Gestisci l'app Cloud Security per IBM QRadar

Sommario

Introduzione

Panoramica

Accesso all'app Cisco Cloud Security

Componenti dell'app Cisco Cloud Security

- Panoramica del cloud
- Umbrella
- Indaga
- CloudLock
- Scheda Imposizione

Introduzione

Questo documento descrive come gestire l'app Cisco Cloud Security per IBM QRadar.

Panoramica

QRadar di IBM è un popolare SIEM per l'analisi dei log. Fornisce una potente interfaccia per l'analisi di grandi blocchi di dati, ad esempio i registri forniti da Cisco Umbrella per il traffico DNS della tua organizzazione. Le informazioni visualizzate in Cisco Cloud Security App per IBM QRadar sono disponibili tramite le API di Cisco Umbrella, CloudLock, Investigate and Enforcement.

Quando si configura l'app Cisco Cloud Security per QRadar, integra tutti i dati della piattaforma Cisco Cloud Security e consente di visualizzare i dati in formato grafico nella console QRadar. Dall'applicazione, gli analisti possono:

- Analizza domini, indirizzi IP, indirizzi e-mail
- Bloccare e sbloccare i domini (imposizione)
- Visualizzare le informazioni di tutti gli incidenti della rete.

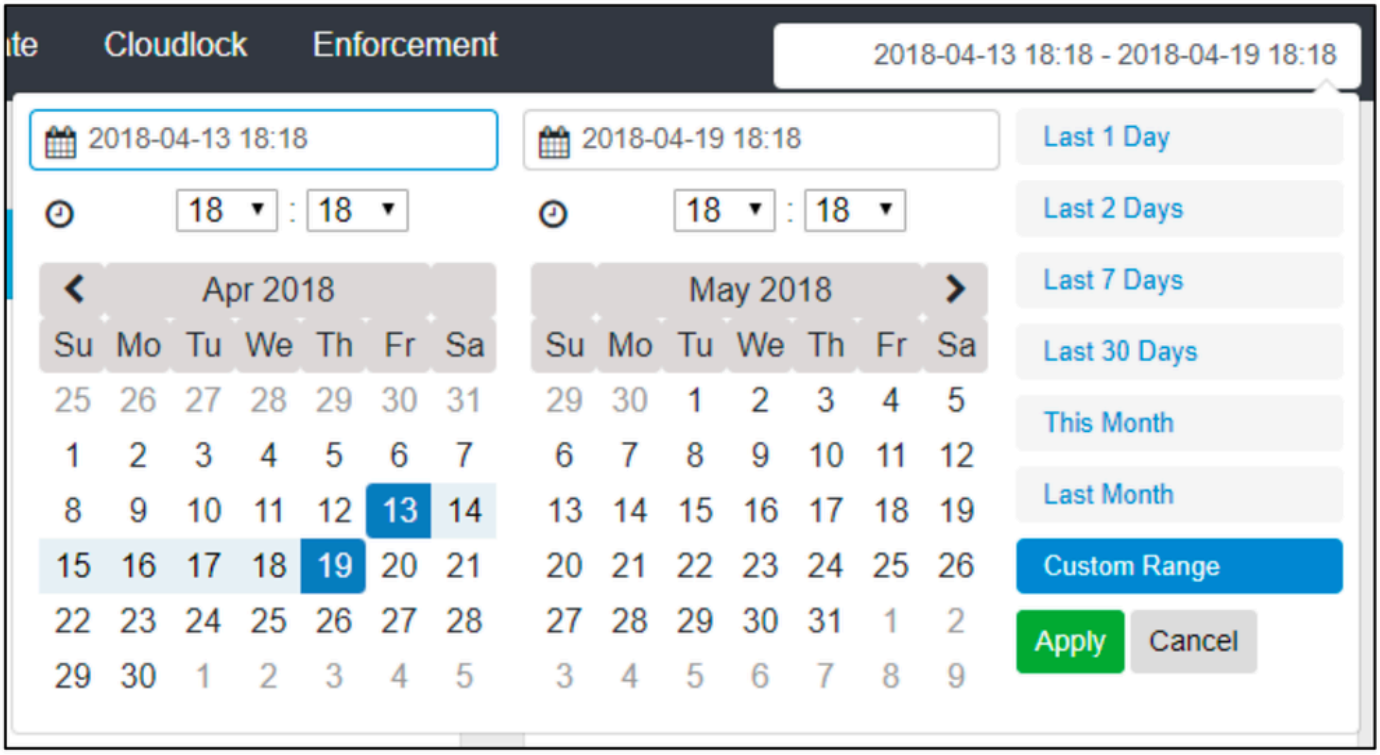
In questo articolo viene illustrato come esplorare Cisco Cloud Security App. Le istruzioni su come configurare l'applicazione sono disponibili qui: Configurazione dell'app Cisco Cloud Security per IBM QRadar

Accesso all'app Cisco Cloud Security

Per passare all'app Cisco Cloud Security in IBM QRadar, vai alla home page e fai clic sulla scheda Cisco Cloud Security. Vengono visualizzate la scheda Panoramica cloud e il dashboard. È quindi possibile accedere alle schede Umbrella, Investigate, CloudLock e Enforcement per

visualizzare i log.

