إدارة تطبيق أمان السحابة لـ IBM QRadar

المحتويات

المقدمة

نظرة عامة

الوصول إلى تطبيق أمان السحابة من Cisco

مكونات تطبيق أمان السحابة من Cisco

- نظرة عامة على السحابة
- Umbrella
- استخبارات
- CloudLock
- عرض توضيحي للميزة

المقدمة

يوضح هذا المستند كيفية إدارة تطبيق أمان السحابة من Cisco لـ IBM QRadar.

نظرة عامة

QRadar من IBM هو SIEM شائع لتحليل السجل. وهو يوفر واجهة قوية لتحليل مجموعات كبيرة من البيانات، مثل السجلات المقدمة من Cisco Umbrella لحركة مرور DNS في مؤسستك. تأتي المعلومات المعروضة في تطبيق أمان السحابة لـ IBM QRadar من خلال واجهة برمجة التطبيقات (API) الخاصة بـ Cisco Umbrella، CloudLock، Investigate and Enforcement.

عند إعداد تطبيق أمان السحابة من Cisco لـ QRadar، فإنه يدمج جميع البيانات من منصة أمان السحابة من Cisco ويسمح لك بعرض البيانات في شكل رسومي في وحدة تحكم QRadar. من التطبيق، يستطيع المحللون:

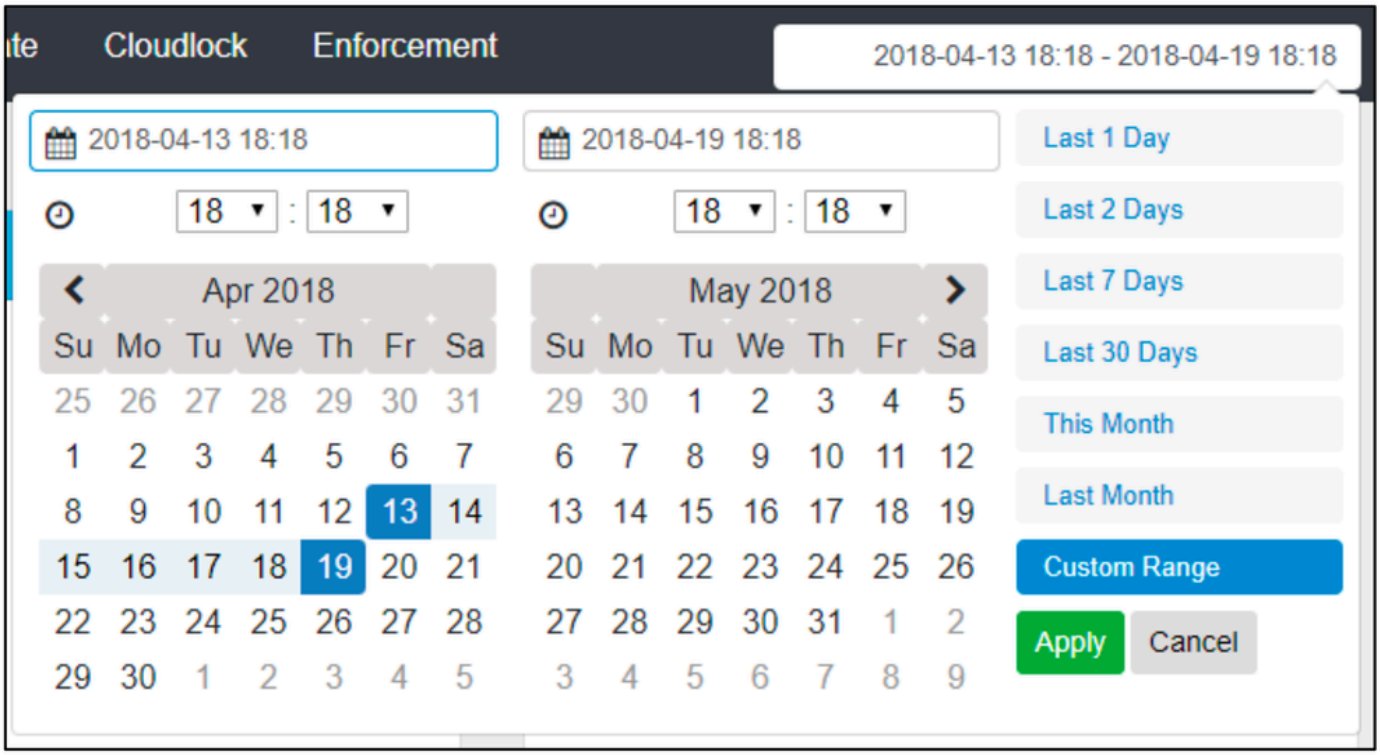
- التحقيق في المجالات وعناوين IP وعناوين البريد الإلكتروني
- حظر المجالات وإلغاء حظرها (الإنفاذ)
- عرض معلومات جميع حوادث الشبكة.

