Attivare una violazione del DLP per testare una politica HIPAA sull'ESA

Sommario

Introduzione

Questo documento descrive come testare il Data Loss Prevention (DLP) Health Insurance Portability and Accountability Act (HIPAA) dopo aver abilitato il DLP sulla policy di posta in uscita in Cisco Email Security Appliance (ESA).

Attiva una violazione DLP per verificare un criterio HIPAA

Questo articolo fornisce alcuni contenuti reali, che sono stati modificati per proteggere le persone, da testare contro la Politica di prevenzione della perdita dei dati sull'ESA. Queste informazioni sono state progettate per attivare i criteri di prevenzione della perdita dei dati per le soluzioni di prevenzione della perdita dei dati per le organizzazioni sanitarie (HIPAA) e le tecnologie informatiche per la salute economica e clinica (HITECH) e per attivare altri criteri di prevenzione della perdita dei dati come il numero di previdenza sociale (SSN), CA AB-1298, CA SB-1386 e così via. Utilizzare queste informazioni quando si invia un messaggio di prova tramite l'ESA o quando si utilizza lo strumento di **traccia**.

> **Nota**: è necessario utilizzare un SSN valido o utilizzato in modo non corretto nell'output in grassetto.

> **Nota**: per i criteri di prevenzione della perdita dei dati HIPAA e HITECH, verificare di aver configurato numeri di identificazione personalizzati come consigliato. Numeri di identificazione del paziente (personalizzazione consigliata) OPPURE US National Provider Identifier O US Social Security Number AND Healthcare Dictionaries. Per attivare correttamente l'opzione, è necessario che sia configurata.

```
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
```

Verifica

I risultati variano in base alle azioni impostate per i criteri di prevenzione della perdita dei dati. Configurare e confermare le azioni per l'appliance con una revisione dalla GUI: **Mail Policies > DLP Policy Customizations > Message Actions**.

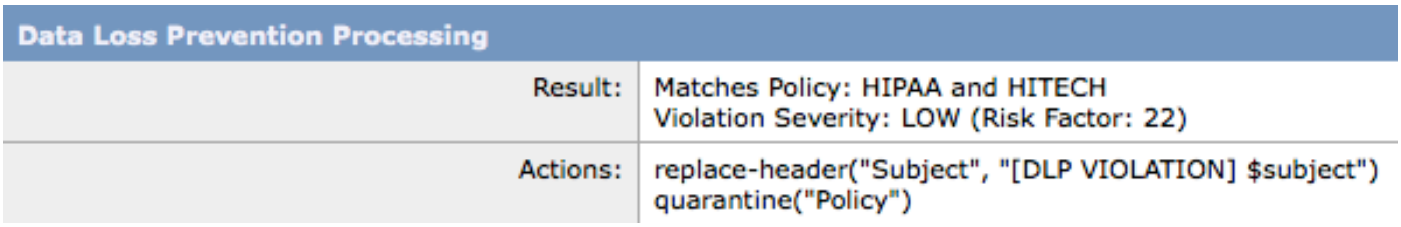
In questo esempio, l'**azione predefinita** è impostata per mettere in quarantena le violazioni dei criteri di prevenzione della perdita dei dati nella quarantena dei criteri e per modificare anche la riga dell'oggetto del messaggio anteponendo "[VIOLAZIONE dei criteri di prevenzione della perdita dei dati]".

Il valore di **mail_logs** dovrebbe essere simile a quello riportato di seguito quando si invia il contenuto precedente tramite come messaggio di prova:

```
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
```

Con lo strumento **trace**, i risultati dovrebbero essere elencati come questa immagine quando si utilizza contenuto precedente nel corpo del messaggio:



Risoluzione dei problemi

Verificare di aver selezionato i criteri di prevenzione della perdita dei dati richiesti da **Mail Policies > DLP Policy Manager > Add DLP Policy...** nella GUI.

Esaminare i criteri di prevenzione della perdita dei dati come aggiunti e assicurarsi di aver specificato il classificatore di corrispondenza contenuto e che il modello di espressione regolare sia valido. Verificare inoltre di avere configurato la **corrispondenza AND con le parole o le frasi correlate**. I classificatori sono i componenti di rilevamento del motore DLP. Possono essere utilizzati in combinazione o singolarmente per identificare i contenuti sensibili.

> **Nota:** I classificatori predefiniti non sono modificabili.

Se non vedi il trigger di prevenzione della perdita dei dati in base al contenuto, consulta anche **Mail Policies > Outgoing Mail Policies > DLP** e assicurati di aver abilitato i criteri di prevenzione della perdita dei dati necessari.

Informazioni correlate

- Cisco Email Security Appliance - Guide per l'utente
- Domande frequenti ESA: Come eseguire il debug del modo in cui un messaggio viene elaborato dall'ESA?
- SSA.gov: Codici previdenziali utilizzati in modo improprio
- Tester regex online
- Documentazione e supporto tecnico – Cisco Systems