تشغيل انتهاك DLP لاختبار سياسة HIPAA على ESA

المحتويات

المقدمة

يوضح هذا المستند كيفية إختبار إمكانية نقل التأمين الصحي وخضوعه للمساءلة (HIPAA) ومنع فقدان البيانات (DLP) بمجرد تمكين DLP على سياسة البريد الصادر لديك على جهاز أمان البريد الإلكتروني من Cisco (ESA).

تشغيل انتهاك DLP لاختبار سياسة HIPAA

تقدم هذه المقالة بعض المحتويات الحقيقية، التي تم تعديلها لحماية الأشخاص، للاختبار ضد سياسة DLP على ESA لديك. تم تصميم هذه المعلومات لإطلاق سياسة DLP الخاصة بمؤشر HIPAA وتقنية المعلومات الصحية للصحة الاقتصادية والإكلينيكية (HITECH)، كما يتم تشغيل سياسات DLP الأخرى مثل رقم الضمان الاجتماعي (SSN) و CA AB-1298 و CA SB-1386 وما إلى ذلك. أستخدم المعلومات عندما تقوم بإرسال بريد إلكتروني للاختبار من خلال ESA أو عندما تستخدم أداة **التتبع**.

ملاحظة: يجب إستخدام شبكة SSN صالحة أو يساء إستخدامها بشكل شائع في الإخراج حيث يتم مزجها.

ملاحظة: بالنسبة لنهج HIPAA و HITECH DLP، تأكد من أنك قمت بتكوين أرقام تعريف مخصصة على النحو الموصى به. أرقام تعريف المرضى (التخصيص الموصى به) أو معرف المزود الوطني الأمريكي أو رقم الضمان الاجتماعي وقواميس الرعاية الصحية في الولايات المتحدة. أنت ينبغي يتلقى هذا شكلت in order to أطلقت بشكل صحيح.

```
                                                                Procedure Notes
                                                                 Progress Notes
                                    Archie M Johnson Tue Jun 30, 2009 10:31 AM Pended
                                                                     June 30, 2009
                                          Patient Name: Gina, Lucas DOB: 01/23/1945
                                                          Telephone #: (559) 221-2345
                                                  [[[SS#: [[[PLACE SSN HERE
--------------------------------------------------------------------------------
                                                                  Insurance: UHC
                                    ({How was the patient referred to the office: *** ({:20
                   {Is a family member currently being seen by the requested physician? {YES/NO:63
                                          *** : If yes, what is the family members name
                                                  *** ?Previous PCP / Medical Group
                                                       *** .Physician Requested: Dr
                                                                         :REASON
                                    {Get established, no current problems: {YES/NO:63 (1
                                                    {Chronic Issues: {YES/NO:63 (2
```

{Specific Problems: {YES/NO:63 (3
:Description of specific problem and/or chronic conditions
.{OPMED SYMPTOMS:11123} the problem started {1-10:5044} {Time Units:10300}
{Any Medications that may need a refill? {YES/NO:63
*** :Current medications

Archie M Johnson
Community Health Program Assistant Chief
Family Practice & Community Medicine
221-1234 (559)
Lucas Gina Wed Jul 8, 2009 10:37 AM Pended
ELECTIVE NEUROLOGICAL SURGERY
HISTORY & PHYSICAL
.CHIEF COMPLAINT: No chief complaint on file
*** HISTORY OF PRESENT ILLNESS: Mary A Xxtestfbonilla is a
Past Medical History
Diagnosis Date
Other Deficiency of Cell-Mediated Immunity •
Def of cell-med immunity
Erythema Multiforme •
Allergic Rhinitis, Cause Unspecified •
Allergic rhinitis
Unspecified Osteoporosis 12/8/2005 •
DEXA scan - 2003
Esophageal Reflux 12/8/2005 •
priolosec, protonix didn't work, lost weight
Primary Hypercoagulable State •
MUTATION FACTOR V LEIDEN
Unspecified Glaucoma 1/06 •
OPIOID PAIN MANAGEMENT 1/24/2007 •
Patient is on opioid contract - see letter 1/24/2007
Chickenpox with Other Specified Complications 2002 •

التحقق من الصحة

ستختلف النتائج، استنادا إلى إجراءات الرسائل التي قمت بتعيينها لنهج DLP الخاص بك. قم بتكوين وتأكيد الإجراءات الخاصة بك للجهاز باستخدام مراجعة من واجهة المستخدم الرسومية (GUI): **سياسات البريد > تخصيصات سياسة DLP > إجراءات الرسائل**.

