민감한 데이터 탐지

다음 주제에서는 민감한 데이터 탐지 및 그 구성 방법을 설명합니다.

민감한 데이터 탐지 기본 사항

사회 보장 번호, 신용카드 번호, 운전면허증 번호 같은 민감한 정보가 인터넷에 고의적으로 또는 실수로 유출될 수 있습니다. 이 시스템에서는 ASCII 텍스트로 된 민감한 데이터에 대한 이벤트를 탐지하고 생성할 수 있는 민감한 데이터 전처리기를 제공하며, 이는 실수로 인한 데이터 유출을 탐지할 때 특히 유용합니다.

전역 민감한 데이터 전처리기 옵션은 전처리기가 작용하는 방법을 제어합니다. 다음을 지정하는 전역 옵션을 변경할 수 있습니다.

- 시작하는 패킷에서 전처리기가 신용 카드 번호 또는 사회 보장 번호의 마지막 네 자리를 제외한 모든 것을 대체하는지 여부
- 네트워크에서 민감한 데이터에 대해 모니터링하는 대상 호스트의 종류
- 단일 세션에서 단일 이벤트로 귀결되는 모든 데이터 유형의 총 발생 횟수

개별 데이터 유형은 지정된 대상 네트워크에서 이벤트를 탐지하고 생성할 수 있는 민감한 데이터를 식별합니다. 다음을 지정하는 데이터 유형 옵션에 대한 기본 설정을 변경할 수 있습니다.

- 탐지된 데이터 유형이 단일한 세션별 이벤트를 생성하려면 충족해야 하는 임계값
- 각 데이터 유형을 모니터링할 대상 포트
- 각 데이터 유형을 모니터링할 애플리케이션 프로토콜

사용자 지정 데이터 유형을 만들고 수정하여 지정하려는 데이터 패턴을 탐지할 수 있습니다. 예를 들어, 병원이 환자 번호를 보호하기 위해 데이터 유형을 만들 수 있으며 대학이 고유 번호 패턴이 있는 학생 수를 탐지하기 위해 데이터 유형을 만들 수도 있습니다.

시스템에서는 개별 데이터 유형을 트래픽과 일치시켜 TCP 세션당 민감한 데이터를 탐지합니다. 사용자 침입 정책에서 모든 데이터 유형에 적용되는 전역 옵션 및 각 데이터 유형에 대한 기본 설정을 수정할 수 있습니다. Firepower System는 일반적으로 사용되는 미리 정의된 데이터 유형을 제공합니다. 또한 사용자 지정 데이터 유형을 만들 수 있습니다.

민감한 데이터 전처리기 규칙은 각 데이터 유형과 연결됩니다. 각 데이터 유형의 전처리기 규칙을 활성화하여 각 데이터 유형에 대한 민감한 데이터 탐지 및 이벤트 생성을 활성화할 수 있습니다. 구성 페이지 링크를 통해 Rules(규칙) 페이지에서 민감한 데이터를 필터링하여 볼 수 있는데, 여기서 규칙을 활성화/비활성화하고 다른 규칙 속성을 구성할 수 있습니다.

데이터 유형과 관련된 규칙이 활성화되고 민감한 데이터 탐지가 비활성화된 경우, 침입 정책에 변경 사항을 저장하면, 자동으로 민감한 데이터 전처리기를 활성화하는 옵션이 제공됩니다.

팁 민감한 데이터 전처리기는 FTP 또는 HTTP를 사용하여 업로드되고 다운로드된 암호화되지 않은 Microsoft에서 민감한 데이터를 탐지할 수 있습니다. Word 파일이 ASCII 텍스트 및 서식 설정 명령을 별도로 분류하는 방식 때문에 이것이 가능합니다.

시스템에서는 암호화되거나 위장된 형태의 민감한 데이터나 압축 또는 인코딩된 형식(예: Base64 인코딩 이메일 첨부 파일)의 민감한 데이터를 탐지하지 않습니다. 예를 들어 시스템은 전화 번호 (555)123-4567은 탐지하지만 (5 5 5) 1 2 3 - 4 5 6 7과 같이 공백으로 각 번호가 분리되어 있거나 (555)-123-4567과 같이 HTML 코드가 끼어 있는 애매한 버전은 탐지하지 못합니다. 하지만 시스템은 중간 코드가 번호 패턴을 방해하지 않는 HTML 코드 번호 (555)-123-4567은 탐지합니다.

