فهم واجهة برمجة تطبيقات فرض المظلة لعمليات التكامل المخصصة

المحتويات

المقدمة

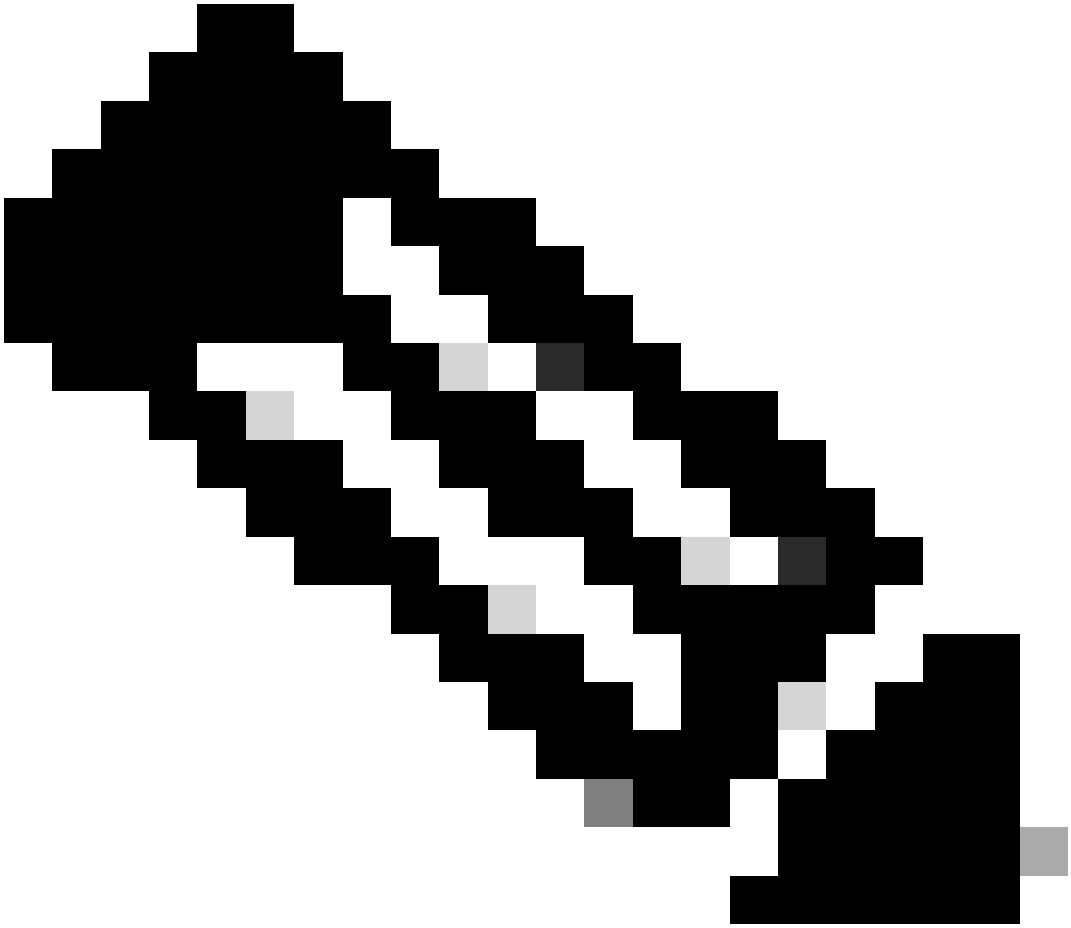
يصف هذا المستند واجهة برمجة تطبيقات فرض Umbrella (واجهة برمجة تطبيقات) لعمليات التكامل المخصصة.

ما هي واجهة برمجة تطبيقات Umbrella Enforcement API؟

تسمح واجهة برمجة تطبيقات Umbrella Enforcement API للشركاء والعملاء الذين لديهم بيئات منصات عمل SIEM/Threat Intelligence (TIP) المحلية الخاصة بهم لضخ الأحداث و/أو المعلومات الاستخباراتية الخاصة بالتهديدات في بيئة المظلة لديهم. يتم بعد ذلك تحويل هذه الأحداث بشكل فوري إلى حالة رؤية وتطبيق يمكن أن تمتد إلى ما هو أبعد من النطاق الأمني وبالتالي نطاق الأنظمة التي يمكن أن تكون قد ولدت تلك الأحداث أو المعلومات الإستخباراتية حول التهديدات.