ترشدك هذه المقالة إلى كيفية التنقل عبر تطبيق أمان السحابة من Cisco. يمكن العثور على إرشادات حول كيفية إعداد التطبيق هنا: تكوين تطبيق أمان السحابة لـ IBM QRadar

الوصول إلى تطبيق أمان السحابة من Cisco

للتنقل إلى تطبيق أمان السحابة من Cisco في IBM QRadar، انتقل إلى الصفحة الرئيسية وانقر فوق علامة التبويب أمان سحابة Cisco. سوف تظهر علامة التبويب نظرة عامة على السحابة ولوحة المعلومات. يمكنك بعد ذلك الوصول إلى علامات التبويب Umbrella والتحقيق وCloudLock والتنفيذ لعرض سجلاتك.

تم تعيين تطبيق أمان السحابة لإظهار البيانات من آخر 7 أيام بشكل افتراضي. يمكنك تغيير الإطار الزمني بالنقر فوق نطاق التاريخ الموجود أعلى اليمين:

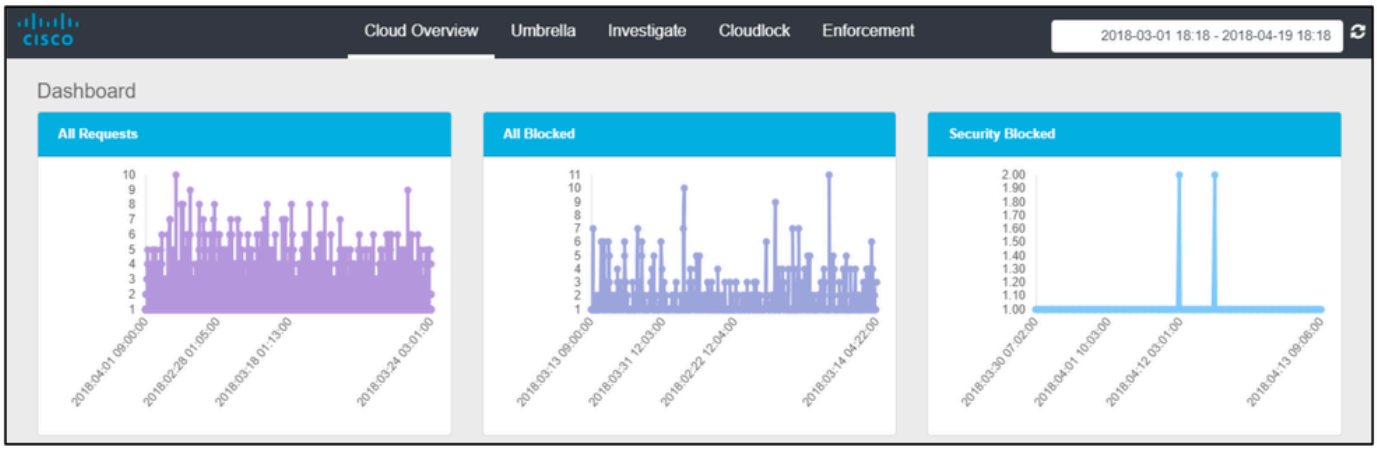


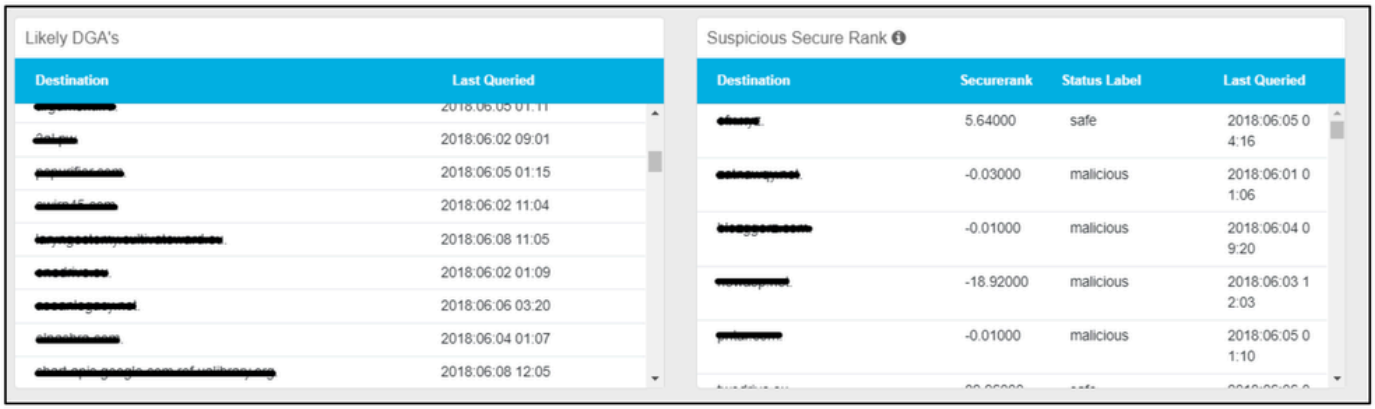
360072030052

مكونات تطبيق أمان السحابة من Cisco

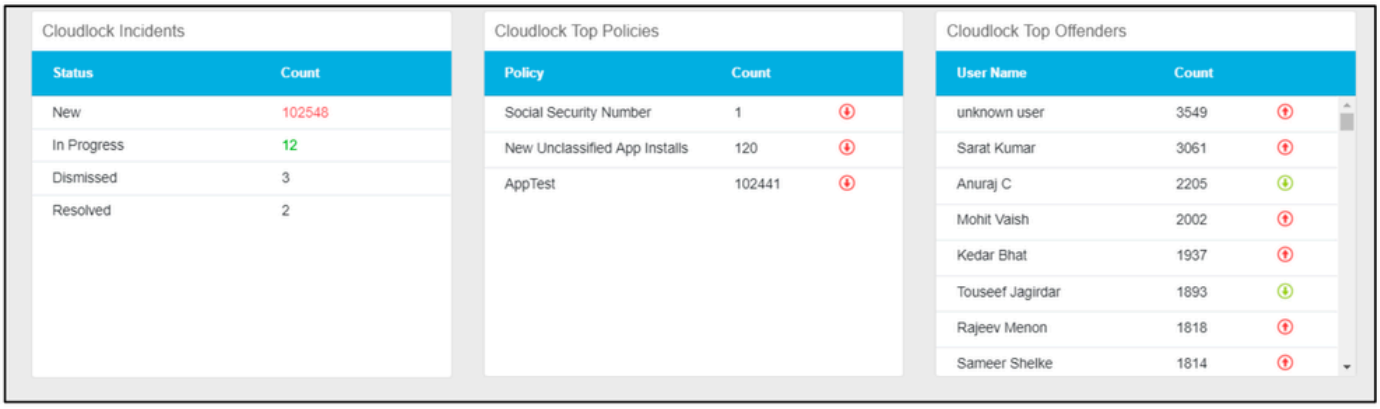
نظرة عامة على السحابة

تعرض علامة التبويب نظرة عامة على السحابة معلومات مثل جميع الطلبات، وكل عمليات الحظر، ومنع الأمان، واحتمال DGA، والرتبة الآمنة المشبوهة، وحوادث CloudLock بشكل عام، النهج العليا، والمجرمين المتميزين في التمثيل المرئي المستند إلى المخطط.





