فهم تخطيط الجهاز و Hostname و IP المحلي في XDR-A

المحتويات

المقدمة

يوضح هذا المستند كيفية فهم سلوك تحليلات XDR فيما يتعلق باسم مضيف الجهاز، وتخطيط IP.

الخلفية

يحاول XDRA تعقب سلوك منطقي للأجهزة عبر الوقت، يعرف باسم الجهاز.

وهو يستخدم تقنيات مختلفة لربط حركة مرور الشبكة بهذه الأجهزة المنطقية بمرور الوقت.

ومع ذلك، في بيئة محلية بشكل خاص، هناك حدود لمدى قدرة النظام على ربط حركة المرور بالجهاز.

يقوم XDRA في المقام الأول بتجميع بيانات القياس عن بعد للبيئات المحلية من خلال Cisco Meraki (المكمل "الجديد" Meraki). وأ CTB وأ ONA المكمل عبر NetFlow. ثانياً، يمكنه الحصول على حل اسم المضيف من خلال:

- دقة اسم المضيف النشطة عبر عمليات بحث DNS العكسية واستعلامات SMB الاختيارية عبر ONA
- دمج ISE عبر ONA
- تكامل ميراكي "القديم"
- دمج NVM، مع تحذيرات إضافية

يحتوي NetFlow على عناوين IP بدون معلومات اسم المضيف.

بدون معلومات اسم المضيف، يفترض أن كل عنوان IP داخلي (راجع التعريف أدناه) يرى وهو الجهاز، نظرا لأنه ال يتوفر على مزيد من المعلومات لجعل اقتران الجهاز أكثر ذكاء.

في حالة تكوين مجموعة اسم المضيف، يستخدم XDRA أسماء المضيف، عند رؤيتها، لربطها بتمثيل داخلي للجهاز.

وهذا يسمح ل XDRA بتجميع عناوين IP المتعددة عبر الوقت لجهاز واحد.

يمكن تكوين تتبع NVM إختياريا كجزء من XDR.

يوفر مصدر بيانات القياس عن بعد هذا موجز بيانات شبيه ب NetFlow، ولكنه يوفر أيضا معلومات نقطة النهاية مع معرفات فريدة.

يكون للطريقة التي تستفيد بها XDRA من هذه المعلومات التأثير الصافي لتتبع الجهاز الذي يتصرف بشكل مماثل للحالة التي يتم فيها تمكين مجموعة اسم المضيف على ONA.

ولجميع هذه المحطات قيود تستند إلى حدود بيانات القياس عن بعد المتاحة.

يرجى ملاحظة أن XDRA يفترض أن طبيعة عناوين IP وتعييناتأسماء المضيف هي علاقة متعددة إلى واحدة (يمكن أن يترجم العديد من عناوين IP إلى اسم مضيف واحد).

يمكن أن يحتوي جهاز منطقي واحد على العديد من بروتوكولات IPs في وقت واحد (على سبيل المثال واجهتين فيزيائيتين أو IPv4 و IPv6).

ونظرا لطبيعة عملية المراقبة، لا يمكن أن يفترض XDRA وجود جميع علاقات الشبكة الفعلية في أي وقت من الأوقات.

الشبكات الفرعية المتداخلة

في حالة قيام مستأجر XDRA واحد بمراقبة شبكات فرعية محلية متعددة في وقت واحد، لا يمكن للنظام التمييز بين نفس IP الذي يظهر في كل منها.

وعلى هذا النحو، فإنه يقوم بربط عناوين IP بالأجهزة بشكل زائد. لا يعمل توفر اسم المضيف على تحسين هذه الحالة.

ومن بين الطرق التي يتم بها التغلب على هذه المشكلة أن يتوفر لديك أكثر من بوابة XDRA (بوابة واحدة لكل شبكة فرعية). بينما تتمثل الأخرى في إستخدام تكامل Cisco Meraki "الجديد" بسبب عزل مساحة الاسم التي يجلبها هذا التكامل.

بيئة لا تتوفر بها معلومات عن اسم المضيف

نتيجة للأثر الجانبي الناجم عن محدودية معلومات القياس عن بعد، يمكن أن يصل النظام إلى فهم غير صحيح لمحفوظات الأجهزة.

في بعض الحالات يكون تعيين عناوين IP ديناميكيا، ولا يكون لدى XDRA طريقة لمعرفة أن الجهاز المنطقي الأساسي قد تغير، على سبيل المثال، كمبيوتر محمول على أوراق WiFi، ويتم تعيين عنوان IP لكمبيوتر محمول جديد.

في غياب اسم المضيف أو معلومات التعريف الأخرى، يقوم النظام بربط أنشطة الأجهزة المنطقية المتعددة بجهاز واحد. قد يؤدي ذلك إلى إرباك معلومات ملف تعريف الجهاز.

