Gerencie o aplicativo Cloud Security para IBM QRadar

Contents

Introdução

Este documento descreve como gerenciar o aplicativo Cisco Cloud Security para IBM QRadar.

Overview

O QRadar da IBM é um SIEM popular para análise de registros. Ele fornece uma interface eficiente para analisar grandes blocos de dados, como os logs fornecidos pelo Cisco Umbrella para o tráfego DNS da sua organização. As informações exibidas no Cisco Cloud Security App para IBM QRadar são fornecidas através das APIs do Cisco Umbrella, CloudLock, Investigate e Enforcement.

Quando você configura o aplicativo Cisco Cloud Security para QRadar, ele integra todos os dados da plataforma Cisco Cloud Security e permite que você visualize os dados em forma gráfica no console QRadar. No aplicativo, os analistas podem:

- Investigar domínios, endereços IP, endereços de e-mail
- Bloquear e desbloquear domínios (imposição)
- Exibir as informações de todos os incidentes da rede.

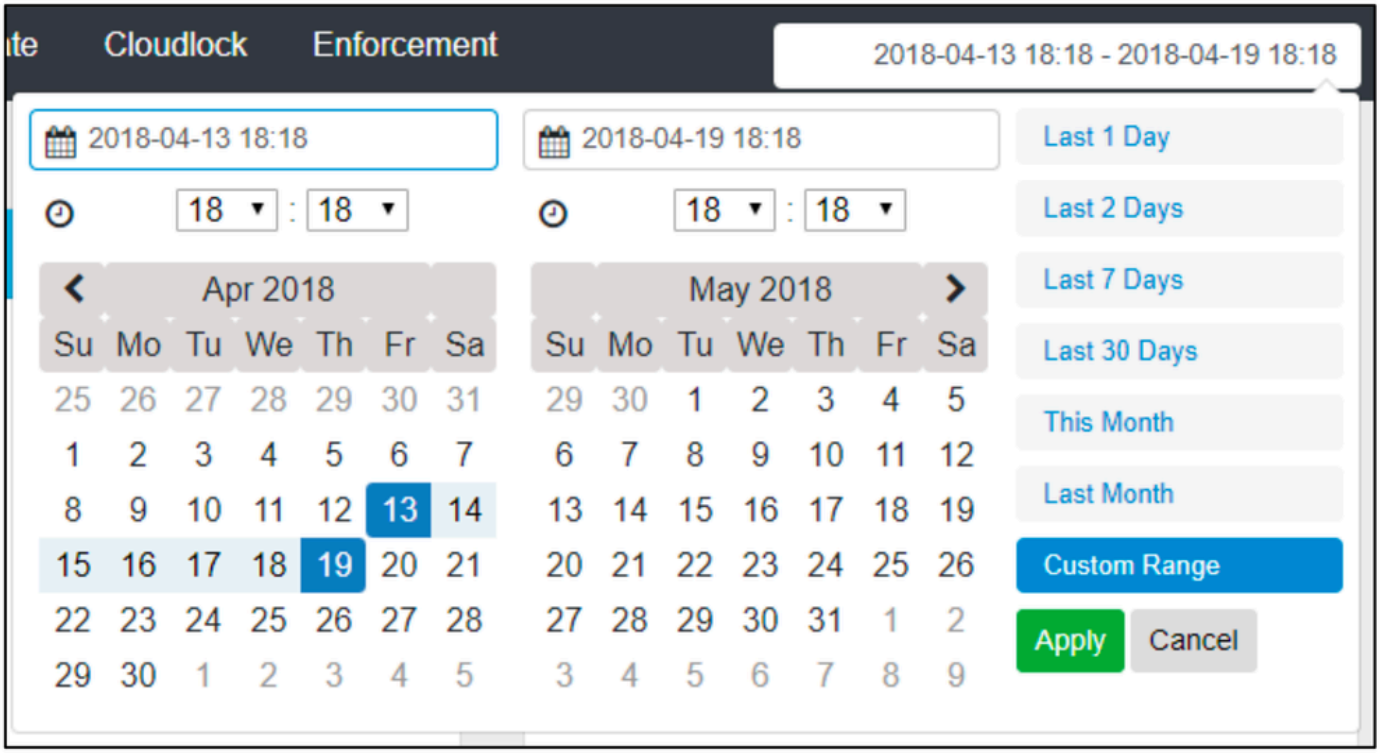
Este artigo mostra como navegar no aplicativo Cisco Cloud Security. As instruções sobre como configurar o aplicativo podem ser encontradas aqui: Configurando o aplicativo Cisco Cloud Security para IBM QRadar

Como acessar o aplicativo Cisco Cloud Security

Para navegar para o aplicativo Cisco Cloud Security no IBM QRadar, vá para a página inicial e

clique na guia Cisco Cloud Security. A guia Visão geral da nuvem e o Painel são exibidos. Você pode acessar as guias Umbrella, Investigate, CloudLock e Enforcement para exibir seus logs.