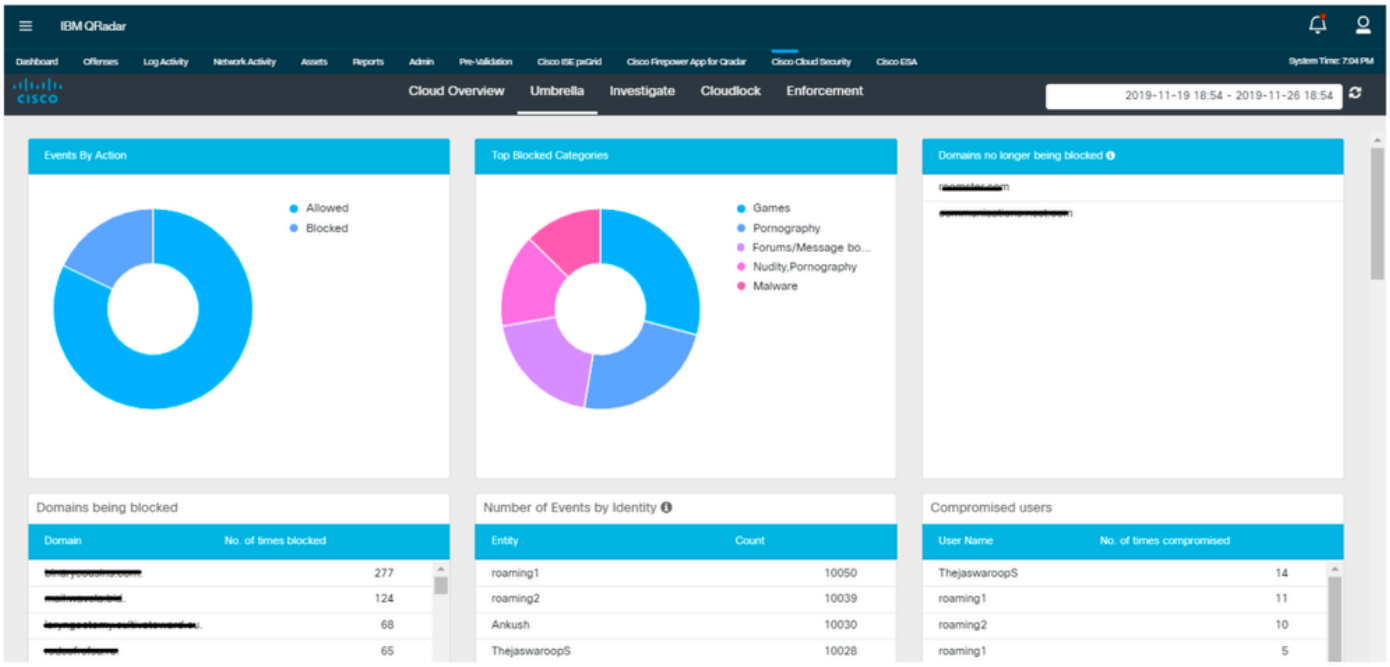
360072257631



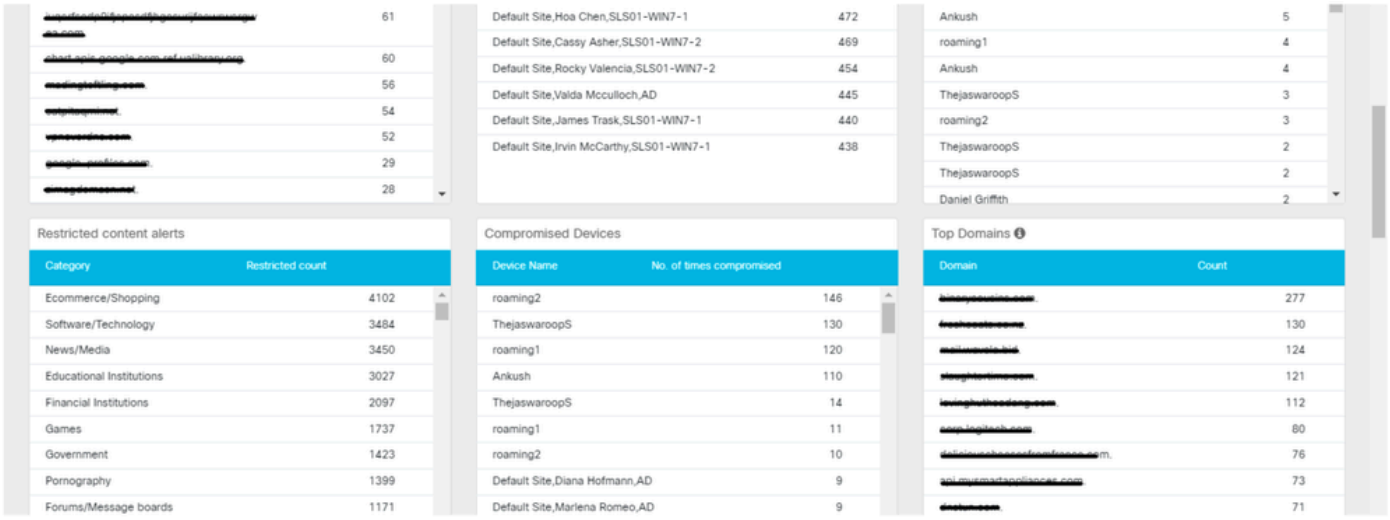
360072257611

Umbrella

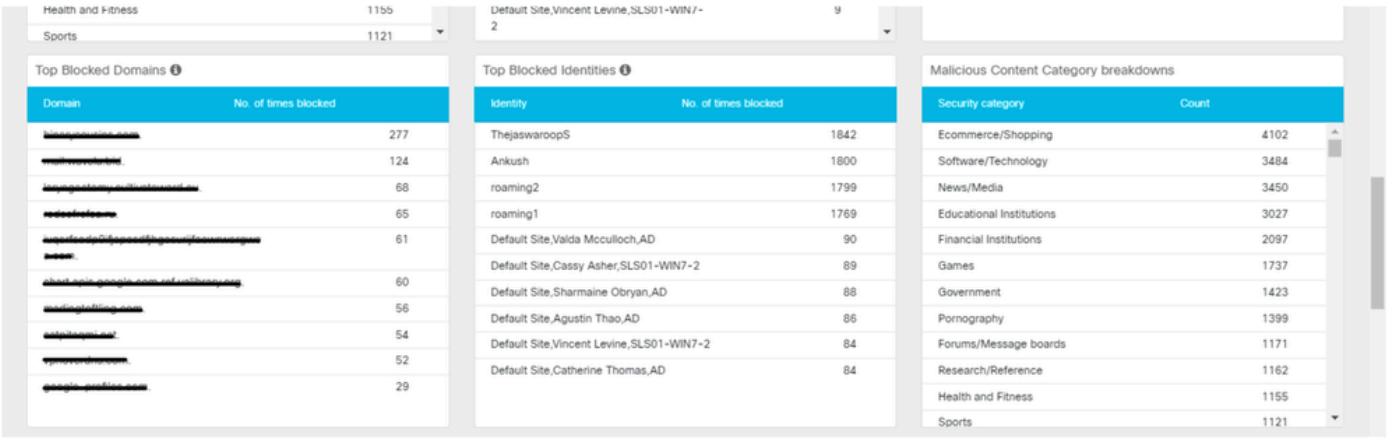
تعرض علامة التبويب "المظلة" معلومات مثل الأحداث حسب الإجراء، والفئات المحظورة العليا، وعدد الأحداث حسب الهوية، والمجالات التي يتم حظرها، والمجالات التي لم تعد محظورة، والمستخدمين الذين تم تعريضهم للخطر، وتنبيهات المحتوى المقيد، والأجهزة التي تم إختراقها، والمجالات العليا المحظورة، والهويات المحظورة العليا، وأعطال فئات المحتوى الضارة، والفئات العليا، والنشاط واتجاه وصول المستخدم في تمثيل مرئي مستند إلى المخطط.