Per impostazione predefinita, l'app Cloud Security è impostata per visualizzare i dati degli ultimi 7 giorni. È possibile modificare l'intervallo di tempo facendo clic sull'intervallo di date in alto a destra:

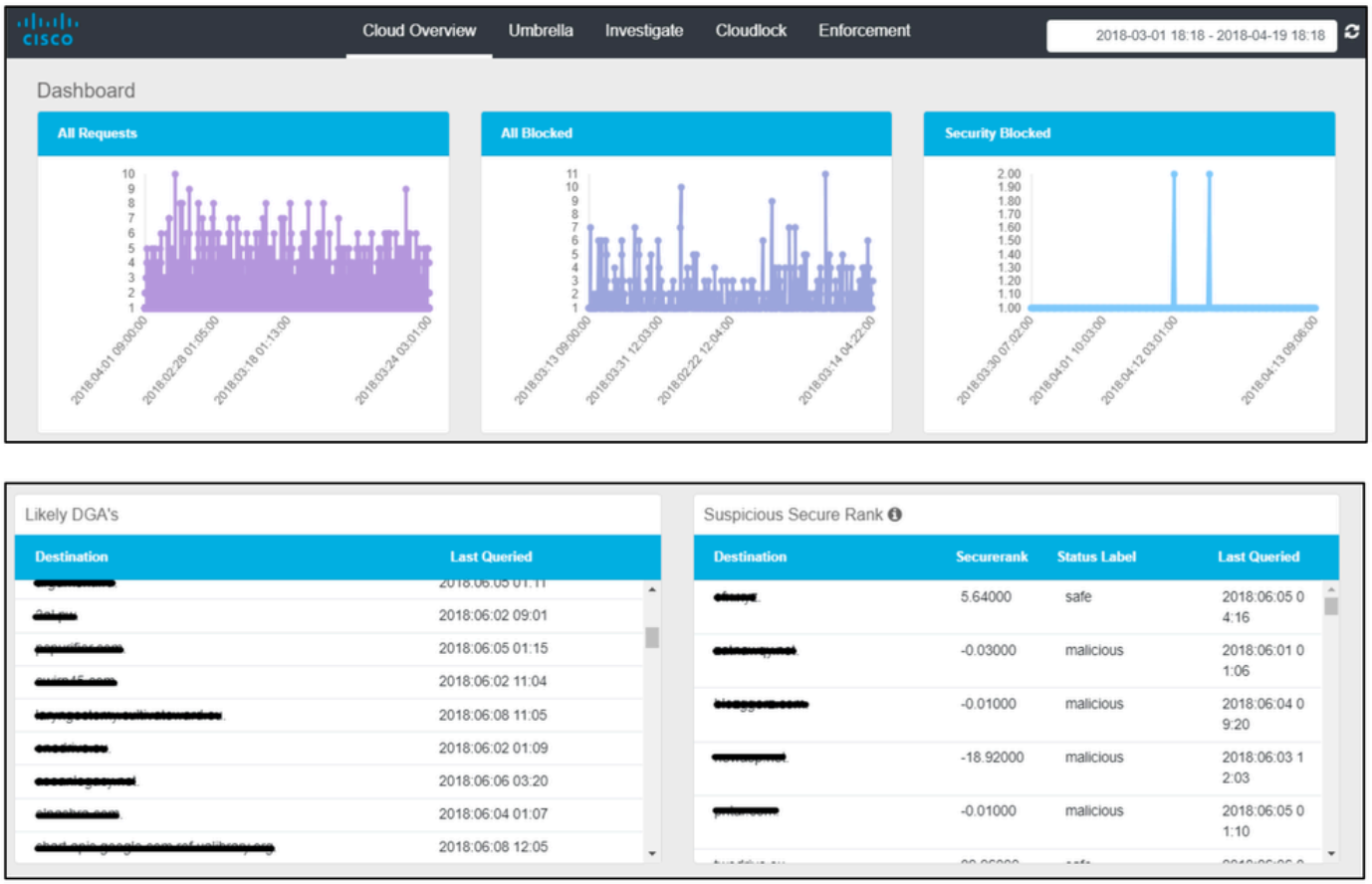


360072030052

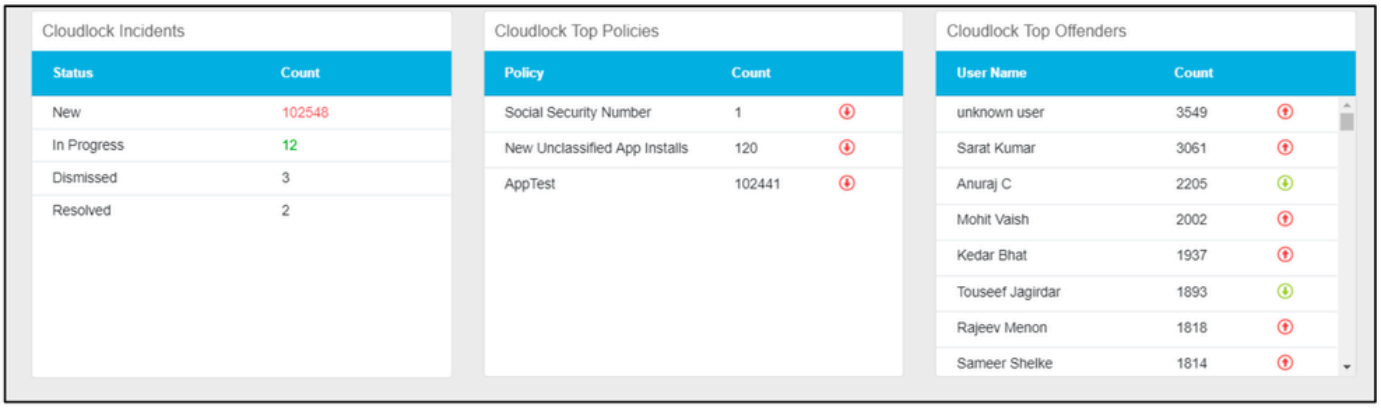
Componenti dell'app Cisco Cloud Security

Panoramica del cloud

Nella scheda Panoramica cloud vengono visualizzate informazioni quali Tutte le richieste, Tutte le richieste bloccate, Sicurezza bloccata, DGA probabile, Classificazione sicura sospetta, Incidenti di blocco cloud, Blocco cloud complessivo, Primi criteri e Primi offensori in una rappresentazione grafica basata su grafico.



