

Gegevensverliespreventie - misclassificaties en scanfouten voor probleemoplossing

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Belangrijke informatie](#)

[Schending vs. Geen geweld Meld Voorbeelden](#)

[Selectieknop voor probleemoplossing](#)

[De versie van de DLP-motor bevestigen](#)

[Aangepaste contentvastlegging inschakelen](#)

[De configuratie van het scangedrag bekijken](#)

[De configuratie van de prioriteitsschaal bekijken](#)

[De e-mailadressen bekijken die toegevoegd zijn aan de velden van filteraars en -ontvangers](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft gemeenschappelijke methoden voor het oplossen van fouten en scanfouten (of fouten) die te maken hebben met betrekking tot Data Loss Prevention (DLP) op de e-mail security applicatie (ESA).

Voorwaarden

- ESA met AsyncOS 11.x of nieuwer.
- DLP-toets is geïnstalleerd en in gebruik.

Belangrijke informatie

Het is van cruciaal belang op te merken dat DLP op het ESA plug-and-play is in de zin dat u het in staat stelt, een beleid maakt en begint te scannen voor gevoelige gegevens. U dient er zich echter ook van bewust te zijn dat de beste resultaten pas zullen worden behaald nadat DLP is afgestemd op uw bedrijfsspecifieke vereisten. Dit zou dingen omvatten zoals types van DLP beleid, beleid dat details matching, het aanpassen van de ernst van schaal, het filteren en extra aanpassingen.

Schending vs. Geen geweld Meld Voorbeelden

Hier zijn een paar voorbeelden van schendingen van DLP die u kunt zien in de maillogbestanden en/of Berichttracing. De loglijn zal een tijdstempel, houtkapniveau, MID #, schending of geen schending, ernst en risicofactor bevatten, en het beleid dat is afgestemd.

policy match: 'US HIPAA and HITECH'.

Thu Jul 11 16:41:50 2019 Info: MID 46 DLP violation. Severity: LOW (Risk Factor: 24). DLP policy match: 'US State Regulations (Indiana HB 1101)'.

Wanneer er geen overtreding is gevonden, worden de e-maillogbestanden en/of Berichttracering bij DLP automatisch geregistreerd.

Mon Jan 20 12:59:01 2020 Info: MID 26245883 DLP no violation

Selectieknop voor probleemoplossing

Hieronder vermelde algemene items zijn gebruikelijk die kunnen worden herzien bij de behandeling van DLP-verkeerde indelingen of scanfouten/missen.

Opmerking: Dit is geen volledige lijst. Neem contact op met Cisco TAC als u iets hebt dat u inclusief wilt zien.

De versie van de DLP-motor bevestigen

DLP motor updates zijn standaard niet automatisch, dus is het van cruciaal belang om te zorgen dat u de nieuwste versie draait die recente verbeteringen of bug fixes bevat.

U kunt onder *Beveiligingsservices* in de GUI navigeren naar *gegevensverloren preventie* om de huidige versie van de motor te bevestigen en om te zien of er updates beschikbaar zijn. Als een update beschikbaar is, kunt u op *Nu bijwerken* klikken om de update uit te voeren.

Current DLP Files			
File Type	Last Update	Current Version	New Update
DLP Engine	Mon Apr 20 15:41:29 2020	1.0.18.d7b4601	No updates available.
No updates in progress.			Update Now

Aangepaste contentvastlegging inschakelen

DLP biedt de optie om de inhoud te loggen die uw DLP-beleid schendt, evenals de omliggende inhoud. Deze gegevens kunnen dan in *Message Tracking* worden bekeken om te helpen bij het opsporen van de inhoud van een e-mail die een bepaalde schending kan veroorzaken.

Voorzichtig: Het is belangrijk om te weten dat indien mogelijk, deze inhoud gevoelige gegevens kan omvatten zoals kredietkaartnummers en socialezekerheidsnummers, enz.

U kunt onder *Beveiligingsservices* in de GUI naar *gegevensverliespreventie* navigeren om te zien of *Aangepaste contentvastlegging* is ingeschakeld.

Data Loss Prevention Settings	
Data Loss Prevention:	Enabled
Matched Content Logging:	Enabled
Edit Settings...	