전역 민감한 데이터 탐지 옵션

전역 민감한 데이터 옵션은 정책 단위이며 모든 데이터 유형에 적용됩니다.

마스크

시작하는 패킷에서 신용 카드 번호 또는 사회 보장 번호의 마지막 네 자리를 제외한 모든 것을 X로 대체합니다. 마스크 처리된 번호는 웹 인터페이스의 침입 이벤트 보기 및 다운로드한 패킷에 표시됩니다.

네트워크

민감한 데이터를 위해 모니터링할 대상 호스트를 지정합니다. 단일 IP 주소 또는 주소 블록을 지정하거나, 쉼표로 구분된 하나 또는 둘 다의 목록을 지정할 수 있습니다. 시스템은 비어 있는 필드를 모든으로 해석하며, 모든 대상 IP 주소를 의미합니다.

시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다. 하위 도메인 관리자는 재정의가 활성화된 개체를 사용하여 로컬 환경에 맞게 글로벌 컨피그레이션을 조정할 수 있습니다.

전역 임계값

전처리기가 전역 임계값 이벤트를 생성하기 전에 모든 조합에서 탐지해야 하는 단일 세션 동안 모든 데이터 유형의 모든 항목 수를 지정합니다. 1부터 65535까지 지정할 수 있습니다.

Cisco는 이 옵션 값을 정책에서 활성화한 모든 개별 데이터 유형의 가장 높은 임계값보다 높게 설정할 것을 권장합니다.

전역 임계값에 관해 다음 사항에 유의하십시오.

- 조합된 데이터 유형 발생에서 이벤트를 탐지 및 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.하려면 전처리기 규칙 139:1을 활성화해야 합니다.
- 전처리기는 세션당 하나의 전역 임계값 이벤트를 생성합니다.
- 전역 이벤트 임계값은 개별 데이터 유형 이벤트와 상관없습니다. 즉 전처리기는 모든 개별 데이터 유형에 대한 이벤트 임계값에 도달했는지에 관계없이, 그리고 그 반대의 경우에도 그에 관계없이, 전역 임계값에 도달했을 때 이벤트를 생성합니다.

관련 항목

Firepower System IP 주소 규칙

개별 민감한 데이터 유형 옵션

최소한 각 맞춤형 데이터 유형은 이벤트 임계값 및 모니터링할 하나 이상의 포트 또는 애플리케이션 프로토콜을 지정해야 합니다.

시스템이 제공하는 각각의 데이터 유형은 다른 경우에는 액세스할 수 없는 `sd_pattern` 키워드를 사용하여 트래픽에서 탐지할 내장형 데이터 패턴을 정의합니다. 또한 간단한 정규 표현식을 사용하여 사용자 고유의 데이터 패턴을 지정할 수 있는 사용자 지정 데이터 유형을 생성할 수도 있습니다.

민감한 데이터 유형은 Senstivie Data Detection(민감한 데이터 탐지)가 활성화된 모든 침입 정책에 표시됩니다. 시스템에서 제공한 데이터 유형은 읽기 전용으로 표시됩니다. 맞춤형 데이터 유형의 경우, 이름 및 패턴 필드가 읽기 전용으로 표시되지만 다른 옵션은 정책별 값으로 설정할 수 있습니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 민감한 데이터 유형을 표시하며, 이 데이터 유형은 수정할 수 있습니다. 상위 도메인에서 생성된 데이터 유형도 표시되며, 이 데이터 유형은 제한적 방법으로 수정할 수 있습니다. 상위 데이터 유형의 경우, 이름 및 패턴 필드가 읽기 전용으로 표시되지만 다른 옵션은 정책별 값으로 설정할 수 있습니다.