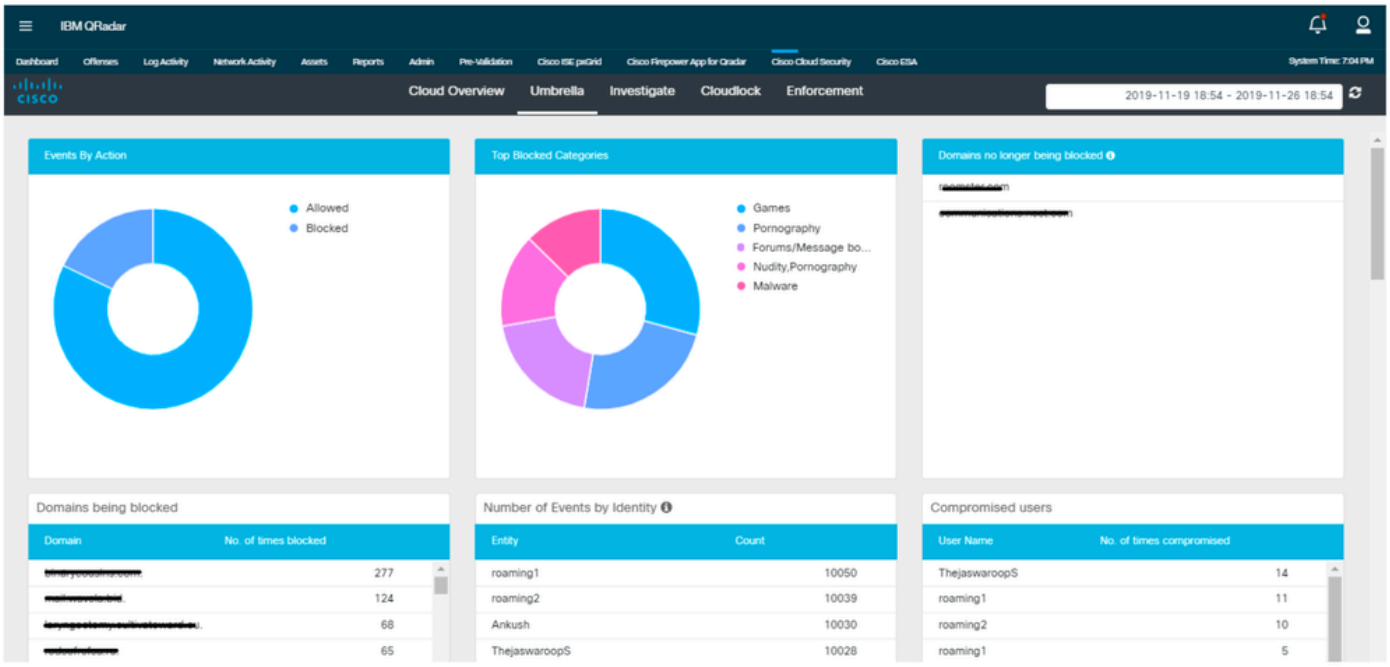
360072257631



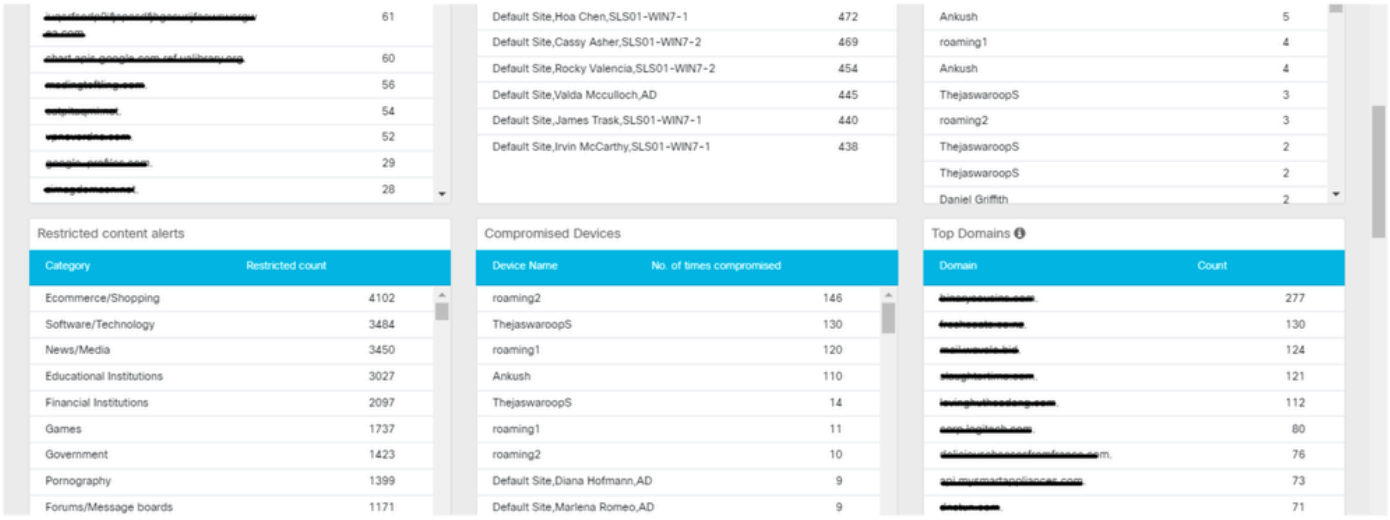
360072257611

Umbrella

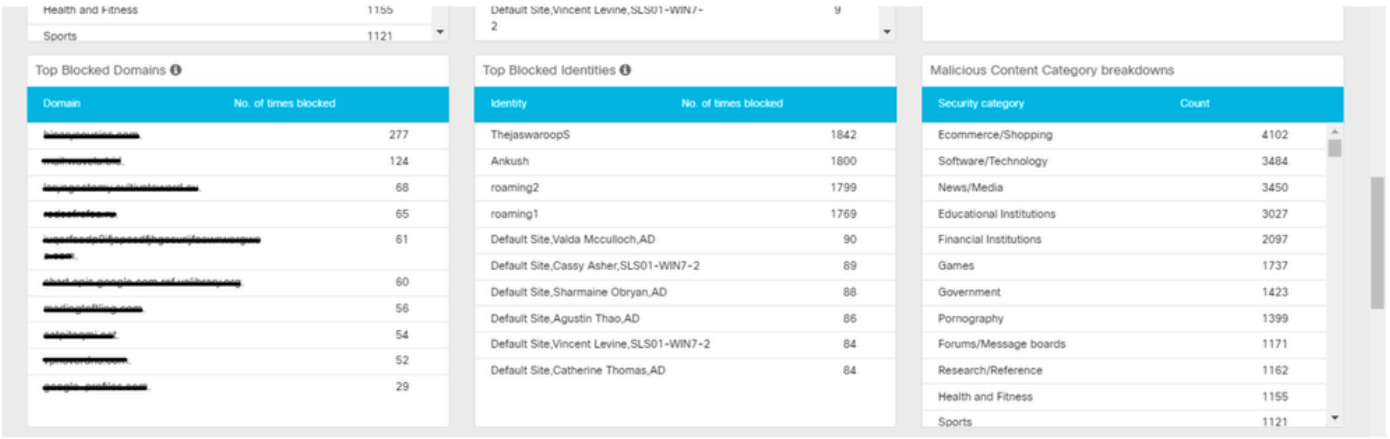
Nella scheda Umbrella vengono visualizzate informazioni quali Eventi per azione, Categorie bloccate principali, Numero di eventi per identità, Domini bloccati, Domini non più bloccati, Utenti compromessi, Avvisi di contenuto con restrizioni, Dispositivi compromessi, Primi domini, Primi domini bloccati, Primi identità bloccate, Suddivisioni categorie di contenuto dannoso, Principali categorie, Attività e Tendenza accesso utente in una rappresentazione grafica basata su grafico.