O aplicativo Cloud Security está configurado para mostrar os dados dos últimos 7 dias por padrão. Você pode alterar o período clicando no intervalo de datas no canto superior direito:

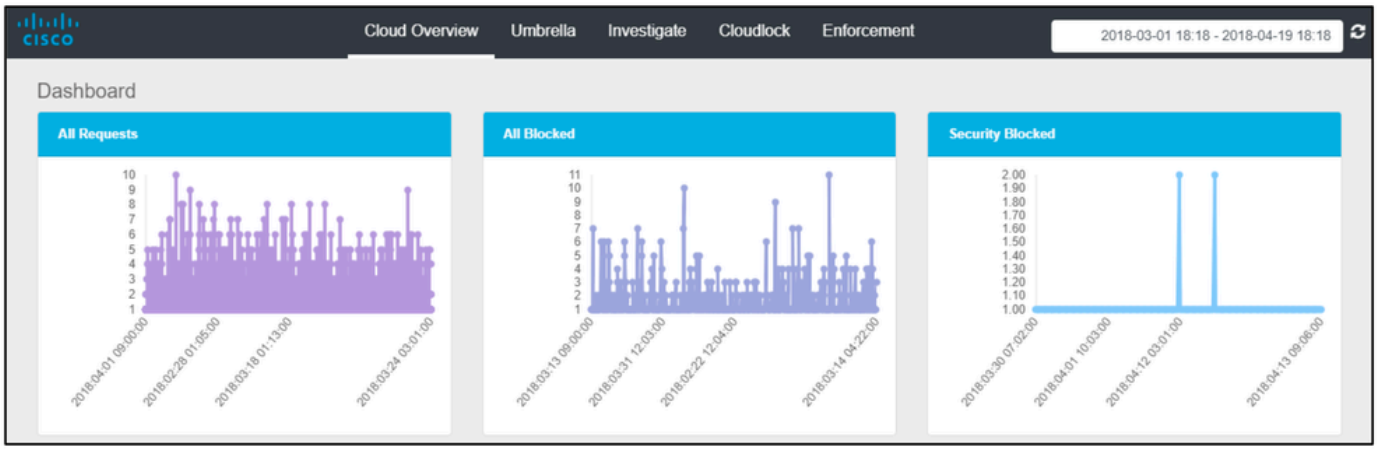


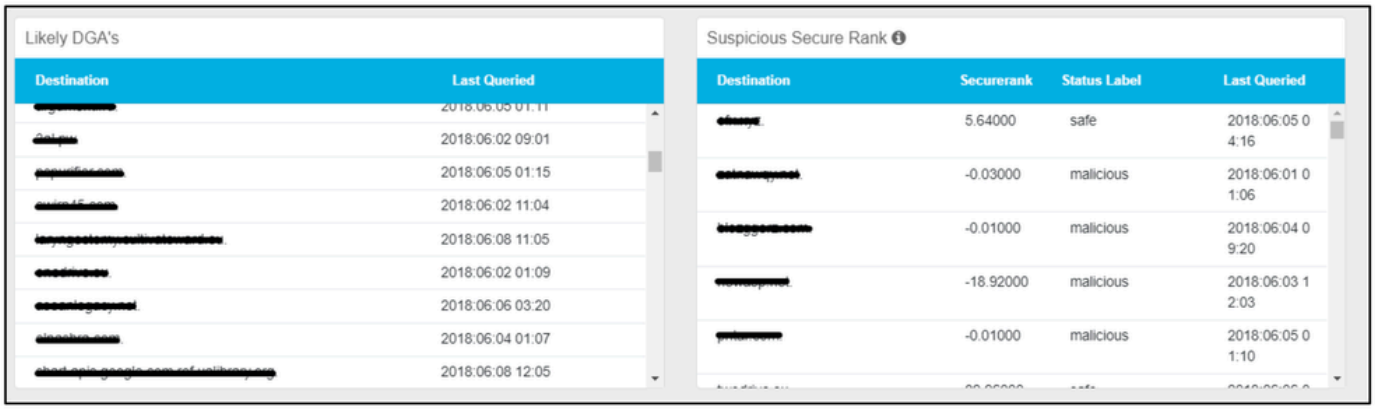
360072030052

Componentes do aplicativo Cisco Cloud Security