يمكن أن تقوم واجهة برمجة التطبيقات بأحداث بتنسيق الحدث العام الموضح في [وثائق](#)

واجهة برمجة التطبيقات هذه ويمكن أن تدعم وظائف إضافة أو حذف أو قائمة.



ملاحظة: إذا لم يكن لديك واجهة برمجة تطبيقات Umbrella Enforcement API للتكاملات المخصصة في لوحة معلومات Umbrella الخاصة بك وتريد أن يكون لديك حق الوصول، فيرجى الاتصال بممثل Cisco Umbrella لديك.

لماذا أستخدمه؟

قد تقوم بالفعل بمعالجة وإدارة وإدارة وإدارة نظام معلومات التهديد والعمليات التي ينتج عنها الرغبة في إتخاذ إجراءات في المجالات التي يتم تحديدها على أنها ضارة أو مشبوهة. في هذه الحالة، بعد إتخاذ قرار بأن الحدث يجب أن يتم إتخاذ إجراء بشأنه (على سبيل المثال، تحويله إلى حماية)، بدلا من إضافة الحماية يدويا إلى Umbrella لأغراض الإنفاذ، يمكنك إستخدام واجهة برمجة التطبيقات (API) الخاصة بالإنفاذ لأتمتة هذه العملية وفرض الحماية بشكل فوري استنادا إلى المجالات المرتبطة بالحدث.

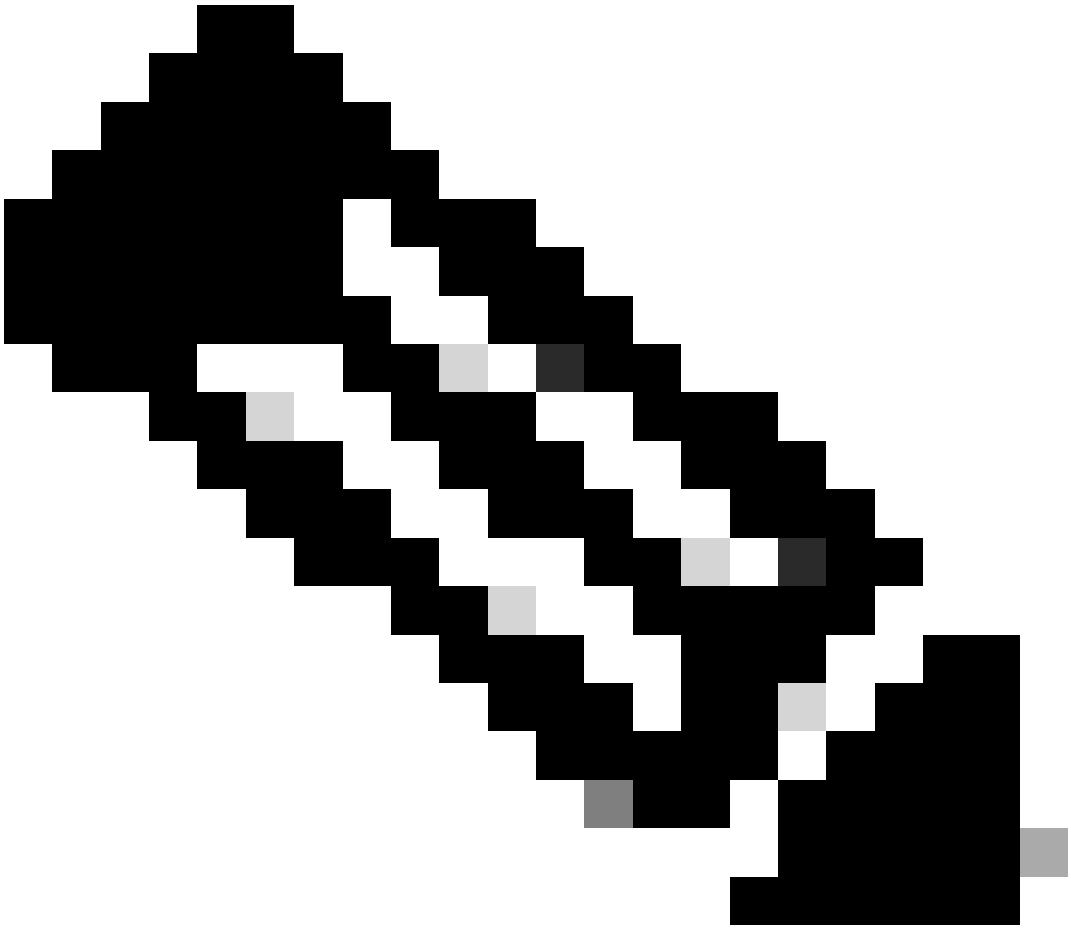
وهذا يسمح لفريق الأمن لديك بتركيز وقته وجهوده على التحقيقات بدلا من التهيئة الجارية لشركة Umbrella. فهي تسمح لفريق الأمان لديك بالبقاء داخل أدواتهم وعملياتهم

