네트워크 위협

안티맬웨어

안티 멀웨어 프로파일은 Talos ClamAV 바이러스 탐지 엔진을 사용하여 안티 멀웨어 보호를 활성화합니다. ClamAV®는 트로이 목마, 바이러스, 악성코드 및 기타 악성 위협을 탐지하기 위한 안티바이러스 엔진입니다.

다음 단계에서는 안티 멀웨어 프로파일을 생성하고 정책 규칙에 연결하는 방법을 설명합니다.

안티맬웨어 생성

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **Network Threats(**네트워크 위협**)**로 이동합니다.

단계 **2** **Anti-malware(**악성코드 차단**)**를 선택합니다.

단계 **3** Name(이름)과 Description(설명)을 제공합니다.

단계 **4** Talos 규칙 집합 버전 선택에 대해 수동 또는 자동 모드를 클릭합니다.

단계 **5** Manual(수동) 모드의 경우 드롭다운에서 Talos Ruleset Version(Talos 규칙 집합 버전)을 선택합니다. 선택한 규칙 집합 버전은 이 프로파일을 사용하는 모든 게이트웨이의 멀티 클라우드 방어 데이터 경로 엔진에 의해 사용되며 최신 규칙 집합 버전으로 자동 업데이트되지 않습니다.

단계 **6** Automatic(자동) 모드의 경우, 멀티 클라우드 방어에서 규칙 집합 버전을 게시한 후 구축을 며칠 단위로 지연할지 선택합니다. 멀티 클라우드 방어에서는 새 규칙 집합을 매일 게시하며 이 프로파일을 사용하는 게이트웨이는 N일 이상의 최신 규칙 집합 버전으로 자동 업데이트됩니다. 여기서 N은 드롭다운에서 선택한 "delay by days(지연 일수)" 인수입니다. 예를 들어 2021년 1월 10일의 구축을 5일 연기하도록 선택하는 경우 멀티 클라우드 방어 컨트롤러은(는) 1월 5일 또는 그 이전에 게시된 규칙 집합 버전을 선택합니다. 해당 규칙 집합 버전을 사용한 내부 테스트가 어떤 이유로 실패할 경우 멀티 클라우드 방어이(가) 게시되지 않을 수도 있습니다.

단계 **7** 바이러스 서명과 일치하는 항목이 발견된 경우 수행할 작업을 선택합니다.

다음에 수행할 작업

안티멀웨어 프로파일을 규칙 집합과 연결

이 문서를 확인하여 규칙 생성/편집

데이터 손실 방지(DLP)

DLP(Data Loss Prevention) 프로파일은 멀티 클라우드 방어 솔루션이 정방향 프록시(이그레스) 모드로 구축될 때 데이터에서 유출 패턴을 찾는 것을 탐지하고 조치를 취하는 정책 규칙을 지정할 수 있는 기능을 멀티 클라우드 방어 고객에게 제공합니다.

멀티 클라우드 방어은(는) 고객이 이를 통해 맞춤형 PCRE 기반 정규식 패턴 외에도 사회 보장 번호(SSN), AWS 비밀번호, 신용카드 번호와 같은 사전 패키징된 일반적인 데이터 패턴을 지정할 수 있도록 합니다. 따라서 쉽게 PCI, PII 및 PHI 데이터에 대한 보호를 시행하여 규정 준수 요건을 충족할 수 있습니다. 이 기능은 별도의 DLP(데이터 손실 방지) 서비스가 필요하지 않은 기존 멀티 클라우드 방어 기능 집합과 통합됩니다.

다음 단계에서는 DLP 프로필을 생성하고 정책 규칙과 연결하는 과정을 안내합니다.

데이터 손실 방지 프로파일 생성

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **Network Threats(**네트워크 위협**)**로 이동합니다.

단계 **2** **Create Intrusion Profile(**침입 프로파일 생성**)**을 클릭합니다.

단계 **3** **Data Loss Prevention(**데이터 손실 방지**)**을 선택합니다.

단계 **4** 프로파일의 이름과 설명을 제공합니다.

단계 **5** 테이블에 **DLP** 필터 목록을 입력합니다. 필요에 따라 행을 더 삽입하려면 **Add(**추가**)**를 클릭합니다.

- 필터에 대한 설명을 제공합니다.
- 드롭다운 목록에서 사전 정의된 정적 패턴(예: CVE 번호)을 선택하거나 사용자 정의 정규식을 제공합니다.
- 카운트를 입력하여 트래픽에서 패턴이 표시되어야 하는 횟수를 정의합니다.
- 패턴이 개수와 일치하는 경우 수행할 작업을 선택합니다.

참고 패턴이 더 제한적이므로 AWS 액세스 키 및 AWS 암호 키에 대해 사전 정의된 패턴이 DLP 검사에서 일치하지 않는 경우가 있습니다. DLP 프로파일에서 다음과 같은 완화된 사용자 지정 패턴을 사용하여 AWS 액세스 키와 AWS 암호 키를 탐지합니다. 하지만 이렇게 하면 오탐 로그 이벤트가 생성될 수 있습니다.