표 *1:* 개별 데이터 유형 옵션

옵션	설명
데이터 유형	데이터 유형의 고유한 이름을 지정합니다.
임계값	시스템이 이벤트를 생성할 때 데이터 유형 발생 수를 지정합니다. 1부터 255까지 지정할 수 있습니다. 전처리기는 세션당 탐지한 데이터 유형에 대한 1가지 이벤트를 생성한다는 점에 유의하십시오. 전역 이벤트 임계값은 개별 데이터 유형 이벤트와 상관없습니다. 즉 전처리기는 전역 이벤트 임계값에 도달했는지 여부와 그 반대의 경우에도 관계없이, 데이터 유형 이벤트 임계값에 도달했을 때 이벤트를 생성합니다.
대상 포트	각 데이터 유형을 모니터링할 대상 포트를 지정합니다. 단일 포트나 쉼표로 구분된 포트 목록 또는 모든 대상 포트를 뜻하는 `any`(모든)를 지정할 수 있습니다.
애플리케이션 프로토콜	데이터 유형에 대해 모니터링하기 위해 최대 8개의 애플리케이션 프로토콜을 지정합니다. 모니터링할 애플리케이션 프로토콜을 식별하려면 애플리케이션 탐지기를 활성화해야 합니다. 기본 디바이스의 경우, 이 기능에는 제어 라이선스가 필요합니다.
패턴	탐지할 패턴을 지정합니다. 이 필드는 맞춤형 데이터 유형에만 있습니다.

관련 항목

탐지기 활성화 및 비활성화

시스템 제공 민감한 데이터 유형

각 침입 정책은 대시가 있거나 없는 신용 카드 번호, 전자 메일 주소, 미국 전화 번호 및 미국 사회 보장 번호와 같은 일반적으로 사용되는 데이터 패턴 탐지를 위한 시스템 제공 데이터 유형을 포함합니다.

각각의 시스템 제공 데이터 유형은 생성기 ID(GID) 138을 가진 단일 민감한 데이터 전처리기 규칙과 연결됩니다. 정책에서 사용할 각 데이터 유형에 대해 연결된 민감한 데이터 규칙을 침입 정책에서 활성화하여 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.해야 합니다.

다음 표에서는 각 데이터 유형을 설명하고 해당 전처리기 규칙을 나열합니다.

표 *2:* 시스템 제공 민감한 데이터 유형

데이터 유형	설명	전처리기 규칙 **GID:SID**
신용 카드 번호	표준 구분 대시나 공백을 사용하거나 사용하지 않고 Visa®, MasterCard®, Discover® 및 American Express® 15/16자리 신용 카드 번호를 매칭합니다. 또한 Luhn 알고리즘을 사용하여 신용 카드 확인 번호를 확인합니다.	138:2
이메일 주소	이메일 주소에 일치합니다.	138:5
미국 전화 번호	패턴 `(\d{3}) ?\d{3}-\d{4}`를 준수하는 미국 전화 번호를 매칭합니다.	138:6
대시 없는 미국 사회 보장 번호	유효한 3자리 지역 번호와 유효한 2자리 그룹 번호가 있으며 대시를 포함하지 않는 9자리 미국 사회 보장 번호를 매칭합니다.	138:4
대시 있는 미국 사회 보장 번호	유효한 3자리 지역 번호와 유효한 2자리 그룹 번호가 있으며 대시를 포함하는 9자리 미국 사회 보장 번호를 매칭합니다.	138:3

사회 보장 번호 외의 9자리 번호에서 오탐을 줄이기 위해 전처리기는 각 사회 보장 번호에서 4자리 일련 번호 앞에 오는 3자리 지역 번호와 2자리 그룹 번호를 검증하는 알고리즘을 사용합니다. 전처리기는 2009년 11월까지 사회 보장 그룹 번호를 승인합니다.

민감한 데이터 탐지 라이선스 요건

FTD 라이센스

위협

기본 라이선스

보호 또는 절차에 나와 있습니다.

민감한 데이터 탐지 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 침입 관리자

민감한 데이터 탐지 구성

민감한 데이터 탐지는 Firepower System의 성능에 큰 영향을 미칠 수 있으므로 Cisco에서는 다음 지침을 따를 것을 권장합니다.

- 기본 침입 정책으로 No Rules Active(활성 규칙 불가) 기본 정책을 선택합니다.
- 해당 네트워크 분석 정책에서 다음 구성이 활성화되어 있는지 확인하십시오.
  - **Application Layer Preprocessors(**애플리케이션 레이어 전처리기**)** 아래의 **FTP and Telnet Configuration(FTP** 및 텔넷 구성**)**
  - **Transport/Network Layer Preprocessors(**전송/네트워크 레이어 전처리기**)** 아래의 **IP Defragmentation(IP** 조각 모음**)** 및 **TCP Stream Configuration(TCP** 스트림 컨피그레이션**)**

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 정책을 표시하며 이러한 정책은 수정할 수 있습니다. 상위 도메인에서 생성된 정책도 표시되지만, 이러한 정책은 수정할 수 없습니다. 하위 도메인에서 생성된 정책을 보고 수정하려면 해당 도메인으로 전환하십시오.

