적응형 프로파일

다음 주제에서는 적응형 프로파일을 설정하는 방법을 설명합니다.

적응형 프로파일 정보

다음을 수행하려면 적응형 프로파일을 활성화해야 합니다.

- AMP(Malware Protection)를 비롯한 애플리케이션 및 파일 제어를 수행하고 침입 규칙이 서비스 메타 데이터를 사용하도록 허용합니다.

주의 액세스 컨트롤 규칙이 AMP를 비롯한 애플리케이션 또는 파일 제어를 수행하거나, 침입 규칙이 서비스 메타데이터를 사용하게 하려면 적응형 프로파일 구성, 5 페이지에서 설명한 대로 적응형 프로파일을 반드시 활성화(기본 상태)해야 합니다.

- 패시브 구축에서는 적응형 프로파일 업데이트를 활성화하여 대상 호스트의 운영 체제에 따라 IP 트래픽을 조각 모음하고 리어셈블합니다.

참고 인라인 구축의 경우, Cisco는 적응형 프로파일 업데이트를 활성화하는 대신 **Normalize TCP Payload(TCP** 페이로드 표준화**)** 옵션이 활성화된 인라인 표준화 전처리기를 구성할 것을 권장합니다.

적응형 프로파일 라이선스요구 사항

Threat Defense 라이선스

IPS

기본 라이선스

보호

적응형 프로파일 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 액세스 관리자
- 네트워크 관리자

적응형 프로파일 업데이트

일반적으로, 시스템은 트래픽을 전처리하고 분석하기 위해 네트워크 분석 정책의 정적 설정을 사용합니다. 적응형 프로파일 업데이트을 이용하면, 시스템은 네트워크 검색으로 탐지하거나 서드파티로부터 가져온 호스트 정보를 이용해 처리 동작을 조정할 수 있습니다.

프로파일 업데이트대상 기반 프로파일에서처럼 네트워크 분석 정책에서 수동으로 설정할 수 있어, 대상 호스트의 운영체제와 같은 방식으로 IP 패킷을 조각 모음하고 스트림을 리어셈블하는 데 도움이 됩니다. 침입은 엔진을 통제한 다음 대상 호스트에서 사용하는 것과 동일한 형식으로 데이터를 분석합니다.

수동으로 설정한 대상 기반 프로파일은 사용자가 선택한 기본 운영체제 프로파일이나 특정 호스트에 구속한 프로파일을 적용합니다. 하지만 프로파일 업데이트은(는) 대상 호스트의 호스트 프로파일 내 운영체제에 맞는 적절한 운영체제 프로파일로 전환합니다.

10.6.0.0/16 서브넷에 프로파일 업데이트을(를) 구성하고 Linux에 기본 IP Defragmentation(조각 모음) 대상 기반 정책을 설정하는 방법을 고려해 보십시오. 설정을 구성하는 management center에는 10.6.0.0/16 서브넷을 포함하는 네트워크 맵이 있습니다.

- 시스템에서 10.6.0.0/16 서브넷에 없는 호스트 A의 트래픽을 탐지하면 디바이스는 Linux 대상 기반 정책을 사용하여 IP 조각을 리어셈블합니다.
- 10.6.0.0/16 서브넷에 있는 호스트 B의 트래픽을 탐지하면, 시스템은 네트워크 맵에서 호스트 B의 운영체제 데이터를 검색합니다. 시스템은 해당 운영체제를 기반으로 하는 프로파일을 이용해 호스트 B로 향하는 트래픽을 조각 모음합니다.

적응형 프로파일 업데이트 및 Cisco 추천 규칙

적응형 프로파일 업데이트 기능은 액세스 제어 정책에 의해 호출되는 모든 침입 정책에 전역 적용되는 액세스 제어 정책의 고급 설정입니다. Cisco 권장 규칙 기능은 이 기능을 구성하는 개별 침입 정책에 적용됩니다.

Cisco 권장 규칙과 마찬가지로 프로파일 업데이트은 규칙의 메타데이터를 호스트 정보와 비교하여 특정 호스트에 규칙을 적용해야 할지 여부를 결정합니다. 그러나 Cisco 권장 규칙은 해당 정보를 사용하여 규칙의 활성화 또는 비활성화를 위한 권장 사항을 제공하는 반면 프로파일 업데이트은 해당 정보를 사용하여 특정 트래픽에 특정 규칙을 적용합니다.

Cisco 권장 규칙의 경우, 제안된 변경 사항을 규칙 상태에 구현하기 위해 상호 작용이 필요합니다. 반면 프로파일 업데이트은 침입 정책을 수정하지 않습니다. 프로파일 업데이트에 기반한 규칙 처리는 패킷별로 이루어집니다.

또한 Cisco 권장 규칙으로 비활성화된 규칙이 활성화될 수 있습니다. 반면 프로파일 업데이트은 침입 정책에서 이미 활성화된 규칙의 적용에만 영향을 미칩니다. 프로파일 업데이트은 규칙 상태를 변경하지 않습니다.

