XDR-A에서 온-프레미스 디바이스, 호스트 이름 및 IP 매핑 이해

목차

소개

이 문서에서는 디바이스 호스트 이름 및 IP 매핑과 관련하여 XDR-Analytics 동작을 이해하는 방법에 대해 설명합니다.

배경

XDRA는 시간이 지남에 따라 논리적 디바이스 동작(디바이스라고 함)을 추적하려고 시도합니다.

네트워크 트래픽을 시간이 지남에 따라 이러한 논리적 디바이스에 상관시키는 데 다양한 기술을 사용합니다.

그러나 특히 온프레미스 환경에서는 시스템이 트래픽을 디바이스에 얼마나 잘 연결할 수 있는가에 대한 제한이 있습니다.

XDRA는 주로 ONA, CTB 또는 Cisco Meraki 통합("새로운" Meraki 통합)을 통해 netflow를 통해 온프레미스 환경에 대한 텔레메트리를 수집합니다. 둘째, 다음을 통해 호스트 이름 확인을 얻을 수 있습니다.

- 역방향 DNS 조회를 통한 활성 호스트 이름 확인 및 선택적으로 ONA를 통한 SMB 쿼리
- ONA를 통한 ISE 통합
- "기존" Meraki 통합
- NVM 통합, 추가 주의 사항

Netflow에는 호스트 이름 정보가 없는 IP 주소가 있습니다.

호스트 이름 정보가 없을 경우, 더 지능적인 디바이스 연결을 위한 추가 정보가 없기 때문에 표시된 각 내부 IP 주소(아래 정의 참조)가 디바이스인 것으로 가정합니다.

호스트 이름 컬렉션이 구성된 경우 XDRA는 호스트 이름을 사용하여(표시되는 경우) 디바이스의 내부 표시에 연결합니다.

이를 통해 XDRA는 시간에 따라 여러 IP 주소를 하나의 디바이스에 그룹화할 수 있습니다.

NVM 원격 분석은 XDR의 일부로 선택적으로 구성할 수 있습니다.

이 텔레메트리 소스는 netflow와 유사한 데이터 피드를 제공하지만 고유한 식별자를 포함한 엔드포인트 정보도 제공합니다.

XDRA에서 이 정보를 활용하는 방식은 호스트 이름 수집이 ONA에서 활성화된 경우와 유사하게 디바이스 추적이 작동하는 데 따른 최종 효과가 있습니다.

이러한 설정은 모두 사용 가능한 텔레메트리의 제한에 따라 제한이 있습니다.

참고 XDRA는 IP 주소 및 호스트 이름 매핑의 특성이 다대일 관계라고 가정합니다(많은 IP가 하나의 호스트 이름에 매핑될 수 있음).

하나의 논리적 디바이스는 여러 IP를 동시에 가질 수 있습니다(예: 두 개의 물리적 인터페이스 또는 IPv4 및 IPv6).

모니터링의 특성상 XDRA는 특정 시점에 실제 네트워크의 모든 관계를 가진다고 가정할 수 없습니다.

겹치는 서브넷

단일 XDRA 테넌트가 여러 온프레미스 서브넷을 동시에 모니터링하는 경우, 시스템은 각 서브넷에 표시되는 동일한 IP를 구분할 수 없습니다.

따라서 IP와 디바이스의 상관관계를 과도하게 파악합니다. 호스트 이름을 사용할 수 있다고 해서 이 상황이 개선되지는 않습니다.

이 문제를 해결하는 한 가지 방법은 둘 이상의 XDRA 포털(서브넷당 하나)을 보유하는 것입니다. 또 다른 방법은 "새로운" Cisco Meraki 통합을 사용하는 것입니다. 이 통합으로 인한 네임스페이스 격리 때문입니다.

사용 가능한 호스트 이름 정보가 없는 환경

제한된 텔레메트리 정보의 부작용으로 인해 시스템에서 디바이스 내역을 잘못 이해할 수 있습니다.

한 가지 시나리오는 IP가 동적으로 할당되는 경우입니다. XDRA는 기본 논리적 디바이스가 변경되었음을 알 수 있는 방법이 없습니다. 예를 들어 WIFI의 랩톱이 사라지고 IP가 새 랩톱에 할당되는 경우입니다.

