Schutz vor Datenverlust - Fehlerbehebung bei Fehlklassifizierungen und Scannerfehlern

Inhalt

Einführung

In diesem Dokument werden allgemeine Methoden zur Behebung von Fehlklassifizierungen und Scan-Fehlern (oder Fehlern) im Zusammenhang mit dem Schutz vor Datenverlust (Data Loss Prevention, DLP) auf der E-Mail-Security-Appliance (ESA) beschrieben.

Voraussetzungen

- ESA mit AsyncOS 11.x oder höher
- Der SvD-Feature-Schlüssel ist installiert und wird verwendet.

Wichtige Informationen

Es ist wichtig, darauf hinzuweisen, dass DLP auf der ESA Plug-and-Play ist, d. h. dass Sie DLP aktivieren, eine Richtlinie erstellen und nach vertraulichen Daten suchen können. Sie sollten sich jedoch auch darüber im Klaren sein, dass die besten Ergebnisse erst nach der Anpassung von DLP an Ihre unternehmensspezifischen Anforderungen erreicht werden. Dazu gehören beispielsweise Typen von SvD-Policys, Details zur Richtlinienzuordnung, Anpassen der Schweregrad-Skalierung, Filtern und zusätzliche Anpassungen.

Verstöße gegen das Verbot von Protokollbeispielen

Im Folgenden finden Sie einige Beispiele für DLP-Verletzungen, die Sie möglicherweise in den Mail-Protokollen und/oder der Nachrichtenverfolgung sehen. Die Logline umfasst einen Zeitstempel, die Protokollierungsebene, die MID-Nummer, die Verletzung oder keine Verletzung, den Schweregrad und den Risikofaktor sowie die Richtlinie, die zugeordnet wurde.

```
Thu Jul 11 16:05:28 2019 Info: MID 40 DLP violation. Severity: CRITICAL (Risk Factor: 96). DLP
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)'.
```

Wenn keine Verletzung gefunden wird, protokollieren die E-Mail-Protokolle und/oder die Nachrichtenverfolgung einfach *SvD ohne Verletzung*.

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

Fehlerbehebungs-Checkliste

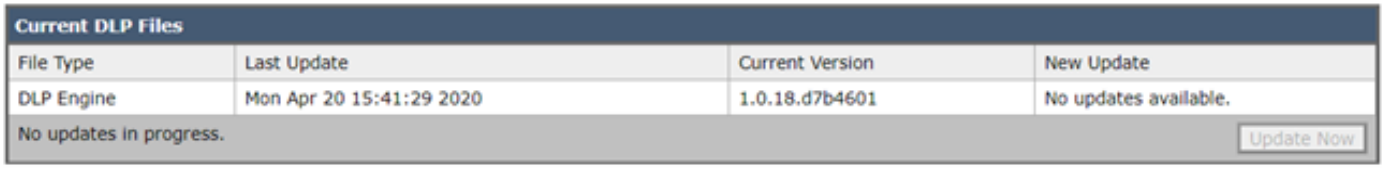
Im Folgenden finden Sie allgemeine Elemente, die bei fehlerhaften SvD-Klassifizierungen oder Scanfehlern/Fehlern überprüft werden können.

> **Hinweis**: Diese Liste ist nicht vollständig. Wenden Sie sich an das Cisco TAC, wenn Sie etwas einschließen möchten.

Bestätigen der Version der SvD-Engine

SvD-Engine-Updates sind nicht standardmäßig automatisch. Daher ist es wichtig, sicherzustellen, dass Sie die neueste Version ausführen, die alle aktuellen Erweiterungen oder Bugfixes enthält.

Sie können unter *Sicherheitsdienste* in der GUI zu *Data Loss Prevention* navigieren, um die aktuelle Engine-Version zu bestätigen und zu überprüfen, ob Updates verfügbar sind. Wenn eine Aktualisierung verfügbar ist, können Sie auf *Jetzt aktualisieren* klicken, um die Aktualisierung durchzuführen.

