SOPHOS

1405/04/20

راهنمای جامع مدیریت و اعمال خودکار آدرس آی‌پی‌های مخرب در فایروال Sophos

سازمان پدافند غیرعامل کشور

مقدمه

به منظور بهبود فرآیند شناسایی و مسدودسازی منابع ناشناخته و مخرب، کانال IRANCTI یک سرویس متمرکز Threat Feed راه اندازی کرده که فهرست آدرس آی‌پی‌های استخراج شده از تله‌های سایبری را از طریق یک دامنه اختصاصی منتشر می‌کند. هدف از ارائه‌ی این راهنما، اتصال دوره‌ای فایروال به این منبع و دریافت آخرین تغییرات بصورت خودکار می‌باشد. همچنین به منظور تسهیل دسترسی کاربران به آخرین فهرست آدرس آی‌پی‌ها و ارائه‌ی برخی آسیب پذیری‌ها، کانال اطلاع‌رسانی IRANCTI در پیام‌رسان‌های بله و ایتا قابل بهره‌برداری می‌باشد .

در بسیاری از سازمان‌ها و مراکز داده، نیاز به مسدودسازی خودکار آدرس‌های آی‌پی مشکوک یا پرخطر وجود دارد. با افزایش تعداد این آدرس‌ها، مدیریت دستی آن‌ها در فایروال نه‌تنها زمان‌بر است، بلکه احتمال بروز خطاهای انسانی را نیز افزایش می‌دهد.

فایروال Sophos از نسخه ۲۱ به بعد، قابلیتی تحت عنوانThird-Party Threat Feeds ارائه می‌کند که به کمک آن می‌توان یک منبع خارجی حاوی لیست آی‌پی ها را به فایروال معرفی کرد. پس از انجام این کار، فایروال به‌صورت خودکار و دوره‌ای این لیست را دریافت کرده و بر اساس تنظیماتی که برای آن قرار می دهیم قانون (Rule) با اقدام (Action) مورد نظر ایجاد می کند. این قابلیت امکان مدیریت متمرکز و به‌روزرسانی خودکار لیست‌های مسدودسازی را فراهم می‌کند و نیاز به اضافه یا حذف دستی آدرس‌ها نمی‌باشد. همچنین این قابلیت از لیست URL و DOMAIN مخرب نیز برای مسدود سازی خودکار پشتیبانی می کند .

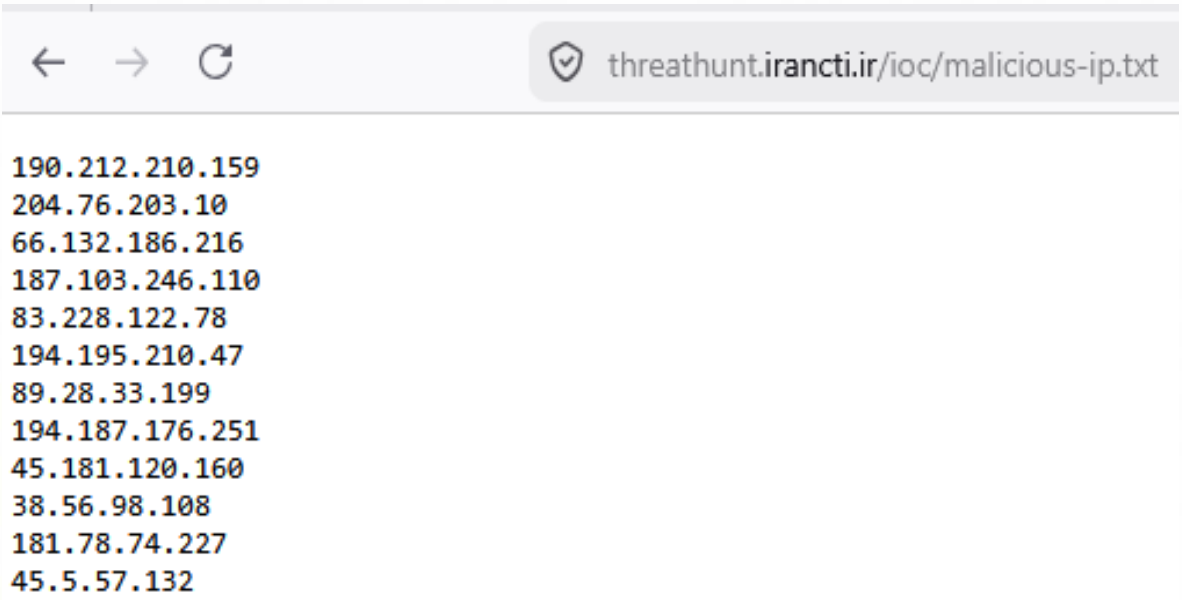
سناریوی عملیاتی

آدرس موردنیاز جهت دسترسی به محتوای آی‌پی‌های مخرب موجود در دامنه IRANCTI به شرح زیر می‌باشد:

https://threathunt.irancti.ir/ioc/malicious-ip.txt

در این آدرس تنها لیست آی‌پی‌های مخرب در ۲۴ ساعت گذشته نمایش داده می‌شود و هیچ اطلاعات دیگری به جز آن وجود ندارد .