시작하기 전에

클래식 디바이스의 경우, 이 절차에는 보호 또는 제어 라이선스가 필요합니다.

프로시저

단계 **1** 선택 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**

단계 **2** 편집하려는 정책 옆에 있는 수정( )을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 탐색 패널에서 **Advanced Settings(**고급 설정**)**를 클릭합니다.

단계 **4** **Specific Threat Detection(**특정 위협 탐지**)**의 **Sensitive Data Detection(**민감한 데이터 탐지**)**이 비활성화되었다면 **Enabled(**활성화**)**를 클릭합니다.

단계 **5** **Sensitive Data Detection(**민감한 데이터 탐지**)** 옆에 있는 수정( )을(를) 클릭합니다.

단계 **6** 다음 옵션을 이용할 수 있습니다.

- 전역 민감한 데이터 탐지 옵션, 2 페이지에 설명된 대로 전역 설정을 수정합니다.
- **Targets(**대상**)** 섹션에서 데이터 유형을 선택하고 개별 민감한 데이터 유형 옵션, 3 페이지에 설명된 대로 데이터 유형 구성을 수정합니다.
- 맞춤형 민감한 데이터를 검사하려면 맞춤형 데이터 유형을 생성합니다(맞춤형 민감한 데이터 유형, 10 페이지 참조).

단계 **7** 데이터 유형을 모니터링할 애플리케이션 프로토콜을 추가 또는 제거합니다(모니터링된 애플리케이션 프로토콜 및 민감한 데이터, 8 페이지 참조).

참고 FTP 트래픽에서 민감한 데이터를 탐지하려면 `Ftp data` 애플리케이션 프로토콜을 추가해야 합니다.

단계 **8** 원하는 경우, 민감한 데이터 전처리기 규칙을 표시하려면 **Configure Rules for Sensitive Data Detection(**민감한 데이터 탐지 규칙 구성**)**을 클릭합니다.

나열된 규칙 중 원하는 항목을 활성화 또는 비활성화할 수 있습니다. 또한 Rules(규칙) 페이지에서 규칙 억제, 속도 기반 공격 방지 등과 같은 사용 가능한 다른 작업에 대한 민감한 데이터 규칙을 구성할 수 있습니다. 자세한 내용은 침입 규칙 유형를 참고하십시오.

단계 **9** 마지막 정책 커밋 이후 이 정책에 적용된 변경 사항을 저장하려면 탐색창에서 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경 사항 커밋**)**를 클릭합니다.

민감한 데이터 탐지를 활성화하지 않고 정책에서 민감한 데이터 전처리기 규칙을 활성화한 경우, 정책에 변경 사항을 저장하면 민감한 데이터 탐지를 활성화하라는 메시지가 표시됩니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 침입 이벤트를 생성하려면 민감한 데이터 탐지 규칙 138:2, 138:3, 138:4, 138:5, 138:6, 138:>999999 또는 139:1을 활성화합니다. 자세한 내용은 침입 규칙 상태, 전역 민감한 데이터 탐지 옵션, 2 페이지, 시스템 제공 민감한 데이터 유형, 4 페이지, 맞춤형 민감한 데이터 유형, 10 페이지를 참고하십시오.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

관련 항목

특별 케이스: FTP 트래픽에서 민감한 데이터 탐지, 9 페이지

모니터링된 애플리케이션 프로토콜 및 민감한 데이터

각 데이터 유형에 대해 모니터링하기 위해 최대 8개의 애플리케이션 프로토콜을 지정할 수 있습니다. 선택한 각 애플리케이션 프로토콜에 대해 하나 이상의 탐지기가 활성화되어야 합니다. 기본적으로 모든 시스템 제공 탐지기는 활성화되어 있습니다. 애플리케이션 프로토콜에 활성화된 탐지기가 없는 경우, 시스템은 해당 애플리케이션의 모든 시스템 제공 탐지기를 자동으로 활성화합니다. 탐지기가 없는 경우, 시스템은 가장 최근에 수정된 해당 애플리케이션의 맞춤형 탐지기를 활성화합니다.

