Beheer de Cloud Security App voor IBM QRadar

Inhoud

Inleiding

In dit document wordt beschreven hoe u de Cisco Cloud Security-app voor IBM QRadar kunt beheren.

Overzicht

QRadar van IBM is een populaire SIEM voor log-analyse. Het biedt een krachtige interface voor het analyseren van grote hoeveelheden gegevens, zoals de logs die door Cisco Umbrella worden geleverd voor het DNS-verkeer van uw organisatie. Informatie die wordt weergegeven in de Cisco Cloud Security App voor IBM QRadar wordt geleverd via de API's van Cisco Umbrella, CloudLock, Investigate en Enforcement.

Wanneer u de Cisco Cloud Security-app voor QRadar instelt, worden alle gegevens van het Cisco Cloud Security-platform geïntegreerd en kunt u de gegevens in grafische vorm bekijken in de QRadar-console. Vanuit de applicatie kunnen analisten:

- Domeinen, IP-adressen, e-mailadressen onderzoeken
- Domeinen blokkeren en deblokkeren (handhaving)
- Bekijk de informatie over alle incidenten van het netwerk.

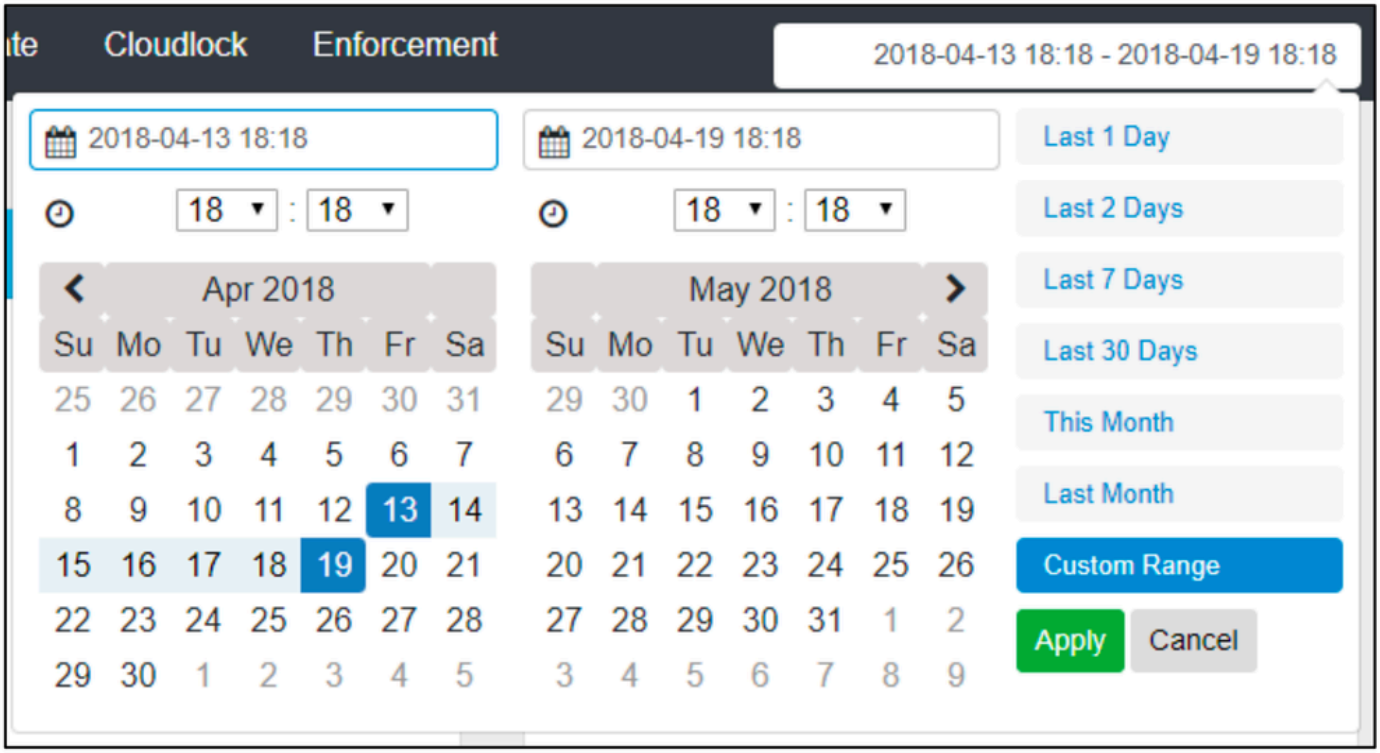
In dit artikel wordt uitgelegd hoe u door de Cisco Cloud Security-app kunt navigeren. Instructies voor het instellen van de toepassing vindt u hier: De Cisco Cloud Security App configureren voor IBM QRadar

Toegang tot de Cisco Cloud Security App

Om naar de Cisco Cloud Security App in IBM QRadar te navigeren, gaat u naar de startpagina en klikt u op het tabblad Cisco Cloud Security. Het tabblad Cloud Overview en het Dashboard worden

weergegeven. U kunt vervolgens toegang krijgen tot de tabbladen Umbrella, Investigate, CloudLock en Enforcement om uw logs te bekijken.