محتوای فایل می‌تواند مشابه نمونه زیر باشد:



شکل ۱.دامنه شکارتهدید IRANCTI

هر خط شامل یک آدرس آی‌پی است و Sophos هنگام دریافت فایل، این مقادیر را استخراج و در اختیار Policy های امنیتی قرار می‌دهد.

نحوه عملکرد فایروال Sophos

پس از معرفی URL مربوط به منبع اطلاعات تهدید درSophos ، فرآیند زیر انجام می‌شود:

- فایروال در بازه‌های زمانی مشخص به URL تعریف‌شده متصل می‌شود.
- فایل موجود در URL را دانلود می‌کند.
- محتویات فایل را بررسی می‌کند.
- آی‌پی های موجود را استخراج می‌کند.
- لیست داخلی خود را به‌روزرسانی می‌کند.
- تغییرات را درPolicy های مرتبط اعمال می‌کند.

در نتیجه، هر زمان که فایل اصلی تغییر کند، Sophos نیز پس از همگام‌سازی، تغییرات را دریافت خواهد کرد.

مثال کاربردی

فرض کنید در روز اول محتوای فایل به شکل زیر باشد:

۱۸۵.۱۰.۱۰.۱
۹۱.۲۰۰.۱۰۰.۵
۴۵.۶۶.۷۷.۸۸

سوفوس این سه آی‌پی را دریافت و آن‌ها را مسدود می‌کند.

در روز دوم فایل به شکل زیر تغییر می‌کند:

۱۸۵.۱۰.۱۰.۱
۹۱.۲۰۰.۱۰۰.۵
۱۰۳.۴۴.۵۵.۶۶

در این حالت:

آی‌پی جدید ۱۰۳.۴۴.۵۵.۶۶ به لیست اضافه می‌شود و آی‌پی قبلی که ۴۵.۶۶.۷۷.۸۸ می‌باشد از لیست حذف می‌شود . یعنی با هر بار درخواست از Threat Feed فقط آی‌پی‌های موجود در همان درخواست را دریافت و اعمال می‌کند و حتی ممکن است در درخواست بعدی تمام آی‌پی‌ها تغییر و به روزرسانی شوند .

به‌روز رسانی این سرویس می‌تواند قابل تنظیم باشد و بهتر است این به روز رسانی توسط فایروال با به روز رسانی منبع اطلاعات تهدید یکسان باشد تا تمام آی‌پی ها در Policy های امنیتی اعمال شود. (این آی‌پی‌ها در دامنه IRANCTI به صورت هر ۲۴ ساعت یکبار به روز می‌شوند.)

به عنوان مثال اگر آی‌پی های موجود در منبع اطلاعات تهدید به صورت روزانه به‌روز شوند و فایروال به‌گونه‌ای تنظیم شده باشد که آن‌ها را به صورت هفته ای یکبار دریافت کند، فقط آی‌پی های روز هفتم در فایروال اعمال می‌شود و آی‌پی های ۶ روز گذشته را از دست خواهد داد .

استفاده در سیاست‌های امنیتی

پس از تعریف منبع اطلاعات تهدید، یک شی(object) در Sophos ایجاد می‌شود که نماینده تمامی آی‌پی های موجود در فایل است و می‌تواند در Policy ها مورد استفاده قرار گیرد. (در سوفوس پس از ایجاد منبع اطلاعات تهدید، به صورت خودکار یک سیاست ایجاد می شود و نیازی به ایجاد دستی نمی باشد).

مفهوم Rule تعریف شده:

در قانون تعریف شده هر ترافیکی که از آدرس‌های موجود در Threat Feed ارسال شود، توسط فایروال مسدود خواهد شد . همچنین می‌توان از این Threat Feed در بخش Destination Address نیز استفاده کرد تا ارتباط با مقاصد مشخص‌شده نیز مسدود شود.

مزایای استفاده :

- **مدیریت متمرکز**

تمامی تغییرات در یک نقطه انجام می‌شود و نیازی به اعمال دستی تغییرات روی هر فایروال وجود ندارد.

- **کاهش بار مدیریتی**

مدیر شبکه نیازی به ثبت، ویرایش یا حذف دستی تعداد زیادی آی‌پی نخواهد داشت.

- **افزایش امنیت سیستم کاربران**

اگر که بر روی سیستم کاربران شبکه داخلی agent مربوط به سوفوس نصب شده باشد، در صورت ارتباط سیستم کاربران با آدرس های دریافت شده از منبع اطلاعات تهدید (به عنوان مبدا یا مقصد)، فایروال سوفوس متوجه شده و هشدار صادر می‌کند و در صورت وجود قانون مورد نظر، شبکه آن سیستم را قطع و یا ارتباط با آن آدرس آی‌پی را مسدود می کند .

- **به‌روزرسانی خودکار**

هرگونه تغییر در فایل اصلی به‌صورت خودکار در فایروال اعمال می‌شود.

- **مقیاس‌پذیری**

این سرویس می‌تواند همزمان توسط چندین Sophos در شعب یا مراکز داده مختلف مورد استفاده قرار گیرد.