في هذا المثال، يتم تعيين **الإجراء الافتراضي** على عزل انتهاكات DLP إلى العزل الخاص بالنهج وكذلك تعديل سطر موضوع الرسالة باستخدام التعليق المسبق "[انتهاك DLP]".

يجب أن يظهر mail_log مشابها لهذا عندما تقوم بإرسال المحتوى السابق كبريد إلكتروني إختبار:

(Wed Jul 30 11:07:14 2014 Info: New SMTP ICID 656 interface Management (172.16.6.165
address 172.16.6.1 reverse dns host unknown verified no
Wed Jul 30 11:07:14 2014 Info: ICID 656 RELAY SG RELAY_SG match 172.16.6.1 SBRS
not enabled
Wed Jul 30 11:07:14 2014 Info: Start MID 212 ICID 656
<Wed Jul 30 11:07:14 2014 Info: MID 212 ICID 656 From: <my_user@gmail.com
<Wed Jul 30 11:07:14 2014 Info: MID 212 ICID 656 RID 0 To: <test_person@cisco.com
Wed Jul 30 11:07:14 2014 Info: MID 212 Message-ID
'<A85EA7D1-D02B-468D-9819-692D552A7571@gmail.com>'
'Wed Jul 30 11:07:14 2014 Info: MID 212 Subject 'My DLP test
<Wed Jul 30 11:07:14 2014 Info: MID 212 ready 2398 bytes from <my_user@gmail.com
Wed Jul 30 11:07:14 2014 Info: MID 212 matched all recipients for per-recipient
policy DEFAULT in the outbound table
Wed Jul 30 11:07:16 2014 Info: MID 212 interim verdict using engine: CASE spam
negative
Wed Jul 30 11:07:16 2014 Info: MID 212 using engine: CASE spam negative

```
Wed Jul 30 11:07:16 2014 Info: MID 212 interim AV verdict using Sophos CLEAN
Wed Jul 30 11:07:16 2014 Info: MID 212 antivirus negative
Wed Jul 30 11:07:16 2014 Info: MID 212 Outbreak Filters: verdict negative
Wed Jul 30 11:07:16 2014 Info: MID 212 DLP violation
(Wed Jul 30 11:07:16 2014 Info: MID 212 quarantined to "Policy" (DLP violation
Wed Jul 30 11:08:16 2014 Info: ICID 656 close
```

من أداة **التتبع**، يجب أن ترى النتائج معروضة مثل هذه الصورة عند إستخدام المحتوى السابق في نص الرسالة:

Data Loss Prevention Processing	
Result:	Matches Policy: HIPAA and HITECH Violation Severity: LOW (Risk Factor: 22)
Actions:	replace-header("Subject", "[DLP VIOLATION] $subject") quarantine("Policy")

استكشاف الأخطاء وإصلاحها

تأكد من تحديد سياسة DLP المطلوبة من **نهج البريد > مدير سياسة DLP > إضافة سياسة DLP..** في واجهة المستخدم الرسومية.

راجع نهج DLP كما تمت إضافته وتأكد من تحديد تصنيف مطابقة المحتوى ومن صحة نمط التعبير العادي. تأكد أيضا من تكوين قسم AND الخاص **بالمطابقة مع الكلمات أو العبارات ذات الصلة**. التصنيفات هي مكونات الكشف الخاصة بمحرك DLP. يمكن إستخدامها في مجموعة أو بشكل فردي للتعرف على المحتوى الحساس.

ملاحظة: التصنيفات المحددة مسبقا غير قابلة للتحرير.

إذا لم ترى مشغل DLP بناء على المحتوى، راجع أيضا **نهج البريد > نهج البريد الصادر > DLP** وتأكد من تمكين نهج DLP المطلوب.

معلومات ذات صلة

- جهاز أمان البريد الإلكتروني من Cisco - أدلة المستخدم النهائي
- الأسئلة المتداولة حول ESA: كيف يمكنني تصحيح أخطاء كيفية معالجة رسالة بواسطة ESA؟
- SSA.gov: إساءة إستخدام أرقام الضمان الاجتماعي
- إختبار ال Regex على الإنترنت
- الدعم التقني والمستندات - Cisco Systems

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).