

On-premises apparaattoewijzing, hostnaam en IP-toewijzing in XDR-A begrijpen

Inhoud

Inleiding

In dit document wordt beschreven hoe u het gedrag van XDR-Analytics kunt begrijpen met betrekking tot de hostnaam van het apparaat en IP-toewijzing.

Achtergrond

XDRA probeert het gedrag van een logisch apparaat in de loop van de tijd te volgen, bekend als een apparaat.

Het gebruikt verschillende technieken om netwerkverkeer in de loop van de tijd met deze logische apparaten te correleren.

Met name in een on-premises omgeving zijn er echter grenzen aan hoe goed het systeem verkeer aan een apparaat kan koppelen.

XDRA verzamelt voornamelijk telemetrie voor on-premises omgevingen door middel van netflow via de ONA-, CTB- of Cisco Meraki-integratie (de "nieuwe" Meraki-integratie). Ten tweede kan het hostname-resolutie krijgen via:

- Actieve hostname-resolutie via reverse DNS-lookups en optioneel SMB-query's via de ONA
- ISE-integratie via de ONA
- De "oude" Meraki-integratie
- NVM-integratie, met aanvullende kanttekeningen

Netflow heeft IP-adressen zonder hostnaam-informatie.

Zonder hostnaam-informatie wordt ervan uitgegaan dat elk intern IP-adres (zie definitie hieronder) een apparaat is, omdat het geen verdere informatie heeft om een intelligentere apparaatkoppeling te maken.

In een geval waarin hostnamecollectie is geconfigureerd, gebruikt XDRA hostnamen, wanneer deze worden gezien, om deze te koppelen aan een interne representatie van een apparaat.

Hierdoor kan XDRA meerdere IP-adressen in de loop van de tijd op één apparaat groeperen.

NVM-telemetrie kan optioneel worden geconfigureerd als onderdeel van XDR.

Deze telemetriebron biedt een netflow-achtige datafeed, maar biedt ook eindpuntinformatie met

unieke identifiers.

De manier waarop XDRA deze informatie gebruikt, heeft het netto-effect dat Device Tracking zich op dezelfde manier gedraagt als het geval waarin het verzamelen van hostnamen is ingeschakeld op de ONA.

Al deze opstellingen hebben beperkingen op basis van de beperkingen van de beschikbare telemetrie.

Let op: XDRA gaat ervan uit dat de aard van IP-adres en hostname mappings een veel-op-één relatie is (veel IP's kunnen aan één hostnaam worden toegewezen).

Een logisch apparaat kan meerdere IP's tegelijk hebben (bijvoorbeeld twee fysieke interfaces of IPv4 en IPv6).

Vanwege de aard van de monitoring kan XDRA er nooit van uitgaan dat alle relaties van het werkelijke netwerk op een bepaald moment in de tijd aanwezig zijn.

Overlappende subnetten

Als één XDRA-tenant meerdere on-premises subnetten tegelijkertijd bewaakt, kan het systeem geen onderscheid maken tussen hetzelfde IP dat in elk van deze subnetten wordt gezien.

Als zodanig overcorreleert het IP's met apparaten. Hostname beschikbaarheid verbetert deze situatie niet.

Een manier om dit te omzeilen is om meer dan één XDRA-portaal te hebben (één per subnet). Een andere is om de ["Nieuwe" Cisco Meraki-integratie](#) te gebruiken vanwege de naamruimte-isolatie die deze integratie met zich meebrengt.

Omgeving zonder beschikbare hostnaam-informatie

Als neveneffect van de beperkte telemetrie-informatie kan het systeem tot een onjuist begrip van de geschiedenis van een apparaat komen.

Een scenario is dat wanneer IP's dynamisch worden toegewezen, XDRA geen manier heeft om te weten dat het onderliggende logische apparaat is gewijzigd, bijvoorbeeld een laptop op WIFI verlaat en het IP wordt toegewezen aan een nieuwe laptop.

Bij afwezigheid van hostnaam of andere identificerende informatie koppelt het systeem de activiteiten van meerdere logische apparaten aan één apparaat. Dit kan leiden tot verwarrende profielinformatie van het apparaat.