- **کاهش خطاهای انسانی**

حذف فرآیندهای دستی موجب کاهش اشتباهات عملیاتی خواهد شد.

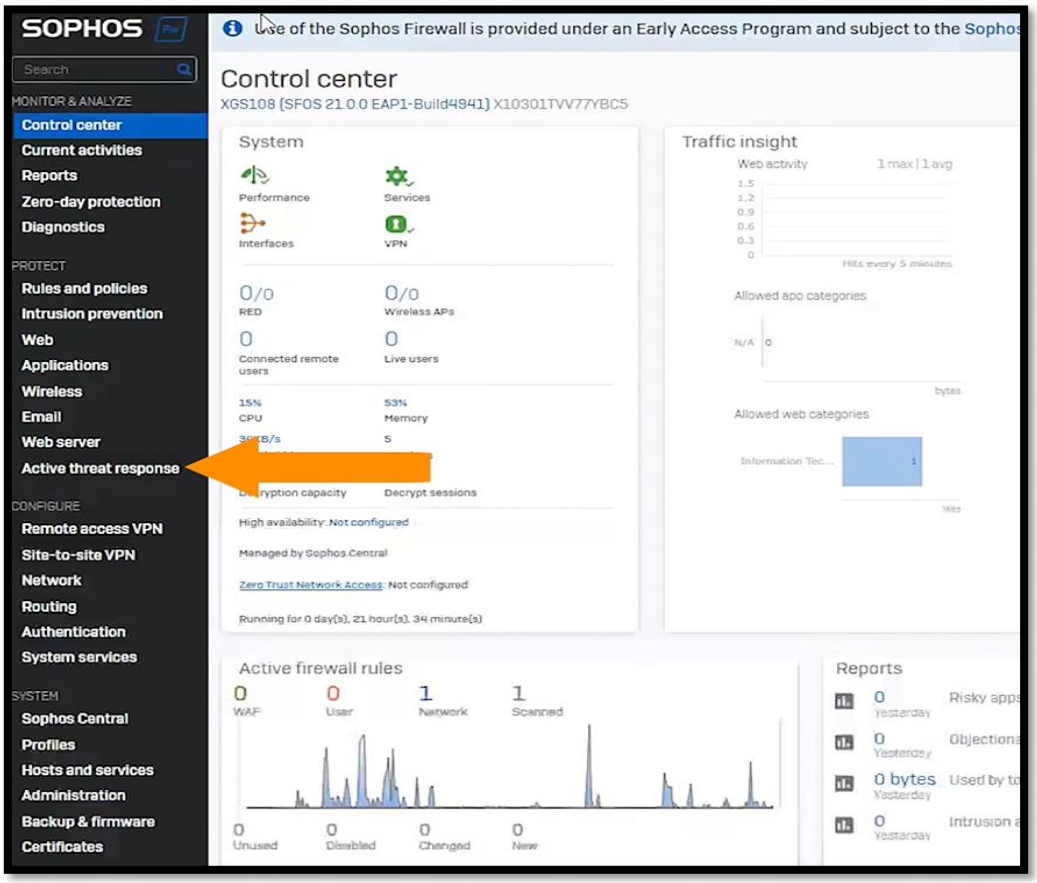
تشریح پیاده سازی

در این مرحله با فرض اینکه فایروال سوفوس به صورت مستقیم و دائمی به اینترنت متصل است شرح داده شده است .

در انتها روش های دیگر نیز ارائه می شود تا در صورتی که سوفوس به اینترنت متصل نیست، بتوان از این قابلیت استفاده کرد .

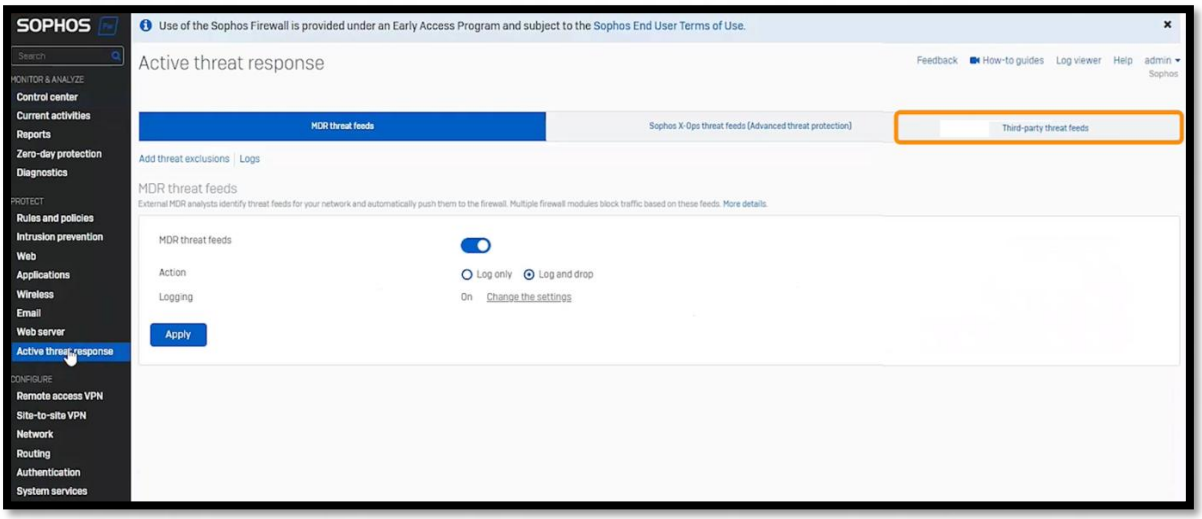
مرحله ۱: اضافه کردن منبع اطلاعات تهدید

در صفحه اصلی قسمت Active threat response را انتخاب می‌کنیم.