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

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

وعلى العكس من ذلك، في الحالات التي يكون فيها أحد الأجهزة المنطقية لديه أكثر من

عنوان IP (على سبيل المثال واجهتين فيزيائيتين أو IPv4 و IPv6)، ال توجد معلومات يمكننا من خاللها ربط هذه األجهزة بنفس الجهاز بشكل موثوق، وبالتالي ال يتوفر النظام.

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

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

بيئة تحتوي على معلومات اسم المضيف

حيث يمكن ل XDRA رؤية معلومات اسم المضيف، يتمتع النظام بالقدرة على إقران أكثر من عنوان IP مع جهاز واحد. بيد أنه بالنظر إلى طبيعة البيانات، ال تزال هناك حدود لما يمكن للنظام أن يحدده بشكل موثوق به. قد يؤدي ذلك إلى زيادة إرتباط عناوين IP باألجهزة الموجودة في النظام.

إذا قام جهاز يحتوي على اقتران IP ب hostname في XDRA، ثم قام الجهاز المنطقي بتغيير عنوان IP، فإن بيانات تتبع القياس ستعكس أخيرا تعيين IP الجديد إلى اسم المضيف.

ومع ذلك، ونظرا الحتمال أن تكون هذه العالقة عبارة عن عالقة متعددة إلى واحدة، ال يمكن ل XDRA افتراض أن IP الذي تم عرضه سابقا لم يعد مرتبطا باسم المضيف (وبالتالي الجهاز).

على سبيل المثال، يمكن أن تكون واجهة مادية منفصلة إلى نفس الجهاز المنطقي. وبالتالي يحتفظ XDRA بكل من عناوين IP التي تم رؤيتها سابقا مع أحدث IP، حتى يتم فصل خريطة مترسة التي يتم رسمها من إيجابية لعنوان IP إلى اسم مضيف مختلف.

عند هذه النقطة، تنتهي صالحية XDR للتعيين ويتم ترسيه كعنوان IP سابق.

ال توجد طريقة إلخطار النظام بكسر المعاشرة "في وقت مبكر".

مالحظة في مطابقة اسم المضيف

لمحاولة معالجة الحاالت بشكل أفضل حيث يكون لدى المستأجر نفس اسم المضيف الذي تم تكوينه في مجاالت متعددة، يستخدم XDRA مطابقة "مرنة" ويعامل اإلدخاالت التي تظهر في هذا الجدول كأسماء مضيف مطابقة عند البحث عن تطابق جهاز موجود (في حالة IP مطابق):

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

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

وبمعنى آخر، تأخذ في الاعتبار اسم المضيف فقط بينما تتجاهل باقي اسم المجال.

البيئة باستخدام NVM

يعمل هذا الإعداد بشكل مشابه جدا للبيئة مع قسم معلومات اسم المضيف باستخدام معلومات اسم المضيف، ولكن هناك نوعان من الاختلافات.

يوفر موجز البيانات هذا ميزات إضافية للتمكن من توفير بعض معرفات نقاط النهاية الفريدة للمستخدم، ومن المحتمل أن تسمح لنا هذه المعرفات بتعقب جهاز فعلي يخضع لتغييري في اسم المضيف (وهو ما لا يمكن تتبعه بخلاف ذلك، كما أننا سننشئ جهازين مختلفين).

بينما يتم إنشاء الأجهزة استنادا إلى موجز بيانات نقطة النهاية (مع معرفات نقاط النهاية الفريدة)، لا يوجد اسم مضيف وأو عناوين IP مرتبطة بهذه الأجهزة حتى يتم إجراء ملاحظة حول نقطة النهاية هذه استنادا إلى بيانات التدفق.

البيئات الموزودة بتقنية ISE

وينتهي الأمر بمطابقة ميزات تعقب اسم المضيف (ISE) إلى الجهاز مع البيئة.

يتم إستخدام بيانات ISE لإقران معلومات اسم المضيف التي تجمعها إلى عناوين IP، ولكنها لا تقوم بإنشاء جهاز جديد أو تعقب عناوين IP التي لم يتم رؤيتها في NetFlow.

بيئات باستخدام Meraki

دمج Meraki "القديم" (أي مع XDRA)

يعمل تكامل Meraki هذا بشكل استباقي على جمع معلومات اسم المضيف من أجهزة Meraki، وتعيين أسماء المضيف هذه إلى عناوين IP كالمعتاد للأجهزة الموجودة على الجهاز (وهي "مساحة الاسم الافتراضية").

تقوم هذه العملية بإنشاء أجهزة إذا لم تكن موجودة بالفعل.

لا يقوم بزيادة معلومات الجهاز وأ IP التي تم تجميعها من دمج Cisco Meraki "الجديد" الآخر بسبب إختلافات مساحة الاسم.

وفي الواقع، يتسبب ذلك في أن يتصرف هذا التكوين كبيئة باستخدام معلومات اسم المضيف.