De Cloud Security App is standaard ingesteld om de gegevens van de afgelopen 7 dagen weer te geven. U kunt het tijdsbestek wijzigen door rechtsboven op het datumbereik te klikken:

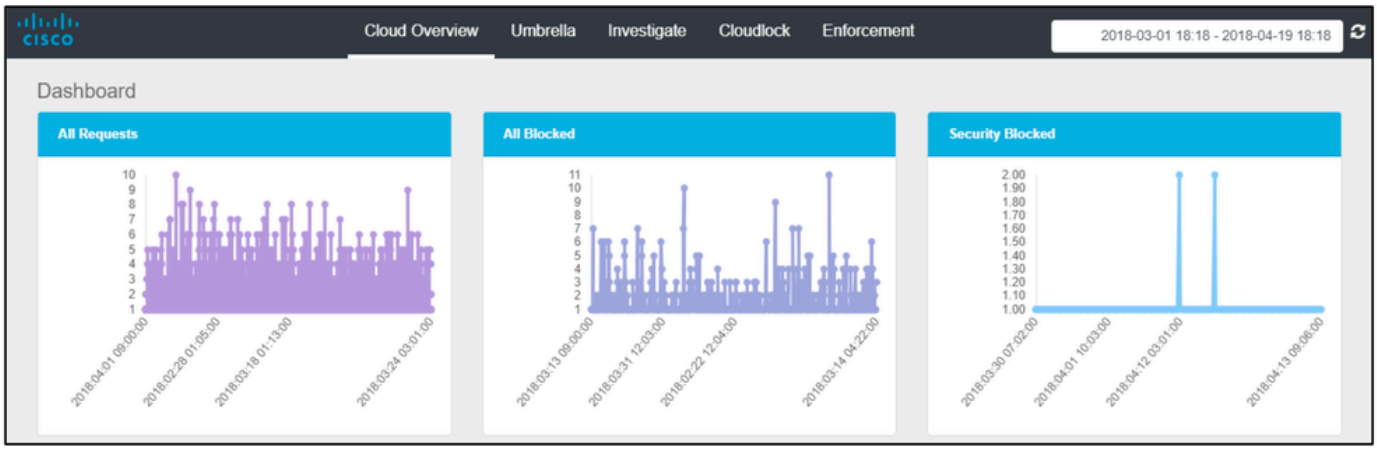


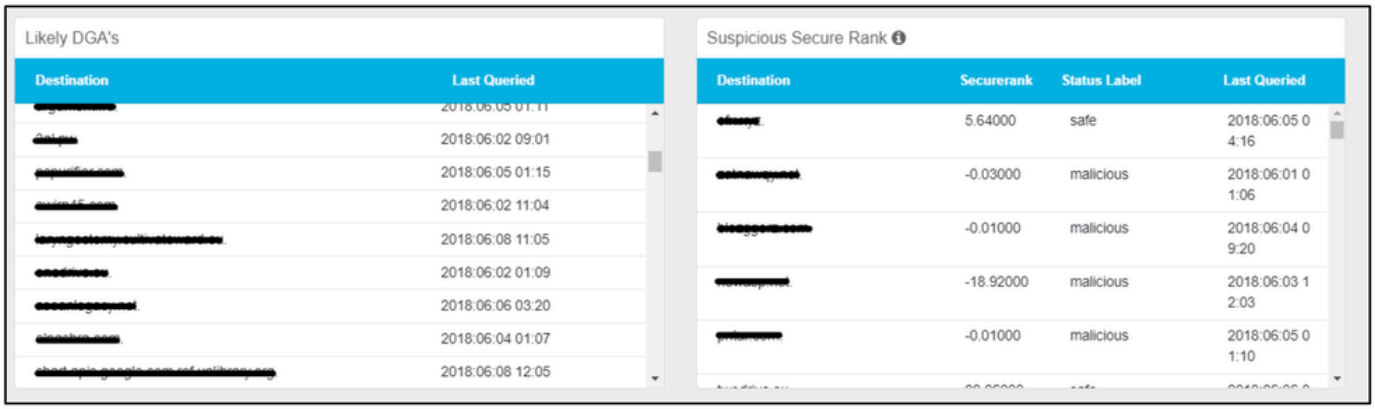
360072030052

Onderdelen van Cisco Cloud Security App

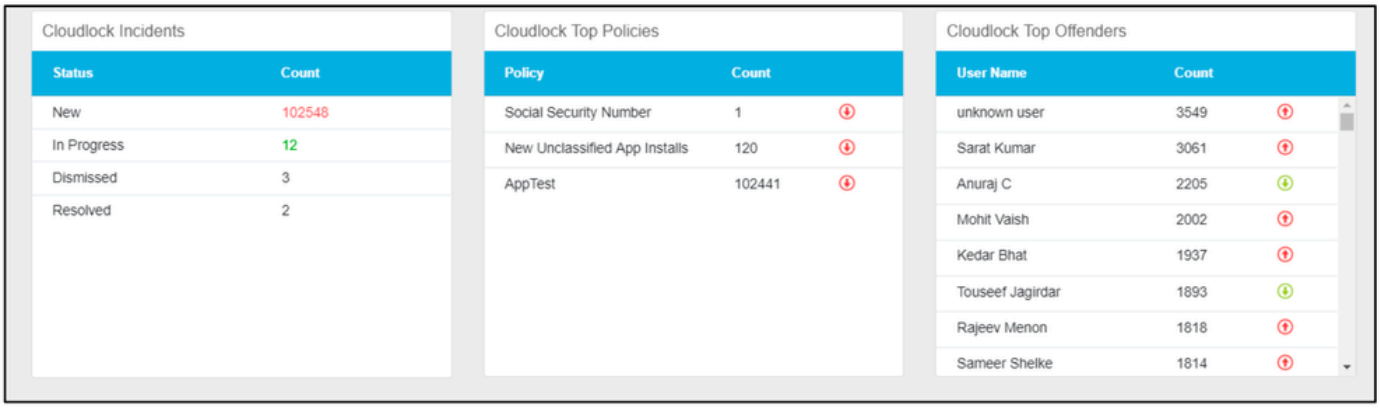
Overzicht van de cloud

Op het tabblad Cloud Overview wordt informatie weergegeven zoals Alle aanvragen, Alle geblokkeerde aanvragen, Beveiliging geblokkeerd, Waarschijnlijk DGA's, Verdachte veilige rang, Cloudlock-incidenten, CloudLock Overall, Top Policies en Top Offenders in een op diagrammen gebaseerde visuele weergave.