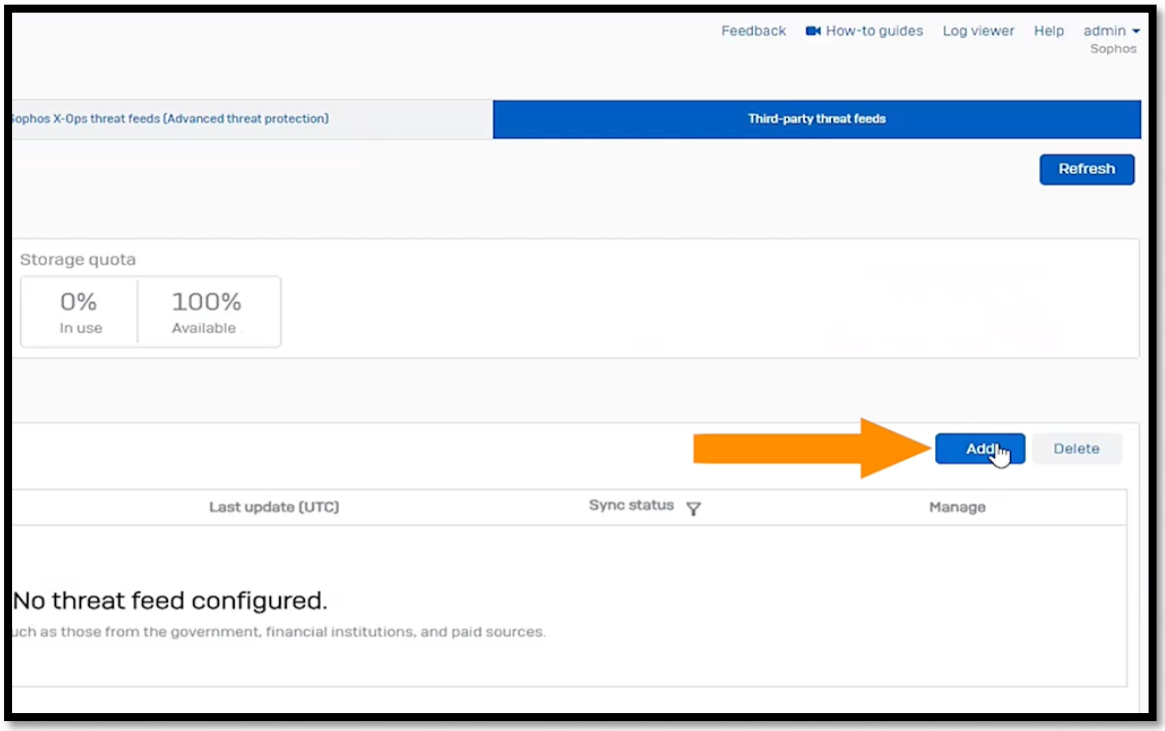
شکل۲. ورود به صفحه Active threat response

در صفحه باز شده Third-Party Threat Feeds را انتخاب می کنیم.



شکل۳. ورود به قسمت Third-Party Threat Feeds

سپس بر روی گزینه Add کلیک می‌کنیم تا وارد قسمت ایجاد منبع اطلاعات تهدید شویم.