각 데이터 유형에 대해 모니터링하기 위해 최소 1개의 애플리케이션 프로토콜 또는 포트를 지정해야 합니다. 그러나 FTP 트래픽에서 민감한 데이터 탐지를 원하는 경우를 제외하고 Cisco는 완벽한 적용을 위해 애플리케이션 프로토콜을 지정할 때 해당 포트를 지정할 것을 권장합니다. 예를 들어 HTTP를 지정하는 경우, 잘 알려진 HTTP 포트 80도 구성할 수 있습니다. 네트워크의 새 호스트가 HTTP를 구현하면, 시스템은 새 HTTP 애플리케이션 프로토콜을 검색하는 사이에 포트 80을 모니터링합니다.

FTP 트래픽에서 민감한 데이터를 탐지하려는 경우, `FTP data` 애플리케이션 프로토콜을 지정해야 합니다. 포트 번호 지정에는 이점이 없습니다.

관련 항목

탐지기 활성화 및 비활성화

특별 케이스: FTP 트래픽에서 민감한 데이터 탐지, 9 페이지

모니터링할 애플리케이션 프로토콜 선택

시스템에서 제공하는 민감한 데이터 유형 및 맞춤형 민감한 데이터 유형에서 모니터링할 애플리케이션 프로토콜을 지정할 수 있습니다. 선택하는 애플리케이션 프로토콜은 정책별로 다릅니다.

시작하기 전에

클래식 디바이스의 경우 이 절차에는 제어 라이선스가 필요합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**을(를) 선택합니다.

단계 **2** 편집하려는 정책 옆에 있는 수정( )을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 탐색 패널에서 **Advanced Settings(**고급 설정**)**를 클릭합니다.

단계 **4** **Specific Threat Detection(**특정 위협 탐지**)**의 **Sensitive Data Detection(**민감한 데이터 탐지**)**이 비활성화되었다면 **Enabled(**활성화**)**를 클릭합니다.

단계 **5** **Sensitive Data Detection(**민감한 데이터 탐지**)** 옆에 있는 수정( )을 클릭합니다.

단계 **6** **Data Types(**데이터 유형**)**에서 데이터 유형 이름을 클릭합니다.

단계 **7** **Application Protocols(**애플리케이션 프로토콜**)** 필드 옆의 수정( )을 클릭합니다.

단계 **8** 다음 옵션을 이용할 수 있습니다.

- 모니터링할 애플리케이션 프로토콜을 추가하려면 **Available(**사용 가능**)** 목록에서 하나 이상의 애플리케이션 프로토콜을 선택한 다음 오른쪽 화살표(>) 버튼을 클릭합니다. 모니터링할 최대 8개의 애플리케이션 프로토콜을 추가할 수 있습니다.
- 애플리케이션 프로토콜을 모니터링에서 제거하려면 **Enabled(**활성화**)** 목록에서 선택한 다음 왼쪽 화살표(<) 버튼을 클릭합니다.

단계 **9** **OK(**확인**)**를 클릭합니다.

단계 **10** 마지막 정책 커밋 이후 이 정책에서 변경한 사항을 저장하려면 탐색 창에서 **Policy Information(**정책 정보**)**을 클릭하고 **Commit Changes(**변경사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

관련 항목

특별 케이스: FTP 트래픽에서 민감한 데이터 탐지, 9 페이지

특별 케이스: FTP 트래픽에서 민감한 데이터 탐지

어떤 트래픽에서 민감한 데이터를 모니터링할지를 결정할 때에는 일반적으로 모니터링할 포트를 지정하거나 구축에서 애플리케이션 프로토콜을 지정합니다.

그러나, 포트 또는 애플리케이션 프로토콜을 지정하는 것은 FTP 트래픽의 민감한 데이터를 탐지하는 데 충분하지 않습니다. FTP 트래픽 내 민감한 데이터가 FTP 애플리케이션 프로토콜의 트래픽에서 발견되는 일이 간헐적으로 발생하는데, 일시적 포트 번호를 사용하여 탐지하는 것을 어렵게 만듭니다. FTP 트래픽에서 민감한 데이터를 검색하려면 반드시 구성에 다음을 포함해야 합니다.

