الحماية من فقدان البيانات - أستكشاف أخطاء التصنيفات وإصلاحها وحالات فشل المسح الضوئي

المحتويات

المقدمة

يصف هذا المستند الأساليب الشائعة لاستكشاف أخطاء التصنيف وإصلاحها وحالات الفشل في المسح الضوئي (أو حالات الفشل) المتعلقة بمنع فقدان البيانات (DLP) على جهاز أمان البريد الإلكتروني (ESA).

المتطلبات الأساسية

- ESA الذي يشغل نظام التشغيل AsyncOS 11.x أو الأحدث.
- مفتاح ميزة DLP مثبت وقيد الاستخدام.

معلومات مهمة

من المهم للغاية ملاحظة أن تقنية DLP على ESA هي ميزة سهلة الاستخدام بمجرد التوصيل بمعنى أنه يمكنك تمكينها وإنشاء سياسة وبدء المسح بحثا عن بيانات حساسة، ومع ذلك، يجب أيضا أن تكون على دراية بأن أفضل النتائج لن تتحقق إلا بعد ضبط ميزة DLP لتتناسب مع المتطلبات الخاصة بشركتك. وقد يتضمن ذلك أمورا مثل أنواع سياسات DLP وتفاصيل مطابقة النهج وتعديل مقياس الخطورة والتصفية والتخصيصات الإضافية.

أمثلة سجل الانتهاك مقابل لا يوجد انتهاك

فيما يلي بعض الأمثلة على انتهاكات DLP التي قد تراها ضمن سجلات البريد و/أو تعقب الرسائل. سيتضمن سطر السجل طابع وقت ومستوى تسجيل وعدد متوسط وانتهاك أو لا يوجد انتهاك وعامل خطورة ونهج تم مطابقته.

```
Thu Jul 11 16:05:28 2019 Info: MID 40 DLP violation. Severity: CRITICAL (Risk Factor: 96). DLP
.'policy match: 'US HIPAA and HITECH
```

```
Thu Jul 11 16:41:50 2019 Info: MID 46 DLP violation. Severity: LOW (Risk Factor: 24). DLP policy
.'(match: 'US State Regulations (Indiana HB 1101
```

عندما لا يوجد انتهاك، بعد ذلك سجلات البريد و/أو تعقب الرسائل سوف يقوم ببساطة بتسجيل *DLP ما من انتهاك*.

```
Mon Jan 20 12:59:01 2020 Info: MID 26245883 DLP no violation
```

قائمة إختيار أستكشاف الأخطاء وإصلاحها

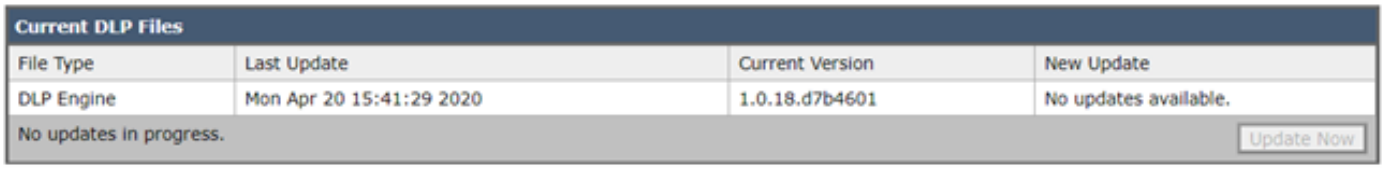
العناصر المتوفرة أدناه هي عناصر شائعة يمكن مراجعتها عند التعامل مع حالات سوء تصنيف DLP أو حالات الفشل/الإخفاق في المسح الضوئي.

ملاحظة: هذه ليست قائمة شاملة. رجاء اتصل ب cisco TAC إن يتلقى أنت شيء أنت تريد أن يرى يتضمن.

تأكيد إصدار محرك DLP

إن تحديثات محرك DLP ليست تلقائية بشكل افتراضي، لذلك فمن المهم التأكد من أنك تقوم بتشغيل أحدث إصدار يتضمن أي تحسينات أو إصلاحات للأخطاء حديثة.