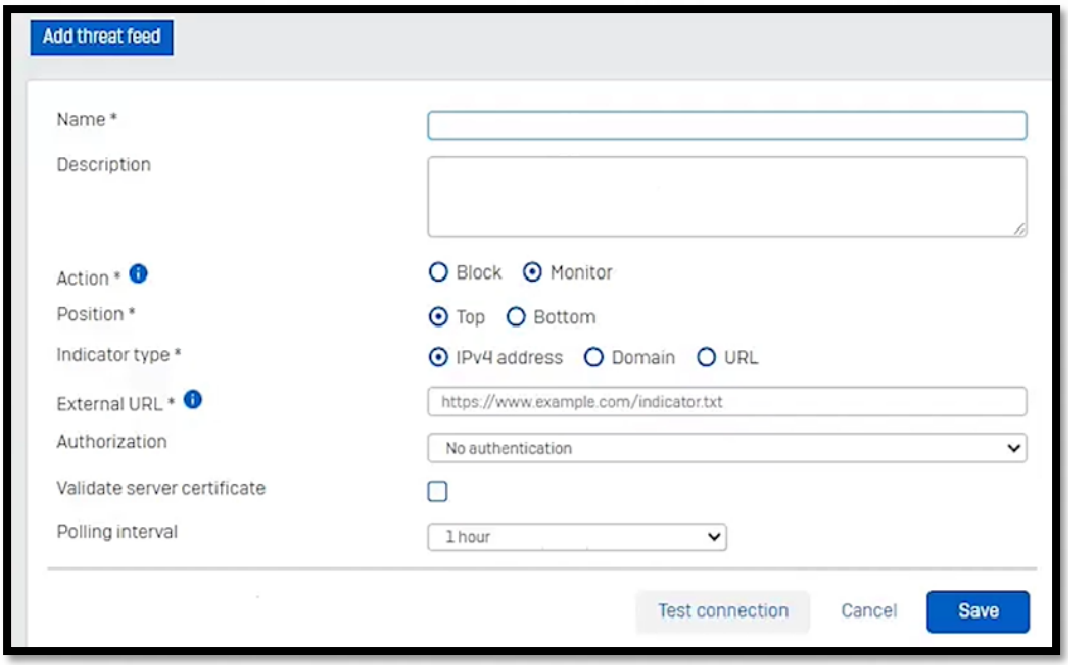
شکل۴. اضافه کردن feed

مرحله ۲: انجام تنظیمات منبع اطلاعات تهدید

در این قسمت می توان جزئیات منبع اطلاعات تهدید را وارد کرد. این جزئیات به صورت زیر می باشد:

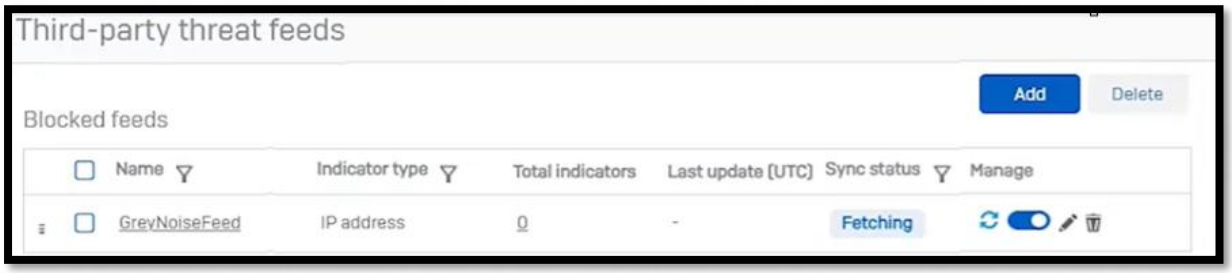
- Name : نام منبع
- Description : توضیحات
- Action : در این قسمت می توان مشخص کرد که رول ایجاد شده ترافیک را فقط مانیتور کند و یا اینکه آن را بلاک کند.
- Postion : جایگاه قرار گیری و اولویت رول ایجاد شده در لیست رول ها در فایروال است.
- Indicator type : مشخص کننده نوع داده منبع اطلاعات تهدید است که می‌تواند آی‌پی یا domainیا url باشد.
- External url : آدرسی که محتوای منابع اطلاعات را از آن دریافت می‌کند .
- Authorization: در صورتی که ادرس مورد نظر نیاز به احراز هویت دارد باید در این قسمت وارد شود در غیر این صورت در حالت no authentication قرار می دهیم .
- Validate server certificate: در صورتی که سرور مورد نظر داخلی و یا مورد تایید باشد نیازی به این قسمت نیست .
- Polling interval: مدت زمان چرخه دریافت اطلاعات از آدرس داده شده را مشخص می‌کند .

بعد از وارد کردن مقادیر مورد نیاز می توان از طریق گزینه test connection برقراری ارتباط با آدرس داده شده را بررسی کرد. در نهایت گزینه save را می زنیم تا feed مورد نظر ایجاد شود .



