Grundlegendes zu lokalen Geräten, Hostnamen und IP-Zuordnung in XDR-A

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie das Verhalten von XDR-Analytics in Bezug auf den Hostnamen des Geräts und die IP-Zuordnung verstehen.

Hintergrund

XDRA versucht, das Verhalten logischer Geräte über einen längeren Zeitraum zu verfolgen. Dies wird als Gerät bezeichnet.

Dabei werden verschiedene Techniken verwendet, um den Netzwerkverkehr mit diesen logischen Geräten im Laufe der Zeit zu korrelieren.

Vor allem in einer standortbasierten Umgebung ist es jedoch begrenzt, wie gut das System Datenverkehr mit einem Gerät verknüpfen kann.

XDRA erfasst in erster Linie Telemetriedaten für standortbasierte Umgebungen über NetFlow. Dies geschieht über die Integration von ONA, CTB oder Cisco Meraki (die "neue" Meraki-Integration). Außerdem kann die Hostnamenauflösung folgendermaßen erfolgen:

- Aktive Hostnamensauflösung über umgekehrte DNS-Lookups und optional SMB-Abfragen über die ONA
- ISE-Integration über die ONA
- Die "alte" Meraki-Integration
- NVM-Integration, mit weiteren Vorbehalten

NetFlow hat IP-Adressen ohne Hostnamen-Informationen.

Ohne Hostnamen-Informationen geht er davon aus, dass jede interne IP-Adresse (siehe unten stehende Definition) ein Gerät ist, da es keine weiteren Informationen für eine intelligentere Gerätezuordnung besitzt.

In einem Fall, in dem die Hostnamensammlung konfiguriert ist, verwendet XDRA Hostnamen, wenn diese angezeigt werden, um sie mit einer internen Darstellung eines Geräts zu verbinden.

Auf diese Weise kann XDRA mehrere IP-Adressen im Laufe der Zeit zu einem Gerät gruppieren.

Die NVM-Telemetrie kann optional als Teil von XDR konfiguriert werden.

Diese Telemetriequelle bietet einen Datenfeed ähnlich einem NetFlow, aber auch Endgeräteinformationen mit eindeutigen IDs.

Die Art und Weise, wie XDRA diese Informationen nutzt, hat den Nettoeffekt, dass sich die Geräteverfolgung ähnlich verhält wie der Fall, bei dem die Hostnamensammlung auf der ONA aktiviert ist.

All diese Einrichtungen unterliegen Einschränkungen, die auf den Einschränkungen der verfügbaren Telemetrie basieren.

Bitte beachten Sie, dass XDRA davon ausgeht, dass es sich bei der Zuordnung von IP-Adressen und Hostnamen um eine n:1-Beziehung handelt (viele IPs können einem Hostnamen zugeordnet werden).

Ein logisches Gerät kann mehrere IPs gleichzeitig haben (beispielsweise zwei physische Schnittstellen oder IPv4 und IPv6).

Aufgrund der Art der Überwachung kann XDRA niemals davon ausgehen, dass alle Beziehungen des tatsächlichen Netzwerks zu einem bestimmten Zeitpunkt vorliegen.

Überlappende Subnetze

Wenn ein einzelner XDRA-Tenant mehrere Subnetze vor Ort gleichzeitig überwacht, kann das System nicht zwischen denselben IP-Adressen unterscheiden, die in jedem von ihnen vorhanden sind.

Daher werden IPs zu Geräten überkorreliert. Die Verfügbarkeit des Hostnamens verbessert diese Situation nicht.

Eine Möglichkeit, dies zu umgehen, besteht darin, mehr als ein XDRA-Portal zu haben (eines pro Subnetz). Eine weitere Möglichkeit besteht in der Verwendung der "neuen" Cisco Meraki-Integration aufgrund der Namespace-Isolierung, die diese Integration mit sich bringt.

Umgebung ohne verfügbare Hostnamen-Informationen

Als Nebeneffekt der begrenzten Telemetrieinformationen kann das System zu einem falschen Verständnis des Geräteverlaufs kommen.

Ein Szenario ist, wenn IPs dynamisch zugewiesen werden, XDRA hat keine Möglichkeit zu wissen, dass das zugrunde liegende logische Gerät hat sich geändert, zum Beispiel ein Laptop auf WIFI Blätter, und die IP ist einem neuen Laptop zugewiesen.