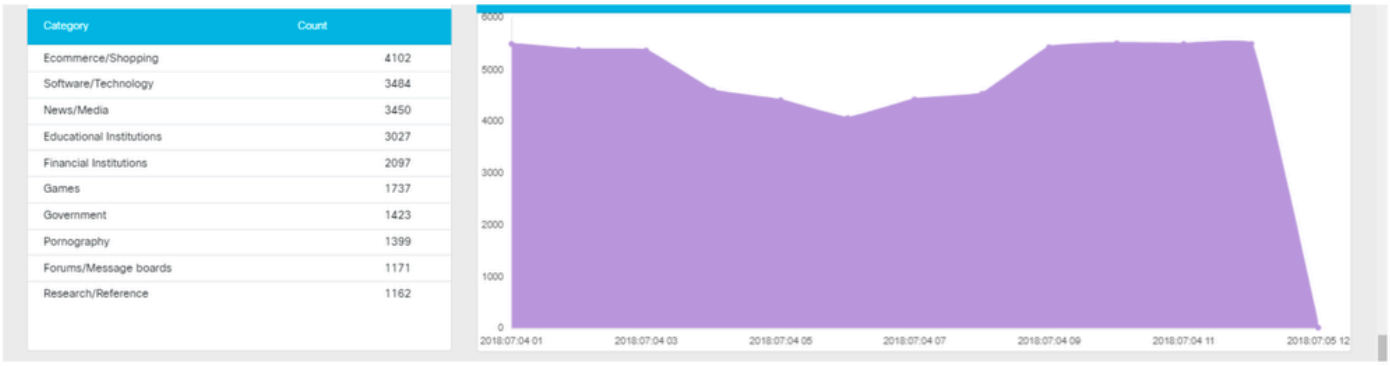
360072263411



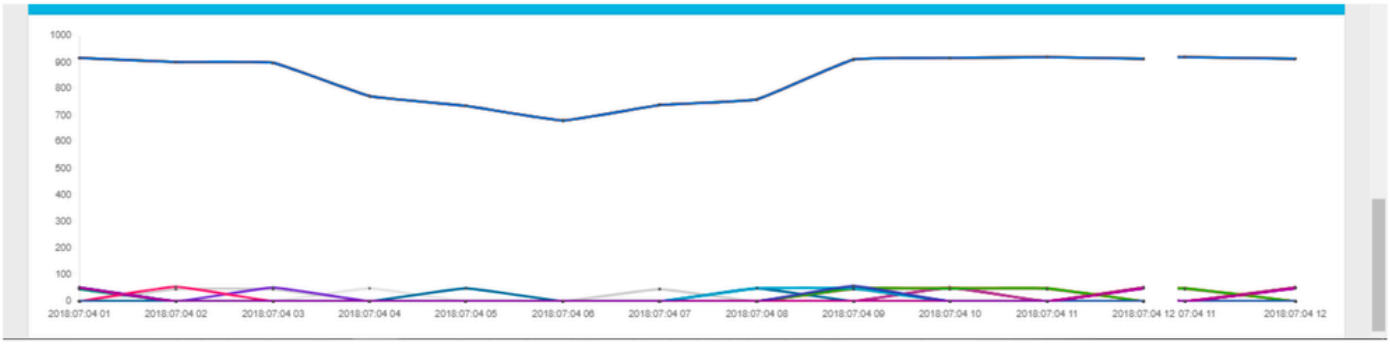
360072263391



360072037372



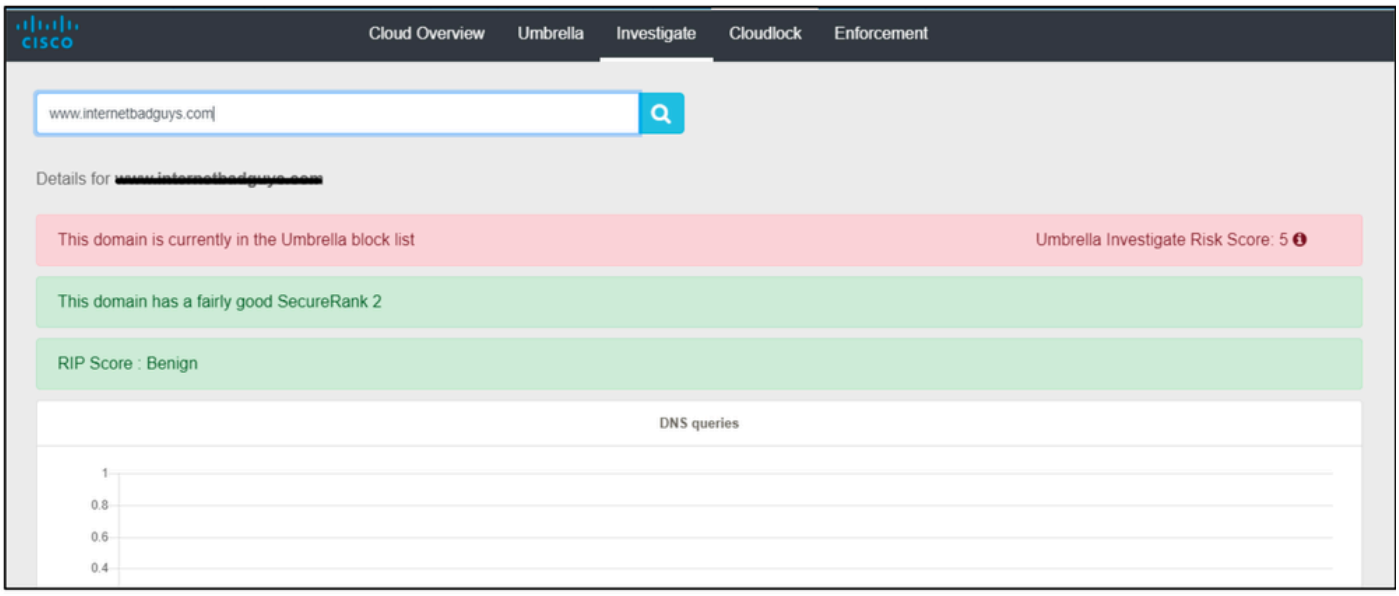
360072263331



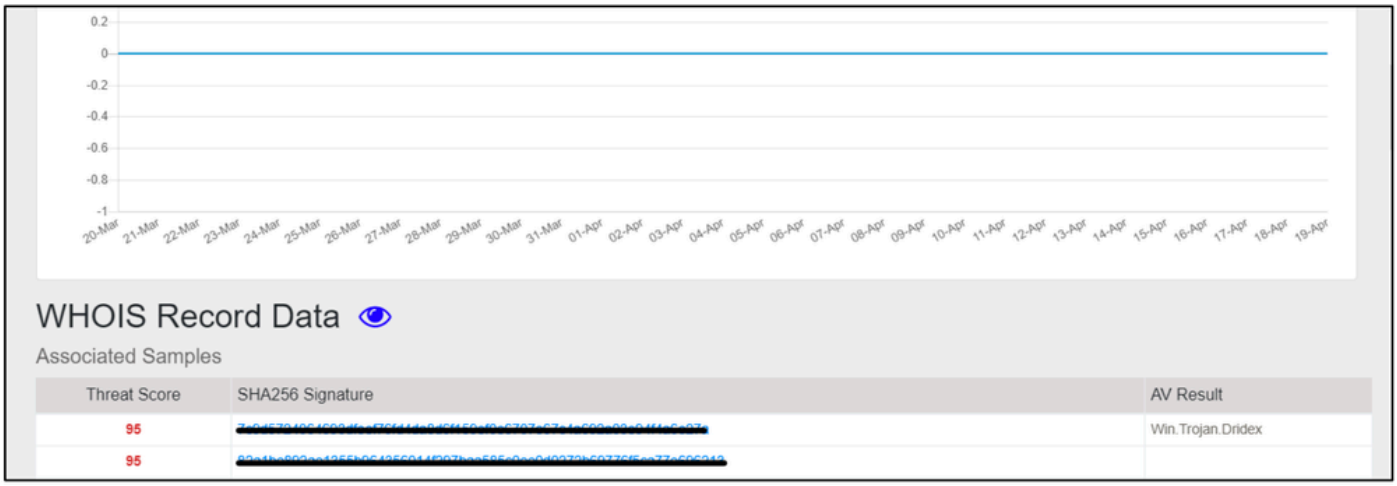
360072263351

Indaga

