Présentation du périphérique local, du nom d'hôte et du mappage IP dans XDR-A

Table des matières

Introduction

Ce document décrit comment comprendre le comportement de XDR-Analytics en relation avec le nom d'hôte du périphérique et le mappage IP.

Fond

XDRA tente de suivre le comportement d'un périphérique logique au fil du temps, appelé périphérique.

Il utilise diverses techniques pour corréler le trafic réseau à ces périphériques logiques au fil du temps.

Cependant, en particulier dans un environnement sur site, il existe des limites à la capacité du système à associer le trafic à un périphérique.

XDRA collecte principalement des données télémétriques pour les environnements sur site via netflow via l'intégration ONA, CTB ou Cisco Meraki (la « nouvelle » intégration Meraki). En second lieu, il peut obtenir la résolution de nom d'hôte via :

- Résolution active des noms d'hôte via des recherches DNS inversées et éventuellement des requêtes SMB via l'ONA
- Intégration ISE via l'ONA
- L'« ancienne » intégration Meraki
- Intégration NVM, avec des mises en garde supplémentaires

Netflow a des adresses IP sans informations de nom d'hôte.

Sans les informations de nom d'hôte, il suppose que chaque adresse IP interne (voir la définition ci-dessous) vue est un périphérique, car il n'a pas d'autres informations pour faire une association de périphérique plus intelligente.

Dans le cas où la collection de noms d'hôte est configurée, XDRA utilise les noms d'hôte, lorsqu'ils sont affichés, pour les lier à une représentation interne d'un périphérique.

Cela permet à XDRA de regrouper plusieurs adresses IP sur un seul périphérique.

La télémétrie NVM peut être configurée en option dans XDR.

Cette source de télémétrie fournit une source de données de type NetFlow, mais fournit également des informations de point d'extrémité avec des identificateurs uniques.

La manière dont XDRA exploite ces informations a pour effet net que le suivi des périphériques se comporte de la même manière que lorsque la collecte de noms d'hôte est activée sur l'ONA.

Toutes ces configurations présentent des limitations basées sur les limitations de la télémétrie disponible.

Remarque : XDRA suppose que la nature des mappages d'adresse IP et de nom d'hôte est une relation plusieurs-à-un (plusieurs adresses IP peuvent correspondre à un nom d'hôte).

Un périphérique logique peut avoir plusieurs adresses IP simultanément (par exemple, deux interfaces physiques ou IPv4 et IPv6).

En raison de la nature de la surveillance, XDRA ne peut jamais supposer avoir toutes les relations du réseau réel à un moment donné.

Chevauchement de sous-réseaux

Dans le cas où un seul locataire XDRA surveille simultanément plusieurs sous-réseaux sur site, le système ne peut pas faire la distinction entre les mêmes adresses IP visibles dans chacun d'eux.

En tant que tel, il surcorrèle les adresses IP aux périphériques. La disponibilité du nom d'hôte n'améliore pas cette situation.

Pour contourner ce problème, vous pouvez disposer de plusieurs portails XDRA (un par sous-réseau). Il est également possible d'utiliser la « nouvelle » intégration Cisco Meraki en raison de l'isolation de l'espace de nommage que cette intégration apporte.

Environnement sans informations de nom d'hôte disponibles

En raison des informations de télémétrie limitées, le système peut avoir une mauvaise compréhension de l'historique des périphériques.

L'un de ces scénarios consiste à attribuer dynamiquement des adresses IP, à dire que XDRA n'a aucun moyen de savoir que le périphérique logique sous-jacent a changé, par exemple un ordinateur portable sur les feuilles WIFI, et que l'adresse IP est attribuée à un nouvel ordinateur portable.

En l'absence de nom d'hôte ou d'autres informations d'identification, le système associe les activités de plusieurs périphériques logiques à un seul périphérique. Cela peut entraîner une confusion dans les informations de profil du périphérique.