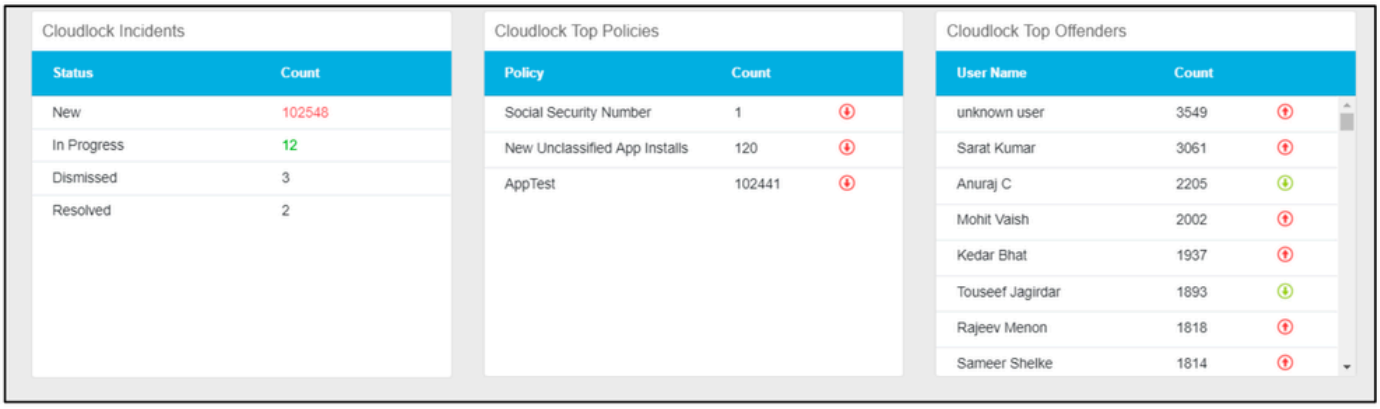
Visão geral da nuvem

A guia Visão geral da nuvem exibe informações como Todas as solicitações, Todas bloqueadas, Segurança bloqueada, DGAs prováveis, Classificação segura suspeita, Incidentes de Cloudlock, CloudLock Geral, Principais políticas e Principais infratores em uma representação visual baseada em gráfico.