بدلا من الاضطرار إلى الانتقال إلى لوحة معلومات Umbrella لتحديث قوائم الوجهة. وفي الأساس، يمكنك إنشاء قائمة وجهة في Umbrella من مصدر خارجي تقوم بإدارته مباشرة من خلال واجهة برمجة التطبيقات، ثم أختر حظر تلك الوجهات للهويات ضمن Umbrella.

كيف أستخدمه؟

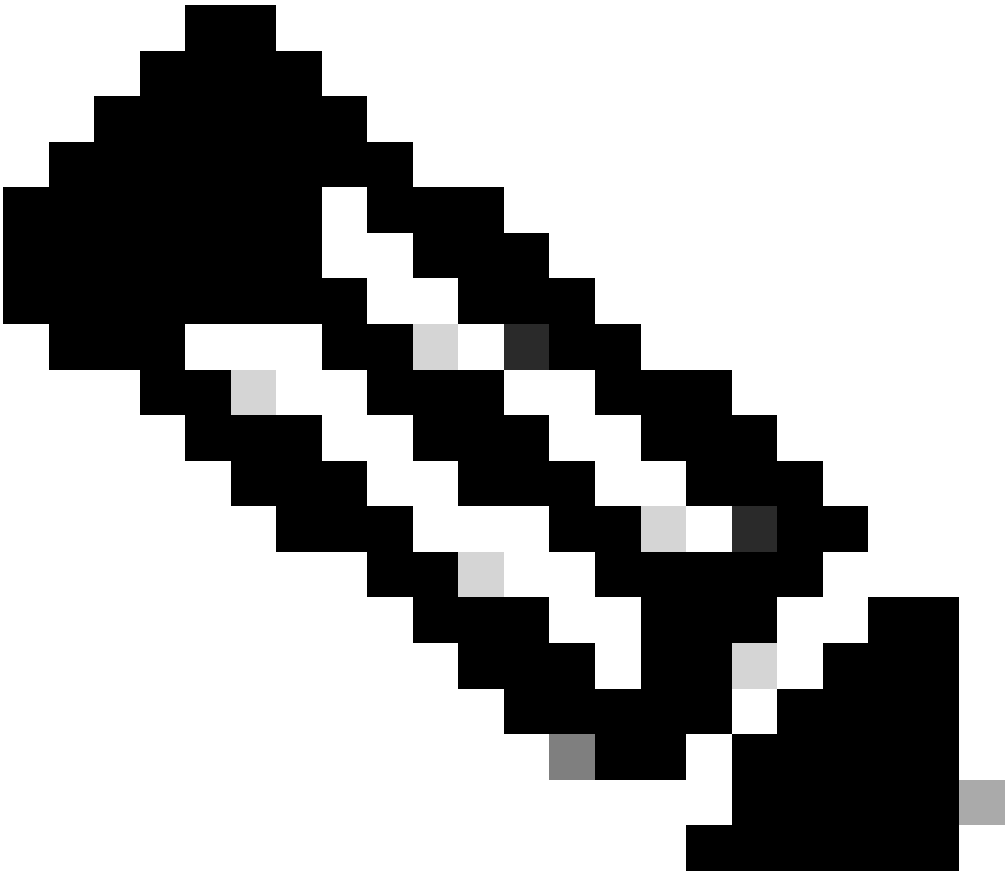
إضافة حدث إلى واجهة برمجة التطبيقات

بمجرد إضافة حدث، يحاول Enforcement إستخلاص مجالات من الحدث.



ملاحظة: تتم إضافة دعم عناوين IP وعناوين URL في المستقبل.

- يمكن أن يحتوي الحدث على أي مقدار من تفاصيل الحدث الأصلي تحبه، لكن يجب أن يلتزم بالمواصفات الموصوفة في وثائق واجهة برمجة التطبيقات.



ملاحظة: يمكن إضافة دعم لتفاصيل الحدث الظاهر داخل لوحة معلومات Umbrella في المستقبل.