호스트 이름 또는 기타 식별 정보가 없는 경우 시스템은 여러 논리적 디바이스의 활동을 하나의 디바이스에 연결합니다. 이로 인해 디바이스 프로파일 정보가 혼란스러워질 수 있습니다.

```
Actual Situation
    t0      t1      t2      t3
ip1 d1------        d2------

As seen by XDRA
    t0      t1      t2      t3
ip1 d1----------------------
```

반대로, 하나의 논리적 디바이스에 둘 이상의 IP 주소가 있는 경우(예: 두 개의 물리적 인터페이스 또는 IPv4 및 IPv6), 이를 동일한 디바이스에 안정적으로 연결할 수 있는 정보가 없으므로 시스템은 이를 수행하지 않습니다.

```
Actual Situation
    t0      t1      t2      t3
ip1 d1--------------
ip2 d1--------------

As seen by XDRA
    t0      t1      t2      t3
ip1 d1--------------
ip2 d1--------------
```

호스트 이름 정보가 있는 환경

여기서 XDRA는 호스트 이름 정보를 볼 수 있으며 시스템은 하나 이상의 IP 주소를 하나의 디바이스에 연결할 수 있습니다. 그러나 데이터의 특성을 감안할 때 시스템에서 안정적으로 확인할 수 있는 사항에는 여전히 한계가 있습니다. 이로 인해 IP가 시스템의 디바이스에 과상관(over-correlation)될 수 있습니다.

XDRA에서 IP와 호스트 이름 간의 연결이 설정된 디바이스에서 논리적 디바이스가 IP 주소를 변경하는 경우, 원격 측정은 결국 새 IP를 호스트 이름에 반영합니다.

그러나 이것이 다대일 관계일 가능성이 있기 때문에 XDRA는 이전에 확인한 IP가 더 이상 호스트 이름(및 따라서 디바이스)과 연결되지 않는다고 가정할 수 없습니다.

예를 들어 동일한 논리적 디바이스에 대한 별도의 물리적 인터페이스가 될 수 있습니다. 따라서 XDRA는 IP 주소를 다른 호스트 이름에 긍정적으로 매핑하는 텔레메트리를 확인할 때까지 이전에 확인한 IP와 가장 최근에 확인한 IP를 모두 유지합니다.

이때 XDR은 매핑을 '만료'하고 이전 IP 주소로 나열합니다.

시스템이 연관성을 '조기'로 깨라고 말할 수 있는 방법은 없다.

호스트 이름 일치에 대한 참고 사항

테넌트가 여러 도메인에 구성된 동일한 호스트 이름을 갖는 경우를 더 잘 처리하기 위해 XDRA는 '유연한' 일치를 채택하고, 기존 디바이스(즉, 일치하는 IP의 경우)와 일치할 경우 이 테이블에 표시된 항목을 일치하는 호스트 이름으로 처리합니다.

```
example
example.com
example.net
example.obsrvbl.com
example.invalid.obsrvbl.com
example.example.com
```

즉, 도메인 이름의 나머지 부분은 무시하면서 호스트 이름만 고려합니다.

NVM이 있는 환경

이 설정은 호스트 이름 정보가 있는 호스트 이름 정보 섹션의 환경과 매우 유사하지만 몇 가지 차이점이 있습니다.

이 데이터 피드는 사용자에게 몇 가지 고유한 엔드포인트 식별자를 제공할 수 있다는 추가적인 이점을 제공합니다. 이러한 ID를 사용하면 호스트 이름이 변경되는 물리적 디바이스를 추적할 수 있습니다(다른 방법으로는 추적할 수 없음, 2개의 다른 디바이스를 생성함).

디바이스는 엔드포인트 데이터 피드(고유한 엔드포인트 ID 포함)를 기반으로 생성되지만, 플로우 데이터를 기반으로 해당 엔드포인트에 대한 관찰이 이루어질 때까지 이러한 디바이스와 연결된 호스트 이름 또는 IP는 없습니다.

ISE가 있는 환경

ISE의 디바이스 추적 기능은 호스트 이름 정보가 있는 환경과 동일합니다.

ISE 데이터는 ISE가 수집하는 호스트 이름 정보를 IP 주소에 연결하는 데 사용되지만 새 디바이스를 생성하거나 netflow에서 볼 수 없었던 IP를 추적하지는 않습니다.

Meraki가 설치된 환경

"이전" Meraki 통합(XDRA와 함께 사용)

이 Meraki 통합은 Meraki 디바이스에서 호스트 이름 정보를 사전 대응적으로 수집하고, 이러한 호스트 이름을 온프레미스 디바이스의 일반적인 IP에 매핑합니다("기본 네임스페이스").

이 프로세스에서는 디바이스가 아직 없는 경우 디바이스를 생성합니다.

