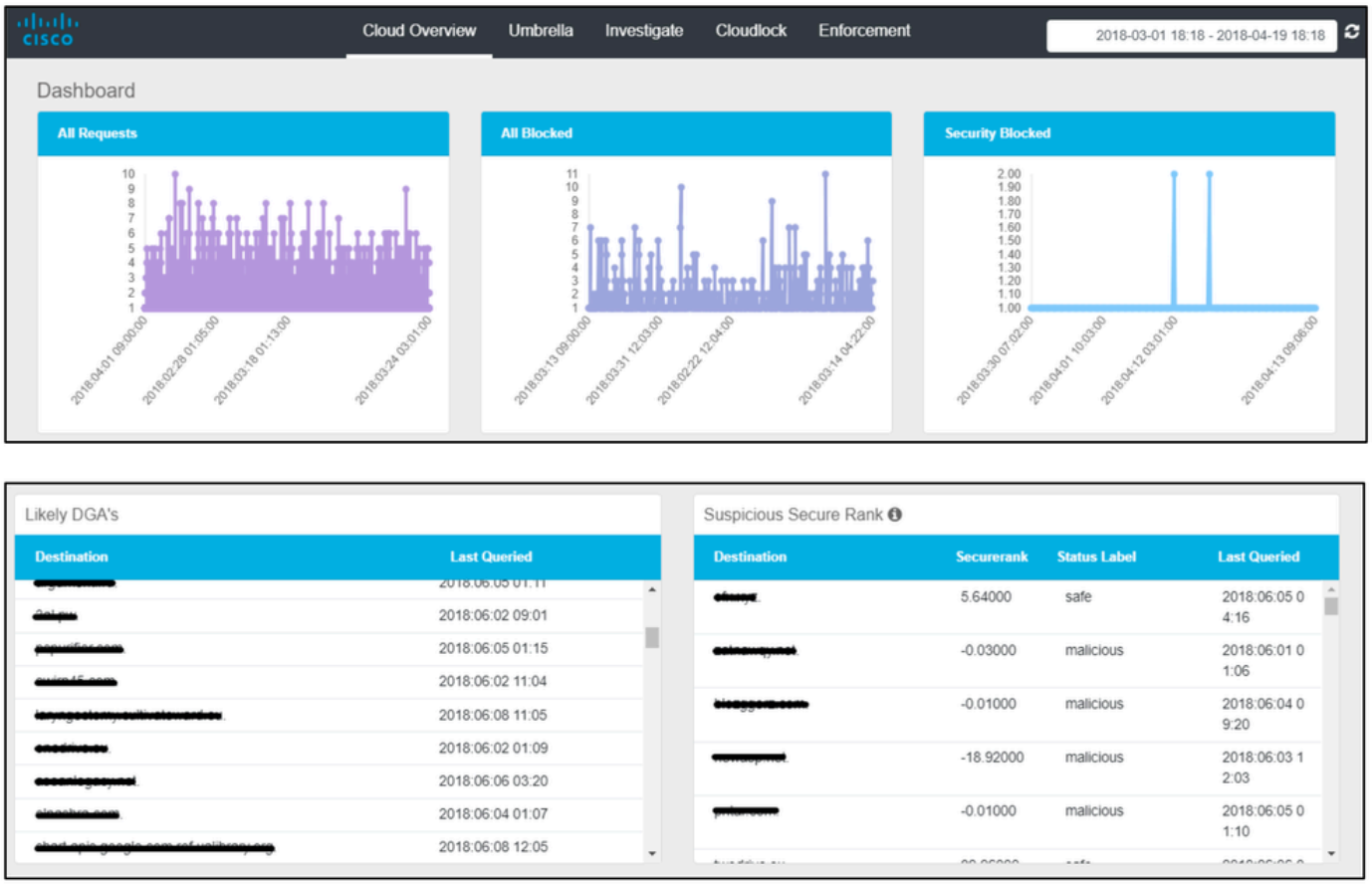



360072030052

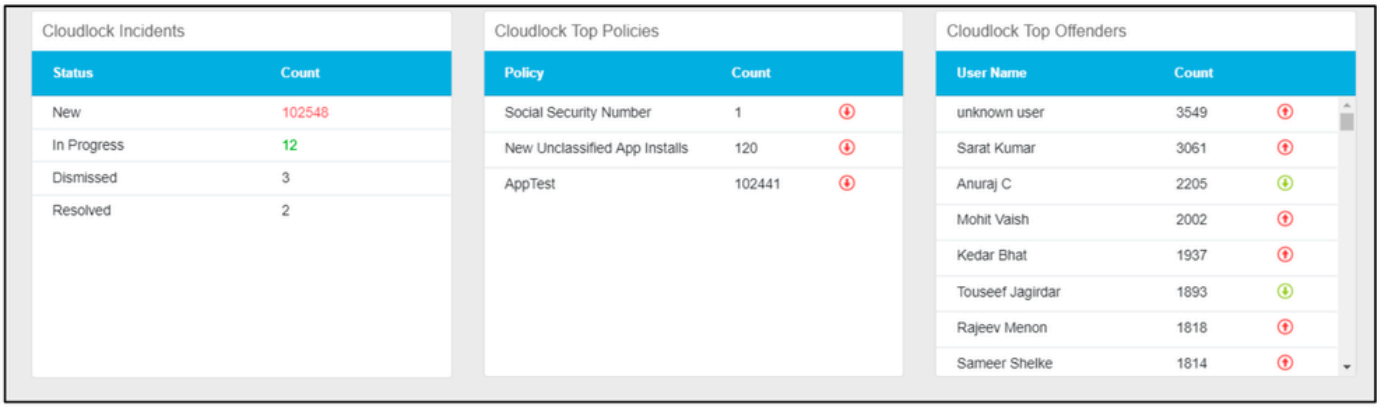
# Componentes de la aplicación Cisco Cloud Security

## Descripción general de nube

La pestaña Descripción general de la nube muestra información como Todas las solicitudes, Todas las bloqueadas, Seguridad bloqueada, DGA probables, Clasificación segura sospechosa, Incidentes de bloqueo de nube, CloudLock en general, Principales políticas y Principales infractores en una representación visual basada en gráficos.



