Entendendo o dispositivo local, nome de host e mapeamento IP no XDR-A

Contents

Introdução

Este documento descreve como entender o comportamento do XDR-Analytics em relação ao nome de host do dispositivo e ao mapeamento IP.

Background

O XDRA tenta rastrear um comportamento de dispositivos lógicos ao longo do tempo, conhecido como Dispositivo.

Ele usa várias técnicas para correlacionar o tráfego de rede a esses dispositivos lógicos ao longo do tempo.

No entanto, particularmente em um ambiente local, há limites para a capacidade do sistema de associar tráfego a um dispositivo.

O XDRA reúne principalmente a telemetria para ambientes locais através do netflow por meio da integração ONA, CTB ou Cisco Meraki (a "nova" integração Meraki). Secundariamente, ele pode obter a resolução do nome do host por meio de:

- Resolução de nome de host ativa através de pesquisas de DNS reverso e, opcionalmente, consultas SMB através do ONA
- Integração do ISE através do ONA
- A "antiga" integração com a Meraki
- Integração com NVM, com advertências adicionais

O Netflow tem endereços IP sem informações de nome de host.

Sem as informações de nome de host, ele assume que cada endereço IP interno (veja a definição abaixo) visto é um dispositivo, já que não tem mais informações para fazer uma associação de dispositivo mais inteligente.

Em um caso onde a coleção de nomes de host é configurada, o XDRA usa nomes de host, quando vistos, para vinculá-los a uma representação interna de um dispositivo.

Isso permite que o XDRA agrupe vários endereços IP ao longo do tempo em um dispositivo.

A telemetria NVM pode ser configurada como parte do XDR.

Essa fonte de telemetria fornece um feed de dados semelhante ao netflow, mas também fornece informações de endpoint com identificadores exclusivos.

A forma como o XDRA aproveita essas informações tem o efeito final do rastreamento de dispositivo que se comporta de forma semelhante ao caso em que a coleta de nome de host está habilitada no ONA.

Todas essas configurações têm limitações baseadas nas limitações da telemetria disponível.

Observe que XDRA supõe que a natureza dos mapeamentos de endereço IP e nome de host é uma relação muitos-para-um (muitos IPs podem mapear para um nome de host).

Um dispositivo lógico pode ter vários IPs simultaneamente (por exemplo, duas interfaces físicas ou IPv4 e IPv6).

Devido à natureza da monitoração, XDRA nunca pode supor ter todas as relações da rede real em um determinado momento no tempo.

Sub-redes sobrepostas

No caso de um único locatário XDRA estar monitorando várias sub-redes locais simultaneamente, o sistema não pode distinguir entre o mesmo IP visto em cada uma delas.

Como tal, correlaciona excessivamente os IPs com os dispositivos. A disponibilidade do nome de host não melhora essa situação.

Uma maneira de contornar isso é ter mais de um portal XDRA (um por sub-rede). Outra opção é usar a "nova" integração com o Cisco Meraki devido ao isolamento do namespace que essa integração traz.

Ambiente sem informações de nome de host disponíveis

Como efeito colateral das informações limitadas de telemetria, o sistema pode chegar a um entendimento incorreto do histórico de dispositivos.

Um cenário é quando os IPs são atribuídos dinamicamente, o XDRA não tem uma maneira de saber se o dispositivo lógico subjacente mudou, por exemplo, um laptop em folhas WIFI e o IP é atribuído a um novo laptop.

Na ausência de nome de host ou outras informações de identificação, o sistema associa as atividades de vários dispositivos lógicos a um dispositivo. Isso pode levar a informações confusas de perfil do dispositivo.