- إذا تم إستخراج مجال، فقد تم التحقق منه بواسطة الرسم البياني Cisco Umbrella Security لضمان أنه ليس مجال جديد معروف من المحتمل أن يؤدي إلى نتائج إيجابية خاطئة أو أنه قد يعتبر ضارا بالفعل بواسطة الرسم البياني Cisco Umbrella Security.
- إذا نجح في التحقق من الصحة (على سبيل المثال، حظره غير معروف وآمن)، فإنه تتم إضافته إلى قائمة الوجهة المرتبطة بهذا الدمج المخصص ويتم عرضه داخل لوحة معلومات Umbrella كفئة أمان مخصصة.
- يمكن حظر فئة الأمان المخصص أو السماح بها على أساس كل سياسة، للسماح بكل من الإنفاذ النشط أو "التدقيق" السلبي للطلبات المشبوهة.

سرد مجالات قائمة واجهة برمجة تطبيقات (API) للتنفيذ

- إذا تضمن سير العمل إلغاء حظر المجالات التي تم حظرها بسبب أحداث تم حقنها مسبقا، يوفر طلب LIST كافة المجالات المضمنة حاليا في قائمة الوجهة المقترنة بهذا التكامل.

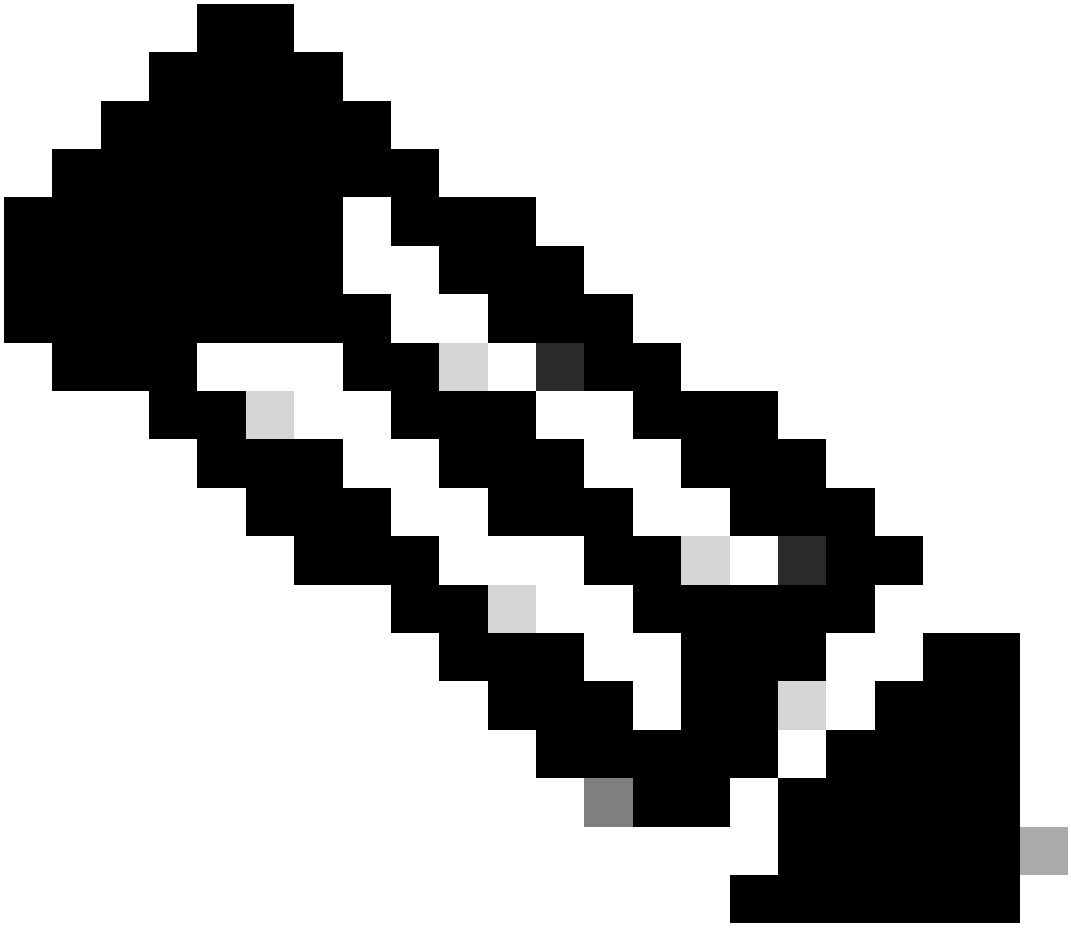
حذف مجال من قائمة الوجهة برمجة التطبيقات الخاصة بالإنفاذ