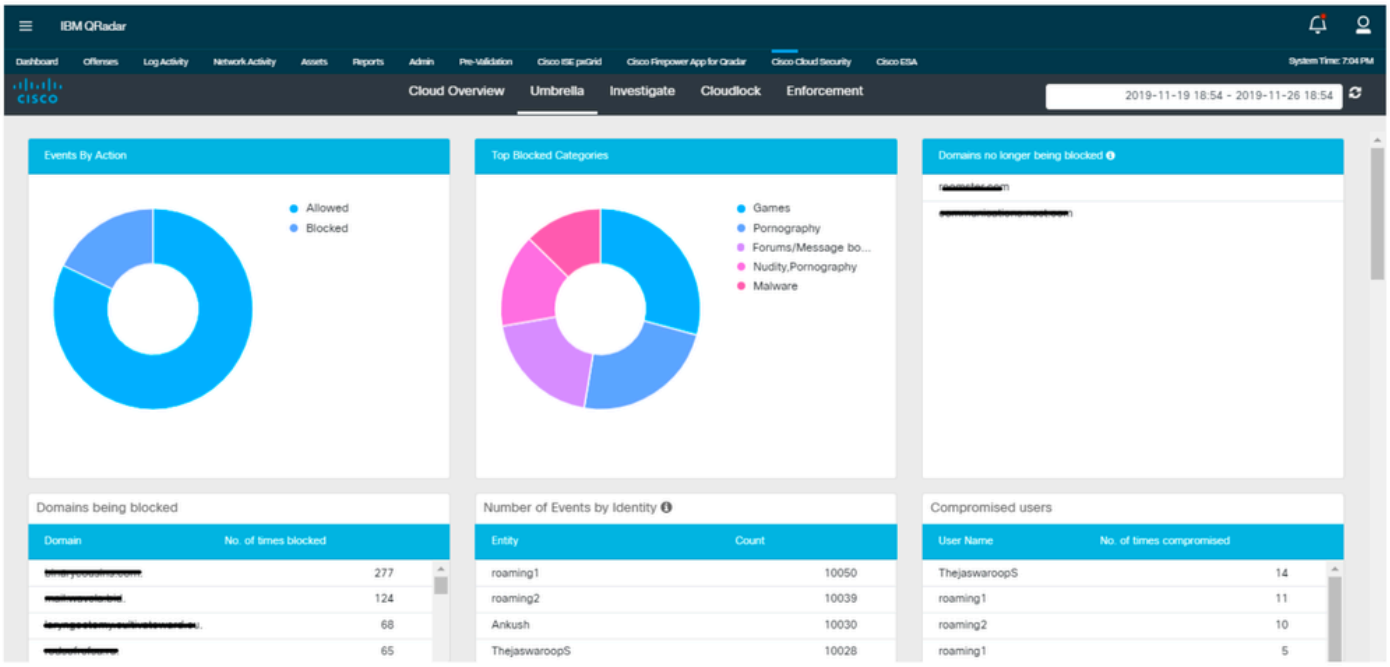
360072257631



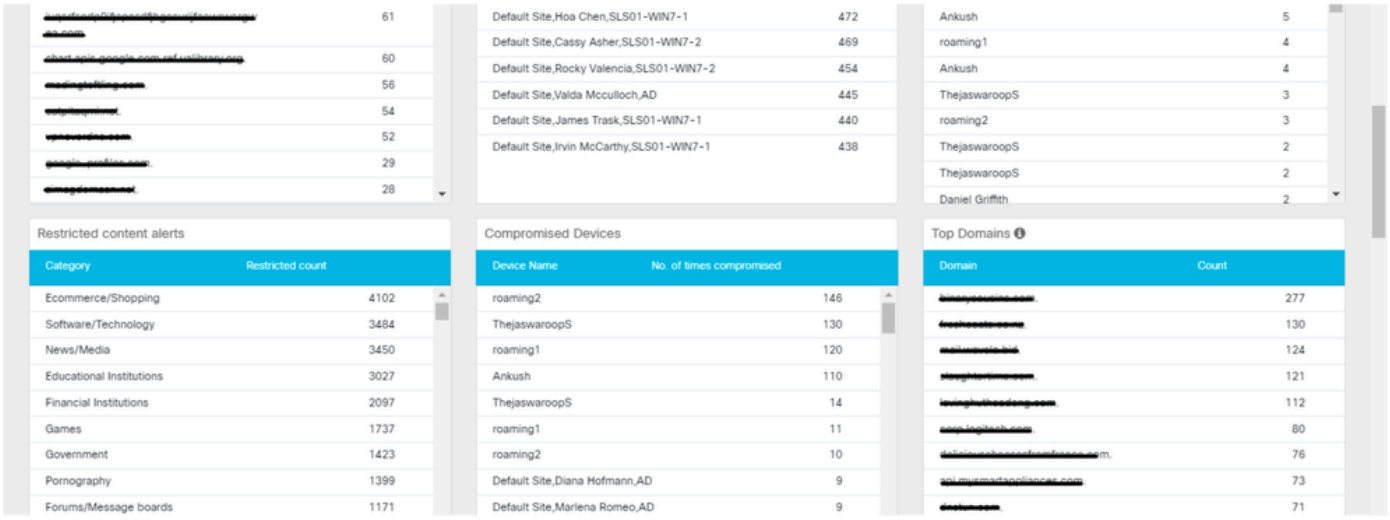
360072257611

Umbrella

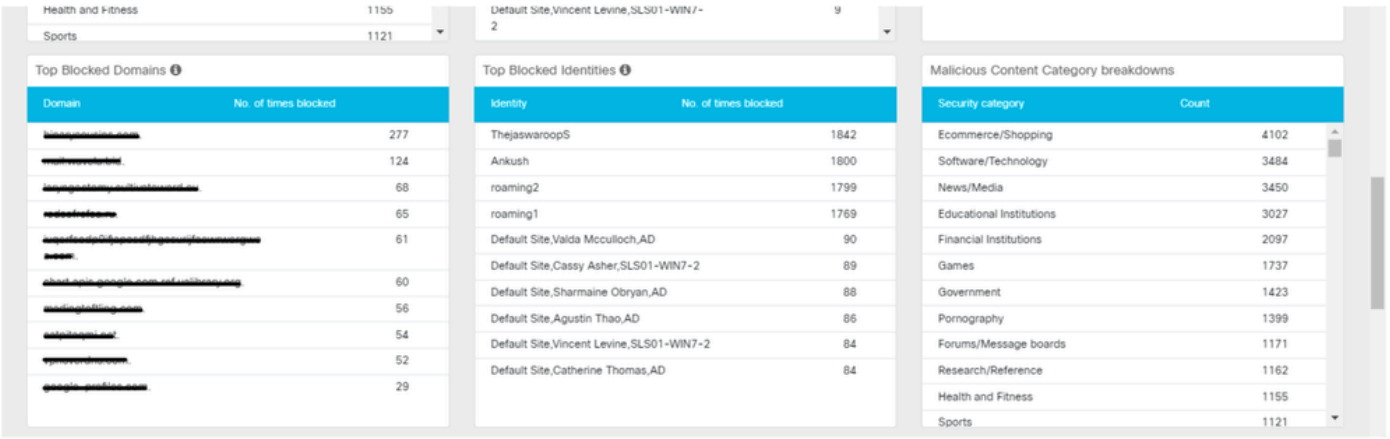
A guia Guarda-chuva exibe informações como Eventos por ação, Principais categorias bloqueadas, Número de eventos por identidade, Domínios que estão sendo bloqueados, Domínios que não estão mais sendo bloqueados, Usuários comprometidos, Alertas de conteúdo restrito, Dispositivos comprometidos, Principais domínios, Principais domínios bloqueados, Principais identidades bloqueadas, Desagregações de categorias de conteúdo mal-intencionado, Principais categorias, Tendência de atividade e acesso do usuário em uma representação visual baseada em gráfico.