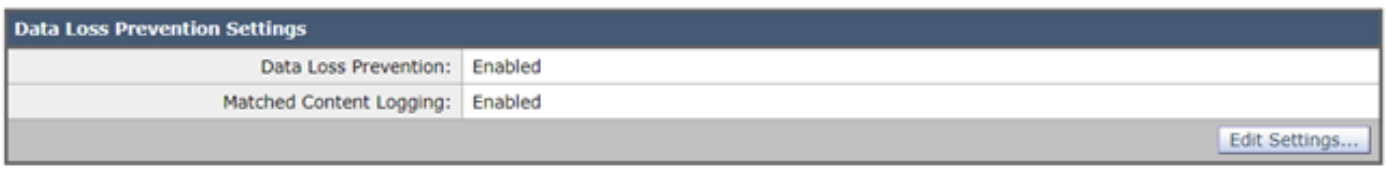


Aktivieren der Protokollierung zugeordneter Inhalte

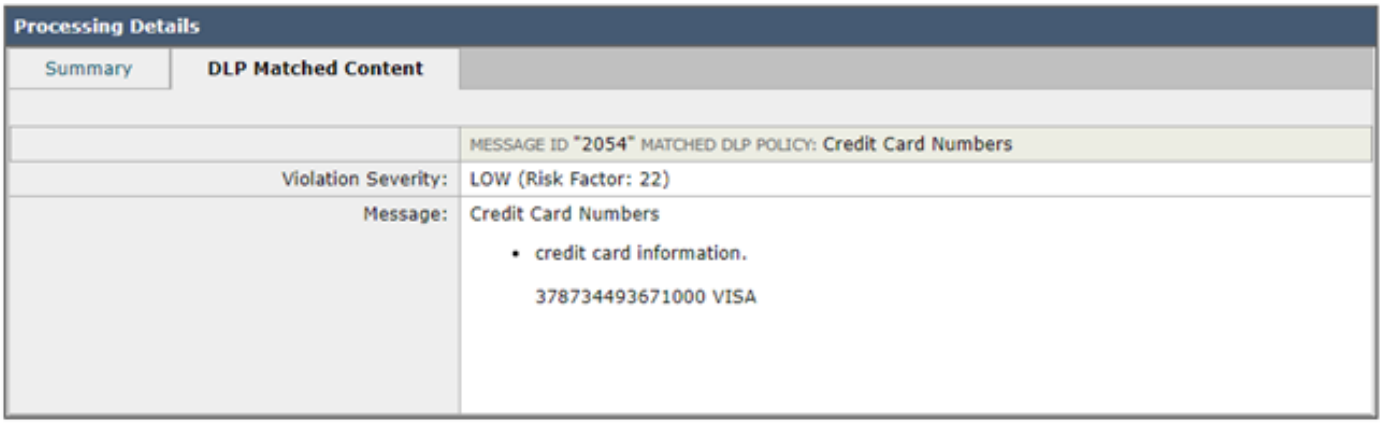
SvD bietet die Möglichkeit, Inhalte zu protokollieren, die Ihre SvD-Policys verletzen, sowie die umgebenden Inhalte. Diese Daten können dann in der *Nachrichtenverfolgung* angezeigt werden, um zu ermitteln, welche Inhalte in einer E-Mail eine bestimmte Verletzung verursachen können.

> **Vorsicht**: Es ist wichtig zu wissen, dass diese Inhalte bei Aktivierung sensible Daten wie Kreditkartennummern und Sozialversicherungsnummern usw. enthalten können.

Sie können unter *Sicherheitsdienste* in der GUI zu *Data Loss Prevention* navigieren, um festzustellen, ob *Matched Content Logging* aktiviert ist.



Beispiel für die Protokollierung zugeordneter Inhalte in der Nachrichtenverfolgung



Überprüfen der Konfiguration des Scan-Verhaltens

Die Konfiguration des Scan-Verhaltens auf der ESA wirkt sich auch auf die Funktionalität der DLP-Prüfung aus. Wenn Sie sich den unten stehenden Screenshot als Beispiel ansehen, der eine konfigurierte **maximale Größe für den Scanvorgang** von **Anhängen** von **5 Mio.** aufweist, kann dies dazu führen, dass DLP-Scans verpasst werden. Die **Aktion für Anhänge mit MIME-Typen-**Einstellung ist ein weiteres gängiges Element, das Sie überprüfen möchten. Dies sollte auf die Standardeinstellung **"Überspringen"** festgelegt werden, sodass die aufgelisteten MIME-Typen übersprungen werden und alles andere gescannt wird. Wenn stattdessen Scan eingestellt ist, *scannen* wir *nur die* in der Tabelle aufgelisteten *MIME-Typen*.

Andere hier aufgelistete Einstellungen können sich ebenfalls auf die DLP-Prüfung auswirken und sollten entsprechend des Anhangs/E-Mail-Inhalts berücksichtigt werden.

Sie können unter *Sicherheitsdienste* in der GUI zu *Scan Behavior* navigieren oder den Befehl **scanconfig** in der CLI ausführen.

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...

Überprüfen der Konfiguration der Schweregrad-Skalierung

Die Standardschwellenwerte für den Schweregrad sind für die meisten Umgebungen ausreichend. Wenn Sie diese jedoch ändern müssen, um die Zuordnung zu False Negative (FN) oder False Positive (FP) zu unterstützen, können Sie dies tun. Sie können auch bestätigen, dass Ihre SvD-Richtlinie die empfohlenen Standardschwellenwerte verwendet, indem Sie eine neue Dummy-Richtlinie erstellen und diese dann vergleichen.

> **Hinweis**: Unterschiedliche vordefinierte Richtlinien (z. B. US HIPAA und PCI-DSS) weisen eine unterschiedliche Skalierung auf.

Severity Scale:

IGNORE	LOW	MEDIUM	HIGH	CRITICAL
0 - 34	35 - 54	55 - 72	73 - 87	88 - 100

Edit Scale...

Überprüfen der E-Mail-Adressen, die den Feldern "Absender und Empfänger filtern" hinzugefügt wurden

Überprüfen Sie, ob alle in eines dieser Felder eingegebenen Einträge der Groß- und Kleinschreibung der E-Mail-Adressen des Absenders und/oder Empfängers entsprechen. Im Feld Absender und Empfänger filtern wird die **Groß- und Kleinschreibung** berücksichtigt. Die SvD-Policy wird nicht ausgelöst, wenn die E-Mail-Adresse im Mail-Client wie "TestEmail@mail.com"

aussieht und als "testemail@mail.com" in diese Felder eingegeben wird.

Zugehörige Informationen

- Cisco Email Security Appliance - Benutzerhandbücher
- Was ist der Schutz vor Datenverlusten?
- Auslösen eines SvD-Verstoßes, um eine HIPAA-Richtlinie auf der ESA zu testen