شکل۵. تعریف feed

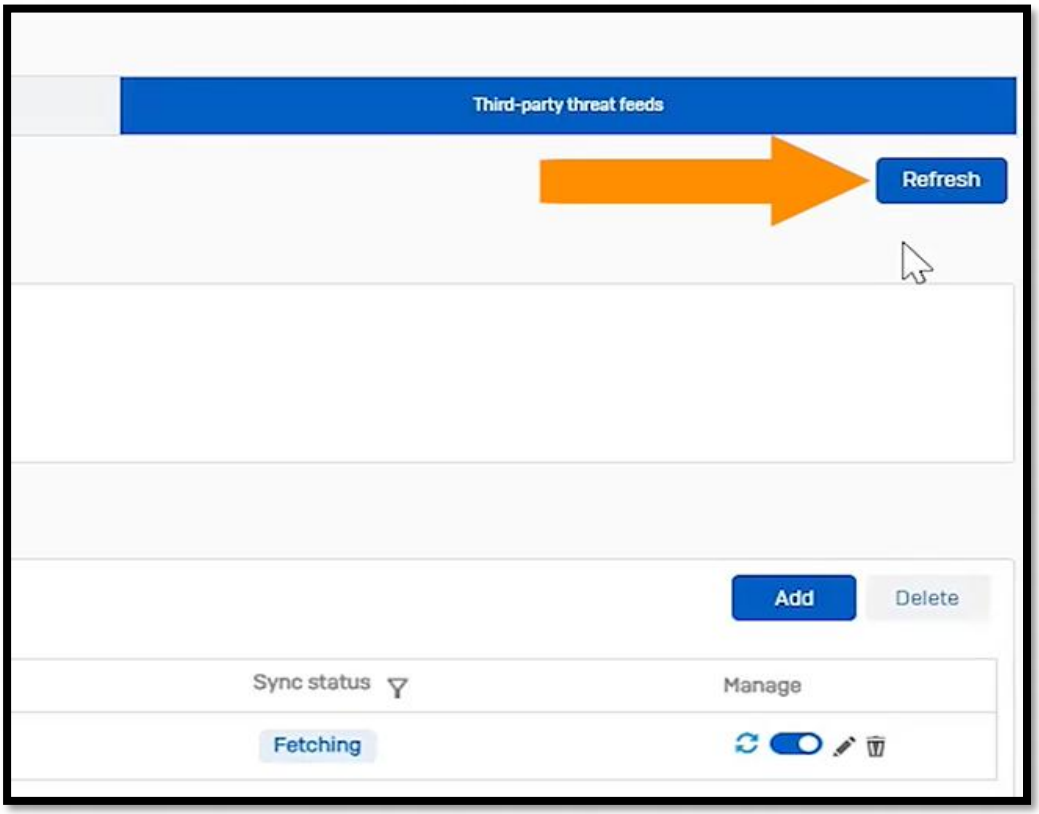
همان طور که در تصویر زیر مشاهده می کنید پس از ایجاد feed، تلاش می کند آدرس ها را دریافت کند.



شکل۶. ذخیره feed

مرحله ۳: بروز رسانی داده ها

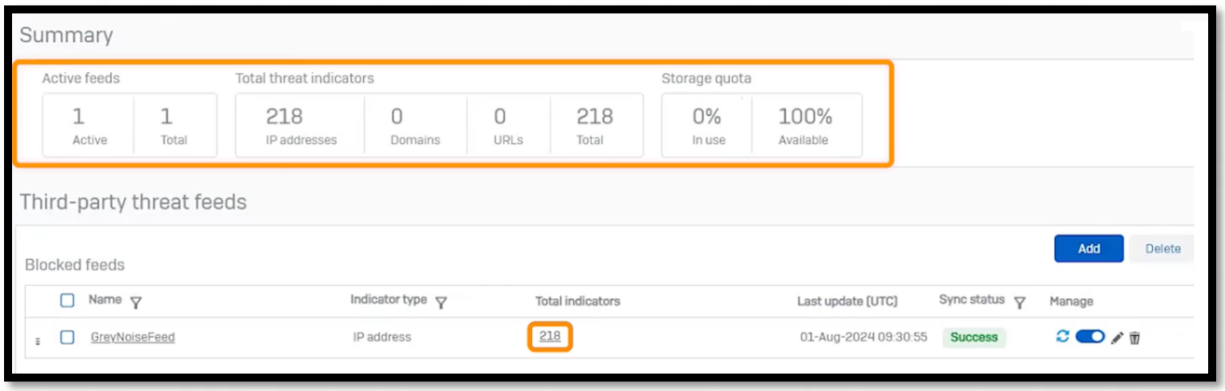
بعد از ایجاد منبع اطلاعات تهدید، ابتدا در حالت fetching قرار دارد و هر بار با زدن گزینه refresh داده های feed استخراج شده و بروزرسانی می شود .