Voorbeeld van aangepaste contentvastlegging gezien in Berichttracering

Processing Details	
Summary	DLP Matched Content
	MESSAGE ID "2054" MATCHED DLP POLICY: Credit Card Numbers
Violation Severity:	LOW (Risk Factor: 22)
Message:	Credit Card Numbers <ul style="list-style-type: none"> • credit card information. 378734493671000 VISA

De configuratie van het scangedrag bekijken

De configuratie van het Scannen gedrag op de ESA zal ook van invloed zijn op de functionaliteit achter het DLP-scannen. Als u het hieronder weergegeven scherm bekijkt, zie u een voorbeeld met een ingesteld **maximale** scangrootte van **5 M**, zodat **het** scannen van DLP gemist wordt. Tevens is de **actie voor bijlagen met MIME-typen** een ander veel voorkomend item dat u wilt bekijken. Dit moet worden ingesteld op de standaard van **Skip** zodat de aangegeven MIME-typen worden overgeslagen en alle andere typen worden gescand. Als deze optie ingesteld is op Scannen, *scannen we alleen de* in de tabel opgenomen *MIME-typen*.

Op dezelfde manier kunnen andere hier genoemde instellingen invloed hebben op het DLP-scannen en moeten ze in aanmerking worden genomen, afhankelijk van de inhoud van de bijlage/e-mail.

U kunt navigeren om *gedrag te scannen* onder *Beveiligingsservices* in de GUI, of door het **scanconfiguratie** opdracht binnen de CLI uit te voeren.

Attachment Type Mappings			
Add Mapping...		Import List...	
Fingerprint / MIME	Type	Edit	Delete
MIME Type	audio/*	Edit...	
MIME Type	video/*	Edit...	
MIME Type	image/*	Edit...	
Fingerprint	Media	Edit...	
Fingerprint	Image	Edit...	
Export List...			

Global Settings		
Action for attachments with MIME types / fingerprints in table above:	Skip	
Maximum depth of attachment recursion to scan:	5	
Maximum attachment size to scan:	5M	
Attachment Metadata scan:	Enabled	
Attachment scanning timeout:	30 seconds	
Assume attachment matches pattern if not scanned for any reason:	No	
Assume zip file to be unscannable if files in the archive cannot be read?	No	
Action when message cannot be deconstructed to remove specified attachments:	Deliver	
Bypass all filters in case of a content or message filter error:	Yes	
Encoding to use when none is specified:	US-ASCII	
Convert opaque-signed messages to clear-signed (S/MIME unpacking):	Disabled	
Safe Print settings	Maximum File Size	5M
	Maximum Page Count	10
	Document Quality	70
Actions for Unscannable Messages due to decoding errors found during URL Filtering Actions:	Disabled	
Action when a message is unscannable due to extraction failures:	Deliver As Is	
Action when a message is unscannable due to RFC violations:	Disabled	
Edit Global Settings...		

De configuratie van de prioriteitsschaal bekijken

De standaardinstellingen voor de ernst van de schade zullen voor de meeste omgevingen voldoende zijn; Als u deze echter moet wijzigen om te helpen met FN (FN) of Fse Positive (FP) bij elkaar te brengen, dan kunt u dit doen. U kunt ook bevestigen dat uw DLP-beleid de aanbevolen standaarddrempels gebruikt door een nieuw schijnbeleid te maken en ze vervolgens te vergelijken.

Opmerking: ander vooraf bepaald beleid (bijvoorbeeld VS HIPAA vs. PCI-DSS) zal verschillende schaalgroottes hebben.

Severity Scale:	IGNORE	LOW	MEDIUM	HIGH	CRITICAL	Edit Scale...
	0 - 34	35 - 54	55 - 72	73 - 87	88 - 100	

De e-mailadressen bekijken die toegevoegd zijn aan de velden van filteraars en -ontvangers

Controleer of een in een van deze velden ingevoerd bestand overeenkomt met het juiste geval van de verzendende en/of het ontvangende e-mailadres. Het veld Afbeeldingen en ontvangers van filter is **hoofdlettergevoelig**. Het DLP-beleid treedt niet op als het e-mailadres eruitziet als "TestEmail@mail.com" in de mailclient en als "testemail@mail.com" in deze velden is ingevoerd.

Filter Senders and Recipients:

Only apply to a message if it sent to one of the following recipient(s):

Separate multiple entries with a line break or comma. (Example: user@example.com, user@, @example.com, @.example.com)

Only apply to a message if it sent from one of the following sender(s):

Separate multiple entries with a line break or comma. (Example: user@example.com, user@, @example.com, @.example.com)

Gerelateerde informatie

- [Cisco e-mail security applicatie - eindgebruikershandleidingen](#)
- [Wat is gegevensverliespreventie?](#)
- [Trigger een DLP-overtreding om een HIPAA-beleid op de ESA te testen](#)