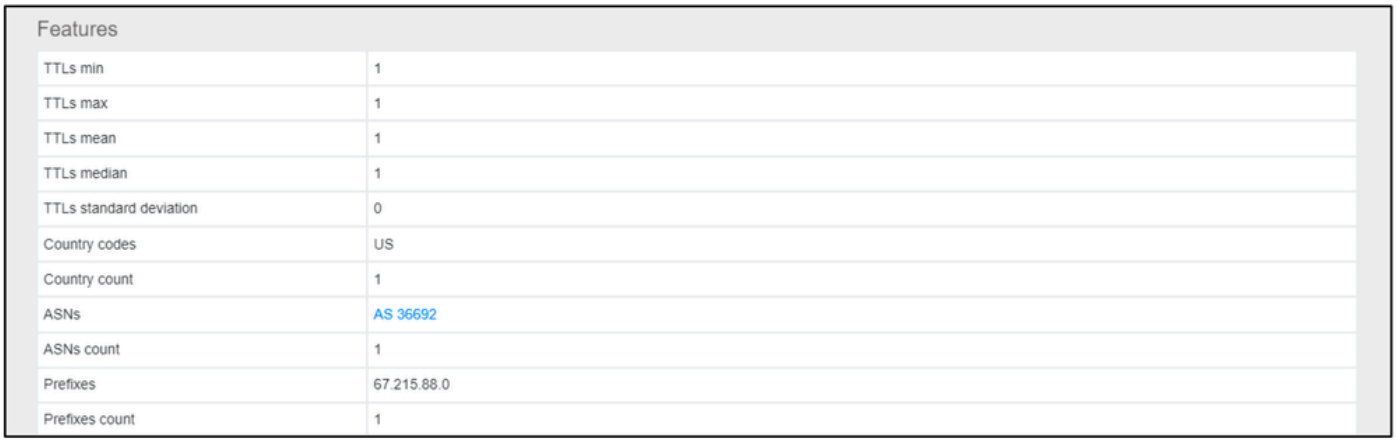
La scheda Indaga consente all'utente di cercare le informazioni relative a nome host, URL, ASN, IP, hash o indirizzo e-mail. Contiene inoltre informazioni quali record WHOIS, informazioni DGA e così via.