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

As seen by XDRA

	t0	t1	t2	t3
ip1	d1-----			

Omgekeerd, in gevallen waarin een logisch apparaat meer dan één IP-adres heeft (bijvoorbeeld twee fysieke interfaces of IPv4 en IPv6), is er geen informatie waarmee we deze betrouwbaar kunnen koppelen aan hetzelfde apparaat, dus het systeem doet dat niet.

Actual Situation

	t0	t1	t2	t3
ip1	d1-----			
ip2	d1-----			

As seen by XDRA

	t0	t1	t2	t3
ip1	d1-----			
ip2	d1-----			

Omgeving met hostnaam-informatie

Waar XDRA hostnaam-informatie kan zien, heeft het systeem de mogelijkheid om meer dan één IP-adres aan één apparaat te koppelen. Gezien de aard van de gegevens zijn er echter nog steeds grenzen aan wat het systeem op betrouwbare wijze kan bepalen. Dit kan leiden tot overcorrelatie van IP's met apparaten in het systeem.

Als een apparaat dat een IP-naar-hostnaamkoppeling heeft in XDRA en vervolgens het logische apparaat het IP-adres wijzigt, weerspiegelt de telemetrie uiteindelijk de nieuwe IP-naar-hostnaamtoewijzing.

Echter, vanwege de mogelijkheid dat dit een veel-op-één relatie is, kan XDRA NIET veilig aannemen dat het eerder geziene IP niet langer geassocieerd is met de hostnaam (en dus het Apparaat).

Het kan bijvoorbeeld een aparte fysieke interface zijn met hetzelfde logische apparaat. Dus XDRA houdt zowel de eerder gezien IP's samen met de meest recent gezien IP, totdat telemetrie wordt gezien die het IP-adres positief in kaart brengt met een andere hostnaam.

Op dit punt 'verloopt' XDR de toewijzing en wordt vermeld als een eerder IP-adres.

Er is geen manier om het systeem te vertellen om een associatie 'vroeg' te verbreken.

Opmerking over het matchen van hostnamen

Om beter om te gaan met gevallen waarin een tenant dezelfde hostnaam heeft geconfigureerd in meerdere domeinen, maakt XDRA gebruik van een 'flexibele' matching en behandelt de items die in deze tabel worden weergegeven als overeenkomende hostnamen bij het zoeken naar een bestaand apparaat (dat is in het geval van een overeenkomend IP):

example
example.com
example.net
example.observbl.com
example.invalid.observbl.com
example.example.com

Met andere woorden, het beschouwt alleen de hostnaam terwijl het de rest van de domeinnaam negeert.

Omgeving met NVM

Deze setup gedraagt zich zeer vergelijkbaar met Environment met hostnaam informatie sectie met hostnaam informatie, maar er zijn een paar verschillen.

Deze datafeed biedt de extra voordelen van het kunnen bieden van een aantal unieke endpoint-identifiers aan de gebruiker, en deze ID's stellen ons mogelijk in staat om een fysiek apparaat te volgen dat een wijziging van hostnaam ondergaat (wat niet mogelijk is om te volgen, anders zouden we 2 verschillende apparaten maken).

Hoewel Apparaten worden gemaakt op basis van de eindpuntgegevensfeed (met unieke eindpunt-ID's), zijn er geen hostnaam of IP's gekoppeld aan deze Apparaten totdat een observatie is gemaakt over dat eindpunt op basis van de stroomgegevens.

Omgevingen met ISE

De voordelen van ISE to Device-tracking zijn uiteindelijk identiek aan [Environment met hostnaaminformatie](#).

ISE-gegevens worden gebruikt om hostnaaminformatie die wordt verzameld aan IP-adressen te koppelen, maar er wordt geen nieuw apparaat gemaakt of IP's bijgehouden die niet zijn gezien in netflow.

Omgevingen met Meraki

"Oude" Meraki-integratie (dat is met XDRA)

Deze Meraki-integratie verzamelt proactief hostnaam-informatie van Meraki-apparaten en koppelt die hostnamen aan IP's zoals gebruikelijk voor on-prem-apparaten (dat is de "standaard naamruimte").

Met dit proces worden apparaten gemaakt als deze nog niet bestaan.