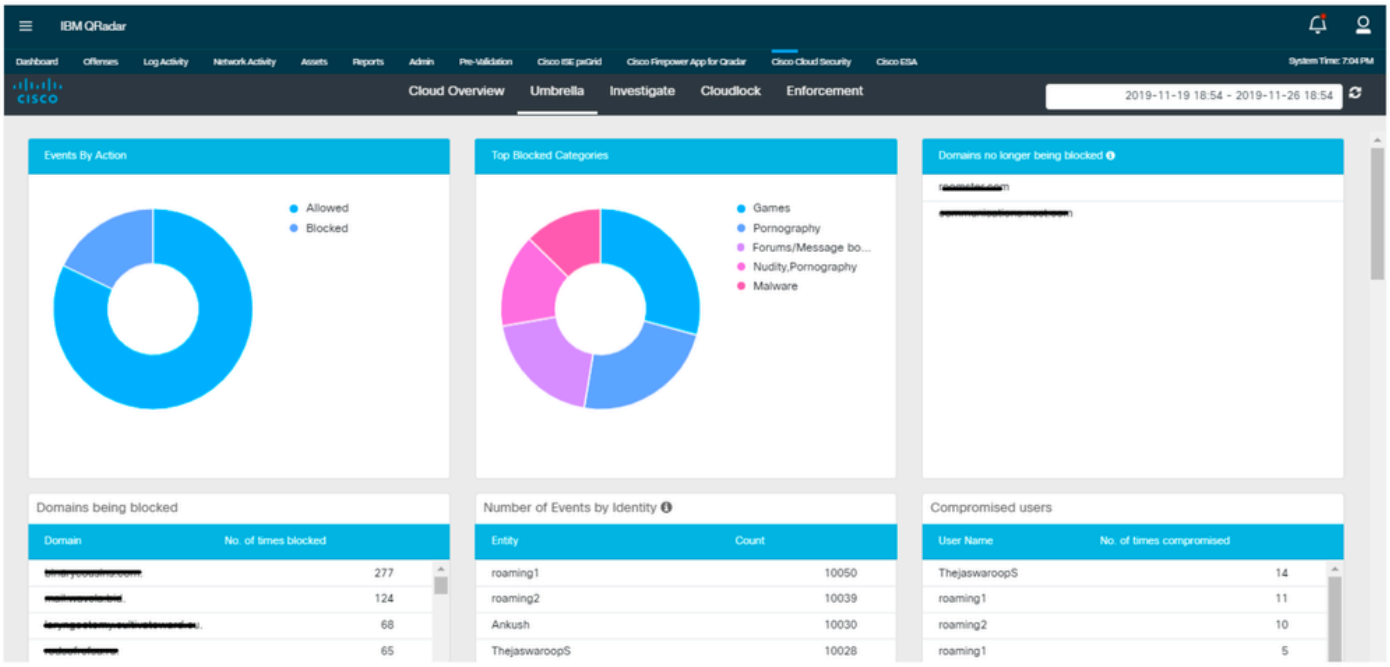

360072257631



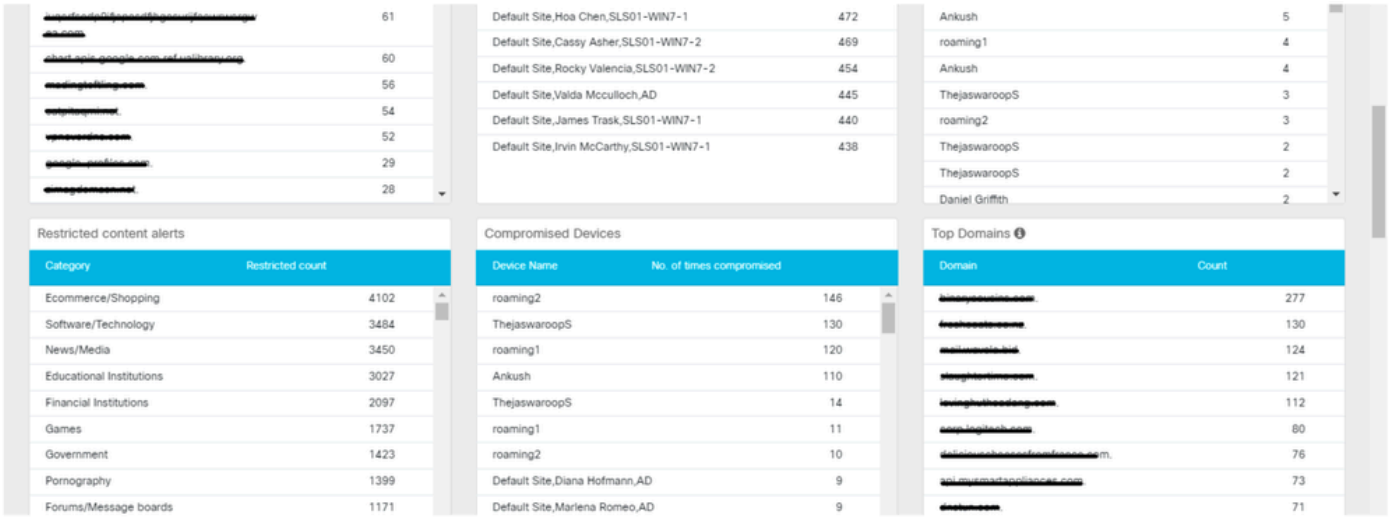

360072257611

## Umbrella

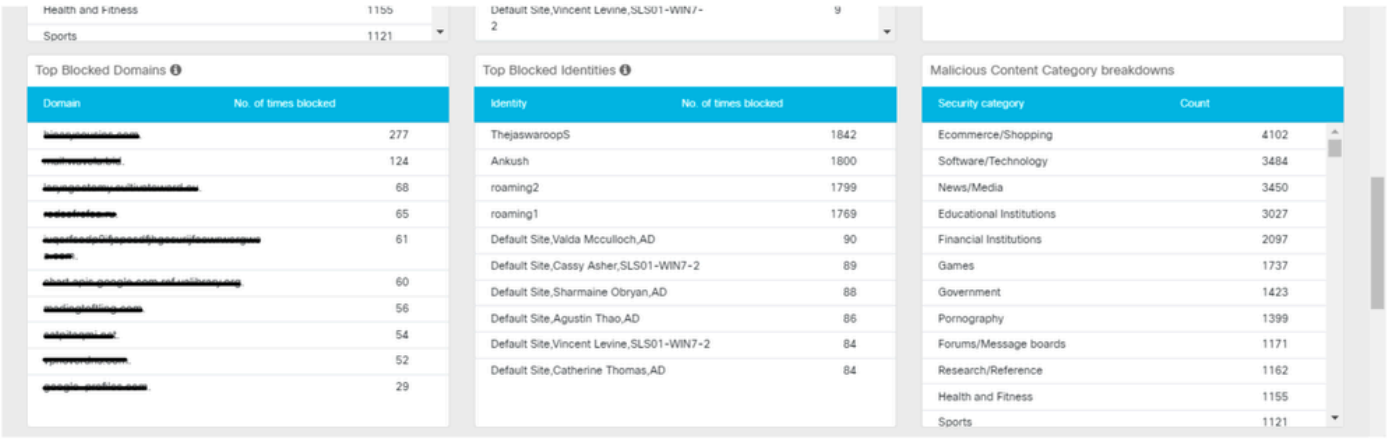
La pestaña Paraguas muestra información como eventos por acción, categorías principales bloqueadas, número de eventos por identidad, dominios que se están bloqueando, dominios que ya no se están bloqueando, usuarios en riesgo, alertas de contenido restringido, dispositivos en riesgo, dominios principales, dominios principales bloqueados, identidades principales bloqueadas, desgloses de categorías de contenido malintencionado, categorías principales, actividad y tendencia de acceso de usuario en una representación visual basada en gráficos.



