Informazioni sul dispositivo locale, sul nome host e sulla mappatura IP in XDR-A

Sommario

Introduzione

In questo documento viene descritto come interpretare il comportamento di XDR-Analytics in relazione al nome host del dispositivo e alla mappatura IP.

Introduzione

XDRA tenta di tenere traccia del comportamento di una periferica logica nel tempo, noto come periferica.

Utilizza varie tecniche per correlare il traffico di rete a queste periferiche logiche nel tempo.

Tuttavia, in particolare in un ambiente locale, esistono dei limiti alla capacità del sistema di associare il traffico a un dispositivo.

XDRA raccoglie principalmente dati di telemetria per ambienti locali tramite netflow tramite l'integrazione ONA, CTB o Cisco Meraki (la "nuova" integrazione Meraki). In secondo luogo, può ottenere la risoluzione dei nomi host tramite:

- Risoluzione attiva dei nomi host tramite ricerche DNS inverse e, facoltativamente, query SMB tramite ONA
- Integrazione di ISE con l'ONA
- La "vecchia" integrazione Meraki
- Integrazione con NVM, con avvertenze aggiuntive

NetFlow dispone di indirizzi IP senza informazioni sul nome host.

Senza informazioni sul nome host, presuppone che ogni indirizzo IP interno (vedere la definizione seguente) rilevato sia un dispositivo, in quanto non dispone di ulteriori informazioni per creare un'associazione più intelligente tra dispositivi.

Nel caso in cui sia configurata la raccolta dei nomi host, XDRA utilizza i nomi host, se visualizzati, per collegarla a una rappresentazione interna di un dispositivo.

Ciò consente a XDRA di raggruppare più indirizzi IP nel tempo in un unico dispositivo.

La telemetria NVM può essere configurata come parte di XDR.

Questa origine di telemetria fornisce un feed di dati simile a netflow, ma fornisce anche

informazioni sull'endpoint con identificatori univoci.

Il modo in cui XDRA sfrutta queste informazioni ha l'effetto di rendere il rilevamento dei dispositivi simile al caso in cui la raccolta dei nomi host è abilitata sull'ONA.

Tutte queste impostazioni hanno limitazioni basate sui limiti della telemetria disponibile.

Si noti che XDRA presume che la natura dei mapping di indirizzi IP e nomi host sia una relazione molti-a-uno (molti IP possono essere mappati a un nome host).

Un dispositivo logico può avere più IP contemporaneamente (ad esempio due interfacce fisiche o IPv4 e IPv6).

Data la natura del monitoraggio, XDRA non può mai supporre di avere tutte le relazioni della rete effettiva in un determinato momento.

Subnet sovrapposte

Nel caso in cui un singolo tenant XDRA stia monitorando più subnet locali contemporaneamente, il sistema non è in grado di distinguere tra lo stesso IP rilevato in ognuna di esse.

correlando gli IP ai dispositivi. La disponibilità del nome host non migliora la situazione.

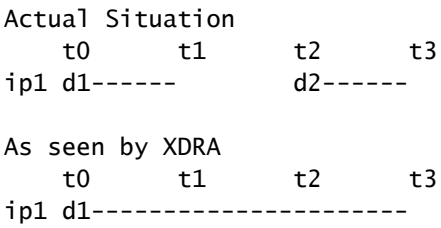
Un modo per risolvere il problema consiste nel disporre di più di un portale XDRA (uno per subnet). In alternativa, è possibile utilizzare la "nuova" integrazione di Cisco Meraki a causa dell'isolamento dello spazio dei nomi causato da questa integrazione.

Ambiente senza informazioni sul nome host disponibili

Come effetto collaterale delle limitate informazioni di telemetria, il sistema può arrivare a una comprensione errata di una storia dei dispositivi.