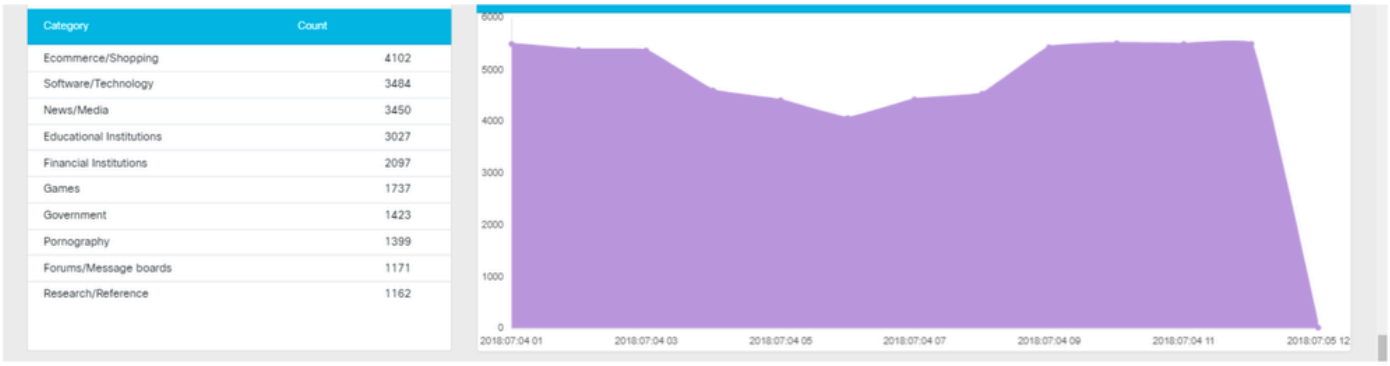
360072263411



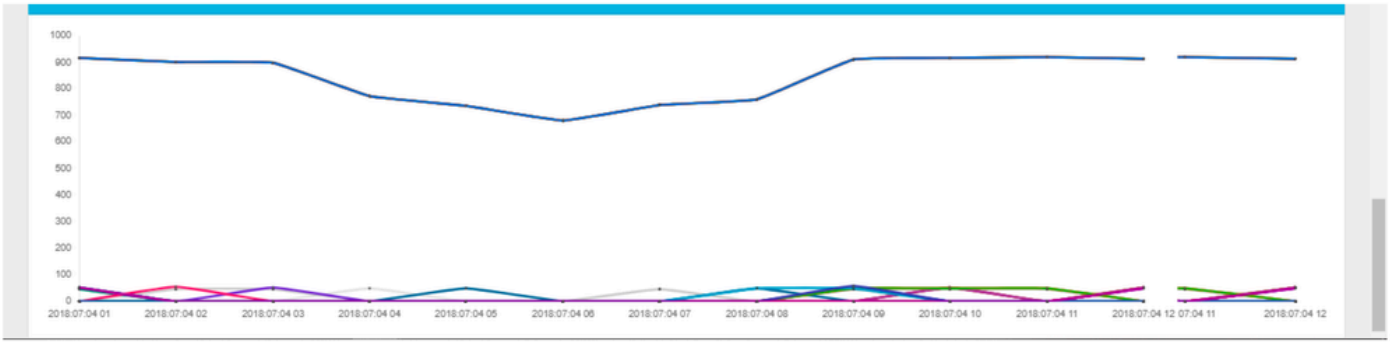
360072263391



360072037372



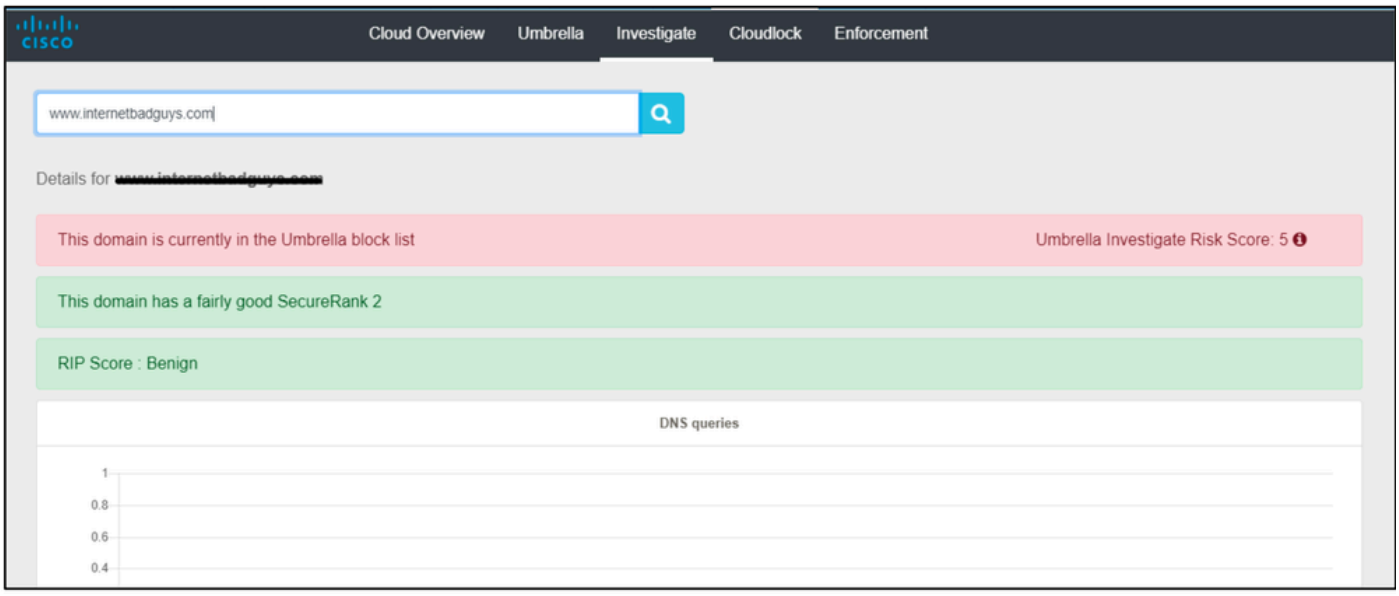
360072263331



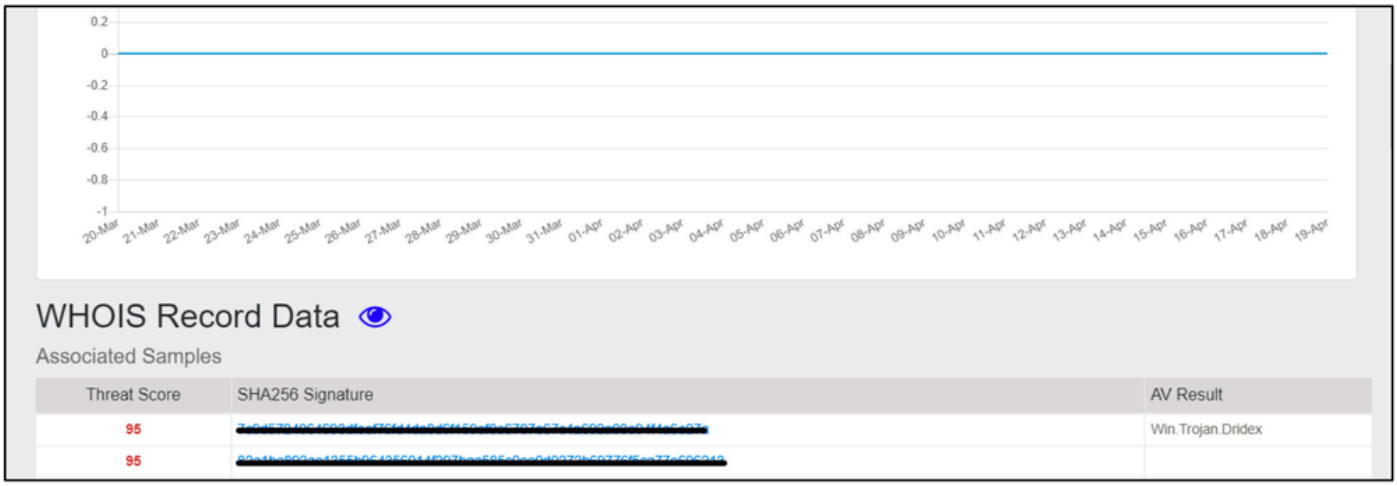
360072263351

Investigar