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

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

Inversement, dans les cas où un périphérique logique a plus d'une adresse IP (par exemple deux interfaces physiques ou IPv4 et IPv6), il n'y a aucune information avec laquelle nous pouvons les lier de manière fiable au même périphérique, donc le système ne le fait pas.

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

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

Environnement avec informations de nom d'hôte

Lorsque XDRA peut voir les informations de nom d'hôte, le système peut associer plusieurs adresses IP à un périphérique. Cependant, compte tenu de la nature des données, il existe encore des limites à ce que le système peut déterminer de façon fiable. Cela peut entraîner une surcorrélation des adresses IP avec les périphériques du système.

Si un périphérique associé à un nom d'hôte IP à IP dans XDRA, puis que le périphérique logique change d'adresse IP, la télémétrie reflète finalement le nouveau mappage IP à nom d'hôte.

Cependant, en raison de la possibilité qu'il s'agisse d'une relation plusieurs-à-un, XDRA ne peut PAS supposer en toute sécurité que l'adresse IP précédemment vue n'est plus associée au nom d'hôte (et donc au périphérique).

Il peut, par exemple, s'agir d'une interface physique distincte vers le même périphérique logique. Ainsi, XDRA conserve les adresses IP précédemment vues ainsi que les dernières, jusqu'à ce que la télémétrie indique que l'adresse IP correspond à un autre nom d'hôte.

À ce stade, XDR « expire » le mappage et doit être répertorié en tant qu'adresse IP précédente.

Il n'y a aucun moyen de dire au système de rompre une association « tôt ».

Remarque sur la correspondance des noms d'hôte

Afin d'essayer de mieux gérer les cas où un locataire a le même nom d'hôte configuré dans plusieurs domaines, XDRA utilise une correspondance « flexible » et traite les entrées présentées dans ce tableau comme des noms d'hôtes correspondants lorsqu'il cherche à faire correspondre un périphérique existant (c'est-à-dire dans le cas d'une adresse IP correspondante) :

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

En d'autres termes, il considère uniquement le nom d'hôte tout en ignorant le reste du nom de domaine.

Environnement avec NVM

Cette configuration se comporte de façon très similaire à la section Environnement avec informations de nom d'hôte avec informations de nom d'hôte, mais il existe quelques différences.

Cette source de données présente l'avantage supplémentaire de pouvoir fournir à l'utilisateur des identifiants de point de terminaison uniques, et ces ID peuvent nous permettre de suivre un périphérique physique qui subit un changement de nom d'hôte (ce qui n'est pas possible autrement, nous créerions 2 périphériques différents).

Bien que les périphériques soient créés en fonction de la source de données de point d'extrémité (avec des ID de point d'extrémité uniques), aucun nom d'hôte ou IP n'est associé à ces périphériques jusqu'à ce qu'une observation soit faite sur ce point d'extrémité en fonction des données de flux.

Environnements avec ISE

Les avantages de l'ISE pour le suivi des périphériques finissent par être identiques à ceux de l'environnement avec les informations de nom d'hôte.

Les données ISE sont utilisées pour associer les informations de nom d'hôte qu'elles collectent aux adresses IP, mais elles ne créent pas de nouveau périphérique ou ne suivent pas les adresses IP qui n'ont pas été vues dans netflow.

Environnements avec Meraki

Intégration Meraki « ancienne » (c'est-à-dire avec XDRA)

Cette intégration Meraki collecte de manière proactive les informations de nom d'hôte à partir des périphériques Meraki, en mappant ces noms d'hôte sur les adresses IP, comme d'habitude pour les périphériques sur site (c'est-à-dire l'« espace de noms par défaut »).

Ce processus crée des périphériques s'ils n'existent pas déjà.

Il n'augmente pas les informations sur les périphériques ou les adresses IP collectées à partir de l'autre « nouvelle » intégration Cisco Meraki en raison des différences d'espace de noms.