Het vergroot de Apparaat- of IP-informatie die is verzameld uit de andere "nieuwe" Cisco Meraki-

integratie niet vanwege naamruimteverschillen.

In feite zorgt dit ervoor dat deze configuratie zich gedraagt als een [omgeving met hostnaaminformatie](#).

"Nieuwe" Cisco Meraki-integratie (dat is met XDR)

Deze integratie krijgt netflow van Meraki-netwerkapparatuur, via het XDR-gegevenspad, naar het standaard XDRA-netwerkstroompad.

Als zodanig creëert het Apparaten zoals elke andere netflow; ook zoals elke andere netflow bevat het geen hostnaam-informatie.

In feite gedraagt deze configuratie zich als [Omgeving zonder beschikbare hostnaam-informatie](#), met één belangrijke uitzondering.

Deze integratie maakt gebruik van de informatie die wordt verzonden om de netflow van verschillende Meraki-apparatuur in verschillende naamruimten te labelen.

Dit voorkomt de gebruikelijke problemen met [overlappende subnetten](#), maar kan nieuwe problemen veroorzaken als meer dan één integratie wordt opgezet.

Het meest voor de hand liggend is dat als zowel "Oude" als "Nieuwe" Meraki-integraties zijn ingesteld, ze niet dezelfde naamruimten gebruiken en dus niet-overlappende apparaten maken, zelfs in gevallen waarin de informatie hetzelfde fysieke apparaat vertegenwoordigt.

Dat wil zeggen, je hebt 2 apparaten, een in de standaard naamruimte met een hostnaam en geen verkeer, een ander met verkeer in een specifieke Meraki-naamruimte en geen hostnaam.

Soortgelijke 'splitsingen' kunnen optreden met andere integraties als ze tegelijkertijd zijn ingeschakeld.

Definities

1. Intern IP-adres: XDRA beschouwt IP-adressen als intern of extern en dit kan worden geconfigureerd via de subnetinstellingen. Subnetten voor on-prem standaard naar de interne RFC-subnetten (RFC1918 en RFC4193), maar subnetten kunnen worden geconfigureerd (toegevoegd of verwijderd).
2. Naamruimte: aanvullende informatie die wordt gebruikt om netflow en apparaten te labelen die vanuit verschillende observatiepunten worden gezien, zodat [overlappende subnetten mogelijk zijn](#) zonder overlappende IP-problemen.

ISE Hostname-gegevensstroom

1. ONA verzamelt ISE-sessiegegevens en uploadt elke 10 minuten naar S3
 1. deze gegevens bevatten gebruiker<->IP-informatie, soms ook hostnaam

2. IseSessionsMiner parseert de geüploade gegevens en koppelt IP's waar mogelijk aan apparaten. Het maakt geen apparaat aan als het nog niet bestaat. Terwijl het dit doet, verzamelt het beschikbare hostname<->IP-toewijzingen wanneer we al een apparaat hebben.
3. Het maakt vervolgens een bestand in s3 met die toewijzingen in hetzelfde formaat als de ONA er een zou uploaden vanuit de omgekeerde DNS-lookups
4. Het vertelt het systeem vervolgens om die hostnamen te laden, net zoals het ONA-hostnamen zou laden.

FAQ

Waarom zie ik IP's op een XDRA-apparaat die niet langer zijn gekoppeld aan dat logische apparaat op mijn netwerk?

Helaas kunnen we hier niets aan doen.

Het systeem kan niet weten of de oude koppeling ongeldig is of het resultaat is van bijvoorbeeld een extra fysieke netwerkinterface.

Ik heb geen hostnaam-informatie die naar XDRA wordt verzonden, waarom wordt mijn apparaat dat zowel IPv4- als IPv6-adressen gebruikt, weergegeven als 2 verschillende apparaten?

Zonder hostname-informatie kunnen we niet weten dat verschillende IP's zijn gekoppeld aan hetzelfde logische apparaat in uw netwerk.

Waarom zie ik meerdere logische apparaten van verschillende subnetten verschijnen in hetzelfde XDRA-apparaat?

XDRA heeft momenteel geen manier om te onderscheiden waar subnettelemetrie vandaan komt, dus hetzelfde IP wordt altijd gegroepeerd in één apparaat.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.