يمكنك الانتقال إلى *منع فقدان البيانات ضمن خدمات الأمان* في واجهة المستخدم الرسومية (GUI) لتأكيد إصدار المحرك الحالي ولمعرفة ما إذا كان هناك أي تحديثات متوفرة. إذا كان هناك تحديث متوفر، فيمكنك النقر فوق *تحديث الآن* لإجراء التحديث.

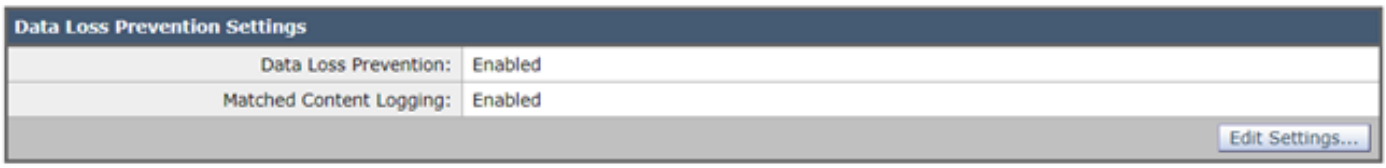


تمكين تسجيل المحتوى المتطابق

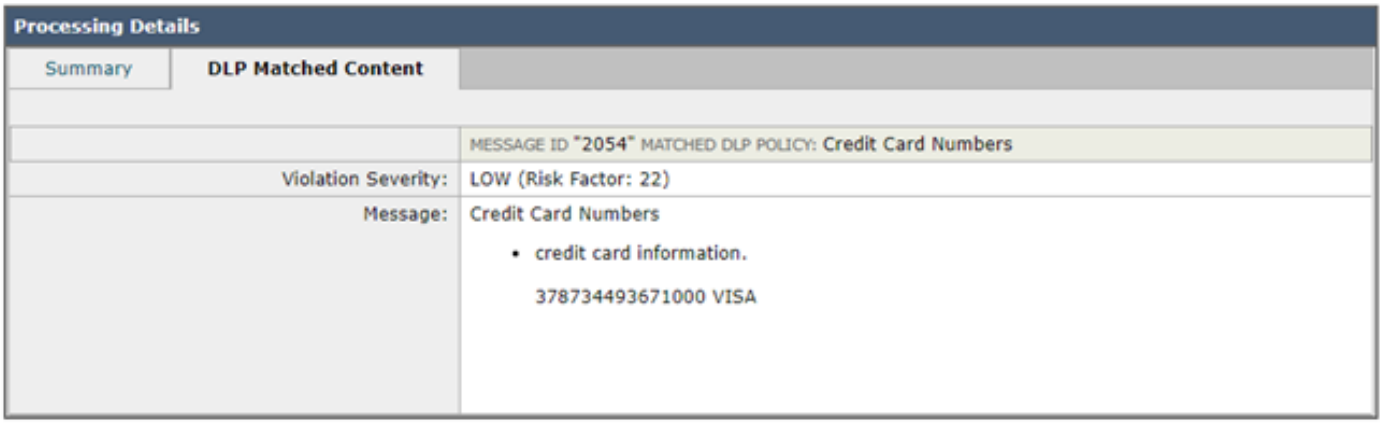
يوفر DLP خيار تسجيل المحتوى الذي ينتهك سياسات DLP الخاصة بك، بالإضافة إلى المحتوى المحيط. ويمكن بعد ذلك عرض هذه البيانات في *تعقب الرسائل* للمساعدة في تعقب المحتوى الموجود داخل البريد الإلكتروني الذي قد يتسبب في حدوث انتهاك معين.

تحذير: من المهم معرفة أنه إذا تم تمكين هذا المحتوى، فقد يتضمن بيانات حساسة مثل أرقام بطاقات الائتمان وأرقام الضمان الاجتماعي، وما إلى ذلك.

يمكنك الانتقال إلى *منع فقدان البيانات ضمن خدمات الأمان* في واجهة المستخدم الرسومية (GUI) لمعرفة ما إذا تم تمكين *تسجيل المحتوى المتطابق* أم لا.