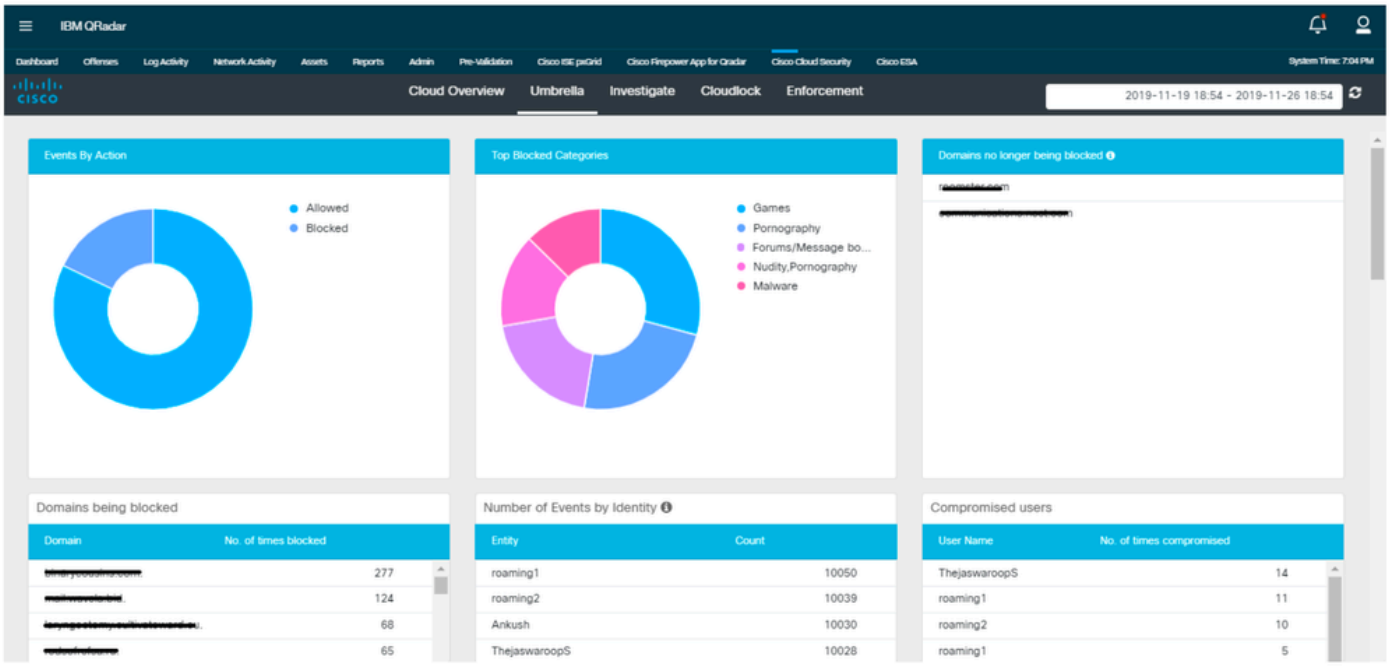
360072257631



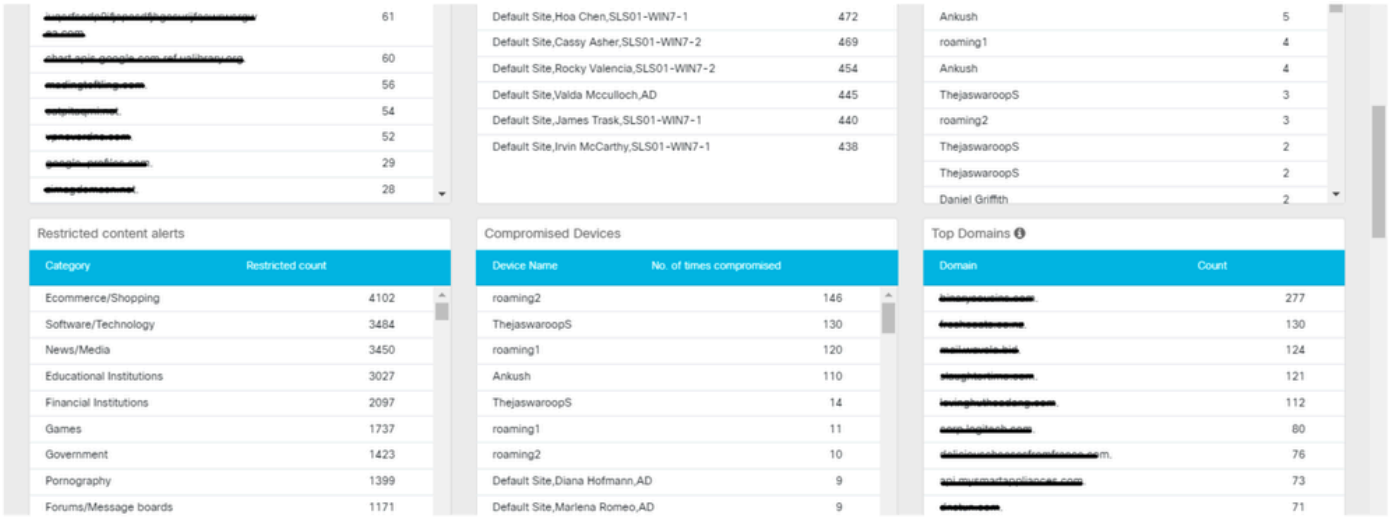
360072257611

Umbrella

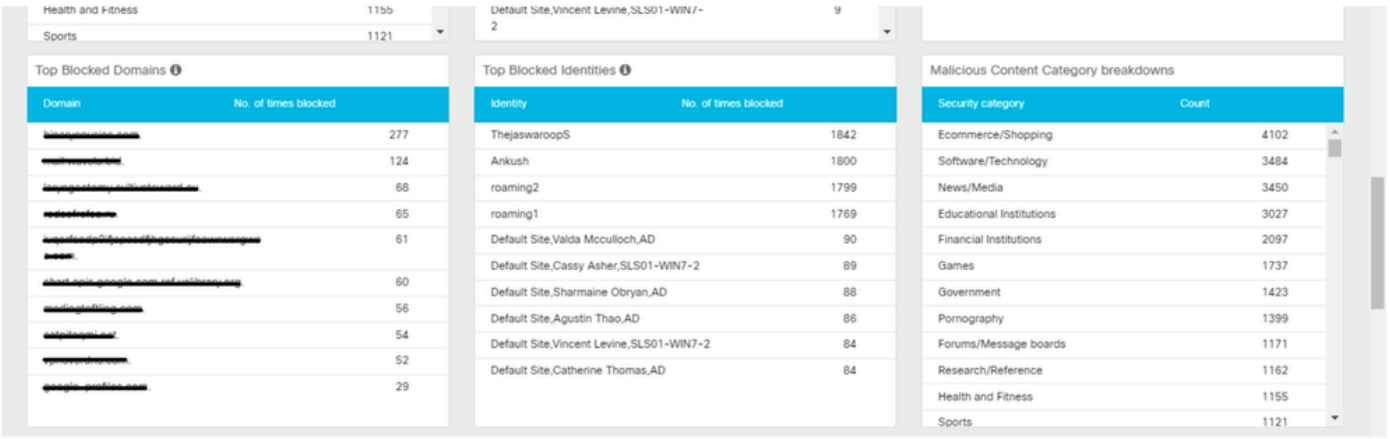
Op het tabblad Umbrella wordt informatie weergegeven zoals Gebeurtenissen op actie, Bovenste geblokkeerde categorieën, Aantal gebeurtenissen op identiteit, Geblokkeerde domeinen, Geblokkeerde domeinen, Gevaarlijke gebruikers, Gevaarlijke inhoudswaarschuwingen, Gevaarlijke apparaten, Bovenste domeinen, Bovenste geblokkeerde domeinen, Bovenste geblokkeerde identiteiten, Uitsplitsingen van kwaadwillige inhoudscategorieën, Bovenste categorieën, Activiteit en Trend gebruikerstoegang in een grafische visuele weergave.



