触发DLP侵害测试在ESA的一项HIPAA策略

目录

简介

本文描述如何测试健康保险轻便和责任操作(HIPAA)数据丢失预防(DLP)，一旦启用在您的流出的邮件策略的DLP在您的思科电子邮件安全工具(ESA)。

触发DLP侵害测试HIPAA策略

此条款提供某实时内容，修改为了保护人民，测试在您的ESA的DLP策略。此信息在HIPAA和运行状况信息技术设计触发经济和临床健康(HITECH) DLP策略的并且触发其他DLP策略类似社会安全号(SSN)， CA AB-1298， CA SB-1386，等等。请使用信息，当您通过您的ESA时发送测验电子邮件或，当您使用**trace**工具时。

> **注意**： 您在输出中必须使用有效或通常被误用的SSN在粗体的地方。

> **注意**： 对于HIPAA和HITECH DLP策略，请保证您配置定制的标识号码如推荐。耐心的标识号码(推荐的自定义)或美国国家供应商标识符或美国社会安全号和卫生保健字典。您必须安排此配置为了适当地触发。

```
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
```

验证

您的结果根据您为您的DLP策略设置的消息操作将变化。配置并且确认您的您的设备的操作有从GUI的一复核的： **邮寄策略> DLP策略自定义>消息操作**。

在本例中，**默认操作**设置检疫DLP侵害到策略检疫和也修改与加在前面的“[DLP VIOLATION]的”消息标题栏。

mail_logs应该看起来与此相似，当您发送通过时上一个内容，测验电子邮件：

```
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
```

从trace工具，当您在消息主题中时，使用上一个内容您应该看到结果列出类似此镜像：

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")

故障排除

保证您选择从**邮件策略> DLP Policy Manager >Add DLP策略的**需要的DLP策略…在GUI。

查看DLP策略如被添加并且保证您指定您的内容匹配的分类器，并且您的常规表示模式有效。并且请保证您有这**并且匹配与**配置的**相关词或说明**部分。分类器是DLP引擎的检测组件。他们能用于组合或为了单个识别敏感内容。

> **注意**：预定义的分类器uneditable。

如果看不到根据内容的DLP触发，也请查看**邮件策略>流出的邮件策略> DLP**并且保证您安排需要的DLP策略启用。

相关信息

- 思科电子邮件安全工具-最终用户指南
- ESA FAQ ：如何能调试消息如何由ESA处理？
- SSA.gov ：被误用的社会保险编号
- 联机REGEX测试程序
- 技术支持和文档 - Cisco Systems