Uno scenario è quello in cui gli IP vengono assegnati in modo dinamico, XDRA non ha modo di sapere se la periferica logica sottostante è cambiata, ad esempio se un laptop su cui è collegato il Wi-Fi si allontana e l'IP è assegnato a un nuovo notebook.

In assenza di un nome host o di altre informazioni di identificazione, le attività di più periferiche logiche vengono associate a un unico dispositivo. Ciò può causare confusione nelle informazioni del profilo del dispositivo.



Viceversa, se un dispositivo logico ha più indirizzi IP (ad esempio due interfacce fisiche o IPv4 e IPv6), non vi sono informazioni con cui collegarli in modo affidabile allo stesso dispositivo, quindi il sistema non lo fa.

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

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

Ambiente con informazioni sul nome host

Se XDRA è in grado di visualizzare le informazioni sui nomi host, il sistema è in grado di associare più indirizzi IP a un unico dispositivo. Tuttavia, data la natura dei dati, esistono ancora dei limiti a ciò che il sistema può determinare in modo affidabile. Ciò può causare una sovra-correlazione degli IP con i dispositivi del sistema.

Se un dispositivo che dispone di un'associazione da IP a nome host in XDRA e quindi il dispositivo logico cambia indirizzo IP, la telemetria rifletterà il nuovo mapping da IP a nome host.

Tuttavia, a causa della possibilità che si tratti di una relazione molti-a-uno, XDRA NON può presumere in modo sicuro che l'indirizzo IP visualizzato in precedenza non sia più associato al nome host (e quindi al dispositivo).

Potrebbe ad esempio essere un'interfaccia fisica separata per lo stesso dispositivo logico. Pertanto, XDRA mantiene sia gli indirizzi IP visti in precedenza che quelli visti più di recente, fino a quando non viene rilevata la telemetria che associa positivamente l'indirizzo IP a un nome host diverso.

A questo punto XDR 'scade' il mapping e viene elencato come un indirizzo IP precedente.

Non c'è modo di dire al sistema di rompere un'associazione "in anticipo".

Nota sulla corrispondenza del nome host

Per cercare di gestire meglio i casi in cui un tenant ha lo stesso nome host configurato in più domini, XDRA utilizza una corrispondenza "flessibile" e tratta le voci mostrate in questa tabella come nomi host corrispondenti quando cerca una corrispondenza con un dispositivo esistente (nel caso di un IP corrispondente):

```
example
```

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

In altre parole, considera solo il nome host ignorando il resto del nome di dominio.

Ambiente con NVM

Questa configurazione è molto simile alla sezione Ambiente con informazioni sul nome host con informazioni sul nome host, ma esistono alcune differenze.

Questo feed di dati offre i vantaggi aggiuntivi della possibilità di fornire alcuni identificatori di endpoint univoci all'utente e questi ID ci consentono potenzialmente di tenere traccia di un dispositivo fisico che subisce una modifica di nome host (che non è possibile tenere traccia altrimenti, creeremmo 2 dispositivi diversi).

Mentre i dispositivi vengono creati in base al feed di dati dell'endpoint (con ID di endpoint univoci), non vi sono nomi host o IP associati a tali dispositivi fino a quando non viene effettuata un'osservazione sull'endpoint in base ai dati del flusso.

Ambienti con ISE

I vantaggi del rilevamento da ISE a dispositivo sono identici a quelli dell'ambiente con informazioni sul nome host.

I dati ISE vengono usati per associare le informazioni sui nomi host raccolte agli indirizzi IP, ma non per creare un nuovo dispositivo o tenere traccia degli IP che non sono stati rilevati in netflow.

Ambienti con Meraki

Integrazione Meraki "precedente" (con XDRA)

Questa integrazione con Meraki raccoglie proattivamente informazioni sui nomi host dai dispositivi Meraki, mappando tali nomi host sugli IP nel modo consueto per i dispositivi locali (ossia lo "spazio dei nomi predefinito").

