Инициируйте нарушение DLP для тестирования политики HIPAA по ESA

Содержание

Введение

Этот документ описывает, как протестировать закон о Мобильности и Отслеживаемости Медицинского страхования (HIPAA) Предотвращение потери данных (DLP), как только вы включили DLP на своей политике исходящей почты по вашей Cisco Email Security Appliance (ESA).

Инициируйте нарушение DLP для тестирования политики HIPAA

Эта статья предоставляет некоторое реальное содержание, которое модифицировалось для защиты людей, для тестирования против Политики DLP по ESA. Эта информация разработана для включения HIPAA и медицинских информационных технологий для Экономического и Клинического состояния (HITECH) политика DLP и также инициирует другую политику DLP как Номер социального страхования (SSN), CA AB 1298, CA SB 1386, и так далее. Используйте информацию при отправке тестового электронного письма через ESA или когда вы используете программное средство **трассировки**.

> **Примечание:** Необходимо использовать допустимый или обычно неправильно используемый SSN в выходных данных, где полужирный.

> **Примечание:** Для HIPAA и Политики DLP HITECH, гарантируйте настройку настроенных идентификационных номеров, как рекомендуется. Терпеливые Идентификационные номера (рекомендуемая кастомизация) US OR Национальный Идентификатор Поставщика Номер социального страхования US OR Словари Здравоохранения AND. Необходимо было настроить это для надлежащего инициирования.

```
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:
1) Get established, no current problems: {YES/NO:63}
2) Chronic Issues: {YES/NO:63}
3) Specific Problems: {YES/NO:63}
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
(559) 221-1234
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

Проверка

Ваши результаты будут варьироваться, на основе действий сообщения, которые вы установили для своей политики DLP. Настройте и подтвердите свои действия для вашего устройства с анализом от GUI: **Почтовая Политика> Кастомизации Политики DLP> передает Действия**.

В данном примере **Действие по умолчанию** собирается изолировать нарушения DLP к карантину Политики и также модифицировать линию темы сообщения с предварительным ожиданием" [DLP VIOLATION]".

mail_logs должен казаться подобным этому при передаче предыдущего содержания до как тестовая электронная почта:

```
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
```

От программного средства **трассировки** необходимо видеть результаты, перечисленные как этот образ при использовании предыдущего содержания в теле сообщения:

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")

Устранение неполадок

Гарантируйте выбор необходимой Политики DLP от **Почтовой Политики>, Менеджер Политики DLP> Добавляет Политику DLP...** в GUI.

Рассмотрите Политику DLP, как добавлено и гарантируйте определение содержания соответствующий классификатор и что шаблон регулярного выражения допустим. Также гарантируйте, что у вас есть **соответствие AND со связанным** настроенным разделом **слов или фраз**. Классификаторы являются компонентами обнаружения механизма DLP. Они могут использоваться в комбинации или индивидуально для определения деликатного характера.

> **Примечание:** Предопределенные классификаторы недоступны для редактирования.

Если вы не видите триггер DLP на основе содержания, также рассмотрите **Почтовую Политику> Политика Исходящей почты> DLP** и гарантируйте, что у вас есть необходимая включенная Политика DLP.

Дополнительные сведения

- Устройство безопасности электронной почты Cisco - руководства пользователя
- Часто задаваемые вопросы ESA: Как я могу отладить, как сообщение обработано ESA?

- SSA.GOV: неправильно используемые номера социального страхования
- Онлайновый тестер regex
- Cisco Systems – техническая поддержка и документация