- إذا تضمن سير العمل إلغاء حظر المجالات التي تم حظرها بسبب أحداث تم حقنها مسبقًا، يسمح لك طلب DELETE بإزالة مجال من قائمة الوجهة المقترنة بهذا التكامل.
- إذا تم توجيه طلب DNS وارد من إحدى هويات Umbrella الخاصة بك إلى مجال في قائمة وجهة التكامل المخصص، يتم حظره أو السماح به وفقًا لإعداد أمان التكامل المخصص المرتبط بالنهج الذي قام بتشغيله.
- يتم تسجيل النتائج مع جميع أحداث Umbrella الأخرى، التي يمكن الوصول إليها عبر Amazon S3 باستخدام تكامل S3. وبالتالي، يمكن بشكل إختياري عبر Activity Search أو إلى SIEM/TIP وإغلاق حلقة حركة المرور المرتبطة بالتكامل المخصص مرة أخرى إلى قائمة الوجهة المرتبطة بالتكامل المخصص مرة أخرى إلى SIEM/TIP وإغلاق حلقة الملاحظات.

تطبيقات Enforcement API برمجة واجهة إستخدام عبر المرور

الخطوة 1: إنشاء التكامل المخصص

يمكنك الحصول على ما يصل إلى 10 عمليات تكامل مخصصة في نفس الوقت.



ملاحظة: إذا كانت المؤسسة عبارة عن مؤسسة تابعة ل MSP أو MSSP أو MOC Umbrella، تظهر عمليات التكامل المخصصة المشتركة من مستوى وحدة التحكم قبل عمليات التكامل التي تم إنشاؤها على مستوى المؤسسة التابعة.

---

1. في Umbrella، انتقل إلى السياسات > مكونات السياسة > عمليات التكامل وانقر إضافة.
2. قم بإضافة اسم للتكامل المخصص وانقر فوق إنشاء.
3. قم بتوسيع التكامل المخصص الجديد، تحقق من تمكين، قم بنسخ عنوان URL الخاص بالتكامل ثم انقر فوق حفظ.

الخطوة 2: قم بإنشاء برنامج (برامج) نصي مخصص.

1. راجع البرامج النصية generate_event وdelete_domain العينة في الملحق الخاص بهذا المستند أو استخدم وثائق واجهة برمجة التطبيقات (API) لإنشاء البرامج النصية الخاصة بك لإنشاء الطلبات المنسقة بشكل صحيح لإنشاء الأحداث أو حذف المجالات أو سردها. ستحتاج إلى إستخدام عنوان URL الخاص بالتكامل المخصص في هذه البرامج

النصية التي تمضي قدما.

الخطوة 3: إدخال حدث عينة

1. أستخدم النص البرمجي الذي قمت بإنشائه لإدخال حدث في التكامل المخصص. في مثالنا، حقن حدث يحتوي على المجال "creditcards.com".

الخطوة 4: تحقق من قائمة الوجهة في لوحة معلومات المظلة

1. ارجع إلى الإعدادات > التكاملات وفي الجدول قم بتوسيع التكامل المخصص.
2. طقطقة يري مجال. تظهر قائمة يمكن البحث فيها للمجالات المضافة ويكون نموذج الحدث من الخطوة 4 الآن في القائمة.

الخطوة 5: تحقق من سجل تدقيق المسؤول.

1. هناك طريقة أخرى للتحقق من النشاط المرتبط بالتكامل المخصص تتمثل في مراجعة سجل تدقيق المسؤول.
2. انتقل إلى إعداد التقارير > سجل تدقيق المسؤول.
3. تحت المرشحات، قم بإدخال اسم التكامل المخصص الخاص بك في مرشح حسب الهويات والإعدادات، ثم انقر تشغيل مرشح.

عندما تقوم بتوسيع الإدخال، سترى الآن الحدث الذي أدى إلى إضافة نموذج الحدث (creditcards.com) إلى الدمج المخصص.