Wenn kein Hostname oder keine anderen identifizierenden Informationen vorhanden sind, ordnet das System die Aktivitäten mehrerer logischer Geräte einem Gerät zu. Dies kann zu verwirrenden Geräteprofildaten führen.

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

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

Umgekehrt gibt es in Fällen, in denen ein logisches Gerät mehr als eine IP-Adresse hat (z. B. zwei physische Schnittstellen oder IPv4 und IPv6) keine Informationen, mit denen wir diese zuverlässig mit demselben Gerät verknüpfen können, sodass das System dies nicht tut.

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

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

Umgebung mit Hostnamen-Informationen

Während XDRA Hostnameninformationen sehen kann, kann das System einem Gerät mehrere IP-Adressen zuordnen. Angesichts der Art der Daten sind jedoch die Möglichkeiten des Systems zur zuverlässigen Bestimmung immer noch begrenzt. Dies kann zu einer Überkorrelation von IPs mit Geräten im System führen.

Wenn ein Gerät mit einer Zuordnung von IP zu Hostname in XDRA und dann das logische Gerät die IP-Adresse ändert, spiegelt die Telemetrie schließlich die neue Zuordnung von IP zu Hostname wider.

Aufgrund der potenziellen 1:1-Beziehung kann XDRA jedoch NICHT sicher davon ausgehen, dass die zuvor bekannte IP nicht mehr mit dem Hostnamen (und damit dem Gerät) verknüpft ist.

Es könnte sich beispielsweise um eine separate physische Schnittstelle zu demselben logischen Gerät handeln. XDRA behält also beide zuvor erkannten IPs zusammen mit der zuletzt erkannten IP, bis eine Telemetrie erkannt wird, die die IP-Adresse einem anderen Hostnamen zuordnet.

An diesem Punkt "läuft" XDR die Zuordnung ab und wird als vorherige IP-Adresse aufgeführt.

Es gibt keine Möglichkeit, das System anzuweisen, eine Assoziation "früh" zu brechen.

Hinweis zur Hostnamenzuordnung

Um Fälle besser handhaben zu können, in denen ein Tenant denselben Hostnamen in mehreren Domänen konfiguriert hat, verwendet XDRA eine "flexible" Zuordnung und behandelt die in dieser

Tabelle angezeigten Einträge als übereinstimmende Hostnamen, wenn eine Übereinstimmung mit einem vorhandenen Gerät gesucht wird (d. h. im Fall einer übereinstimmenden IP):

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

Mit anderen Worten, es berücksichtigt nur den Hostnamen, während der Rest des Domänennamens ignoriert wird.

Umgebung mit NVM

Dieses Setup verhält sich sehr ähnlich wie Environment mit Hostname-Informationen Abschnitt mit Hostname-Informationen, aber es gibt ein paar Unterschiede.

Dieser Daten-Feed bietet die zusätzlichen Vorteile der Möglichkeit, dem Benutzer einige eindeutige Endpunkt-IDs bereitzustellen, und diese IDs ermöglichen es uns möglicherweise, ein physisches Gerät zu verfolgen, das eine Änderung des Hostnamens durchläuft (was andernfalls nicht möglich ist, da wir zwei verschiedene Geräte erstellen würden).

Geräte werden zwar basierend auf dem Endpunktdaten-Feed (mit eindeutigen Endpunkt-IDs) erstellt, es sind jedoch erst dann ein Hostname oder IP-Adressen mit diesen Geräten verknüpft, wenn anhand der Flow-Daten eine Beobachtung des Endpunkts durchgeführt wird.

Umgebungen mit ISE

Die Vorteile der ISE-to-Device-Nachverfolgung sind letztlich identisch mit denen der Umgebung mit Hostnamen-Informationen.

Die ISE-Daten werden verwendet, um die erfassten Hostnamensinformationen IP-Adressen zuzuordnen. Es werden jedoch keine neuen Geräte erstellt oder IPs nachverfolgt, die in NetFlow nicht gefunden wurden.

Umgebungen mit Meraki

"Alte" Meraki-Integration (das heißt mit XDRA)

Bei dieser Meraki-Integration werden proaktiv Hostnamen-Informationen von Meraki-Geräten gesammelt, die den IP-Adressen wie bei Geräten vor Ort üblich zugeordnet werden (dies ist der "Standard-Namespace").

Bei diesem Prozess werden Geräte erstellt, sofern diese nicht bereits vorhanden sind.

Es ergänzt nicht die Geräte- oder IP-Informationen, die aufgrund von Namespace-Unterschieden aus der anderen "neuen" Cisco Meraki-Integration gewonnen wurden.

