ESA에서 HIPAA 정책을 테스트하기 위해 DLP 위반 트리거

목차

[소개](#)
[HIPAA 정책을 테스트하기 위해 DLP 위반 트리거](#)
[다음을 확인합니다.](#)
[문제 해결](#)
[관련 정보](#)

소개

이 문서에서는 Cisco ESA(Email Security Appliance)에서 발신 메일 정책에서 DLP를 활성화한 후 HIPAA(Health Insurance Portability and Accountability Act) DLP(Data Loss Prevention)를 테스트하는 방법에 대해 설명합니다.

HIPAA 정책을 테스트하기 위해 DLP 위반 트리거

이 문서에서는 사용자를 보호하고 ESA에서 DLP 정책을 테스트하기 위해 수정된 일부 실제 콘텐츠를 제공합니다.이 정보는 HIPAA 및 HITECH(Health Information Technology for Economic and Clinical Health) DLP 정책을 기반으로 하며 SSN(Social Security Number), CA AB-1298, CA SB-1386 등과 같은 다른 DLP 정책을 트리거하도록 설계되었습니다.ESA를 통해 테스트 이메일을 보내거나 **추적** 툴을 사용할 때 이 정보를 사용합니다.

> **참고**: 굵게 표시된 출력에서 유효하거나 일반적으로 잘못 사용된 SSN을 사용해야 합니다.

> **참고**: HIPAA 및 HITECH DLP 정책의 경우 사용자 지정 식별 번호를 권장 사항으로 구성했는지 확인하십시오.Patient Identification Numbers(환자 식별 번호)(사용자 지정 권장) 또는 미국 National Provider Identifier(국가 사업자 식별자) 또는 미국 Social Security Number and Healthcare Dictionaries(사회 보장 번호 및 의료 사전).제대로 트리거하려면 이 설정을 구성해야 합니다.

```
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
```

다음을 확인합니다.

DLP 정책에 대해 설정한 메시지 작업에 따라 결과가 달라집니다.GUI: Mail Policies(**메일 정책**) > **DLP Policy Customizations(DLP 정책 사용자 지정) > Message Actions(메시지 작업)**에서 검토를 통해 어플라이언스에 대한 작업을 구성하고 확인합니다.

이 예에서 **Default Action(기본 작업)**은 Policy(정책) 격리에 대한 DLP 위반을 격리하고 "[DLP VIOLATION]" 접두사로 메시지 제목 줄을 수정하도록 설정됩니다.

mail_logs는 이전 내용을 테스트 이메일로 보낼 때 다음과 유사한 방식으로 표시되어야 합니다.

```
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
```

추적 도구에서 메시지 본문에서 이전 내용을 사용할 때 다음과 같은 결과가 표시되어야 합니다.

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")

문제 해결

GUI의 Mail Policies(**메일 정책**) > **DLP Policy Manager(DLP 정책 관리자)** > **Add DLP Policy(DLP 정책 추가)...에서** 필요한 DLP 정책을 선택했는지 확인합니다.

추가된 DLP 정책을 검토하고 콘텐츠 일치 분류자를 지정했으며 정규식 패턴이 유효한지 확인합니다.또한 AND가 **관련 단어 또는 구** 섹션**과 일치하는지** 확인합니다.분류자는 DLP 엔진의 탐지 구성 요소입니다.이 두 가지 구성 요소를 조합하거나 개별적으로 사용하여 민감한 내용을 식별할 수 있습니다.

> **참고:**사전 정의된 분류자는 편집할 수 없습니다.

콘텐츠에 따라 DLP 트리거가 표시되지 않으면 **Mail Policies(메일 정책)** > **Outgoing Mail Policies(발신 메일 정책)** > **DLP도 검토하고** 필요한 DLP 정책이 활성화되었는지 확인합니다.

관련 정보

- Cisco Email Security Appliance – 엔드 유저 가이드
- ESA FAQ:ESA에서 메시지를 처리하는 방법을 디버깅하려면 어떻게 해야 합니까?
- SSA.gov:사회 보장 번호 오용
- 온라인 regex 테스터
- 기술 지원 및 문서 – Cisco Systems