AWS 액세스 키: `(?<![A-Z0-9])[A-Z0-9]{20}(?![A-Z0-9])`

AWS 암호 키: `(?<![AZa-z0-9/+=])[A-Za-z0-9/+=]{40}(?![A-Za-z0-9/+=])`

다음에 수행할 작업

데이터 손실 방지 프로파일을 규칙 집합과 연결

이 문서를 확인하여 규칙을 생성/편집합니다.

네트워크 침입(IDS/IPS)

네트워크 침입 프로파일은 트래픽이 악의적이지 않은지 확인하는 트랜잭션을 평가하는 데 사용할 수 있는 침입 탐지 및 보호(IDS/IPS) 규칙의 모음입니다.

멀티 클라우드 방어에서는 다음 IDS/IPS 규칙 집합을 지원합니다.

Table 1: 멀티 클라우드 방어에서는 다음 ***IDS/IPS*** 규칙 집합을 지원합니다.

규칙 집합	설명
Talos 규칙	Rules규칙은 애플리케이션 및 프레임워크에 고급 수준의 보호를 제공하는 실제 조사, 침입 테스트 및 연구를 통해 수집된 인텔리전스를 기반으로 하는 Cisco의 고급 규칙 집합입니다.
사용자 지정 규칙	사용자 지정 규칙은 맞춤형 애플리케이션에 특수 수준의 보호를 제공하며 고객이 작성한 특정 규칙 집합입니다.

사용자 지정 규칙

하나 이상의 규칙을 포함하는 사용자 지정 규칙 규칙 집합은 멀티 클라우드 방어 IDS/IPS 보안 엔진에서 업로드되어 사용될 수 있습니다. 규칙 집합에 포함된 규칙은 특정 애플리케이션 및 프레임워크에 대해 고객이 필요로 하는 특수 애플리케이션 평가를 제공합니다. IDS/IPS 프로파일에 구성된 다른 규칙 집합을 평가하기 전에 IDS/IPS 프로파일에 포함된 사용자 지정 규칙을 먼저 평가합니다.

사용자 지정 규칙 규칙 집합을 업로드할 경우 파일은 확장자가 tar.gz인 Gzip 압축 TAR 파일이어야 합니다. 압축된 TAR 파일은 다음 파일로 구성됩니다.

- Readme 파일 - 규칙 집합의 설명을 제공하는 파일입니다.
- 변경 로그 파일 - 변경 기록을 나타내는 파일입니다.
- 규칙 폴더 - 하나 이상의 ModSecurity 형식의 규칙 파일로 구성된 폴더입니다. 각 파일에는 확장자.conf가 있어야 합니다. 폴더는 하나 이상의 규칙 파일을 포함해야 합니다(비워둘 수 없음). 각 파일은 ModSecurity 규칙 형식 지침을 따라야 합니다.

사용자 지정 **IDS/IPS** 규칙 업로드

단계 **1** **Manage(**관리**)** > **Threat Research(**위협 연구**)** > **Network Intrusion(**네트워크 침입**)**으로 이동합니다.

단계 **2** **Custom(**사용자 지정**)** 탭을 클릭합니다.

단계 **3** **Import(**가져오기**)** 버튼을 클릭하고 맞춤형 규칙 규칙 집합 파일을 업로드합니다.

IDS/IPS 프로파일 생성

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **Network Threats(**네트워크 위협**)**로 이동합니다.

단계 **2** **Create Intrusion Profile(**침입 프로파일 생성**)** > **Network Intrusion(**네트워크 침입 생성**)**을 클릭합니다.

a) 다음 일반 설정을 지정합니다.

1. 프로파일 이름 및 설명을 지정합니다.

2. 작업을 지정합니다.

- 프로파일 이름 및 설명을 지정합니다.
- **Rule Default(**규칙 기본값**)** - 트리거된 각 규칙에 지정된 작업에 따라 요청을 허용하거나 거부하고 이벤트를 로깅합니다.
- **Allow Log(**허용 로그**)** - 요청을 허용하고 이벤트를 로깅합니다.
- **Allow No Log(**허용 로그 없음**)** - 요청을 허용하고 이벤트를 로깅하지 않습니다.
- **Deny Log(**거부 로그**)** - 요청을 거부하고 이벤트를 로깅합니다.
- **Deny No Log(**거부 로그 없음**)** - 요청을 거부하고 이벤트를 로깅하지 않습니다.

3. IDS/IPS 프로파일이 악의적인 활동을 탐지하는 경우 위협 PCAP 파일을 생성할지 여부를 지정합니다.

b) 규칙 집합을 지정합니다.

Note 규칙 라이브러리(Talos, 사용자 지정)에서 하나 이상의 규칙 집합을 IDS/IPS 프로파일을 지정해야 합니다.