En effet, cette configuration se comporte comme un environnement avec des informations de nom d'hôte.

« Nouvelle » intégration Cisco Meraki (c'est-à-dire avec XDR)

Cette intégration permet d'intégrer netflow de l'équipement réseau Meraki, via le lac de données XDR, dans le chemin de flux réseau XDRA standard.

En tant que tel, il crée des périphériques comme n'importe quel autre netflow ; comme tout autre netflow, il ne contient pas d'informations de nom d'hôte.

En effet, cette configuration se comporte comme Environment sans aucune information de nom d'hôte disponible, à une exception majeure près.

Cette intégration tire parti des informations envoyées pour étiqueter le flux réseau de différents équipements Meraki dans différents espaces de noms.

Cela évite les problèmes habituels de chevauchement de sous-réseaux, mais peut introduire de nouvelles difficultés si plus d'une intégration est configurée.

De toute évidence, si les intégrations Meraki « ancienne » et « nouvelle » sont toutes deux configurées, elles n'utilisent pas les mêmes espaces de noms et créent ainsi des périphériques sans chevauchement, même dans les cas où les informations représentent le même périphérique physique.

En d'autres termes, vous avez 2 périphériques, l'un dans l'espace de noms par défaut avec un nom d'hôte et aucun trafic, un autre avec un trafic dans un espace de noms Meraki spécifique et aucun nom d'hôte.

Des « divisions » similaires peuvent se produire avec d'autres intégrations si elles sont activées simultanément.

Définitions

1. Adresse IP interne : XDRA considère les adresses IP comme internes ou externes, et ceci est configurable via les paramètres de sous-réseau. Les sous-réseaux pour les réseaux locaux sont définis par défaut sur les sous-réseaux internes RFC (RFC1918 et RFC4193), mais les sous-réseaux peuvent être configurés (ajoutés ou supprimés).
2. Espace de noms : Informations supplémentaires utilisées pour étiqueter netflow et les périphériques vus à partir de différents points d'observation, permettant le chevauchement de sous-réseaux sans problèmes IP.

Flux de données ISE Hostname

1. ONA collecte les données de session ISE et les télécharge sur S3 toutes les 10 minutes
    1. ces données contiennent des informations sur l'adresse<->IP de l'utilisateur et parfois le nom d'hôte
2. IseSessionsMiner analyse les données téléchargées et associe les adresses IP aux périphériques lorsque cela est possible. Il ne crée PAS de périphérique s'il n'en existe pas déjà un. Ce faisant, il rassemble les mappages IP de nom d'hôte<->disponibles chaque fois que nous avons déjà un périphérique.
3. Il crée ensuite un fichier dans s3 avec ces mappages dans le même format que celui que l'ONA téléchargerait à partir de ses recherches DNS inversées
4. Il indique ensuite au système de charger ces noms d'hôte comme il chargerait les noms d'hôte ONA.

Forum aux questions

Pourquoi vois-je des adresses IP sur un périphérique XDRA qui ne sont plus associées à ce périphérique logique sur mon réseau ?

Malheureusement, nous ne pouvons rien y faire.

Le système ne peut pas savoir si l'ancienne association n'est pas valide ou si elle est le résultat d'une interface réseau physique supplémentaire, par exemple.

Je n'ai pas d'informations de nom d'hôte envoyées à XDRA, pourquoi mon périphérique qui utilise à la fois des adresses IPv4 et IPv6 affiche-t-il 2 périphériques distincts ?

Sans les informations de nom d'hôte, nous ne pouvons pas savoir si différentes adresses IP sont associées au même périphérique logique sur votre réseau.

Pourquoi est-ce que plusieurs périphériques logiques de différents sous-réseaux apparaissent dans le même périphérique XDRA ?

Actuellement, XDRA n'a aucun moyen de distinguer la télémétrie de sous-réseau, de sorte que la même adresse IP est toujours regroupée en un seul périphérique.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.