- FTP 트래픽에서 민감한 데이터 탐지를 활성화하려면 `FTP data` 애플리케이션 프로토콜을 지정합니다.

  FTP 트래픽에서 민감한 데이터를 탐지하는 특정 케이스의 경우 `FTP data` 애플리케이션 프로토콜을 지정해도 탐지되지 않습니다. 대신, 이는 FTP/텔넷 처리기의 신속한 처리를 통해 FTP 트래픽에서 민감한 데이터를 탐지하도록 합니다.

- FTP Data 탐지기(기본적으로 활성화됨)가 활성화되었는지 확인합니다.
- 민감한 데이터에 대해 모니터링하는 최소 1개의 포트가 구성에 포함되어 있는지 확인합니다.

FTP 트래픽에서 민감한 데이터에 대해 탐지만 원하는 가능성이 낮은 경우를 제외하면 FTP 포트를 지정할 필요가 없다는 점에 유의하십시오. 대부분의 민감한 데이터 구성은 HTTP 또는 이메일 포트와 같은 다른 포트를 포함합니다. 모니터링을 위해 1개의 FTP 포트만 지정하고 다른 포트는 지정하지 않을 경우, Cisco는 FTP 명령 포트 23을 지정할 것을 권장합니다.

관련 항목

FTP/텔넷 디코더
탐지기 활성화 및 비활성화
민감한 데이터 탐지 구성, 6 페이지

맞춤형 민감한 데이터 유형

맞춤형 데이터 유형을 생성할 때마다 생성기 ID(GID) 138과 1000000 이상의 Snort ID(SID), 즉 로컬 규칙의 SID를 갖는 단일한 민감한 데이터 전처리기 규칙도 생성됩니다.

연결된 민감한 데이터 규칙을 활성화하여 정책에서 사용할 각 맞춤형 데이터 유형에 대한 탐지 및 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.을 활성화해야 합니다.

민감한 데이터 규칙의 활성화에 도움이 되도록 구성 페이지의 링크를 통해 모든 시스템 제공 및 맞춤형 민감한 데이터 규칙을 표시하는 침입 정책 Rules(규칙) 페이지의 필터링된 보기로 이동할 수 있습니다. 또한 침입 정책 Rules(규칙) 페이지에서 로컬 필터링 카테고리를 선택하여 모든 로컬 맞춤형 지정 규칙과 함께 맞춤형 민감한 데이터 규칙을 표시할 수 있습니다. 맞춤형 민감한 데이터 규칙은 규칙 편집기 페이지(**Objects(**개체**)** > **Intrusion Rules(**침입 규칙**)**)에 나열되지 않습니다.

생성한 맞춤형 데이터 유형은 시스템의 모든 침입 정책 또는 다중 도메인 구축의 경우에는 현재 도메인에서 활성화할 수 있습니다. 맞춤형 데이터 유형을 활성화하려면 해당 맞춤형 데이터 유형 탐지에 사용할 정책에서 연결된 민감한 데이터 규칙을 활성화해야 합니다.

맞춤형 민감한 데이터 유형의 데이터 패턴

다음으로 구성된 정규식 단순 집합을 사용하여 사용자 지정 데이터 유형에 대한 데이터 패턴을 정의합니다.

- 3개의 메타 문자
- 메타 문자를 문자로 사용할 수 있도록 하는 이스케이프된 문자
- 6개의 문자 클래스

메타 문자는 정규 표현식에서 특정 의미가 있는 리터럴 문자입니다.

표 *3:* 민감한 데이터 패턴 메타 문자

메타 문자	설명	예
?	앞선 문자 또는 이스케이프 시퀀스에 0회 또는 1회 발생에 일치합니다. 즉, 앞선 문자 또는 이스케이프 시퀀스는 선택 사항입니다.	colou?r는 color 또는 colour에 일치합니다.
{n}	앞선 문자 또는 이스케이프 시퀀스에 n회 일치합니다.	예를 들어\d{2}는 55, 12 등과 일치하고, \l{3}은 AbC, www 등과 일치하며, \w{3}은 a1B, 25C 등과 일치하고, x{5}는 xxxxx와 일치합니다.
\	메타 문자를 실제 문자로 사용할 수 있으며, 미리 정의된 문자 클래스를 지정하는 데 사용할 수도 있습니다.	\?는 물음표와 일치하고, \\는 백슬래시에 일치하며, \d는 숫자 등과 일치합니다.