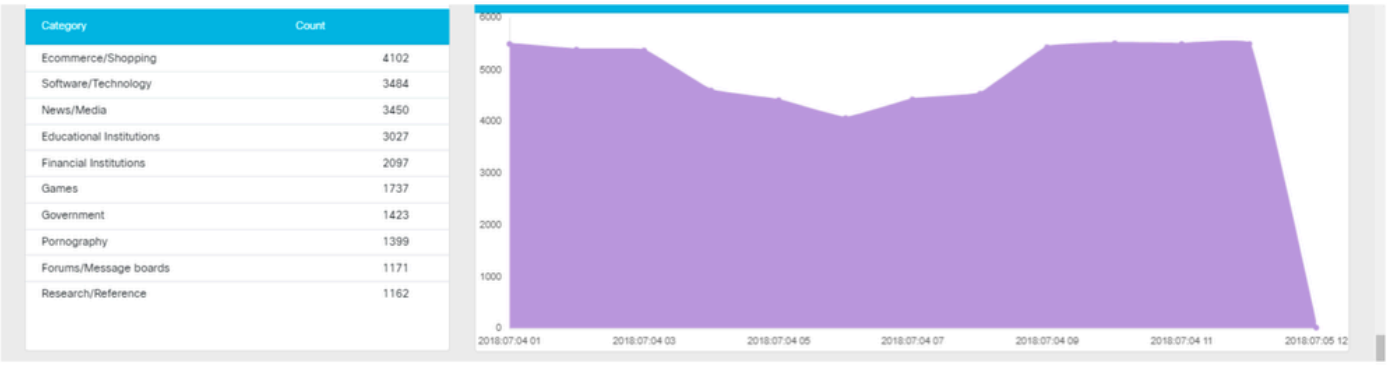

360072263411



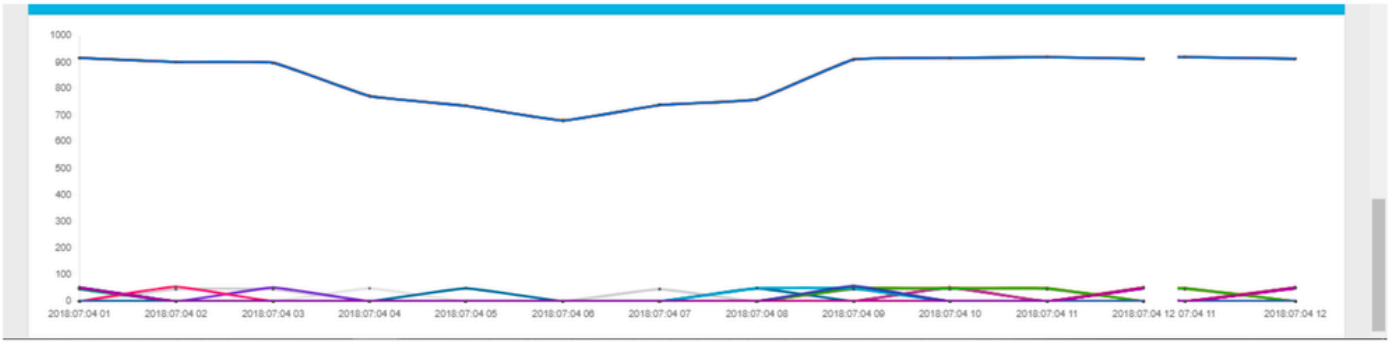

360072263391




360072037372



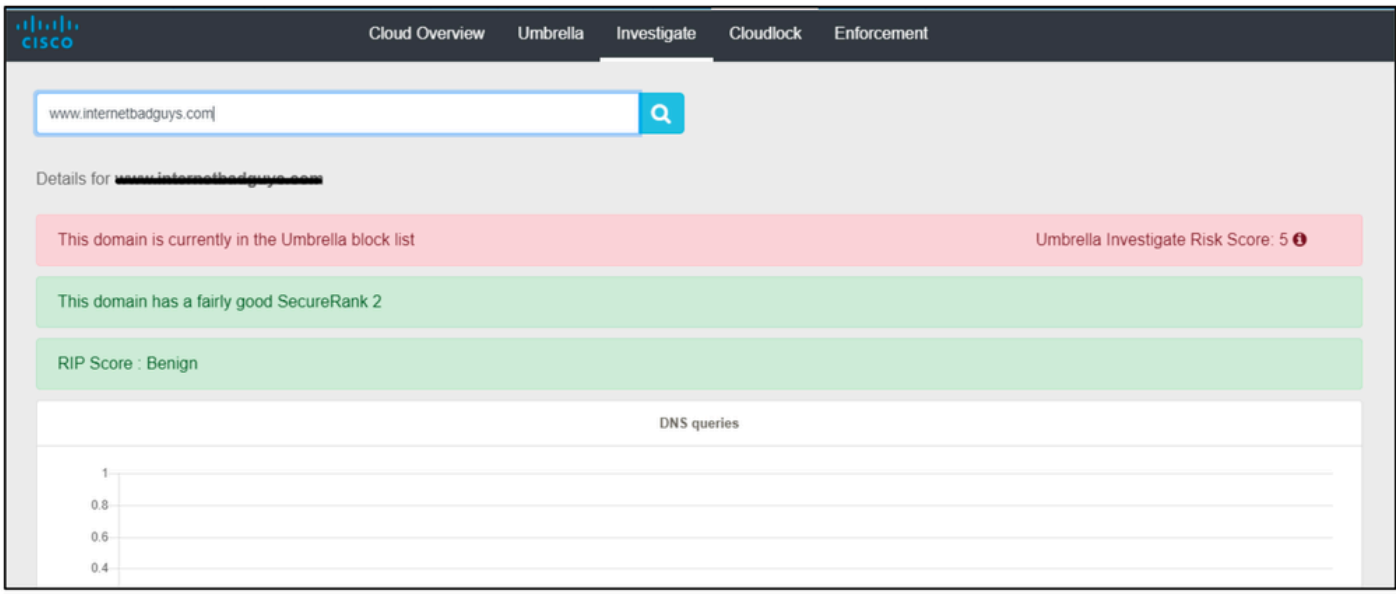