Dadurch verhält sich diese Konfiguration wie eine Umgebung mit Hostnamen-Informationen.

"Neue" Cisco Meraki-Integration (d. h. mit XDR)

Bei dieser Integration fließt der NetFlow von den Meraki-Netzwerkgeräten über die XDR-Datensammlung in den standardmäßigen XDRA-NetFlow-Pfad ein.

Dadurch werden Geräte wie jeder andere NetFlow-Prozess erstellt. wie jeder andere NetFlow enthält er keine Hostnamen-Informationen.

Diese Konfiguration verhält sich wie Environment ohne verfügbare Hostnamen-Informationen, mit einer wichtigen Ausnahme.

Diese Integration nutzt die Informationen, die gesendet wurden, um den NetFlow von verschiedenen Meraki-Geräten in verschiedene Namespaces zu kennzeichnen.

Dadurch werden die üblichen Probleme mit überlappenden Subnetzen vermieden, es können jedoch neue Schwierigkeiten auftreten, wenn mehr als eine Integration eingerichtet wird.

Die offensichtlichste Tatsache ist, dass sowohl "alte" als auch "neue" Meraki-Integrationen nicht dieselben Namespaces verwenden und daher nicht überlappende Geräte erstellen, auch nicht in Fällen, in denen die Informationen dasselbe physische Gerät darstellen.

Das heißt, es gibt 2 Geräte, eines im Standard-Namespace mit einem Hostnamen und ohne Datenverkehr, ein anderes mit Datenverkehr in einem bestimmten Meraki-Namespace und ohne Hostnamen.

Ähnliche "Splits" können bei anderen Integrationen auftreten, wenn sie gleichzeitig aktiviert sind.

Definitionen

1. Interne IP-Adresse: XDRA berücksichtigt IP-Adressen entweder intern oder extern und kann über die Subnetz-Einstellungen konfiguriert werden. Subnetze für standortinterne Standard zu den internen RFC-Subnetzen (RFC 1918 und RFC 4193), aber Subnetze können konfiguriert (hinzugefügt oder entfernt) werden.
2. Namespace Zusätzliche Informationen, die zur Bezeichnung von NetFlow und Geräten verwendet werden, die von verschiedenen Beobachtungspunkten aus gesehen werden, sodass sich überschneidende Subnetze ohne sich überschneidende IP-Probleme entstehen.

ISE-Hostname-Datenfluss

1. ONA sammelt ISE-Sitzungsdaten und lädt alle 10 Minuten auf S3 hoch

1. Diese Daten enthalten Benutzer<->IP-Informationen, manchmal auch Hostnamen.

2. IseSessionsMiner analysiert die hochgeladenen Daten und ordnet IP-Adressen Geräte zu, wo dies möglich ist. Es wird KEIN Gerät erstellt, wenn es noch nicht vorhanden ist. Dabei werden verfügbare Hostname<->IP-Zuordnungen erfasst, wenn bereits ein Gerät vorhanden ist.

3. Anschließend wird eine Datei in s3 erstellt, die diese Zuordnungen im gleichen Format enthält, wie die ONA eine Datei aus den umgekehrten DNS-Abfragen hochladen würde.

4. Das System wird angewiesen, diese Hostnamen genauso zu laden, als ob ONA-Hostnamen geladen würden.

Häufig gestellte Fragen

Warum sehe ich IPs auf einem XDRA-Gerät, die diesem logischen Gerät in meinem Netzwerk nicht mehr zugeordnet sind?

Leider können wir nichts dagegen tun.

Das System kann nicht wissen, ob die alte Zuordnung ungültig ist oder das Ergebnis einer beispielsweise zusätzlichen physischen Netzwerkschnittstelle ist.

Ich habe keine Hostnamen-Informationen, die an XDRA gesendet werden. Warum zeigt mein Gerät, das sowohl IPv4- als auch IPv6-Adressen verwendet, zwei verschiedene Geräte an?

Ohne Hostnamen-Informationen können wir nicht wissen, dass verschiedene IPs demselben logischen Gerät in Ihrem Netzwerk zugeordnet sind.

Warum sehe ich mehrere logische Geräte aus verschiedenen Subnetzen, die im gleichen XDRA-Gerät erscheinen?

XDRA hat derzeit keine Möglichkeit zu unterscheiden, woher die Subnetz-Telemetrie stammt, sodass dieselbe IP immer in einem Gerät gruppiert ist.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.