프로파일 업데이트과 Cisco 권장 규칙을 조합해 사용할 수 있습니다. 프로파일 업데이트은 침입 정책을 구축할 때 규칙의 규칙 상태를 사용하여 해당 규칙을 적용 후보로 포함할지 여부를 결정하며, 권장 사항을 수락하거나 거부하는 사용자의 선택은 해당 규칙 상태에 반영됩니다. 두 가지 기능을 모두 사용하여 모니터링하는 각 네트워크에 가장 알맞은 규칙이 활성화 또는 비활성화되었는지 확인할 수 있으며, 그런 다음 활성화된 규칙을 특정 트래픽에 가장 효율적으로 적용할 수 있습니다.

관련 항목

Cisco 권장 규칙 정보

적응형 프로파일 옵션

Enable

다음에 대해 이 옵션을 활성화해야 합니다.

- 악성 코드 보호(AMP)를 비롯해서 애플리케이션 및 파일 제어를 수행하기 위한 액세스 제어 규칙

- 서비스 메타데이터를 사용하는 침입 규칙

이 옵션은 기본적으로 활성화되어 있습니다.

참고 Snort 3에서 적응형 프로파일을 활성화하려면 **Enable(**활성화**)** 및 **Enable Profile Updates(**프로파일 업데이트 활성화**)** 옵션을 모두 선택해야 합니다.

프로파일 업데이트 활성화

수동 구축에서는, 프로파일 업데이트를 활성화해 네트워크 맵에 있는 호스트가 사용하는 운영체제의 프로파일에 따라 IP 트래픽을 조각 모음하고 리어셈블해야 합니다.

Snort 3의 경우 적응형 프로파일이 활성화된 경우 이를 반드시 활성화해야 합니다.

적응형 프로파일 - 특성 업데이트 간격

프로파일 업데이트를 활성화하면, 사용자는 네트워크 맵 데이터가 management center에서 매니지드 디바이스로 동기화되는 간격(단위: 분)을 제어할 수 있습니다. 시스템은 데이터를 사용하여 트래픽을 처리할 때 어떤 프로파일을 사용할지 결정합니다. 이 옵션 값을 높이면 대규모 네트워크 성능을 개선할 수 있습니다.

적응형 프로파일 - 네트워크

원한다면 프로파일 업데이트를 활성화했을 때 프로파일 업데이트을(를) IP 주소, 주소 블록 및 네트워크 변수의 쉼표로 구분된 목록에 제한하여 성능을 개선할 수도 있습니다. 네트워크 변수를 사용한다면, 시스템은 액세스 컨트롤 정책에 대한 기본 침입 정책과 연결된 변수 모음의 변수 값을 사용합니다. 예를 들어 **192.168.1.101, 192.168.4.0/24, $HOME_NET**을 입력할 수도 있습니다. IPv4 및 IPv6가 지원됩니다.

기본값(**0.0.0.0/0**)은 적응형 프로파일 업데이트를 모든 네트워크에 적용합니다.

참고 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. 상위 정책에서 프로파일 업데이트을(를) 활성화하고 실행했다면, Cisco는 기본 네트워크 제약 조건을 **0.0.0.0/0**으로 유지하거나 `any` 값이 있는 네트워크 변수를 사용하도록 권장합니다. 이 설정은 프로파일 업데이트을(를) 모든 하위 도메인에서 모니터링되는 모든 호스트에 적용합니다.

관련 항목

트래픽이 식별되기 전에 통과하는 패킷 검사
변수 세트

적응형 프로파일 구성

수동 구축의 경우 Cisco는 적응형 프로파일 업데이트 구성을 권장합니다. 인라인 구축의 경우에는 **Normalize TCP Payload(TCP** 페이로드 표준화**)** 옵션이 활성화된 인라인 표준화 전처리기를 설정해야 합니다.

⚠

주의 액세스 컨트롤 규칙이 AMP를 비롯한 애플리케이션 또는 파일 제어를 수행하거나, 침입 규칙이 서비스 메타데이터를 사용하게 하려면 적응형 프로파일을 반드시 활성화(기본 상태)해야 합니다.

시작하기 전에

액세스 제어 정책에는 호스트/서비스 검색을 수행할 수 있는 네트워크 검색 정책이 있어야합니다. 또는 서드파티 소스에서 호스트 데이터를 가져와야 합니다.

프로시저

단계 **1** 액세스 컨트롤 정책 편집기에서 **Advanced(**고급**)**을 클릭하고 Detection Enhancement Settings(탐지 개선 설정) 섹션 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

보기 아이콘(**View(**보기**)** ( ))이 대신 표시되는 경우에는 설정이 상위 정책에서 상속되거나 설정을 수정할 권한이 없는 것입니다.구성이 잠금 해제되어 있으면 **Inherit from base policy(**기본 정책에서 상속**)**의 선택을 취소하여 수정을 활성화합니다.

단계 **2** 적응형 프로파일 옵션, 3 페이지에 설명된 대로 적응형 프로파일 옵션을 설정합니다.

단계 **3** **OK(**확인**)**를 클릭합니다.

단계 **4** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- Deploy configuration changes(구성 변경 사항 구축)참조.

관련 항목

인라인 정상화 전처리기
Snort® 재시작 시나리오