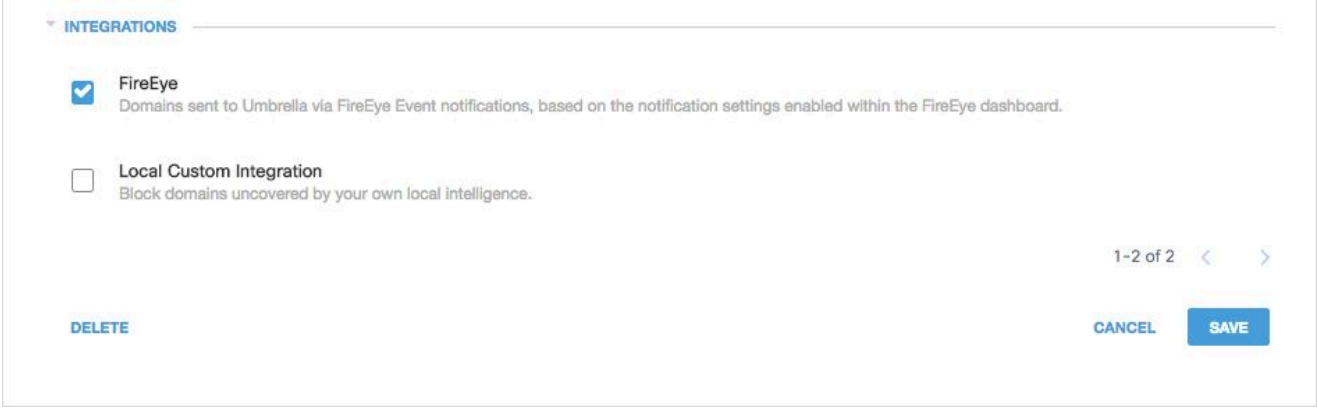
الخطوة الاختيارية: سرد المجالات أو حذفها

قد ترغب أيضا في الاختبار للتأكد من إمكانية سرد المجالات في التكامل المخصص وحذف المجالات في حالة عدم رغبتك في فرض فرض هذا المجال أو وضعه في التكامل الخاص بك. أستخدم الخطوات الموضحة في واجهة برمجة التطبيقات وثائق لسرد المجالات وحذفها.

تكوين إعدادات التأمين

الآن بعد التحقق من صحة إمكانية إدخال الأحداث (ومسرد المجالات وحذفها إختياري)، يمكنك تكوين ما تريد حدوثه لطلبات DNS من الهويات الخاصة بك الموجهة للمجالات في فئة أمان التكامل المخصص.

1. انتقل إلى السياسات > إعدادات التأمين وتحت التكاملات، تحقق من التكامل الذي تم تمكينه (في هذا المثال، FireEye) وانقر حفظ.