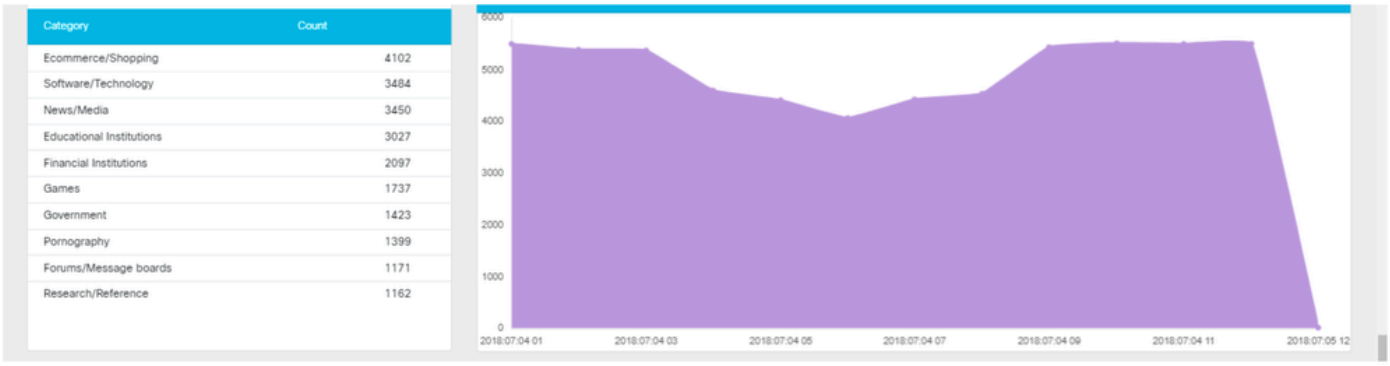
360072263411



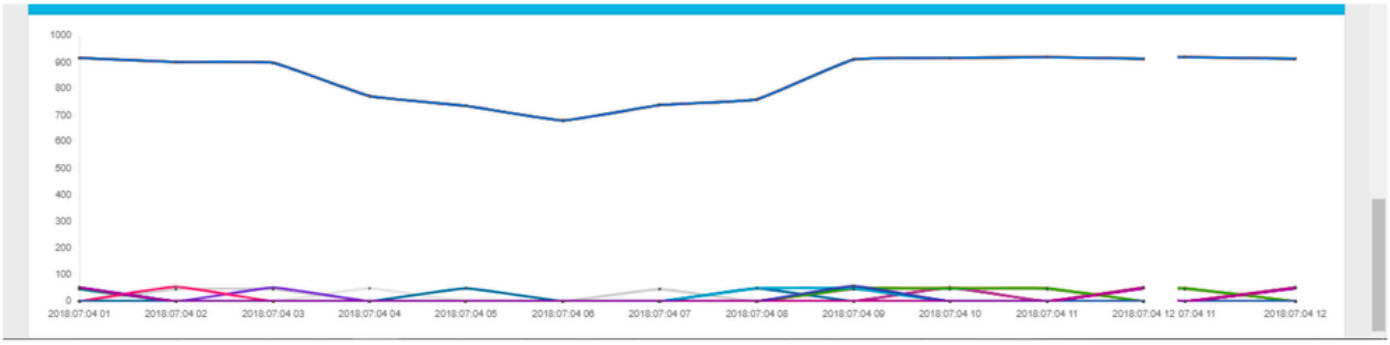
360072263391



360072037372



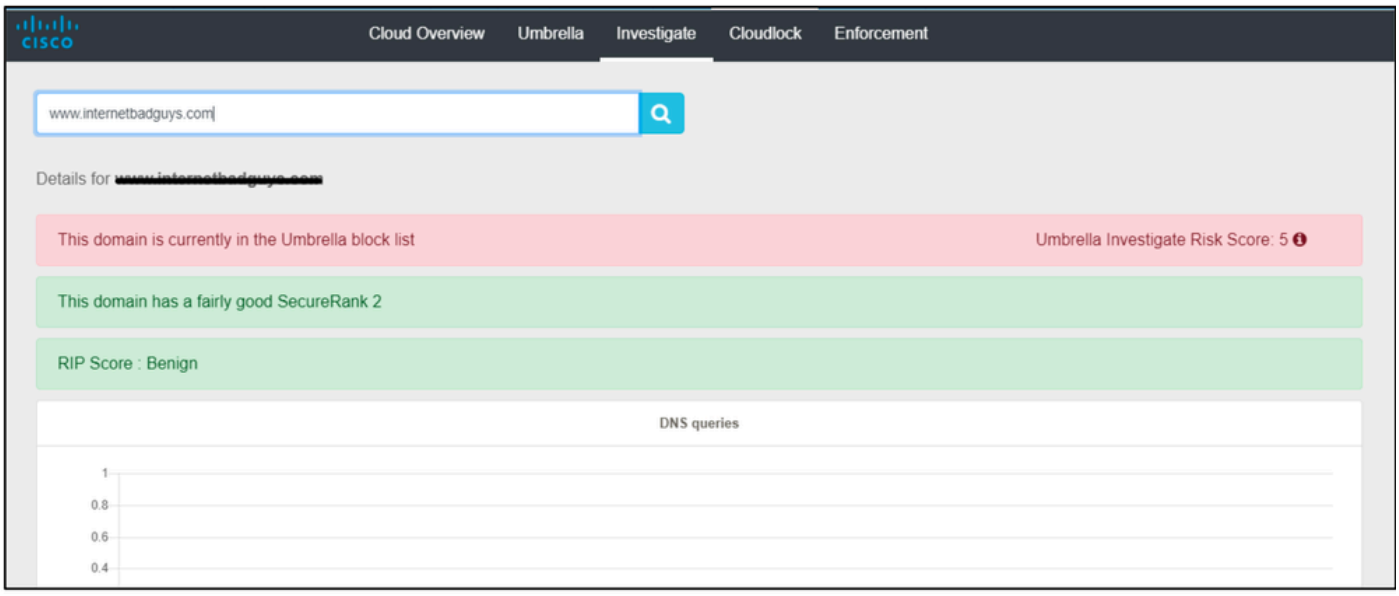
360072263331



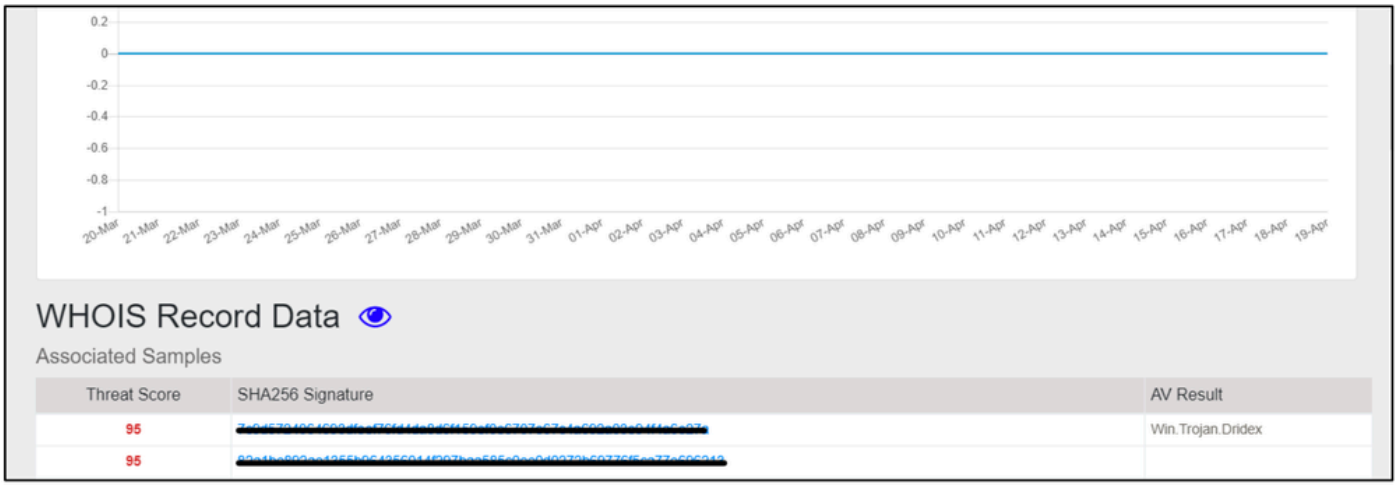
360072263351

نستخبر