네임스페이스의 차이로 인해 다른 "새로운" Cisco Meraki 통합에서 수집한 디바이스 또는 IP 정보를 보강하지 않습니다.

따라서 이 컨피그레이션은 호스트 이름 정보가 있는 환경처럼 작동합니다.

"새로운" Cisco Meraki 통합(XDR과 함께)

이 통합은 Meraki 네트워킹 장비에서 XDR 데이터 레이크를 통해 표준 XDRA netflow 경로로 netflow를 가져옵니다.

따라서 다른 netflow와 같은 디바이스를 생성합니다. 또한 다른 netflow와 마찬가지로 호스트 이름 정보를 포함하지 않습니다.

실제로 이 컨피그레이션은 사용 가능한 호스트 이름 정보가 없는 환경처럼 작동하며, 한 가지 주요 예외가 있습니다.

이러한 통합은 다른 Meraki 장비의 netflow 레이블을 다른 네임스페이스로 지정하기 위해 전송된 정보를 활용합니다.

따라서 일반적인 중첩 서브넷 문제가 방지되지만, 둘 이상의 통합이 설정된 경우 새로운 문제가 발생할 수 있습니다.

가장 분명한 것은 "이전" 및 "새" Meraki 통합을 모두 설정할 경우, 동일한 네임스페이스를 사용하지 않으므로 정보가 동일한 물리적 디바이스를 나타내는 경우에도 겹치지 않는 디바이스를 생성한다는 것입니다.

즉, 기본 네임스페이스에 하나는 호스트 이름이 있고 트래픽이 없는 2개의 디바이스가 있고, 다른 하나는 특정 Meraki 네임스페이스에 트래픽이 있고 호스트 이름이 없는 2개의 디바이스가 있습니다.

동시에 활성화된 경우 다른 통합에서도 유사한 '분할'이 발생할 수 있습니다.

정의

1. 내부 IP 주소: XDRA는 IP 주소를 내부 또는 외부로 간주하며, 이는 서브넷 설정을 통해 구성할 수 있습니다. 온프레미스(on-prem)용 서브넷은 기본적으로 RFC 내부 서브넷(RFC1918 및 RFC4193)이지만 서브넷을 구성(추가 또는 제거)할 수 있습니다.
2. 네임스페이스: 다른 관찰 지점에서 볼 수 있는 netflow 및 디바이스에 레이블을 지정하는 데 사용되는 추가 정보로, 겹치는 IP 문제 없이 겹치는 서브넷을 허용합니다.

ISE 호스트 이름 데이터 흐름

1. ONA는 ISE 세션 데이터를 수집하고 10분마다 S3에 업로드합니다.
    1. 이 데이터에는 사용자<->IP 정보가 포함되며 호스트 이름도 포함되는 경우도 있습니다.
2. IseSessionsMiner는 업로드된 데이터를 구문 분석하고 가능한 경우 IP를 디바이스와 연결합니다. 디바이스가 없는 경우 디바이스를 생성하지 않습니다. 이렇게 하면 디바이스가 이미 있을 때마다 사용 가능한 호스트 이름<->IP 매핑을 수집합니다.
3. 그런 다음 ONA가 역방향 DNS 조회에서 업로드하는 것과 동일한 형식의 매핑을 사용하여 s3에서 파일을 생성합니다
4. 그런 다음 ONA 호스트 이름을 로드하는 것처럼 해당 호스트 이름을 로드하도록 시스템에 지시합니다.

FAQ

XDRA 디바이스에서 네트워크의 논리적 디바이스와 더 이상 연결되지 않는 IP가 표시되는 이유는 무엇입니까?

안타깝게도, 우리가 할 수 있는 일은 아무것도 없습니다.

시스템은 기존 연결이 유효하지 않은지 또는 예를 들어 추가 물리적 네트워크 인터페이스의 결과인지 알 수 없습니다.

XDRA로 전송되는 호스트 이름 정보가 없습니다. IPv4 및 IPv6 주소를 모두 사용하는 내 디바이스가 2개의 서로 다른 디바이스로 표시되는 이유는 무엇입니까?

호스트 이름 정보가 없으면 다른 IP가 네트워크의 동일한 논리적 디바이스에 연결되어 있는지 알 수 없습니다.

동일한 XDRA 디바이스에 표시되는 여러 개의 논리적 디바이스가 서로 다른 서브넷에 있는 이유는 무엇입니까?

XDRA는 현재 어떤 서브넷 텔레메트리를 사용하는지 구분할 방법이 없으므로 동일한 IP가 항상 하나의 디바이스로 그룹화됩니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.