데이터 손실 방지 - 잘못된 분류 및 검사 실패 문제 해결

목차

소개

이 문서에서는 ESA(Email Security Appliance)의 DLP(Data Loss Prevention)와 관련된 잘못된 분류 및 검사 실패(또는 누락)를 트러블슈팅하는 일반적인 방법에 대해 설명합니다.

사전 요구 사항

- AsyncOS 11.x 이상을 실행하는 ESA
- DLP 기능 키가 설치되어 사용 중입니다.

중요 정보

ESA의 DLP는 이를 활성화하고, 정책을 생성하고, 민감한 데이터를 스캔하기 시작할 수 있다는 점에서 플러그 앤 플레이입니다.그러나 회사의 특정 요구 사항에 맞게 DLP를 튜닝한 후에만 최상의 결과를 얻을 수 있다는 점도 알아야 합니다.여기에는 DLP 정책 유형, 정책 일치 세부 정보, 심각도 규모 조정, 필터링, 추가 사용자 지정 등의 사항이 포함됩니다.

위반 및 위반 로그 없음 예

다음은 메일 로그 및/또는 메시지 추적에서 볼 수 있는 DLP 위반의 몇 가지 예입니다.로그라인에는 타임스탬프, 로깅 레벨, MID #, 위반 또는 위반 없음, 심각도 및 위험 요소, 일치하는 정책이 포함됩니다.

```
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)'.
```
위반이 발견되지 않으면 메일 로그 및/또는 메시지 추적으로 DLP *위반*이 *로깅됩니다*.

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

문제 해결 체크리스트

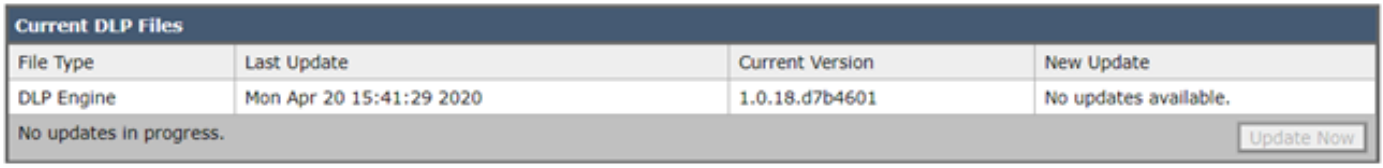
아래에 제공된 공통 항목은 DLP 오분류 또는 검사 실패/실패를 처리할 때 검토할 수 있습니다.

> **참고:**이것은 완전한 목록이 아닙니다.포함하려는 사항이 있으면 Cisco TAC에 문의하십시오.

DLP 엔진 버전 확인

DLP 엔진 업데이트는 기본적으로 자동으로 수행되지 않으므로 최신 개선 사항 또는 버그 픽스가 포함된 최신 버전을 실행하고 있는지 확인해야 합니다.

GUI의 *Security Services(보안 서비스)*에서 *Data Loss Prevention(데이터 손실 방지)*으로 이동하여 현재 엔진 버전을 확인하고 사용 가능한 업데이트가 있는지 확인할 수 있습니다.업데이트를 사용할 수 있는 경우 Update Now(지금 *업데이트)를* 클릭하여 업데이트를 수행할 수 있습니다.