민감한 데이터 전처리기가 일부 문자를 리터럴 문자로 정확하게 해석하려면 백슬래시를 사용하여 해당 문자를 이스케이프해야 합니다.

표 *4:* 이스케이프된 민감한 데이터 패턴 문자

사용할 이스케이프된 문자	나타낼 문자
\?	?
\{	{
\}	}
\\	\

맞춤형 민감한 데이터 패턴을 정의할 때 문자 클래스를 사용할 수 있습니다.

표 *5:* 민감한 데이터 패턴 문자 클래스

문자 클래스	설명	문자 클래스 정의
\d	모든 숫자 ASCII 문자 0-9와 일치합니다.	0-9
\D	숫자 ASCII 문자가 아닌 모든 바이트와 일치합니다.	0-9 아님
\l(소문자 “ell")	모든 ASCII 문자와 일치합니다.	a-zA-Z
\L	ASCII 문자가 아닌 모든 바이트와 일치합니다.	a−zA−Z 아님

문자 클래스	설명	문자 클래스 정의
\w	모든 ASCII 영숫자 문자와 일치합니다. PCRE 정규식과는 달리, 이는 밑줄(_)을 포함하지 않는다는 점에 유의하십시오.	a-zA-Z0-9
\W	ASCII 영숫자 문자가 아닌 모든 바이트와 일치합니다.	a-zA-Z0-9 아님

전처리기는 직접 입력한 문자를 정규식의 일부 대신 문자로 처리합니다. 예를 들어, 데이터 패턴 1234는 `1234`에 일치합니다.

다음 데이터 패턴 예제는 시스템이 제공한 민감한 데이터 규칙 138:4에서 사용되는데, 미국 전화 번호를 검색하기 위해 이스케이프된 디지트 문자 클래스, 승수 및 옵션 지정자 메타 문자, 그리고 문자 대시(-) 및 좌우 괄호() 문자를 사용합니다.

```
(\d{3}) ?\d{3}-\d{4}
```

사용자 지정 데이터 패턴을 만들 때 주의를 기울이십시오. 올바른 구문을 사용하지만 많은 잘못된 긍정을 야기할 수도 있는 전화 번호 탐지를 위해 다음 데이터 패턴을 고려하십시오.

```
(?\d{3})? ?\d{3}-?\d{4}
```

두 번째 예제는 괄호(선택 사항), 스페이스(선택 사항) 및 대시(선택 사항)를 조합하므로 다음과 같은 원하는 패턴의 전화 번호를 탐지합니다.

- `(555)123-4567`
- `555123-4567`
- `5551234567`

그러나, 두 번째 예제 패턴은 또한 잘못된 긍정을 야기하는 다음과 같은 유효하지 않은 잠재적인 패턴을 탐지합니다.

- `(555 1234567`
- `555)123-4567`
- `555) 123-4567`

마지막으로 이해를 돕기 위해 소규모 회사 네트워크에서 모든 대상 트래픽의 낮은 이벤트 임계값을 사용하여 소문자 `a`를 탐지하는 데이터 패턴을 생성하는 극단적인 예를 고려하십시오. 이러한 데이터 패턴은 단지 몇 분 만에 사용자 시스템을 수백 만개의 이벤트로 마비시킬 수 있습니다.

맞춤형 민감한 데이터 유형 설정

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 민감한 데이터 유형을 표시하며, 이 데이터 유형은 수정할 수 있습니다. 상위 도메인에서 생성된 데이터 유형도 표시되며, 이 데이터 유형은 제

한적 방법으로 수정할 수 있습니다. 상위 데이터 유형의 경우, 이름 및 패턴 필드가 읽기 전용으로 표시되지만 다른 옵션은 정책별 값으로 설정할 수 있습니다.

침입 정책에서 데이터 유형에 대한 민감한 데이터 규칙이 활성화된 경우에는 해당 데이터 유형을 삭제할 수 없습니다.