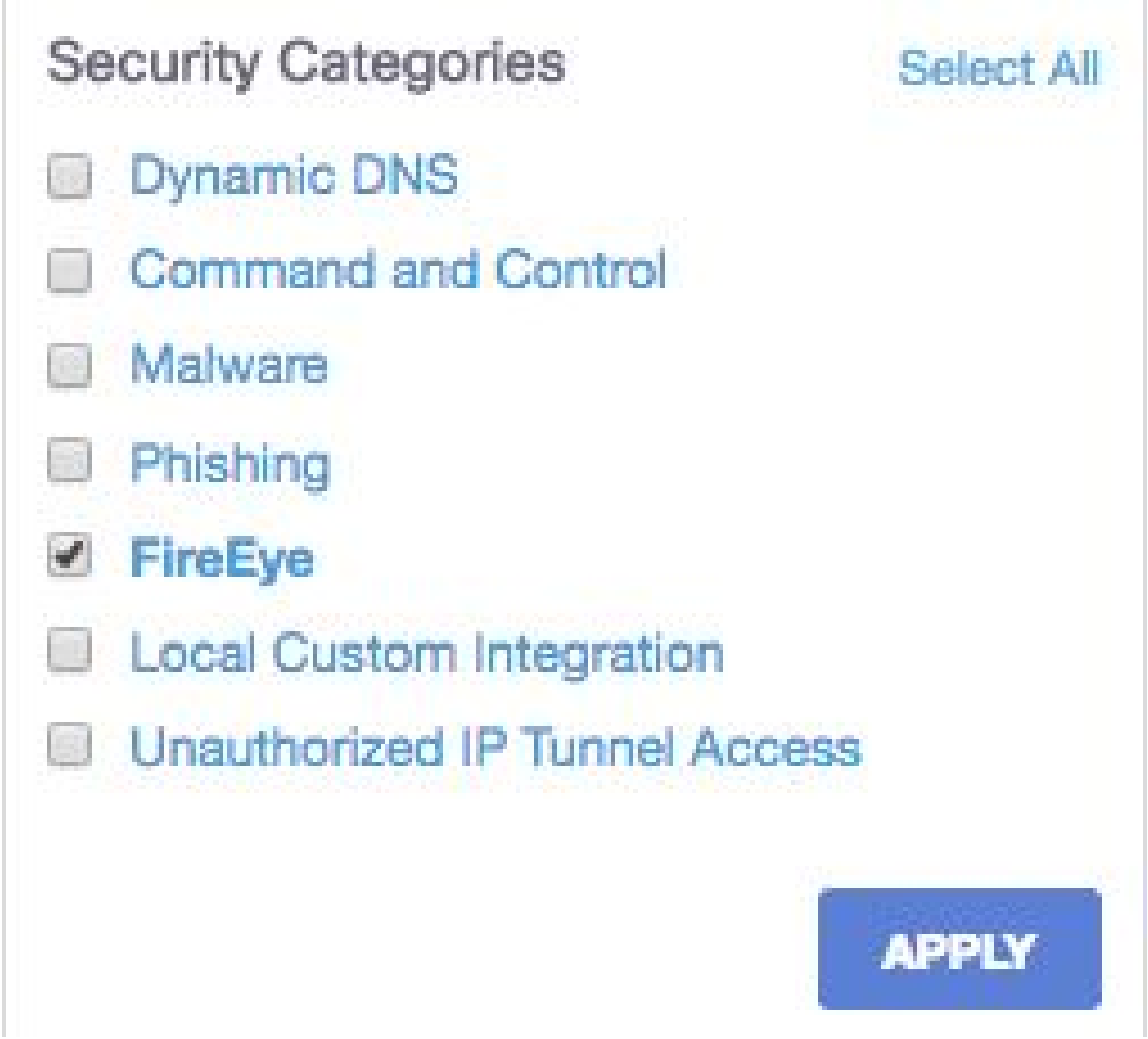


115014145103

عرض التقارير للتكامل المخصص

قم بإنشاء طلبات DNS من إحدى هوياتك (على سبيل المثال، الشبكات أو أجهزة الكمبيوتر المتجولة) المخصصة للمجال في التكامل المخصص ("creditcards.com" في المثال الخاص بنا). من منظور العميل، يمكنك الآن رؤية الحظر المناسب أو السماح بالنتيجة وفقا لكيفية تكوين إعدادات الأمان الخاصة بك.

1. انتقل إلى Reporting > Activity Search وتحت فئات الأمان حدد التكامل المخصص (في هذا المثال FireEye) لتصفية التقرير لإظهار فئة الأمان ل FireEye فقط.