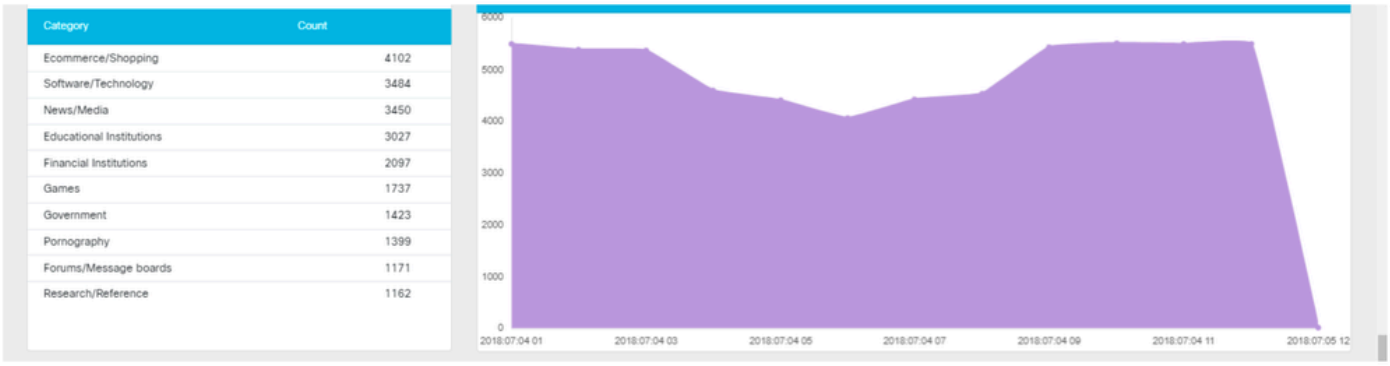
360072263411



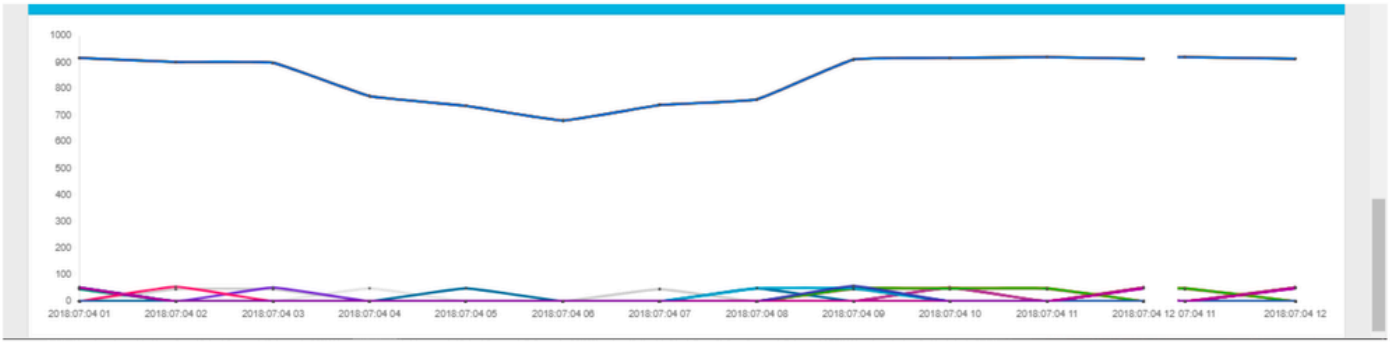
360072263391



360072037372



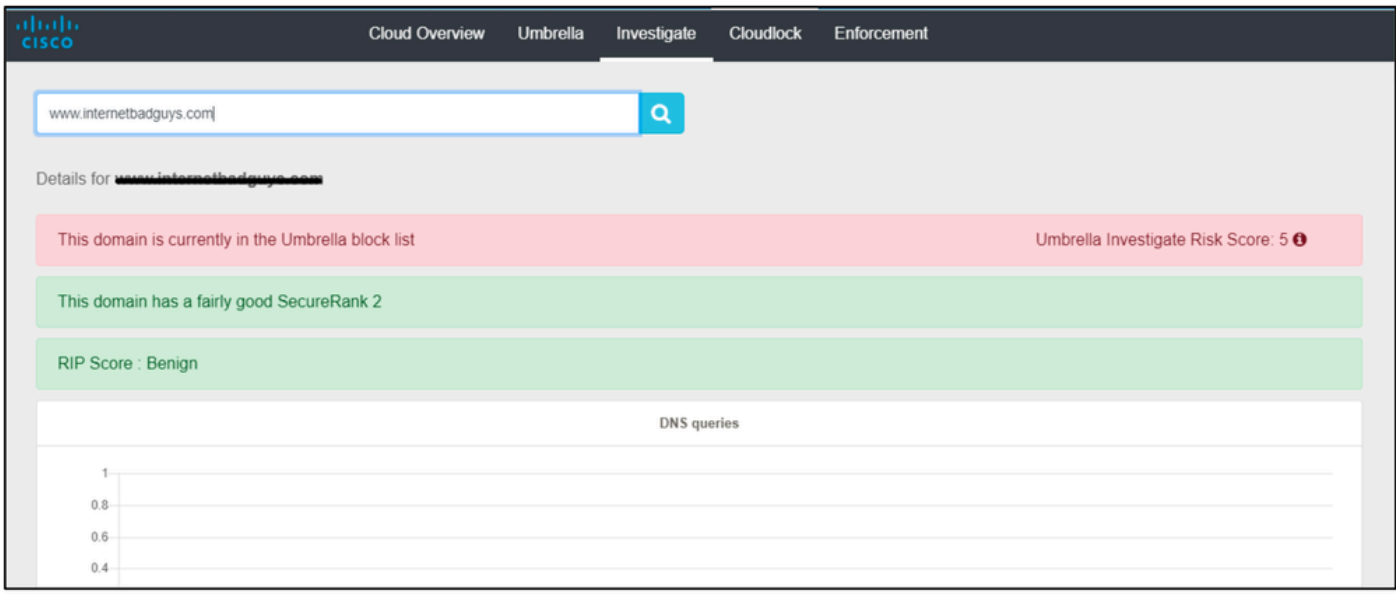
360072263331



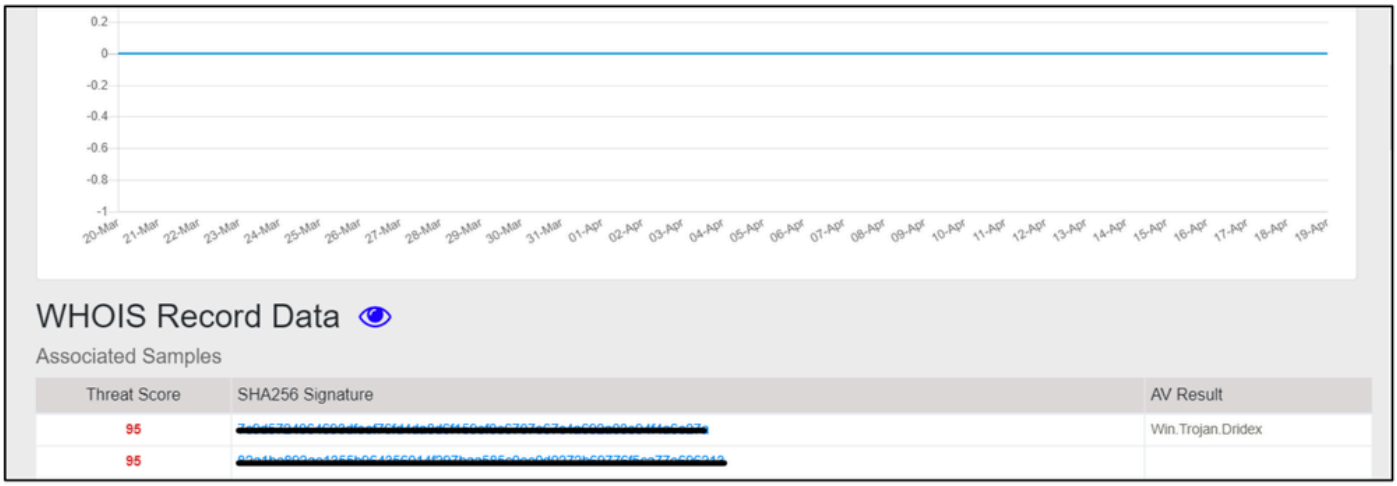
360072263351

onderzoeken