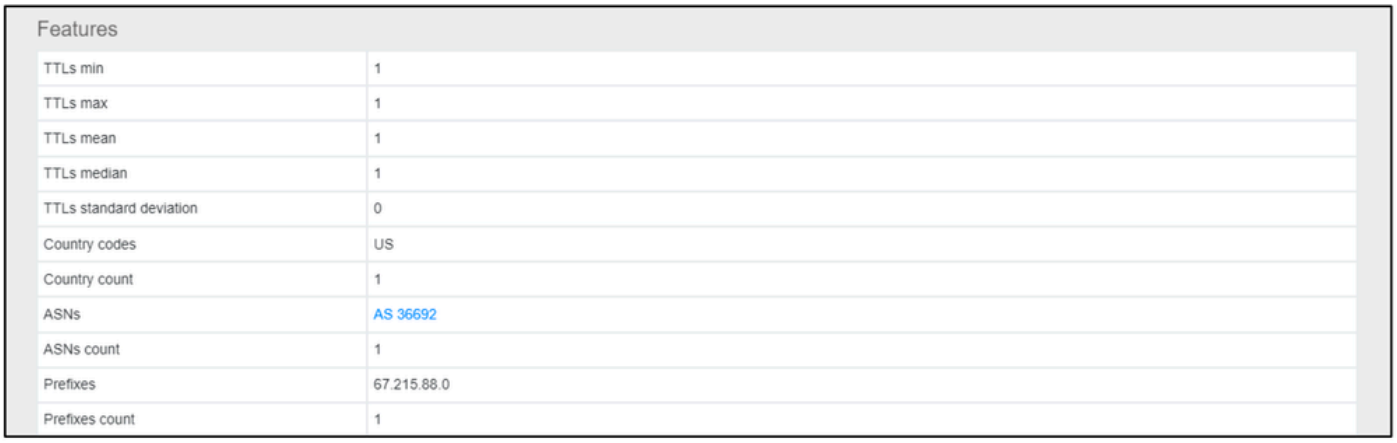
A guia Investigar permite que o usuário pesquise as informações relacionadas ao nome do host, URL, ASN, IP, Hash ou endereço de e-mail. Ele também tem informações como registro WHOIS, informações DGA e assim por diante.