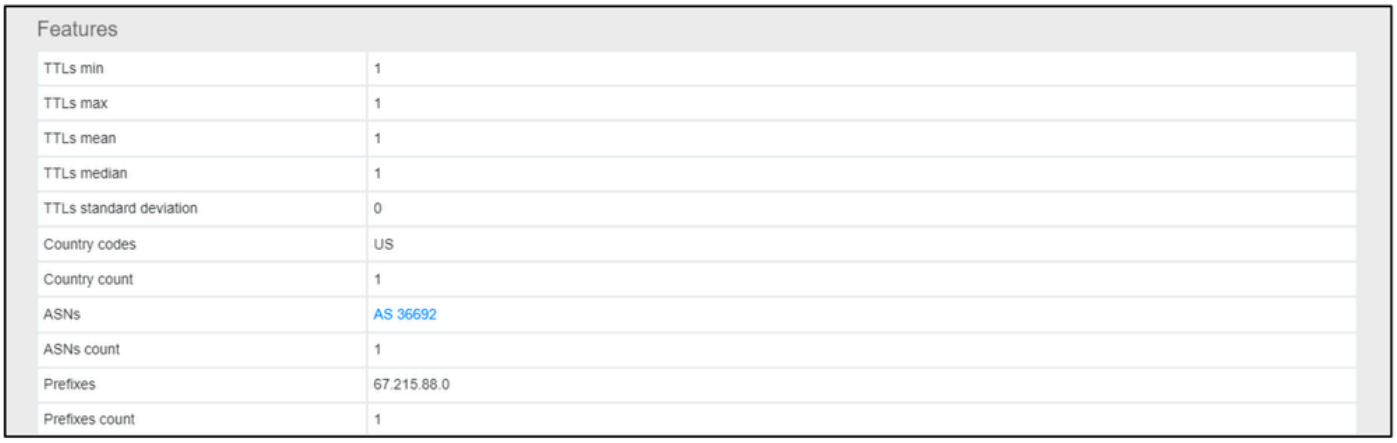
تمكن علامة التبويب "التحقيق" المستخدم من البحث في المعلومات المتعلقة باسم المضيف أو عنوان URL أو ASN أو IP أو التجزئة أو عنوان البريد الإلكتروني. كما أنه يحتوي على معلومات مثل سجل WHO، ومعلومات DGA وما إلى ذلك.