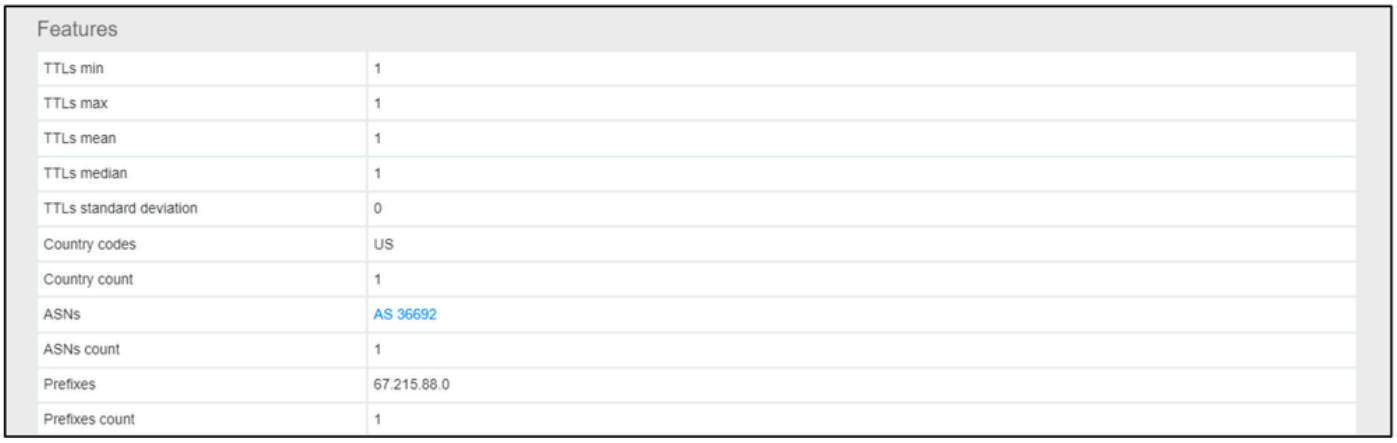
Op het tabblad Onderzoeken kan de gebruiker zoeken naar de informatie met betrekking tot hostnaam, URL, ASN, IP, Hash of e-mailadres. Het heeft ook informatie zoals WHOIS-record, DGA-informatie enzovoort.