360072263511



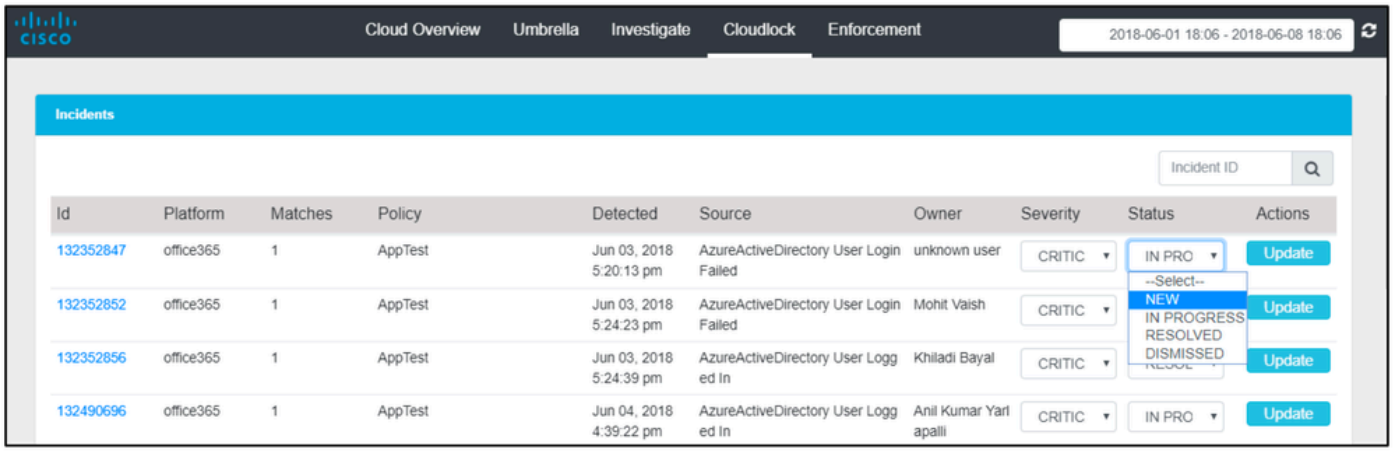
360072037472



360072037452

CloudLock

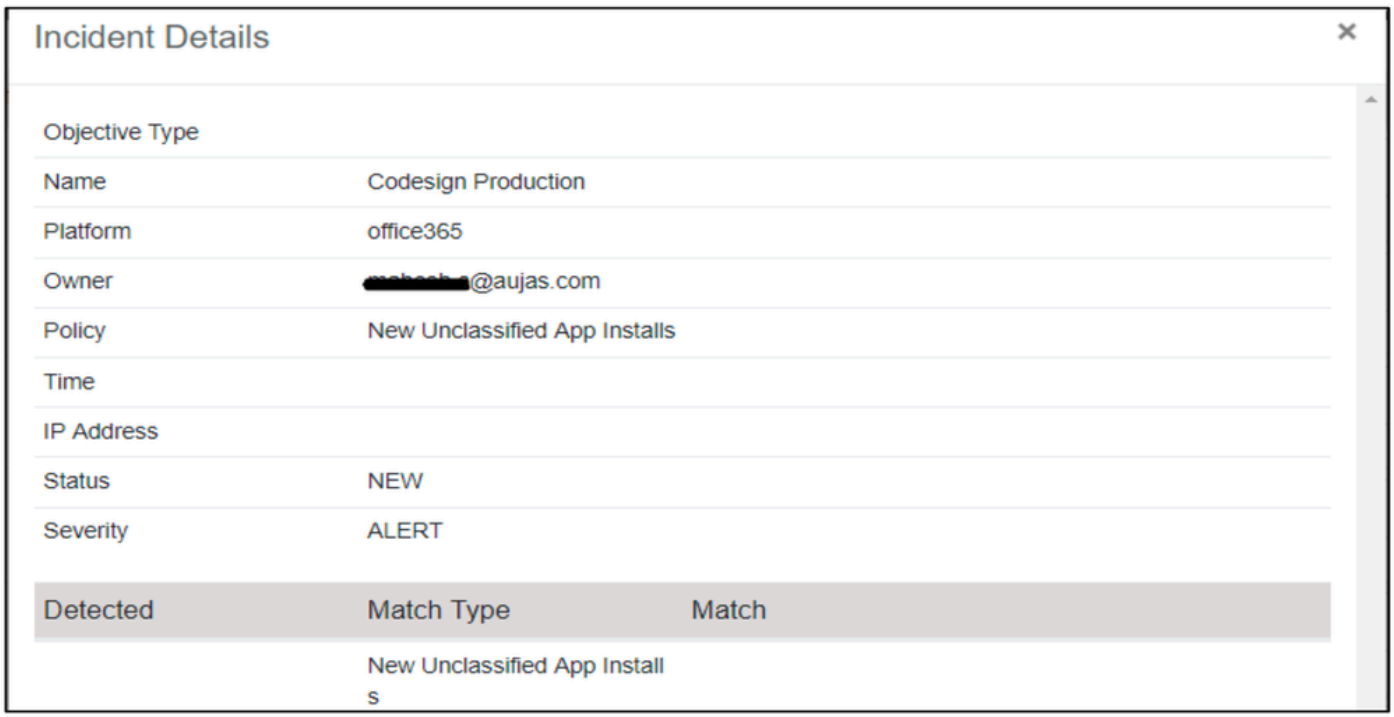
A guia CloudLock permite que os usuários exibam informações sobre todos os incidentes detectados. Os usuários também podem atualizar a gravidade e o status do incidente selecionando os valores no menu suspenso e clicando em "Atualizar".



360072268311

Os usuários podem monitorar a hora em qualquer um dos eventos para visualizar mais detalhes

sobre o incidente.



360072042332

Guia Aplicação

A guia Aplicação exibe informações sobre quais domínios estão bloqueados. Os usuários também podem selecionar domínios bloqueados e desbloqueá-los nessa interface.

360072038472

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.