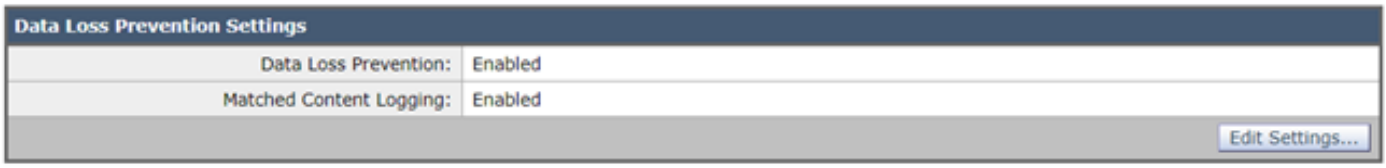


일치하는 콘텐츠 로깅 활성화

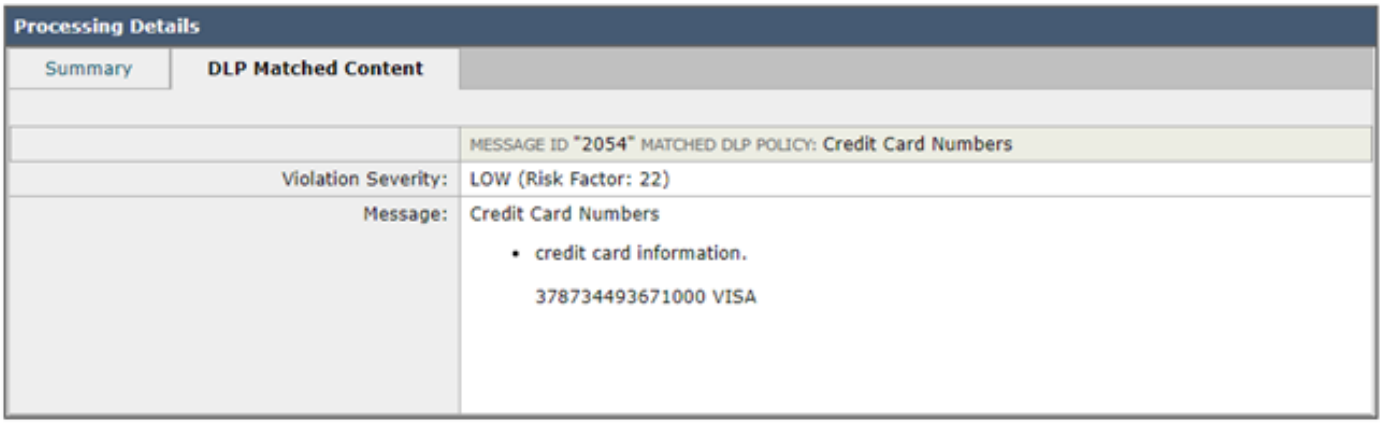
DLP는 DLP 정책을 위반하는 콘텐츠와 주변 콘텐츠를 로깅하는 옵션을 제공합니다.그런 다음 *메시지 추적*에서 이 데이터를 확인하여 전자 메일 내에서 특정 위반의 원인이 될 수 있는 콘텐츠를 추적할 수 있습니다.

> **주의:**활성화된 경우 이 컨텐츠에는 신용카드 번호, 주민등록번호 등의 민감한 데이터가 포함될 수 있다는 점을 알아야 합니다.

GUI의 *Security Services(보안 서비스)*에서 Data Loss *Prevention(데이터 손실 방지)으로* 이동하여 Matched Content Logging(*일치하는 콘텐츠 로깅)이 활성화되었는지* 확인할 수 있습니다.



메시지 추적에 표시된 일치 콘텐츠 로깅 예



스캔 동작 컨피그레이션 검토

ESA의 Scan Behavior 컨피그레이션은 DLP 스캐닝 뒤에 있는 기능에도 영향을 줍니다.아래 스크린샷을 예로 들면 구성된 **최대 첨부 파일 검사 크기**가 **5M**인 것처럼 더 큰 경우 DLP 검사가 누락될 수 있습니다.또한 MIME **유형** 설정**을 가진 첨부 파일에 대한** 작업은 검토할 또 다른 공통 항목입니다.나열된 MIME 유형을 건너뛰고 다른 모든 유형을 스캔하도록 이를 기본값으로 설정해야 합니다.대신 Scan으로 설정하면 테이블에 나열된 *MIME 유형만 스캔합니다*.

마찬가지로, 여기에 나열된 다른 설정은 DLP 검사에 영향을 줄 수 있으며 첨부 파일/이메일 내용에 따라 고려해야 합니다.

GUI의 *Security Services(보안 서비스*)에서 Scan Behavior(*스캔 동작*)로 이동하거나 CLI 내에서 scanconfig 명령**을** 실행하여 이동할 수 있습니다.

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...

심각도 규모 구성 검토

기본 심각도 확장 임계값은 대부분의 환경에서 충분합니다.그러나 FN(False Negative) 또는 FP(False Positive) 매칭을 지원하도록 수정해야 하는 경우 수정할 수 있습니다.또한 새 더미 정책을 만든 다음 비교하여 DLP 정책이 권장 기본 임계값을 사용하고 있는지 확인할 수 있습니다.

참고: 서로 다른 사전 정의된 정책(예: 미국 HIPAA와 PCI-DSS)의 확장성이 다릅니다.

Severity Scale:

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

Edit Scale...

필터 발신자 및 수신자 필드에 추가된 이메일 주소 검토

이러한 필드 중 하나에 입력된 항목이 발신자 및/또는 수신자 이메일 주소의 대/소문자를 일치하는지 확인합니다.Filter Senders and Recipients 필드는 **대/소문자를 구분합니다**.이메일 주소가 메일 클라이언트에서 "TestEmail@mail.com"처럼 보이고 이러한 필드에 "testemail@mail.com"으로 입력되면 DLP 정책이 트리거되지 않습니다.

관련 정보

- Cisco Email Security Appliance – 엔드 유저 가이드
- 데이터 유출 방지란?
- ESA에서 HIPAA 정책을 테스트하기 위해 DLP 위반 트리거