프로시저

단계 **1** 선택 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**

단계 **2** 편집하려는 정책 옆에 있는 수정( )을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 탐색 패널에서 **Advanced Settings(**고급 설정**)**를 클릭합니다.

단계 **4** **Specific Threat Detection(**특정 위협 탐지**)**의 **Sensitive Data Detection(**민감한 데이터 탐지**)**이 비활성화되었다면 **Enabled(**활성화**)**를 클릭합니다.

단계 **5** **Sensitive Data Detection(**민감한 데이터 탐지**)** 옆에 있는 수정( )을 클릭합니다.

단계 **6** **Data Types(**데이터 유형**)** 옆에 있는 추가( )를 클릭합니다.

단계 **7** 데이터 유형의 이름을 입력합니다.

단계 **8** 이 데이터 유형으로 탐지할 패턴을 입력합니다(맞춤형 민감한 데이터 유형의 데이터 패턴, 10 페이지 참조).

단계 **9** **OK(**확인**)**를 클릭합니다.

단계 **10** 원하는 경우, 데이터 유형 이름을 클릭하고 개별 민감한 데이터 유형 옵션, 3 페이지에 설명된 옵션을 수정합니다.

단계 **11** 필요에 따라 삭제( )를 클릭하여 사용자 지정 데이터 유형을 삭제한 다음 **OK(**확인**)**를 클릭하여 확인합니다.

참고 침입 정책에서 해당 데이터 유형에 대한 민감한 데이터 규칙이 활성화된 경우에는 해당 데이터 유형을 삭제할 수 없다고 시스템이 경고합니다. 삭제를 다시 시도하려면 먼저 영향을 받는 정책에서 민감한 데이터 규칙을 비활성화해야 합니다(침입 규칙 상태 설정 참조).

단계 **12** 마지막 정책 커밋 이후 이 정책에 적용된 변경 사항을 저장하려면 탐색창에서 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경 사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 해당 데이터 유형을 사용하려는 각 정책에서 연결된 맞춤형 민감한 데이터 전처리 규칙을 활성화합니다(침입 규칙 상태 설정 참조).

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

관련 항목

맞춤형 민감한 데이터 유형 수정, 14 페이지

맞춤형 민감한 데이터 유형 수정

맞춤형 민감한 데이터 유형의 모든 필드를 편집할 수 있습니다. 하지만 이름 또는 패턴 필드를 수정하는 경우, 시스템의 모든 침입 정책에서 이러한 설정이 변경됩니다. 다른 옵션은 정책별 값으로 설정할 수 있습니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 민감한 데이터 유형을 표시하며, 이 데이터 유형은 수정할 수 있습니다. 상위 도메인에서 생성된 데이터 유형도 표시되며, 이 데이터 유형은 제한적 방법으로 수정할 수 있습니다. 상위 데이터 유형의 경우, 이름 및 패턴 필드가 읽기 전용으로 표시되지만 다른 옵션은 정책별 값으로 설정할 수 있습니다.

프로시저

단계 **1** 선택 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**

단계 **2** 편집하려는 정책 옆에 있는 수정( )을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 탐색 패널에서 **Advanced Settings(**고급 설정**)**를 클릭합니다.

단계 **4** **Specific Threat Detection(**특정 위협 탐지**)**의 **Sensitive Data Detection(**민감한 데이터 탐지**)**이 비활성화되었다면 **Enabled(**활성화**)**를 클릭합니다.

단계 **5** **Sensitive Data Detection(**민감한 데이터 탐지**)** 옆에 있는 **Edit(**편집**)**를 클릭 합니다.

단계 **6** **Targets(**대상**)** 섹션에서 맞춤형 데이터 유형의 이름을 클릭합니다.

단계 **7** **Edit Data Type Name and Pattern(**데이터 유형 이름 및 패턴 수정**)**을 클릭합니다.

단계 **8** 데이터 유형 이름 및 패턴을 수정합니다(맞춤형 민감한 데이터 유형의 데이터 패턴, 10 페이지 참조).

단계 **9** **OK(**확인**)**를 클릭합니다.

단계 **10** 나머지 옵션은 정책별 값으로 설정합니다(개별 민감한 데이터 유형 옵션, 3 페이지 참조).

단계 **11** 마지막 정책 커밋 이후 이 정책에 적용된 변경 사항을 저장하려면 탐색창에서 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경 사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.