포맷되고 포맷되지 않은 사회 보장 번호를 탐지하도록 맞춤형 DLP 정책 설정

목차

소개

이 문서에서는 Cisco ESA(Email Security Appliance)에서 서식이 지정된 SSN(Social Security Numbers)과 서식이 지정되지 않은 SSN을 모두 탐지하도록 사용자 지정 DLP 정책을 설정하는 방법에 대해 설명합니다.

포맷되고 포맷되지 않은 사회 보장 번호를 탐지하도록 맞춤형 DLP 정책 설정

DLP 스캐닝 엔진은 포맷된 사회보장번호만 탐지합니다.다양한 업계에서 사용되는 데이터에 포함된 9자리 숫자로 인해 발생한 높은 오탐이 원인입니다.예를 들어, 은행 ABA 라우팅 번호는 9자리이며 포맷되지 않은 사회 보장 번호를 검색할 때 트리거됩니다.따라서 조직에서 엄격하게 요구하는 경우가 아니면 포맷되지 않은 사회 보장 번호를 검색하지 않는 것이 좋습니다.조직이 포맷되지 않은 Social Security Numbers(사회 보장 번호)를 스캔해야 하는 경우 아래 솔루션에 제공된 단계에 따라 맞춤형 DLP 정책을 생성할 수 있습니다.

AsyncOS는 RSA 또는 조직에서 개발한 분류자를 사용하여 처음부터 사용자 고유의 정책을 생성할 수 있는 옵션을 제공합니다.이 옵션은 고급 옵션으로 간주되며 미리 정의된 정책 템플릿이 네트워크 환경의 고유한 요구 사항을 충족하지 않는 드문 경우에만 사용해야 합니다.

사용자 지정 정책 생성

1. GUI: Mail Policies(**메일 정책) > DLP Policy Manager(DLP 정책 관리자)에서**.
2. Add **DLP Policy..(DLP 정책 추가...)를 클릭합니다.** 단추를 클릭합니다.
3. 화면 하단에서 **Custom Policy**(사용자 지정 정책)를 선택하고 Custom Policy(사용자 지정 정책

) 옆에 있는 **Add(추가)**를 클릭합니다.
4. DLP 정책 이름을 입력합니다. 예:*SSN 사용자 지정 정책.*

분류자 생성

사용자 지정 분류자를 생성하면 DLP 엔진의 스캔된 기준보다 뛰어난 유연성을 제공합니다.이를 통해 포맷된 SSN 및 포맷되지 않은 SSN을 모두 스캔할 수 있습니다.

1. Content Matching Classifier(콘텐츠 일치 분류자) 드롭다운에서 **Create a Classifier(분류자 생성)**를 선택하고 Add(**추가**)버튼을 클릭합니다.
2. 컨텐트 일치 분류자 이름을 입력합니다. 예:*SSN 모든 형식.*
3. Rules(규칙) 섹션에서 Words(단어) 또는 Phrase(구문)에서 Entity(엔티티)로 드롭다운을 **설정합니다**.
4. 엔티티를 선택합니다.**US Social Security Number, Formatted**.
5. Add **Rule을 클릭합니다**.
6. 다시 엔티티**를 선택합니다**.
7. 엔티티를 선택합니다.**미국 사회 보장 번호, 포맷되지 않았습니다**.
8. Submit(제출**)을 클릭합니다**.

심각도 설정 설정

다음 설정은 좋은 시작점입니다. 그러나 이러한 설정은 사용자를 지원하는 지침일 뿐이며 조직의 요구 사항에 따라 일부 보정 또는 대체 구성 설정이 필요할 수 있습니다.

- **중요 심각도 설정**
  메시지에 적용된 작업:**쿼런틴**
  암호화 사용(선택)
  암호화 규칙:**항상 메시지 암호화 사용**
  Encryption Profile(암호화 프로파일)(드롭다운에서 구성된 암호화 프로파일 선택)
  암호화된 메시지 제목:**$subject**
- **높은 심각도 설정**
  메시지에 적용된 작업:**제공**
  암호화 사용(선택)
  암호화 규칙:**항상 메시지 암호화 사용**
  Encryption Profile(암호화 프로파일)(드롭다운에서 구성된 암호화 프로파일 선택)
  암호화된 메시지 제목:**$subject**
- **중간 심각도 설정**
  메시지에 적용된 작업: *제공*
  암호화 사용(선택)
  암호화 규칙:**TLS가 실패하는 경우에만 메시지 암호화 사용**
  Encryption Profile(암호화 프로파일)(드롭다운에서 구성된 암호화 프로파일 선택)
  암호화된 메시지 제목:**$subject**
- **낮은 심각도 설정**
  메시지에 적용된 작업:**제공**
  암호화 사용(선택 취소)

심각도 스케일 설정

다시 한 번, 다음 설정은 좋은 시작점이지만, 이는 단지 사용자를 지원하기 위한 지침일 뿐이며 조직의 요구 사항에 따라 일부 보정 또는 대체 구성 설정이 필요할 수 있습니다.

1. 심각도 배율 다이어그램 오른쪽에서 배율 **편집**을 클릭합니다.
2. IGNORE = 0이 될 때까지 첫 번째 핸들을 밀어 넣습니다.
3. LOW = 1~9까지 두 번째 핸들을 밀어 넣습니다.
4. 세 번째 핸들을 MEDIUM = 10~50까지 밀어 넣습니다.
5. 4번째 핸들을 HIGH = 60~89까지 밀어 넣습니다.
6. 이 값을 올바르게 설정한 경우 CRITICAL은 자동으로 90에서 100으로 설정됩니다.
7. 완료되면 **Done(완료)**을 클릭합니다.

변경 사항 제출 및 커밋

이 정책 생성을 완료하려면 Submit(제출) 버튼을 클릭합니다.GUI의 오른쪽 상단 모서리에 있는 Commit Changes(변경 사항 커밋) 버튼을 클릭합니다.Uncommit Changes(커밋되지 않은 변경 사항) 화면으로 이동한 다음 **Commit Changes(변경 사항 커밋)를 클릭합니다**.GUI의 오른쪽 상단 모서리에 **보류 중인 변경 사항 없음**(성공한 경우)이 표시됩니다.

최종 단계

이제 Mail Policies(**메일 정책**)->**Outgoing Mail Policies(발신 메일 정책)**에서 Outgoing Mail Policy(발신 메일 정책)에서 DLP 정책을 활성화해야 합니다.프로덕션 외부에서 테스트하려면 발신자로 지정된 사용자 자신과 함께 사용자 지정 발신 정책을 생성하고 이 테스트 정책에서 DLP 정책을 활성화할 수 있습니다.

관련 정보

- Cisco Email Security Appliance – 엔드 유저 가이드
- 기술 지원 및 문서 – Cisco Systems