Set Up a Custom DLP Policy to Detect Formatted and Unformatted Social Security Numbers

TAC **Document ID: 118537**

Contributed by Trenton Shaffer and Robert Sherwin, Cisco TAC Engineers.

Oct 09, 2014

Contents

Introduction

This document describes how to set up a custom DLP policy to detect both formatted and unformatted Social Security Numbers (SSN) on the Cisco Email Security Appliance (ESA).

Set Up a Custom DLP Policy to Detect Formatted and Unformatted Social Security Numbers

By design the DLP scanning engine only detects formatted Social Security Numbers. This is due to the high level of false positives caused by 9−digit numbers contained in data used by various industries. For example, Bank ABA Routing Numbers are 9−digits and would trigger when scanning for an unformatted Social Security Number. As such it is recommended to avoid scanning for unformatted Social Security Numbers unless strictly required by your organization. If it is required that your organization scans for unformatted Social Security Numbers, you can create a custom DLP policy by following the steps provided in the solution below.

AsyncOS provides the option to create your own policy from scratch using classifiers developed by RSA or your organization. This option is considered advanced and should be used only in the rare cases when the predefined policy templates do not meet the unique requirements of your network environment.

Create a Custom Policy

1. From the GUI: ***Mail Policies > DLP Policy Manager***.
2. Click the ***Add DLP Policy...*** button.
3. Select ***Custom Policy*** at the bottom of the screen and click ***Add*** next to Custom Policy.
4. Enter a DLP Policy Name. For example: *SSN Custom Policy*.

Create a Classifier

Creating custom classifiers gives you great flexibility over the scanned criteria in the DLP engine. We will use this to our advantage to scan for both formatted SSN and unformatted SSN.

1. From the Content Matching Classifier drop−down, select ***Create a Classifier*** and click the ***Add*** button.
2. Enter a Content Matching Classifier Name.   For example: *SSN All Formats.*
3. Under the Rules section, set the drop down from Words or Phrases to ***Entity***.
4. Select the entity: ***US Social Security Number, Formatted***.
5. Click ***Add Rule***.
6. Again select ***Entity***.
7. Select the entity: ***US Social Security Number, Unformatted***.
8. Click ***Submit***.

Set the Severity Settings

The following settings are a good starting point, however they are merely a guideline to assist you and may require some calibration or alternate configuration settings based on your organizations needs.

- ***Critical Severity Settings***
  Action Applied to Messages: ***Quarantine***
  Enable Encryption (checked)
  Encryption Rule: ***Always use message encryption***
  Encryption Profile (select your configured encryption profile from the drop−down)
  Encrypted Message Subject: ***$subject***
- ***High Severity Settings***
  Action Applied to Messages: ***Deliver***
  Enable Encryption (checked)
  Encryption Rule: ***Always use message encryption***
  Encryption Profile (select your configured encryption profile from the drop−down)
  Encrypted Message Subject: ***$subject***
- ***Medium Severity Settings***
  Action Applied to Messages: *Deliver*
  Enable Encryption (checked)
  Encryption Rule: ***Only use message encryption if TLS fails***
  Encryption Profile (select your configured encryption profile from the drop−down)
  Encrypted Message Subject: ***$subject***
- ***Low Severity Settings***
  Action Applied to Messages: ***Deliver***
  Enable Encryption (unchecked)

Set the Severity Scale

Again, the following settings are a good starting point, however they are merely a guideline to assist you and may require some calibration or alternate configuration settings based on your organizations needs.

1. To the right of the severity scale diagram, click ***Edit Scale***.
2. Slide the first handle until IGNORE = 0.
3. Slide the second handle until LOW = 1 to 9.
4. Slide the third handle until MEDIUM = 10 to 50.
5. Slide the fourth handle until HIGH = 60 to 89.

6. If you have set this correctly, CRITICAL will automatically be set 90 to 100.
7. Click ***Done*** when finished.

Submit and Commit Changes

To finalize creation of this policy, click the ***Submit*** button. Click the ***Commit Changes*** button in the upper−right corner of the GUI. You will be taken to the Uncommitted Changes screen, click ***Commit Changes***. You should see ***No changes pending*** in the upper−right corner of the GUI if successful.

Final Steps

You will now need to enable the DLP policy on an Outgoing Mail Policy under ***Mail Policies−>Outgoing Mail Policies***. For testing outside of production you can create a custom outgoing policy with yourself designated as a sender and enable the DLP policy on this test policy.

Related Information

- ***Cisco Email Security Appliance − End−User Guides***
- ***Technical Support & Documentation − Cisco Systems***

Updated: Oct 09, 2014 Document ID: 118537