تكامل Cisco Meraki "الجديد" (مع XDR)

هذا الدمج يحصل على NetFlow من أجهزة الشبكة Meraki، من خلال بحيرة بيانات XDR، إلى مسار XDRA NetFlow القياسي.

عل هذا النحو، فإنه يقوم بإنشاء أجهزة مثل أي NetFlow آخر؛ كما هو الحال مع أي NetFlow آخر، ال يحتوي عل معلومات اسم المضيف.

في الواقع، يتصرف هذا التكوين مثل [البيئة بدون معلومات اسم المضيف المتاحة](#)، مع إستثناء رئيسي واحد.

يعمل هذا الدمج عل الاستفادة من المعلومات المرسلة لتسمية NetFlow من أجهزة Meraki المختلفة في مساحات أسماء مختلفة.

يتجنب هذا الإجراء مشاكل [الشبكات الفرعية المتداخلة](#) المعتادة، ولكنه يمكن أن يؤدي إلى ظهور صعوبات جديدة في حالة إعداد أكثر من تكامل واحد.

من الواضح أنه إذا تم إعداد كل من عمليات تكامل Meraki "القديمة" و"الجديدة"، فإنها ال تستخدم نفس مساحات الأسماء ومن ثم تنشئ أجهزة غير متداخلة، حتى في الحالات التي تمثل فيها المعلومات نفس الجهاز الفعلي.

وهذا يعني، أن لديك جهازين، أحدهما في مساحة الاسم الافتراضية باسم المضيف وبدون حركة مرور، والآخر مع حركة مرور في مساحة اسم Meraki معينة وبدون اسم المضيف.

يمكن أن تحدث "فواصل" مماثلة مع عمليات التكامل الأخرى إذا تم تمكينها في نفس الوقت.

التعاريف

1. عنوان IP الداخلي: يأخذ XDRA في الاعتبار عناوين IP الداخلية أو الخارجية، وهذا قابل للتكوين عبر إعدادات الشبكة الفرعية. يمكن تكوين الشبكات الفرعية للشبكات الفرعية الافتراضية إلى الشبكات الفرعية الداخلية ل RFC (RFC1918 و RFC4193) ولكن يمكن تكوين الشبكات الفرعية (إضافة أو إزالة).

2. مساحة الاسم: المعلومات الإضافية التي يتم إستخدامها لتسمية NetFlow والأجهزة التي يتم رؤيتها من نقاط المراقبة المختلفة، مما يسمح [بالشبكات الفرعية المتداخلة](#) دون حدوث مشاكل IP متداخلة.

تدفق بيانات اسم المضيف ISE

1. يقوم ONA بجمع بيانات جلسة ISE، وتحميل إلى S3 كل 10 دقائق

    1. تحتوي هذه البيانات عل مستخدم<->معلومات IP، وتتضمن أيضا اسم المضيف في بعض الأحيان

2. يقوم IseSessionsMiner بتحليل البيانات التي تم تحميلها وربط عناوين IP بالأجهزة حيثما كان ذلك ممكنا. وهو ال ينشئ جهازا إذا لم يكن واحدا موجودا بالفعل. وعندما يقوم بذلك، فإنه يجمع اسم المضيف المتوفر<->تعيينات IP كلما كان لديها جهاز بالفعل.

3. ثم يقوم بإنشاء ملف في S3 مع تلك التعيينات في نفس التنسيق كما يقوم ONA بتحميل ملف من عمليات بحث DNS العكسية الخاصة به

4. ومن ثم يطلب من النظام تحميل أسماء المضيف تلك تماما كما ول أنه يحمل أسماء

المضيف ONA.

الأسئلة الشائعة

لماذا أرى عناوين IP على جهاز XDRA لم تعد مرتبطة بهذا الجهاز المنطقي على شبكتي؟

ولكن من المؤسف أننا لا نستطيع أن نفعل شيئا حيال هذا الأمر.

يتعذر على النظام معرفة ما إذا كان القتران القديم غير صالح وأو نتيجة، على سبيل المثال، واجهة شبكة مادية إضافية.

ليس لدي أي معلومات عن اسم المضيف يتم إرسالها إلى XDRA، لماذا يظهر الجهاز الخاص بي الذي يستخدم كلا من عناوين IPv4 و IPv6 على أنه جهازين مميزين؟

بدون معلومات اسم المضيف لا يمكننا معرفة أن عناوين IP المختلفة مقترنة بنفس الجهاز المنطقي على الشبكة الخاصة بك.

لماذا أرى أجهزة منطقية متعددة من شبكات فرعية مختلفة تظهر في جهاز XDRA نفسه؟

ليس لدى XDRA حاليا طريقة لتمييز ما أي تتبع الشبكة الفرعية، لذلك يتم دائما تجميع IP نفسه في جهاز واحد.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).