Déclenchez une violation DLP pour tester une stratégie HIPAA sur l'ESA

Contenu

Introduction

Ce document décrit comment tester la prévention de perte de portabilité d'assurance médicale maladies et de données de la Loi de responsabilité (HIPAA) (DLP) une fois que vous avez activé le DLP sur votre stratégie de mail sortant sur votre appliance de sécurité du courrier électronique de Cisco (ESA).

Déclenchez une violation DLP pour tester une stratégie HIPAA

Cet article prévoit un certain vrai contenu, qui a été modifié afin de protéger les personnes, pour tester contre la stratégie DLP sur votre ESA. Ces informations sont conçues pour déclencher sur le HIPAA et la technologie informatique d'information santé pour la stratégie économique et clinique DLP de santés (TECHNOLOGIE) et déclenchent également d'autres stratégies DLP comme le numéro de sécurité sociale (SSN), CA AB-1298, CA SB-1386, et ainsi de suite. Utilisez les informations quand vous envoyez un email de test par votre ESA ou quand vous utilisez l'outil de **suivi**.

> Remarque: Vous devez utiliser un SSN valide ou généralement abusé dans la sortie là où bolded.

> Remarque: Pour la stratégie DLP HIPAA et de TECHNOLOGIE, assurez-vous que vous avez configuré les numéros d'identification personnalisés comme recommandés. Numéros d'identification patients (personnalisation recommandée) OU identifiant national de fournisseur des USA OU dictionnaires de numéro de sécurité sociale ET de santé des USA. Vous devez faire configurer ceci afin de déclencher correctement.

```
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
```

Vérifiez

Vos résultats varieront, basé sur les actions de message que vous avez placées pour votre stratégie DLP. Configurez et confirmez vos actions pour votre appliance avec un examen du GUI : **Stratégies de messagerie > personnalisations de stratégie DLP > actions de message**.

Dans cet exemple, l'**action par défaut** est placée pour mettre en quarantaine des violations DLP à la quarantaine de stratégie et de modifier au début également le champ objet de message avec ajouter « [VIOLATION DLP] ».

Les mail_logs devraient ressembler à ceci quand vous envoyez le contenu précédent comme un email de test :

```
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
```

De l'outil de **suivi**, vous devriez voir des résultats répertoriés comme cette image quand vous utilisez le contenu précédent au corps du message :

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")

Dépannez

Assurez-vous que vous avez sélectionné la stratégie nécessaire DLP des **stratégies de messagerie > le Policy Manager DLP > ajoutez la stratégie DLP…** dans le GUI.

Passez en revue la stratégie DLP comme ajouté et assurez-vous que vous avez spécifié votre classificateur assorti satisfait et que votre modèle d'expression régulière est valide. Assurez-vous également que vous avez **ET la correspondance avec la** section **relative de mots ou expression** configurée. Les classificateurs sont les composants de détection de l'engine DLP. Ils peuvent être utilisés en association ou individuellement afin d'identifier le contenu sensible.

> Remarque: Les classificateurs de prédéfinis sont uneditable.

Si vous ne voyez pas le déclencheur DLP basé sur le contenu, également passez en revue les **stratégies de messagerie > les stratégies de mail sortant > le DLP** et assurez-vous que vous faites activer la stratégie nécessaire DLP.

Informations connexes

- Appliance de sécurité du courrier électronique de Cisco - Guides d'utilisateur
- FOIRE AUX QUESTIONS ESA : Comment est-ce que je peux mettre au point comment un message est traité par l'ESA ?
- SSA.gov : Numéros de sécurité sociale abusés
- Testeur en ligne d'expression régulière
- Support et documentation techniques - Cisco Systems