مثال على تسجيل المحتوى المطابق الذي تمت مشاهدته في تعقب الرسائل



مراجعة تكوين سلوك المسح الضوئي

كما سيؤثر تكوين سلوك المسح الضوئي على ESA على وظائف الفحص باستخدام بروتوكول DLP. بالنظر إلى لقطة الشاشة أدناه كمثال، والذي يحتوي على **الحد الأقصى لحجم** **للمرفق** للمسح الضوئي الذي تم تكوينه **وهو 5 أمتار**، فإن أي شيء أكبر قد يتسبب في فقد فحص DLP. أيضا، يعد **الإجراء الخاص بالمرفقات ذات** إعداد **أنواع MIME** عنصرا مشتركا آخر ترغب في مراجعته. يجب تعيين هذا إلى الإعداد الافتراضي ل **التخطي** بحيث يتم تخطي أنواع MIME المدرجة ويتم مسح كل شيء آخر. في حالة ضبطه على "مسح ضوئي"، فسنعمل *فقط على مسح أنواع MIME* المدرجة في الجدول.

وبالمثل، قد تؤثر الإعدادات الأخرى المذكورة هنا على المسح الضوئي ل DLP ويجب أخذها في الاعتبار وفقا لمحتوى المرفق/البريد الإلكتروني.

يمكنك التنقل إلى *سلوك المسح الضوئي ضمن خدمات الأمان* في واجهة المستخدم الرسومية (GUI)، أو من خلال تشغيل الأمر **scanConfig** داخل واجهة سطر الأوامر (CLI).

Attachment Type Mappings

Add Mapping... | Import List...

Fingerprint / MIME	Type	Edit	Delete
MIME Type	audio/*	Edit...	
MIME Type	video/*	Edit...	
MIME Type	image/*	Edit...	
Fingerprint	Media	Edit...	
Fingerprint	Image	Edit...	

Export List...

Global Settings

Action for attachments with MIME types / fingerprints in table above:	Skip
Maximum depth of attachment recursion to scan:	5
Maximum attachment size to scan:	5M
Attachment Metadata scan:	Enabled
Attachment scanning timeout:	30 seconds
Assume attachment matches pattern if not scanned for any reason:	No
Assume zip file to be unscannable if files in the archive cannot be read?	No
Action when message cannot be deconstructed to remove specified attachments:	Deliver
Bypass all filters in case of a content or message filter error:	Yes
Encoding to use when none is specified:	US-ASCII
Convert opaque-signed messages to clear-signed (S/MIME unpacking):	Disabled
Safe Print settings	Maximum File Size: 5M; Maximum Page Count: 10; Document Quality: 70
Actions for Unscannable Messages due to decoding errors found during URL Filtering Actions:	Disabled
Action when a message is unscannable due to extraction failures:	Deliver As Is
Action when a message is unscannable due to RFC violations:	Disabled

Edit Global Settings...

مراجعة تكوين مقياس الخطورة

ستكون حدود مقياس الخطورة الافتراضية كافية لمعظم البيئات، ومع ذلك، إذا كنت بحاجة إلى تعديلها للمساعدة في مطابقة السالب الكاذب (FN) أو موجب كاذب (FP)، عندئذ يمكنك القيام بذلك. يمكنك أيضا تأكيد أن سياسة DLP تستخدم العتبات الافتراضية الموصى بها عن طريق إنشاء نهج وهمي جديد ثم مقارنتها.

ملاحظة: ستختلف مستويات السياسات المختلفة المحددة مسبقا (مثل HIPAA في الولايات المتحدة مقابل PCI-DSS).

Severity Scale:

IGNORE	LOW	MEDIUM	HIGH	CRITICAL
0 - 34	35 - 54	55 - 72	73 - 87	88 - 100

Edit Scale...

مراجعة عناوين البريد الإلكتروني التي تمت إضافتها إلى حقول المرسلين والمستلمين

تحقق من أن أي إدخالات يتم إدخالها في أي من هذين الحقلين تطابق الحالة الصحيحة لعناوين البريد الإلكتروني للمرسل و/أو المستلم. إن حقل المرسلين والمستلمين للتصفية **حساس لحالة الأحرف**. لن يتم تشغيل نهج DLP إذا كان عنوان البريد الإلكتروني يبدو مثل "TestEmail@mail.com" في عميل البريد وتم إدخاله ك "testemail@mail.com" في هذه الحقول.

معلومات ذات صلة

- جهاز أمان البريد الإلكتروني من Cisco - أدلة المستخدم النهائي
- ما هو منع فقدان البيانات؟
- تشغيل انتهاك DLP لاختبار سياسة HIPAA على ESA

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).