Questo processo crea i dispositivi se non esistono già.

ma non aggiunge le informazioni su dispositivi o IP raccolte dalla "nuova" integrazione di Cisco Meraki a causa delle differenze tra gli spazi dei nomi.

In questo modo, la configurazione si comporta come un ambiente con informazioni sul nome host.

"Nuova" integrazione Cisco Meraki (ossia con XDR)

Questa integrazione consente di inserire il netflow dalle apparecchiature di rete Meraki, attraverso il Data Lake XDR, nel percorso di netflow XDRA standard.

Per questo motivo, crea Devices come qualsiasi altro netflow; inoltre, come per tutti gli altri netflow, non contiene informazioni sul nome host.

In effetti, questa configurazione si comporta come un ambiente in cui non sono disponibili informazioni sul nome host, con una delle principali eccezioni.

Questa integrazione sfrutta le informazioni inviate per etichettare il netflow da diverse apparecchiature Meraki in diversi namespace.

In questo modo si evitano i comuni problemi di sovrapposizione delle subnet, ma è possibile introdurre nuove difficoltà se viene impostata più di un'integrazione.

Ovviamente, se sono configurate sia la "vecchia" che la "nuova" integrazione di Meraki, non utilizzano gli stessi spazi dei nomi e quindi creano dispositivi non sovrapposti, anche nei casi in cui le informazioni rappresentano lo stesso dispositivo fisico.

ovvero si dispone di 2 dispositivi, uno nello spazio dei nomi predefinito con un nome host e nessun traffico, un altro con il traffico in uno spazio dei nomi Meraki specifico e nessun nome host.

Se si abilita la funzione contemporaneamente, è possibile che si verifichino "divisioni" simili con altre integrazioni.

Definizioni

1. Indirizzo IP interno: XDRA considera gli indirizzi IP interni o esterni e questo è configurabile tramite le impostazioni della subnet. Per impostazione predefinita, le subnet per le subnet locali sono quelle interne RFC (RFC1918 e RFC4193), ma è possibile configurarle (aggiungerle o rimuoverle).
2. Spazio dei nomi: Informazioni aggiuntive utilizzate per etichettare netflow e dispositivi visti da punti di osservazione diversi, consentendo la sovrapposizione delle subnet senza problemi di IP.

Flusso di dati ISE Hostname

1. ONA raccoglie i dati della sessione ISE, li carica su S3 ogni 10 minuti
    1. questi dati contengono informazioni sull'utente <->IP e talvolta includono anche il nome host
2. IseSessionsMiner analizza i dati caricati e, se possibile, associa gli IP ai dispositivi. NON crea un dispositivo se non ne esiste già uno. Durante questa operazione, raccoglie le mappature dei nomi host <->IP disponibili ogni volta che si dispone già di un dispositivo.
3. Viene quindi creato un file in s3 con tali mapping nello stesso formato in cui l'ONA ne carica

uno dalle ricerche DNS inverse

4. Quindi indica al sistema di caricare i nomi host come se caricasse i nomi host ONA.

Domande frequenti

Perché nella rete vengono visualizzati IP su un dispositivo XDRA che non sono più associati a tale dispositivo logico?

Sfortunatamente, non possiamo fare nulla al riguardo.

Il sistema non è in grado di stabilire se l'associazione precedente non è valida o è il risultato di, ad esempio un'interfaccia di rete fisica aggiuntiva.

Non è stata inviata alcuna informazione sul nome host a XDRA. Perché il dispositivo che utilizza indirizzi IPv4 e IPv6 viene visualizzato come due dispositivi distinti?

Senza le informazioni sul nome host, non è possibile sapere che alla stessa periferica logica della rete sono associati IP diversi.

Perché sullo stesso dispositivo XDRA vengono visualizzati più dispositivi logici di subnet diverse?

Attualmente XDRA non è in grado di distinguere la telemetria della subnet, quindi lo stesso IP è sempre raggruppato in un unico dispositivo.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).