360072263331



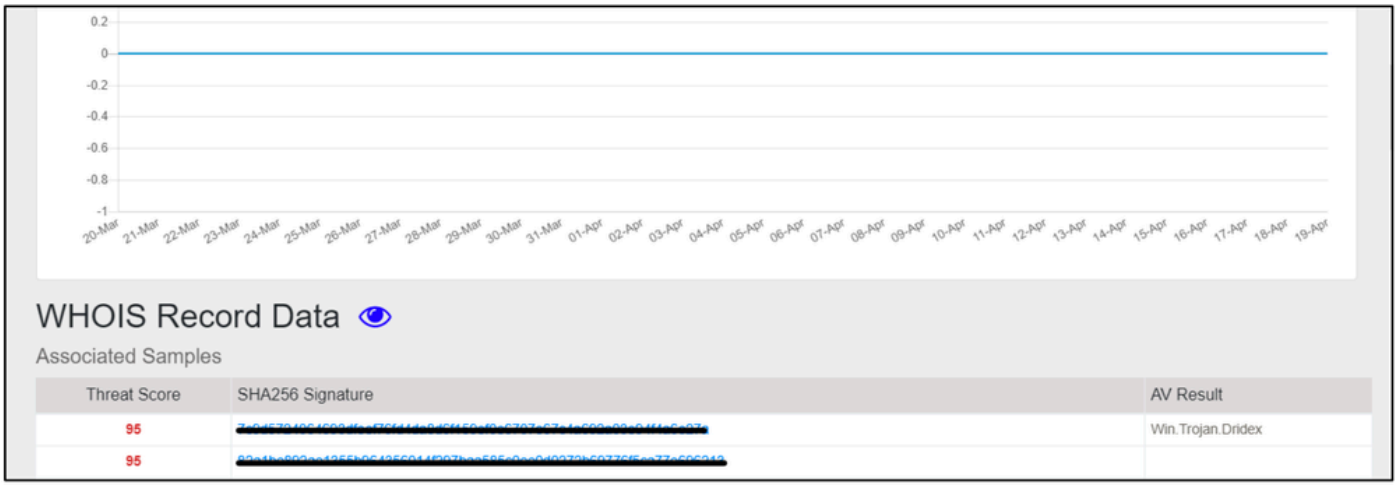
360072263351

## Investigar

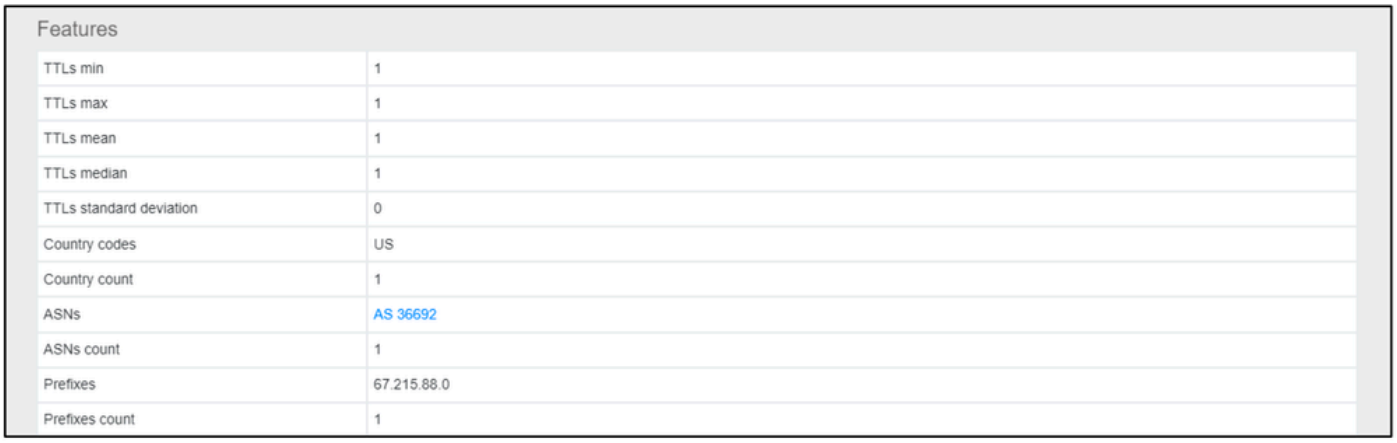
La ficha Investigar permite al usuario buscar la información relacionada con el nombre de host, URL, ASN, IP, Hash o dirección de correo electrónico. También tiene información como el registro WHOIS, información DGA, etc.