شکل۶. بروزرسانی feed

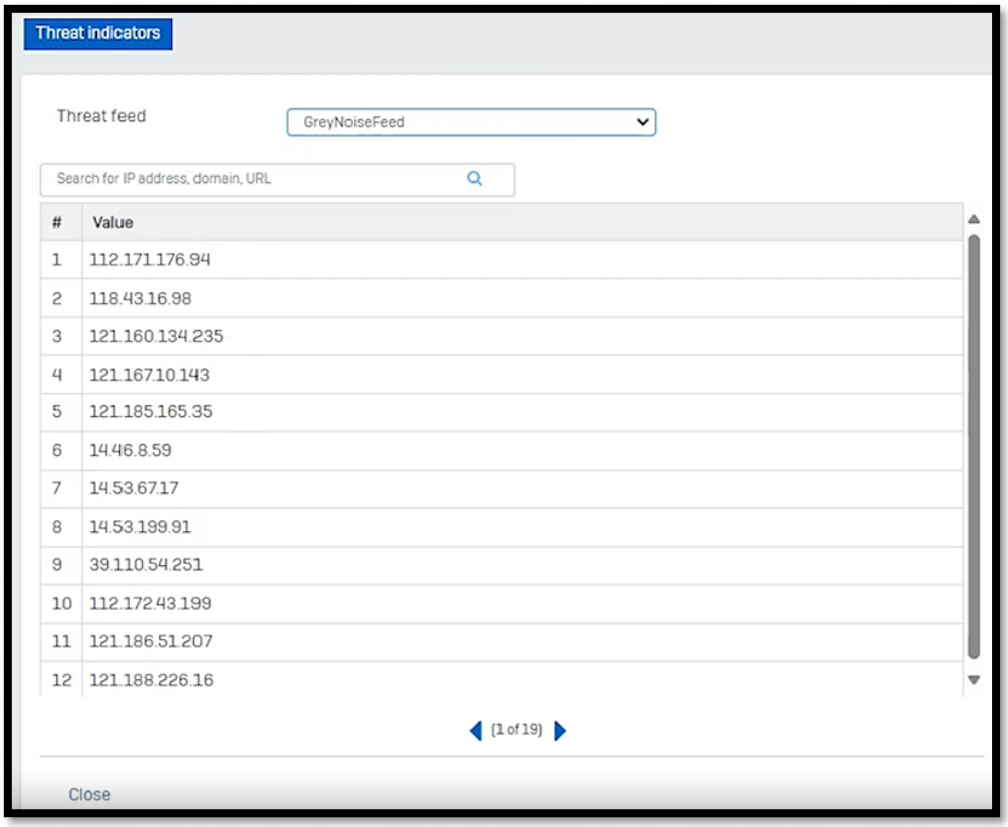
مرحله ۴: بررسی اطلاعات بروز شده

پس از همگام سازی و گرفتن اطلاعات، موارد دریافت شده را می توان مشاهده نمود .



شکل ۷.اطلاعات feed

با کلیک بر روی قسمت total indicator می توان آی‌پی های دریافت شده را مشاهده کرد .

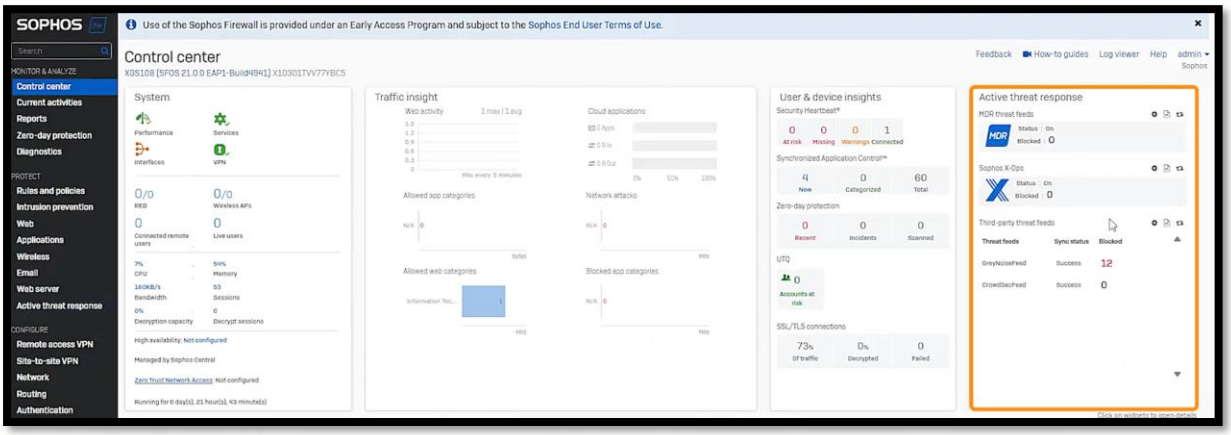


شکل ۸.مشاهده آی‌پی

در این مرحله تنظیمات مربوط به منبع اطلاعات تهدید به اتمام رسیده و در ادامه به بررسی لاگ ها و فعالیت های مربوطه می پردازیم .

مرحله ۵: بررسی وضعیت third-party threat feed

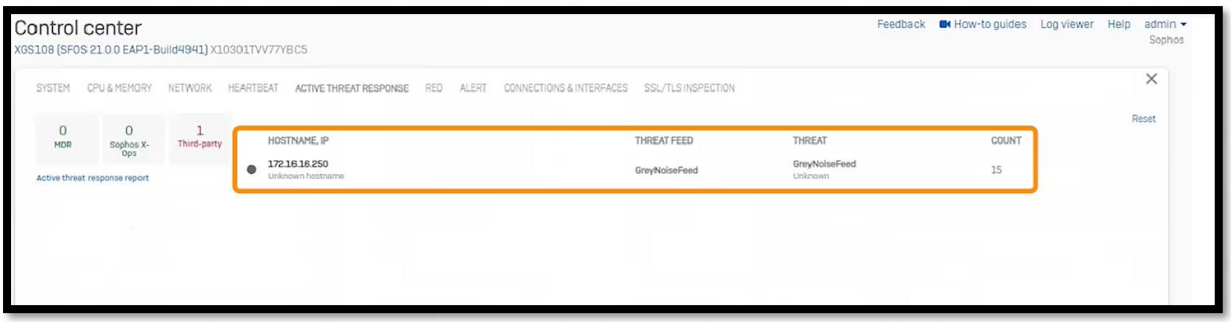
شکل زیر یک نمای کلی از feed های ایجاد شده را نشان می دهد که می‌توان وضعیت به‌روز بودن آن ها و تعداد رول های ایجاد شده را مشاهده کرد .



شکل۹.بررسی وضعیت feed

همانطور که در شکل زیر مشاهده می‌کنید با کلیک بر روی این قسمت وضعیت کلاینت ها (از نظر ارتباط به feed های دریافت شده) را می‌توان مشاهده نمود.