360072263511



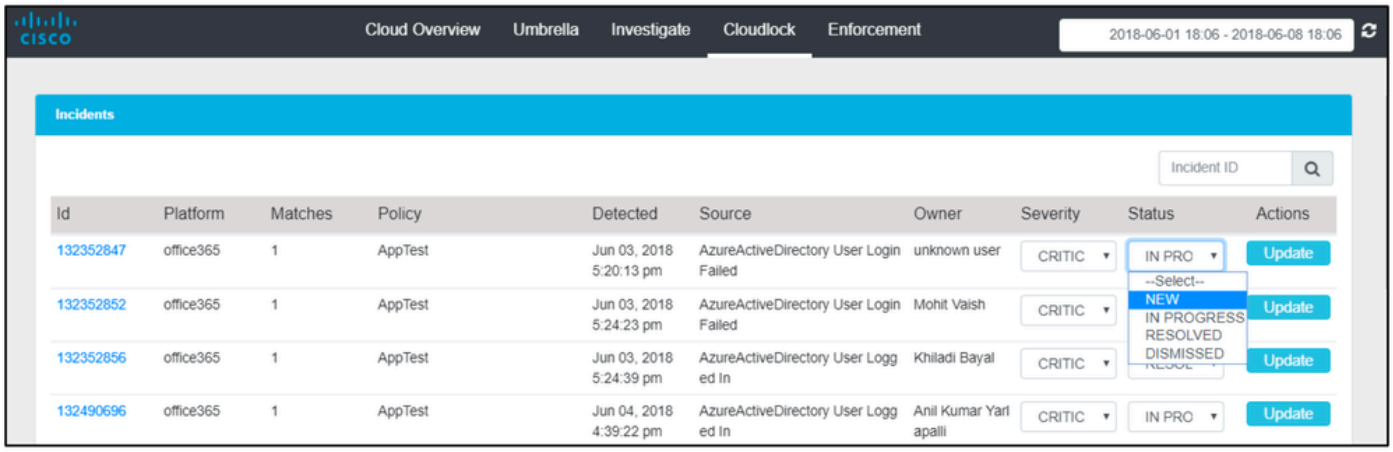
360072037472



360072037452

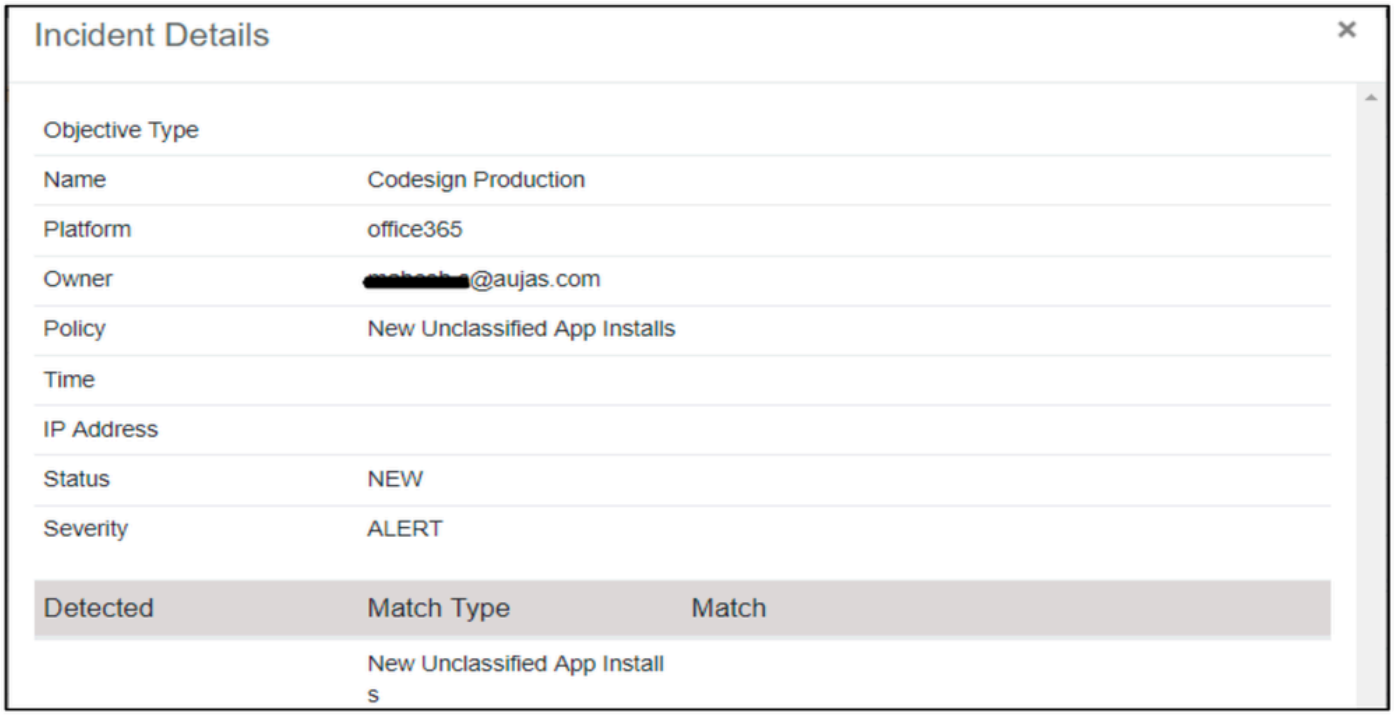
CloudLock

تتيح عالمة التبويب CloudLock للمستخدمين عرض المعلومات حول جميع الحوادث التي تم اكتشافها. كما يمكن للمستخدمين تحديث خطورة الحادث وحالته بتحديد القيم من القائمة المنسدلة والنقر فوق "تحديث".



360072268311

يمكن للمستخدمين تحديد وقت أي من الأحداث لعرض مزيد من التفاصيل حول الحدث.



360072042332

علامة تبويب فرض

تعرض علامة التبويب فرض معلومات عن المجالات التي يتم حظرها. يمكن للمستخدمين أيضا تحديد المجالات المحظورة وإلغاء حظرها من هذه الواجهة.

360072038472

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).