360072263511



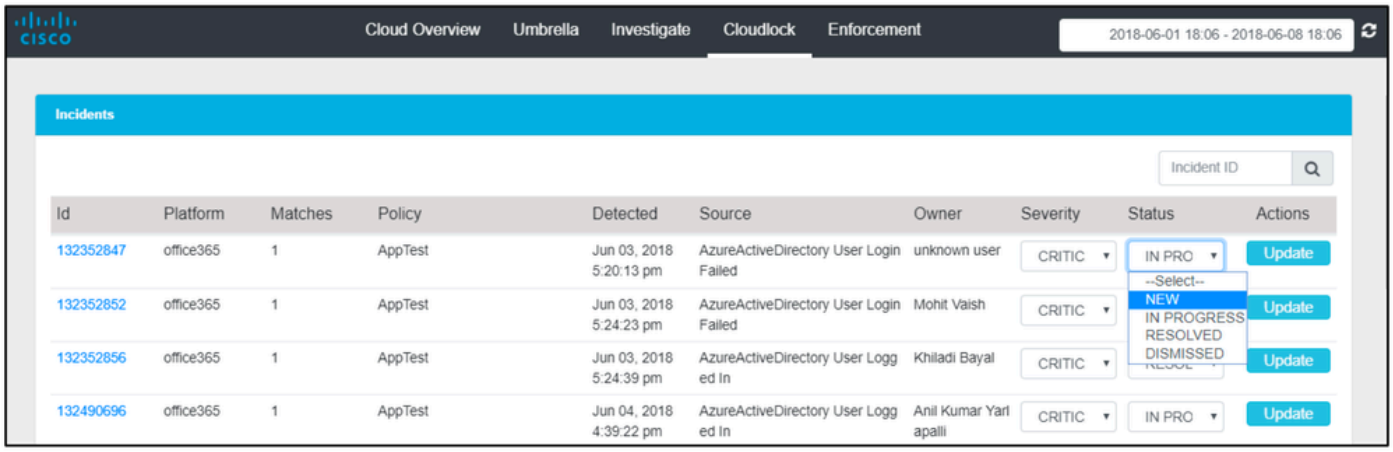
360072037472



360072037452

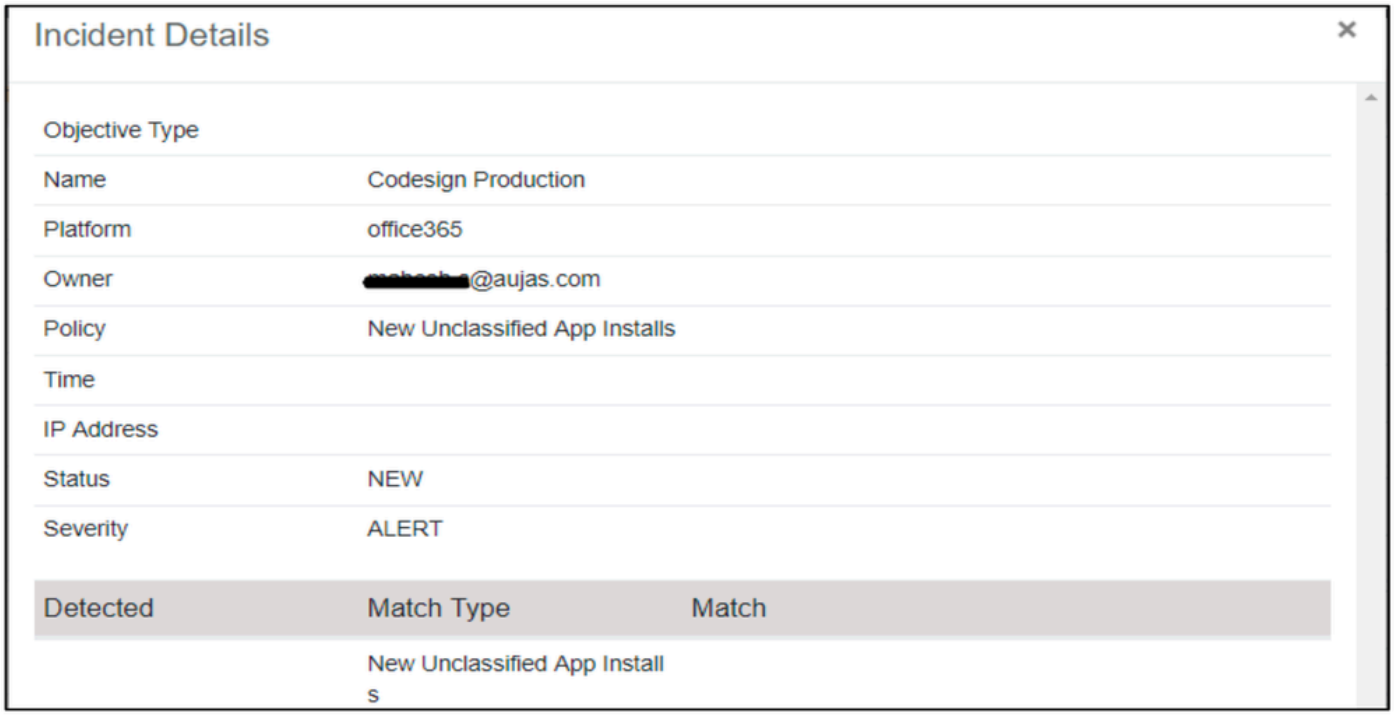
CloudLock

La scheda CloudLock consente agli utenti di visualizzare informazioni su tutti gli incidenti rilevati. Gli utenti possono anche aggiornare la gravità e lo stato dell'incidente selezionando i valori dal menu a discesa e facendo clic su "Aggiorna".



360072268311

Gli utenti possono registrare gli eventi per visualizzare ulteriori dettagli sull'incidente.



360072042332

Scheda Imposizione

Nella scheda Imposizione vengono visualizzate informazioni sui domini bloccati. Gli utenti possono anche selezionare i domini bloccati e sbloccarli da questa interfaccia.

360072038472

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).