360072263511



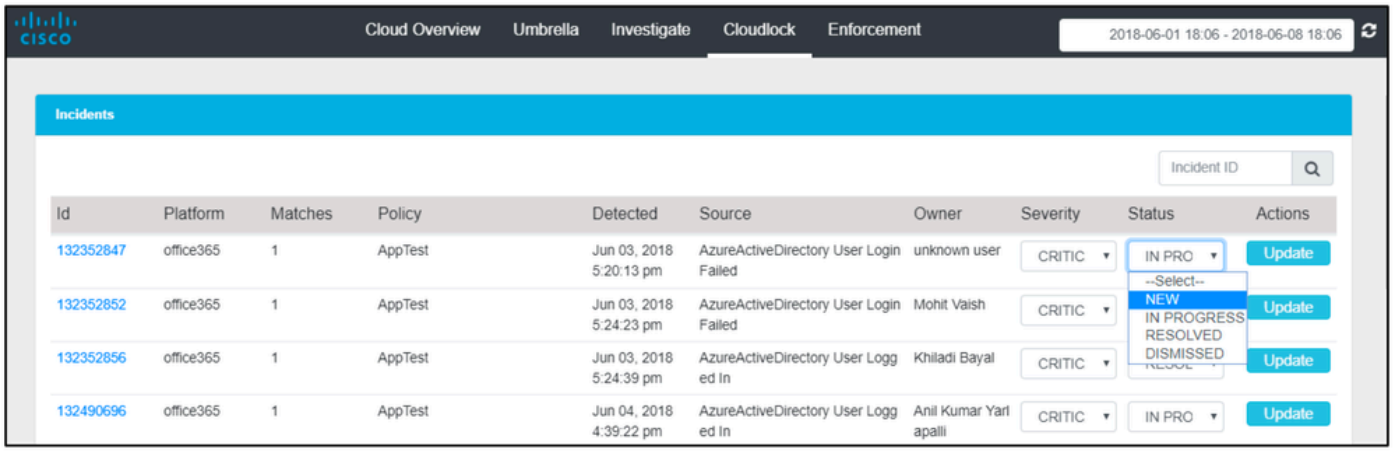

360072037472




360072037452

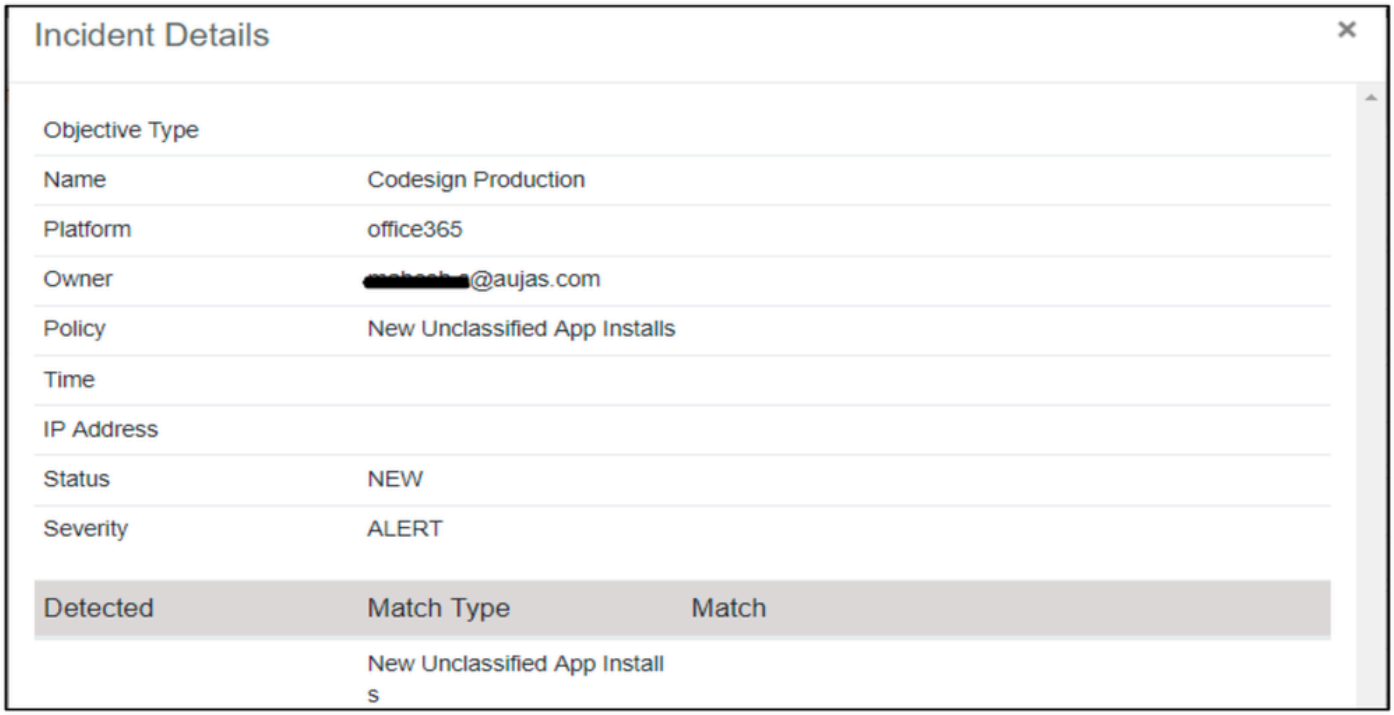
## CloudLock

La pestaña CloudLock permite a los usuarios ver información sobre todos los incidentes detectados. Los usuarios también pueden actualizar la gravedad y el estado del incidente seleccionando los valores en el menú desplegable y haciendo clic en "Actualizar".




360072268311

Los usuarios pueden registrar cualquiera de los eventos para ver más detalles sobre el incidente.




360072042332

## Ficha Aplicación

La ficha Aplicación muestra información sobre los dominios que están bloqueados. Los usuarios también pueden seleccionar dominios bloqueados y desbloquearlos de esta interfaz.


360072038472

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).