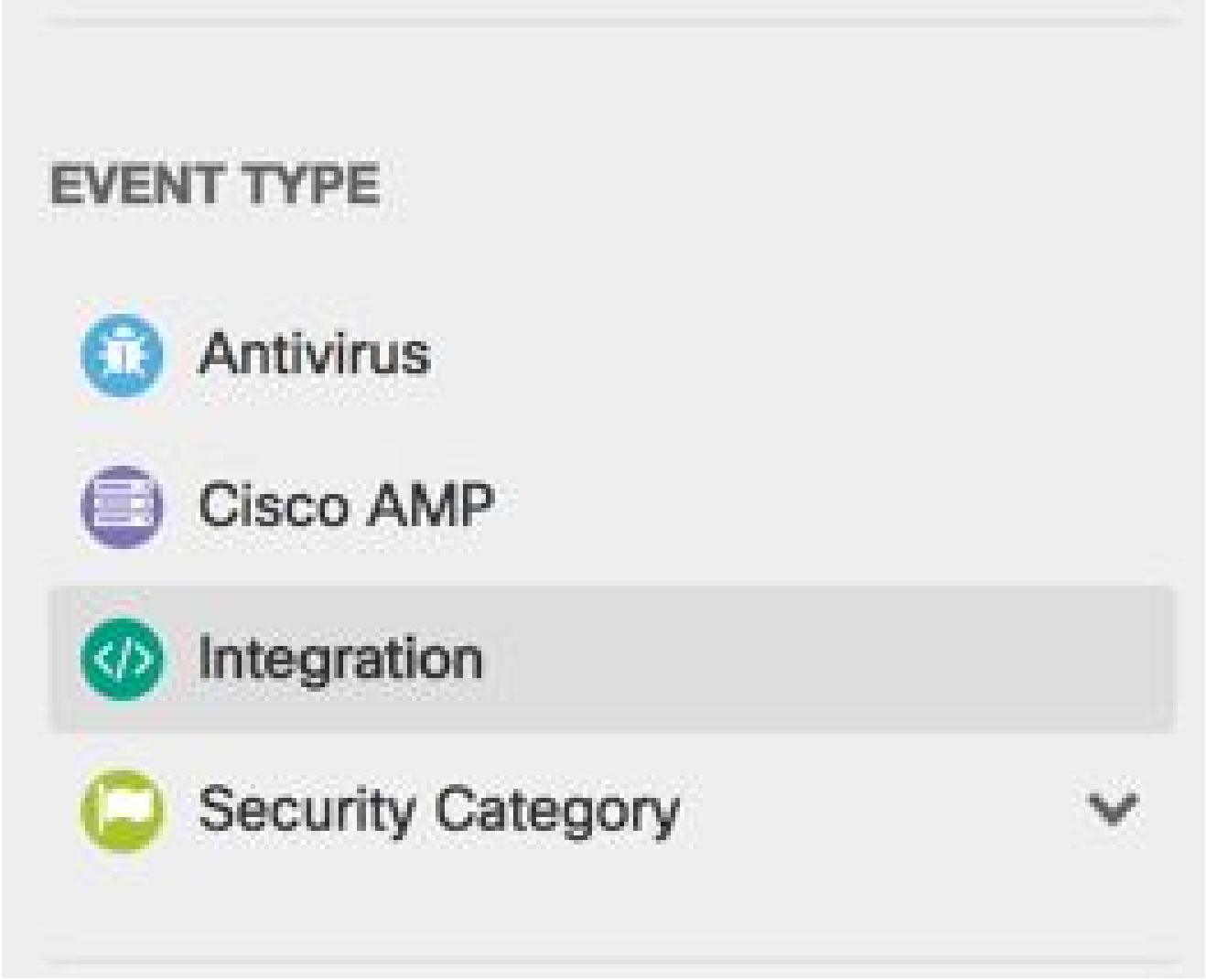


115013981706

2. انقر فوق تطبيق للاطلاع على نشاط الفترة الزمنية المحددة في التقرير.

كما يمكنك أيضا عرض تقرير وحدة تخزين النشاط لعرض تقارير اللقطة أو الإتجاه عبر حساب الوقت بما في ذلك التكامل (التكامل) المخصص.

1. انتقل إلى التقارير > وحدة تخزين نشاط الأمان.
2. تحت نوع الحدث، حدد التكامل.



115013982286

قم بتكوين تكامل S3 لتخزين السجلات واستهلاكها (إختياري)

إذا أردت بعد ذلك تغذية سجلات Umbrella التي تحتوي على كافة طلبات بيئتك مرة أخرى في بيئة SIEM/TIP، يمكنك القيام بذلك باستخدام تكامل S3، الذي يسمح لك بإعادة أحداث نشاط DNS.

الملحق: أمثلة البرامج النصية

توفر هذه البرامج الإرشادية إرشادات حول كيفية توليد حدث للتكامل المخصص. الرجاء إستبدال قيمة CustomerKey من التكامل في كل الكتابين. ملاحظة، يتم توفير هذه البرامج النصية كأمثلة وقد يلزم التخصيص أو التحديثات.

generate_event.pl:

```
#!/usr/bin/perl -w

# Custom integration - ADD EVENT URL

my $cust_key = 'https://s-platform.api.opendns.com/1.0/events?customerKey=XXXXXXXX-XXXX-XXXX-XXXX-XXXXX

die "Usage: $0 - Please supply a domain\n" if @ARGV < 1;
my $domain = $ARGV[0];

my $json_blob = "{
    \"alertTime\" : \"2013-02-08T11:14:26.0Z\",
    \"deviceId\" : \"ba6a59f4-e692-4724-ba36-c28132c761de\",
    \"deviceVersion\" : \"13.7a\",
    \"dstDomain\" : \"$domain\",
    \"dstUrl\" : \"http://$domain/a-bad-url\",
    \"eventTime\" : \"2013-02-08T09:30:26.0Z\",
    \"protocolVersion\" : \"1.0a\",
    \"providerName\" : \"Security Platform\"
}";

my $curl_request = "curl '" . $cust_key . "' -v -X POST -H 'Content-Type: application/json' -d '" . $js

my $results = exec($curl_request);
```

delete_domain.pl:

```
#!/usr/bin/perl -w

# Custom integration - DELETE URL

my $cust_key = 'https://s-platform.api.opendns.com/1.0/domains?customerKey=XXXXXXXX-XXXX-XXXX-XXXX-XXXX

die "Usage: $0 - Please supply a domain\n" if @ARGV < 1;
my $domain = $ARGV[0];

my $curl_request = "curl '" . $cust_key . "&where[name]=" . $domain . "' -v -i -g -X DELETE -H 'Content
my $results = exec($curl_request);
```

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).