각 Firepower Intrusion Base 정책의 기본 규칙 세트를 결정하는 데 사용되는 메트릭은 무엇입니까?

목차

소개

Cisco Talos는 최신 위협 및 취약성을 해결하기 위해 SRU(Snort Rule Updates)를 릴리스합니다.새 SRU 릴리스에는 각 기본 정책에 대해 업데이트된 규칙 세트가 포함될 수 있습니다.이 문서에서는 Talos에서 Firepower 디바이스에 대한 각 침입 기반 정책에 규칙이 할당되는 방법을 결정하기 위해 사용하는 프로세스에 대해 설명합니다.

규칙 메타데이터에 정의된 Talos 기본 정책 의도

기본 정책은 SRU 자체 내의 메타데이터에 의해 유지 관리됩니다.기본 정책의 제공 규칙의 상태는 규칙 본문의 메타데이터 부분에 정의됩니다.예:

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"MALWARE-CNC 1.php outbound connection
attempt"; sid:38753; gid:3; rev:1; classtype:trojan-activity; metadata:engine shared, soid
3|38753, policy balanced-ips drop, policy security-ips drop, impact_flag red; )
```

위에 표시된 예제 규칙의 경우 메타데이터 섹션에는 policy balanced-ips drop, policy security-ips drop이 포함되어 있습니다.이는 이 규칙 1:38753이 활성화되고 Balanced *Security and Connectivity 정책*과 *Security Over Connectivity 정책*에 *드롭되도록 설정되었음을* 나타냅니다.

기본 규칙 세트를 결정하는 데 사용되는 메트릭

- 사용되는 기본 메트릭은 규칙이 적용될 수 있는 각 취약성에 할당된 CVSS(Common Vulnerability Scoring System) 점수입니다.
- 두 번째 메트릭은 일시적인 기반이며 특정 취약성의 나이를 염려합니다.
- 최종 측정 단위는 규칙에 대한 적용 범위의 특정 영역입니다.예를 들어, SQL 삽입 규칙은 정책 포함에 대해 고려할 때 영향력을 가질 수 있을 만큼 중요한 것으로 간주됩니다.

참고:이러한 카테고리의 규칙에서 다루는 취약성은 연령에 관계없이 중요한 것으로 간주됩니

다.

보안 기반 정책을 통한 연결

참고:연결 정책은 정책의 보안 제어보다 장치 성능을 지원하도록 특별히 설계되었습니다.대부분의 네트워크 구축에서 고객은 오탐 및 정격 성능을 최소화하면서 Cisco 디바이스 중 하나를 구축할 수 있어야 합니다.또한 이 정책은 고객이 경험하는 가장 일반적인 가장 일반적인 위협을 탐지해야 합니다.

1. CVSS 점수는 10이어야 합니다.

2. 취약성이 최근 2년(포함)부터 발생합니다. 예:

- 현재 연도(예: 2019)
- 작년(이 예에서는 2018년)
- 마지막 이전 연도(이 예에서는 2017년)

3. 규칙 범주

- 이 정책에 사용되지 않음

균형 잡힌 기본 정책

참고: Balanced 정책은 초기 구축에 권장되는 기본 정책입니다.이 정책은 Cisco 시스템의 보안 요구 사항과 성능 특성 간의 균형을 이루려고 합니다.고객은 이 정책으로 시작하여 공공 평가 툴을 통해 매우 우수한 차단율을, 평가 및 테스트 툴을 통해 상대적으로 높은 성능을 얻을 수 있어야 합니다.또한 이 정책은 와일드 네트워킹 상황에서 정상적으로 디바이스의 정격 용량의 80%를 수행해야 합니다.Balanced 정책에 항상 유의해야 할 중요한 점은 고객이 잘못된 긍정, 제한적인 탐지, 성능 저하를 경험했을 경우 대부분의 고객이 인프라 구축을 위해 다른 디바이스를 조사한다는 것입니다.Snort.org에서 판매되는 Open-Source Snort용 Snort Subscriber Rule Set의 기본 배송 상태입니다.