360072263511



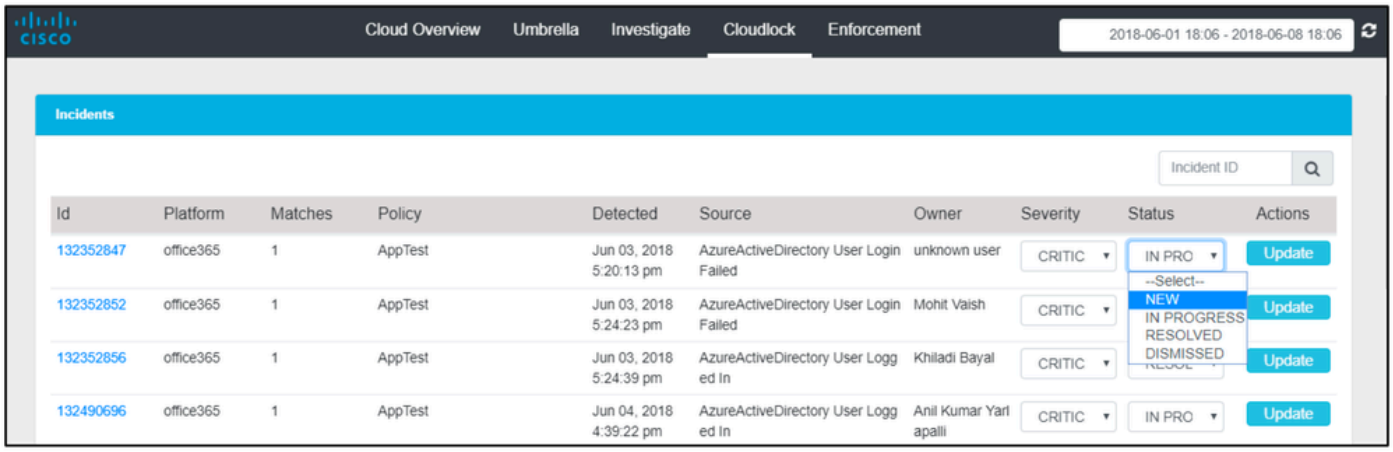
360072037472



360072037452

CloudLock

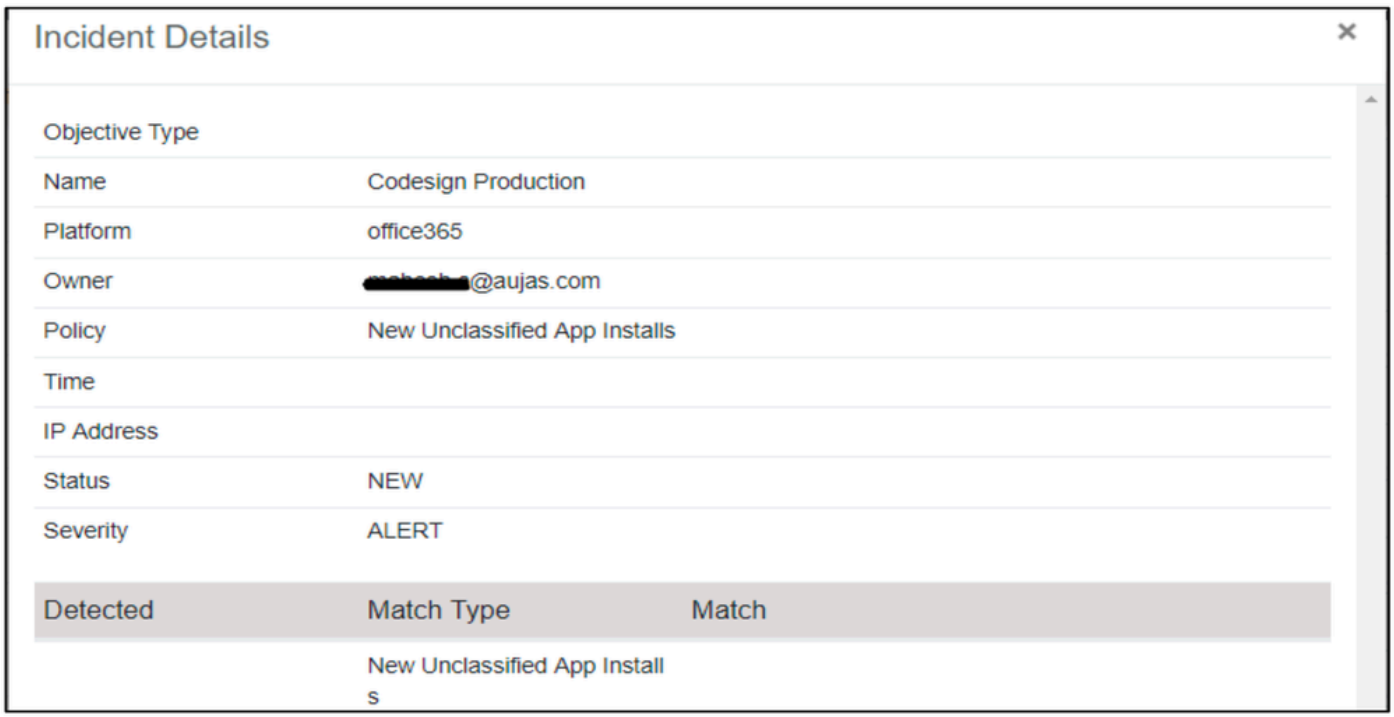
Op het tabblad CloudLock kunnen gebruikers informatie bekijken over alle gedetecteerde incidenten. Gebruikers kunnen ook de ernst en status van het incident bijwerken door de waarden in het vervolgkeuzemenu te selecteren en op "Bijwerken" te klikken.



360072268311

Gebruikers kunnen op elk van de gebeurtenissen klikken om meer details over het incident te

bekijken.



360072042332

Tabblad Handhaving

Op het tabblad Handhaving wordt informatie weergegeven over welke domeinen worden geblokkeerd. Gebruikers kunnen ook geblokkeerde domeinen selecteren en deblokkeren vanuit deze interface.

360072038472

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.