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

As seen by XDRA
```

```
    t0      t1      t2      t3
ip1 d1----------------------
```

Por outro lado, nos casos em que um dispositivo lógico tem mais de um endereço IP (por exemplo, duas interfaces físicas ou IPv4 e IPv6), não há informações com as quais possamos vinculá-las de forma confiável ao mesmo dispositivo, portanto o sistema não tem.

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

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

Ambiente com informações de nome de host

Onde o XDRA pode ver informações de nome de host, o sistema pode associar mais de um endereço IP a um dispositivo. No entanto, dada a natureza dos dados, ainda há limites para o que o sistema pode determinar com segurança. Isso pode levar a uma correlação excessiva de IPs com os dispositivos no sistema.

Se um dispositivo que tem uma associação de IP para nome de host em XDRA e, em seguida, o dispositivo lógico altera o endereço IP, a telemetria eventualmente reflete o novo IP para o mapeamento de nome de host.

No entanto, devido à possibilidade de que este seja um relacionamento muitos-para-um, XDRA NÃO pode assumir com segurança que o IP visto anteriormente não está mais associado ao nome do host (e, portanto, ao dispositivo).

Pode, por exemplo, ser uma interface física separada para o mesmo dispositivo lógico. Assim, o XDRA mantém os IPs vistos anteriormente junto com o IP visto mais recentemente, até que a telemetria seja vista, mapeando positivamente o endereço IP para um nome de host diferente.

Neste ponto, o XDR 'expira' o mapeamento e deve ser listado como um endereço IP anterior.

Não há como dizer ao sistema para quebrar uma associação 'cedo'.

Observação sobre correspondência de nome de host

Para tentar lidar melhor com os casos em que um locatário tem o mesmo nome de host configurado em vários domínios, o XDRA emprega uma correspondência ‘flexível’ e trata as entradas mostradas nesta tabela como nomes de host correspondentes ao procurar corresponder a um dispositivo existente (ou seja, no caso de um IP correspondente):

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

Em outras palavras, ele considera apenas o nome de host, ignorando o restante do nome de domínio.

Ambiente com NVM

Essa configuração se comporta de forma muito semelhante à seção Ambiente com informações de nome de host com informações de nome de host, mas há algumas diferenças.

Esse feed de dados fornece os benefícios adicionais de poder fornecer alguns identificadores de endpoint exclusivos para o usuário, e essas IDs potencialmente nos permitem rastrear um dispositivo físico que passa por uma alteração de nome de host (o que não é possível rastrear de outra forma, criaríamos 2 dispositivos diferentes).

Enquanto os dispositivos são criados com base no feed de dados do ponto final (com IDs de ponto final exclusivas), não há nomes de host ou IPs associados a esses dispositivos até que seja feita uma observação sobre esse ponto final com base nos dados de fluxo.

Ambientes com ISE

Os benefícios do rastreamento do ISE para o dispositivo são idênticos ao ambiente com informações de nome de host.

Os dados do ISE são usados para associar as informações de nome de host coletadas a endereços IP, mas não criam um novo dispositivo ou rastreiam IPs que não foram vistos no netflow.

Ambientes com a Meraki

Integração "antiga" com Meraki (com XDRA)

Essa integração com a Meraki coleta proativamente informações de nome de host dos dispositivos da Meraki, mapeando esses nomes de host para IPs como de costume em dispositivos locais (que é o "namespace padrão").

Esse processo cria dispositivos se eles ainda não existirem.

Ele não aumenta as informações de dispositivo ou IP coletadas de outra "nova" integração com o

Cisco Meraki devido a diferenças de namespace.

Na verdade, isso faz com que essa configuração se comporte como um Ambiente com informações de nome de host.

Integração "nova" com o Cisco Meraki (ou seja, com o XDR)

Essa integração obtém o netflow do equipamento de rede da Meraki, através do lago de dados XDR, no caminho de netflow XDRA padrão.

Como tal, ele cria dispositivos como qualquer outro fluxo de rede; assim como qualquer outro netflow, ele não contém informações de nome de host.

Na verdade, essa configuração se comporta como Ambiente sem informações de nome de host disponíveis, com uma exceção principal.

Essa integração aproveita as informações enviadas para rotular o netflow de equipamentos Meraki diferentes em namespaces diferentes.

Isso evita os problemas comuns de sobreposição de sub-redes, mas pode introduzir novas dificuldades se mais de uma integração for configurada.

Obviamente, se ambas as integrações "Antigas" e "Novas" da Meraki forem configuradas, elas não usarão os mesmos namespaces e, portanto, criarão Dispositivos sem sobreposição, mesmo nos casos em que as informações representarem o mesmo dispositivo físico.

Ou seja, você tem 2 dispositivos, um no namespace padrão com um nome de host e nenhum tráfego, outro com tráfego em um namespace Meraki específico e nenhum nome de host.

Podem ocorrer ‘divisões’ semelhantes com outras integrações se ativadas simultaneamente.

Definições

1. Endereço IP interno: O XDRA considera os endereços IP internos ou externos, e isso é configurável através das configurações de sub-rede. As sub-redes para o padrão local são as sub-redes internas RFC (RFC1918 e RFC4193), mas as sub-redes podem ser configuradas (adicionadas ou removidas).
2. Espaço de nomes: Informações adicionais usadas para rotular o fluxo de rede e os dispositivos vistos de diferentes pontos de observação, permitindo a sobreposição de sub-redes sem problemas de IP sobrepostos.

Fluxo de dados do nome de host ISE

1. O ONA coleta dados de sessão do ISE, carrega no S3 a cada 10 minutos
    1. esses dados contêm informações de<->IP do usuário e, às vezes, também incluem o nome do host

2. O IseSessionsMiner analisa os dados carregados e associa IPs a Dispositivos quando possível. ELE NÃO cria um dispositivo se ainda não houver um. Ao fazer isso, ele reúne os mapeamentos de nome de host<->IP disponíveis sempre que já temos um dispositivo.

3. Em seguida, cria um arquivo em s3 com esses mapeamentos no mesmo formato que o ONA carregaria um de suas pesquisas de DNS reverso

4. Em seguida, ele informa ao sistema para carregar esses nomes de host da mesma forma que carregaria os nomes de host ONA.

FAQ

Por que estou vendo IPs em um dispositivo XDRA que não estão mais associados a esse dispositivo lógico na minha rede?

Infelizmente, não podemos fazer nada a este respeito.

O sistema não pode saber se a associação antiga é inválida ou o resultado de, por exemplo, uma interface de rede física adicional.

Não tenho nenhuma informação de nome de host sendo enviada para XDRA, por que meu dispositivo que está usando endereços IPv4 e IPv6 mostra como 2 dispositivos distintos?

Sem as informações de nome de host, não podemos saber que diferentes IPs estão associados ao mesmo dispositivo lógico em sua rede.

Por que vejo vários dispositivos lógicos de sub-redes diferentes aparecendo no mesmo dispositivo XDRA?

Atualmente, o XDRA não tem como distinguir de qual telemetria de sub-rede vem, portanto, o mesmo IP é sempre agrupado em um dispositivo.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.