1. CVSS 점수 9 이상

2. 취약성이 최근 2년(포함)부터 발생합니다. 예:

- 현재 연도(예: 2019)
- 작년(이 예에서는 2018년)
- 마지막 이전 연도(이 예에서는 2017년)

3. 규칙 범주

- 악성코드-CnC
- 블랙리스트
- SQL 삽입
- 익스플로잇 킷

4. 규칙이 **연결** 정책에 있는 경우

연결 기반 정책에 대한 보안

> **참고:보안** 정책은 조직 보안에 특히 관심을 갖는 고객 기반의 소규모 부문을 위해 설계되었습니다.고객은 대역폭 요구사항이 낮지만 보안 요구 사항이 훨씬 높은 보호 네트워크에 이 정책을 구축합니다.또한 고객은 오탐과 잡음이 많은 서명에 대해 덜 관심을 갖습니다.애플리케이션 제어 및 네트워크 사용량 잠금이 이 정책을 구축하는 고객에게도 문제가 됩니다.최대 보호 및 애플리케이션 제어를 제공해야 하지만 네트워크를 중단해서는 안 됩니다.

1. CVSS 점수 8 이상

2. 취약성이 최근 3년(포함)부터 발생합니다. 예:

   - 현재 연도(예: 2019)
   - 작년(이 예에서는 2018년)
   - 마지막 이전 연도(이 예에서는 2017년)
   - 이전 연도(이 예에서는 2016년)
3. 규칙 범주

   - 악성코드-CnC
   - 블랙리스트
   - SQL 삽입
   - 익스플로잇 킷
4. 규칙이 **균형** 및 **연결** 정책에 있는 경우

Max-Detect(최대 탐지) 기본 정책:

> **참고:**Maximum **Detection** 규칙 세트는 테스트 환경에서 사용되어야 하며 성능에 최적화되어 있지 않습니다.이 정책의 많은 규칙에 대한 오탐(False Positives)은 허용되며/또는 예상되며 FP 조사는 일반적으로 진행되지 않습니다.

1. 현장 테스트를 위해 커버리지가 필요합니다.

2. **보안**, **균형** 및 **연결** 규칙 집합**에** 규칙을 포함합니다.

3. SID 위에 있는 모든 활성 규칙을 포함합니다.달리 명시되지 않는 한 10000.

정책 업데이트 빈도

모든 새 규칙은 이러한 기준에 따라 정책에 배치됩니다.**매년** 정책은 재평가되고 취약성 연령에 따라 이전 연도의 규칙은 정책에서 제거되어 당사**의** 임시 선택 기준을 준수합니다.

규칙에 의해 적용되는 특정 취약성에 대한 CVSS 점수가 변경될 경우 CVSS 메트릭을 기반으로 한 정책에 있는 것이 재평가됩니다.

정책은 지속적으로 성장합니다.주요 리밸런싱을 통해 특정 목표에 맞게 조정되는 것 외에도, 제품의 규칙 수 및 정책 성능에 만족하는 경우 정책에서 주요 규칙 삭제가 항상 발생하는 것은 아닙니다.

참고:기본 정책은 연간 주요 리밸런싱과는 별도로 성장하여 특정 목표에 맞출 수 있습니다 .Talos가 일반적인 네트워크 조건에서 제품의 규칙 수 및 정책 성능에 만족하면 정책에서 주요 규칙 삭제가 항상 발생하는 것은 아닙니다. 나열된 정책의 규칙은 규칙별로 평가됩니다.이전 규칙이며 위의 기준에 없는 일부 규칙이 기본 정책에 포함됩니다.위의 내용은 기본 규칙의 선택 기준이며 위협 환경에 따라 항상 변경될 수 있습니다.

참고: 나열된 정책의 규칙은 규칙별로 평가됩니다.이전 규칙이며 위의 기준에 없는 일부 규칙이 기본 정책에 포함됩니다.위의 내용은 기본 규칙의 선택 기준이며 위협 환경에 따라 항상 변경될 수 있습니다.