觸發DLP違規以測試ESA上的HIPAA策略

目錄

簡介

本文檔介紹在思科郵件安全裝置(ESA)上的傳出郵件策略上啟用DLP後，如何測試健康保險便攜性和責任法案(HIPAA)資料丟失防護(DLP)。

觸發DLP違規以測試HIPAA策略

本文提供一些真實內容，這些內容已經過修改，目的是為了保護人員，以便根據ESA上的DLP策略進行測試。此資訊旨在觸發HIPAA和針對經濟和臨床健康狀況的健康資訊科技(HITECH)DLP策略，並觸發其他DLP策略，如社會保障號(SSN)、CA AB-1298、CA SB-1386等。當您通過ESA傳送測試電子郵件或使用**trace**工具時，請使用這些資訊。

> **注意**：在粗體輸出中，必須使用有效或常用的誤用SSN。

> **注意**：對於HIPAA和HITECH DLP策略，請確保已按照建議配置自定義標識號。患者標識號（建議自定義）、美國國家提供商識別符號或美國社會保障號與醫療保健詞典。您必須對此進行配置才能正確觸發。

```
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
```

驗證

根據您為DLP策略設定的郵件操作，結果會有所不同。通過從GUI中檢視配置DLP策略自定義設定>郵件操作**來配置並確認裝置的操作**。

在本例中，**Default Action**設定為將DLP違規隔離到策略隔離區，並且還修改帶有字首「[DLP違規]」的郵件主題行。

當您以測試電子郵件形式通過傳送以前的內容時，**mail_logs**應顯示與此類似的內容：

```
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
```

在**trace**工具中，當使用郵件正文中的先前內容時，您應該會看到類似以下影象列出的結果：

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")

疑難排解

確保已經從GUI中的**Mail Policies > DLP Policy Manager > Add DLP Policy..**中選擇所需的DLP策略。

檢視新增的DLP策略，並確保已指定內容匹配分類器並且正規表示式模式有效。另請確保已配置**AND match with related words or phrases**部分。分類器是DLP引擎的檢測元件。它們可以組合使用，也可以單獨使用，以便識別敏感內容。

附註：預定義的分類器不可編輯。

如果未看到基於內容的DLP觸發器，請同時檢視**Mail Policies > Outgoing Mail Policies > DLP**，並確保已啟用所需的DLP策略。

相關資訊

- Cisco Email Security Appliance — 最終使用手冊
- ESA常見問題：如何調試ESA處理消息的方式？
- SSA.gov:誤用的社會保障號碼
- 線上正規表示式測試器
- 技術支援與文件 - Cisco Systems