# Auslösen eines SvD-Verstoßes, um eine HIPAA-Richtlinie auf der ESA zu testen

## Inhalt



## Einführung

In diesem Dokument wird beschrieben, wie der Health Insurance Portability and Accountability Act (HIPAA) Data Loss Prevention (DLP) getestet wird, sobald Sie DLP für Ihre ausgehende Mail-Policy auf Ihrer Cisco E-Mail Security Appliance (ESA) aktiviert haben.

## Auslösen einer SvD-Verletzung zum Testen einer HIPAA-Richtlinie

Dieser Artikel enthält einige echte Inhalte, die geändert wurden, um die Menschen zu schützen, um gegen die DLP-Richtlinien auf Ihrer ESA zu testen. Diese Informationen wurden entwickelt, um die DLP-Richtlinie HIPAA und Health Information Technology for Economic and Clinical Health (HITECH) auszulösen und löst auch andere DLP-Richtlinien wie Sozialversicherungsnummer (SSN), CA AB-1298, CA SB-1386 usw. aus. Verwenden Sie die Informationen, wenn Sie eine Test-E-Mail über Ihre ESA senden oder wenn Sie das **Ablaufverfolgungs-**Tool verwenden.

> **Hinweis**: In der Ausgabe, in der das Fett eingefügt wurde, müssen Sie eine gültige oder häufig missbräuchlich verwendete SSN verwenden.

> **Hinweis**: Stellen Sie für die HIPAA- und HITECH SvD-Richtlinie sicher, dass Sie benutzerdefinierte Identifikationsnummern wie empfohlen konfiguriert haben. Patienten-Identifikationsnummern (Anpassung empfohlen) ODER US National Provider Identifier ODER US Social Security Number UND Healthcare Dictionaries. Sie müssen dies so konfigurieren, dass der Trigger ordnungsgemäß ausgelöst wird.

```
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
```

# Überprüfen

Die Ergebnisse hängen von den Nachrichtenaktionen ab, die Sie für Ihre SvD-Policy festgelegt haben. Konfigurieren und bestätigen Sie Ihre Aktionen für Ihre Appliance mit einer Überprüfung in der GUI: **Mail-Policys > SvD-Policy-Anpassungen > Nachrichtenaktionen**.

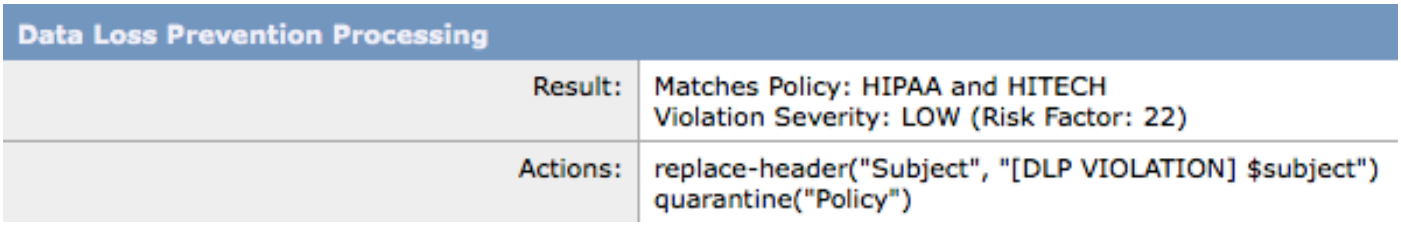
In diesem Beispiel wird die **Standardaktion** so festgelegt, dass SvD-Verletzungen in die Policy-Quarantäne unter Quarantäne gestellt und die Betreffzeile der Nachricht mit dem Vorwort "[SvD-VERLETZUNG]" geändert wird.

Die **mail_logs** sollten ähnlich wie bei dem Senden des vorherigen Inhalts als Test-E-Mail angezeigt werden:

```
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
```

Im **Ablaufverfolgungstool** sollten die Ergebnisse wie dieses Bild angezeigt werden, wenn Sie den vorherigen Inhalt im Nachrichtentext verwenden:




# Fehlerbehebung

Stellen Sie sicher, dass Sie die erforderliche SvD-Policy aus **Mail-Policys > SvD-Policy-Manager > SvD-Policy hinzufügen** ausgewählt haben... in der GUI.

Überprüfen Sie die SvD-Policy wie hinzugefügt, und stellen Sie sicher, dass Sie den Klassifizierer für die Inhaltszuordnung angegeben und das Muster für reguläre Ausdrücke gültig ist. Stellen Sie außerdem sicher, dass der Abschnitt **AND-Übereinstimmung mit verwandten Wörtern oder Sätzen** konfiguriert ist. Klassifizierungen sind die Erkennungskomponenten des SvD-Moduls. Sie können kombiniert oder einzeln verwendet werden, um sensible Inhalte zu identifizieren.

> **Hinweis**: Vordefinierte Klassifizierer können nicht bearbeitet werden.

Wenn Sie den SvD-Trigger nicht basierend auf dem Inhalt sehen, überprüfen Sie auch **Mail-Policys > Mail-Policys für \"Ausgehend\" > SvD** und stellen Sie sicher, dass die erforderliche SvD-Policy aktiviert ist.

# Zugehörige Informationen

- Cisco Email Security Appliance - Benutzerhandbücher
- Häufig gestellte Fragen zur ESA: Wie kann ich debuggen, wie eine Nachricht von der ESA verarbeitet wird?
- SSA.gov: Falsch verwendete Sozialversicherungsnummern
- Online-Regex-Tester
- Technischer Support und Dokumentation - Cisco Systems