Provoque uma violação DLP para testar uma política HIPAA no ESA

Índice

Introdução

Este documento descreve como testar a mobilidade do seguro de saúde e a prevenção de perda de dados do ato da responsabilidade (HIPAA) (DLP) uma vez que você permitiu o DLP em sua política que parte do correio em sua ferramenta de segurança do email de Cisco (ESA).

Provoque uma violação DLP para testar uma política HIPAA

Este artigo fornece algum índice real, que foi alterado a fim proteger os povos, testar contra a política DLP em seu ESA. Esta informação é projetada provocar no HIPAA e no Information Technology da saúde para a política econômica e clínica DLP da saúde (ALTA TECNOLOGIA) e igualmente provoca outras políticas DLP como o número da Segurança Social (SSN), CA AB-1298, CA SB-1386, e assim por diante. Use a informação quando você envia um email do teste com seu ESA ou quando você usa a ferramenta do **traço**.

> Nota: Você deve usar um SSN válido ou geralmente empregado mal na saída onde negrito.

> Nota: Para a política DLP HIPAA e de ALTA TECNOLOGIA, assegure-se de que você configure números de identificação personalizados como recomendado. Números de identificação pacientes (personalização recomendada) OU de fornecedor E.U. identificador nacional OU de número da Segurança Social E de cuidados médicos E.U. dicionários. Você deve ter este configurado a fim provocar corretamente.

```
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
```

Verificar

Seus resultados variarão, com base nas ações que da mensagem você se ajustou para sua política DLP. Configurar e confirme suas ações para seu dispositivo com uma revisão do GUI: **Envie personalizações das políticas > da política DLP > ações da mensagem**.

Neste exemplo, a **ação padrão** é ajustada para quarantine violações DLP à quarentena da política e alterar igualmente a linha de assunto da mensagem com o “[DLP VIOLATION] prepending”.

Os mail_logs devem parecer similares a este quando você envia o índice precedente completamente como um email do teste:

```
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
```

Da ferramenta do **traço**, você deve ver os resultados alistados como esta imagem quando você usa o índice precedente no corpo da mensagem:

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")

Troubleshooting

Assegure-se de que você selecione a política necessária DLP da **política DLP do > Add do gerente das políticas do correio > da política DLP… no** GUI.

Reveja a política DLP como adicionada e assegure-se de que você especifique seu classificador de harmonização satisfeito e que seu padrão de expressão regular é válido. Igualmente assegure-se de que você tenha **E combine-se com a** seção **relacionada das palavras ou das frases** configurada. Os classificadores são os componentes da detecção do motor DLP. Podem ser usados na combinação ou individualmente a fim identificar o índice sensível.

> Nota: Os classificadores predefinidos são uneditable.

Se você não vê o disparador DLP baseado no índice, igualmente reveja **políticas do correio > políticas que parte do correio > DLP** e assegure-se de que você tenha a política necessário DLP permitida.

Informações Relacionadas

- Cisco envia por correio eletrónico a ferramenta de segurança - Guias do utilizador final
- ESA FAQ: Como posso eu debugar como uma mensagem é processada pelo ESA?
- SSA.gov: Números da Segurança Sociais empregados mal
- Verificador em linha do regex
- Suporte Técnico e Documentação - Cisco Systems