Talos 규칙 및 사용자 지정 규칙 규칙 집합을 사용하는 경우, 둘 중 하나 이상을 활성화해야 합니다.

전체 IDS/IPS 프로파일을 비활성화하려는 경우 정책 규칙 집합 규칙에서 IDS/IPS 프로파일을 제거하면 IDS/IPS 프로파일이 평가되지 않습니다.

Talos 규칙:

1. *Disabled(*비활성화됨*)*, *Manual(*수동*)*, *Automatic(*자동*)**을 지정합니다.

- *Disabled(*비활성화됨*)* - Talos 규칙 사용을 비활성화할지 여부를 지정합니다(위의 기술 노트 참조).
- *Manual(*수동*)* - 사용할 Talos 규칙 버전을 지정합니다.
- *Automatic(*자동*)* - 게시 날짜로부터 최신 Talos Rules 버전으로의 자동 업데이트를 연기할 기간(일)을 지정합니다.

2. IDS/IPS 프로파일에 특정 Talos 규칙 규칙 집합을 추가합니다.

사용자 지정 규칙:

1. *Disabled(*비활성화됨*)*, *Manual(*수동*)*, *Automatic(*자동*)**을 지정합니다.
   - *Disabled(*비활성화됨*)* - 사용자 지정 규칙 사용을 비활성화할지 여부를 지정합니다(위의 기술 노트 참조).
   - *Manual(*수동*)* - 사용할 사용자 지정 규칙 버전을 지정합니다.
   - *Automatic(*자동*)* - 게시 날짜로부터 최신 사용자 지정 규칙 버전으로의 자동 업데이트를 지연하는 기간(일)을 지정합니다.
2. IDS/IPS 프로파일에 특정 사용자 지정 규칙 규칙 집합을 추가합니다.

c) 고급 설정을 지정합니다.

Rules Suppression(규칙 억제**):** 특정 IP 또는 CIDR 목록에 대한 규칙을 억제할 수 있습니다.

1. **Advanced Settings(**고급 설정**)** 탭을 클릭합니다.
2. Rule Suppression(규칙 억제)에서 **Add(**추가**)**를 클릭합니다.
3. **Source IP/CIDR List(**소스 **IP/CIDR** 목록**)**에서 쉼표로 구분된 IP 또는 CIDR 목록을 제공합니다.
4. **Rule ID List(**규칙 **ID** 목록**)**에 쉼표로 구분된 규칙 ID 목록을 제공합니다.
5. **Action(**작업**)**의 경우 선택 항목을 제공하지만 이 선택은 억제되는 규칙이 평가되지 않으므로 적용되지 않습니다.

d) 이벤트 필터링을 지정합니다.

IDS/IPS 프로파일이 트리거될 때 생성되는 보안 이벤트 수를 줄이기 위해 이벤트 속도를 제한하거나 샘플링하도록 이벤트 필터링을 구성할 수 있습니다. 설정은 탐지 또는 보호 동작을 변경하지 않습니다.

Type(유형)을 *Rate(*속도*)*로 지정하면 생성되는 이벤트는 *Time(*시간*)* 평가 간격(초) 동안 트리거된 지정된 *Number of Events(*이벤트 수*)*에 따라 속도가 제한됩니다. 예를 들어 *Number of Events(*이벤트 수*)*가 50으로 지정되고 *Time(*시간*)*이 5초로 지정된 경우 초당 10개 이벤트만 생성됩니다.

Type(유형)을 *Sample(*샘플*)*로 지정하면 생성된 Events(이벤트)는 지정된 *Number of Events(*이벤트 수*)*를 기준으로 샘플링됩니다. 예를 들어 *Number of Events(*이벤트 수*)*가 10으로 지정된 경우, 트리거된 10개 이벤트마다 1개의 이벤트만 생성됩니다.

프로파일 이벤트 필터링:

- Type(유형)을 **Rate(**속도**)** 또는 **Sample(**샘플**)**로 지정합니다.
  - *Rate(*속도*)* - *Number of Events(*이벤트 수*)* 및 *Time(*시간*)* 평가 간격(초)을 지정합니다.
  - *Sample(*샘플*)* - *Number of Events(*이벤트 수*)*를 지정합니다.

규칙 이벤트 필터링

1. **Rule Event Filtering(**규칙 이벤트 필터링**)** 아래에서 **Add(**추가**)**를 클릭합니다.

2. *Rule ID List(*규칙 *ID* 목록*)*에서 쉼표로 구분된 *Rule ID(*규칙 *ID)* 목록을 지정합니다.
3. Type(유형)을 *Rate(*속도*)* 또는 *Sample(*샘플*)*로 지정합니다.
   - *Rate(*속도*) - Number of Events(*이벤트 수*)* 및 *Time(*시간*)* 평가 간격(초)을 지정합니다.
   - *Sample(*샘플*) - Number of Events(*이벤트 수*)*를 지정합니다.

What to do next

이벤트 필터링 프로파일 연결:

이 문서를 확인하여 규칙을 생성/편집합니다.