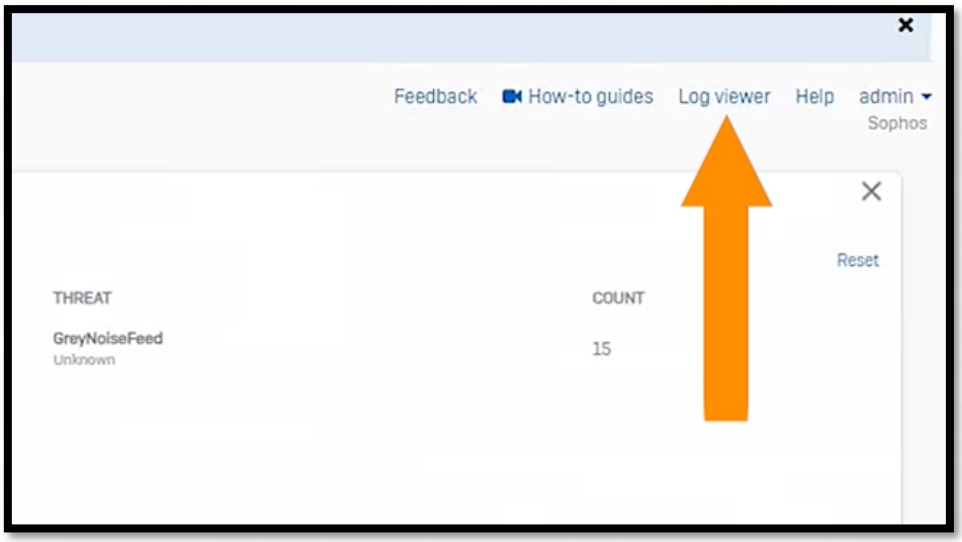
نکته: این قسمت مربوط به زمانی است که agent مروبط به سوفوس (استفاده به عنوان EDR) بر روی کلاینت های شبکه نصب شده باشد.



شکل۱۰.مشاهده وضعیت کلاینت

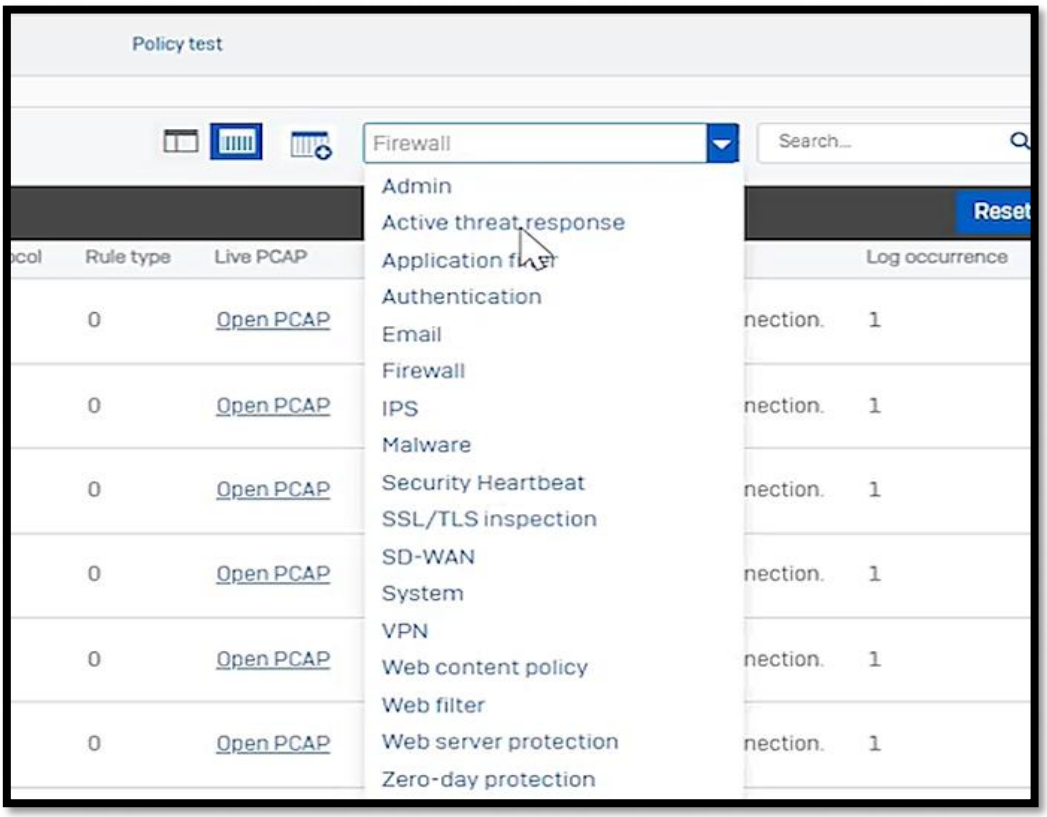
مرحله ۶: بررسی لاگ مربوط به feed در فایروال

با کلیک در بر روی log viewer در بالای صفحه می توان لاگ رول های ایجاد شده به صورت خودکار توسط سوفوس را مشاهده و بررسی نمود.



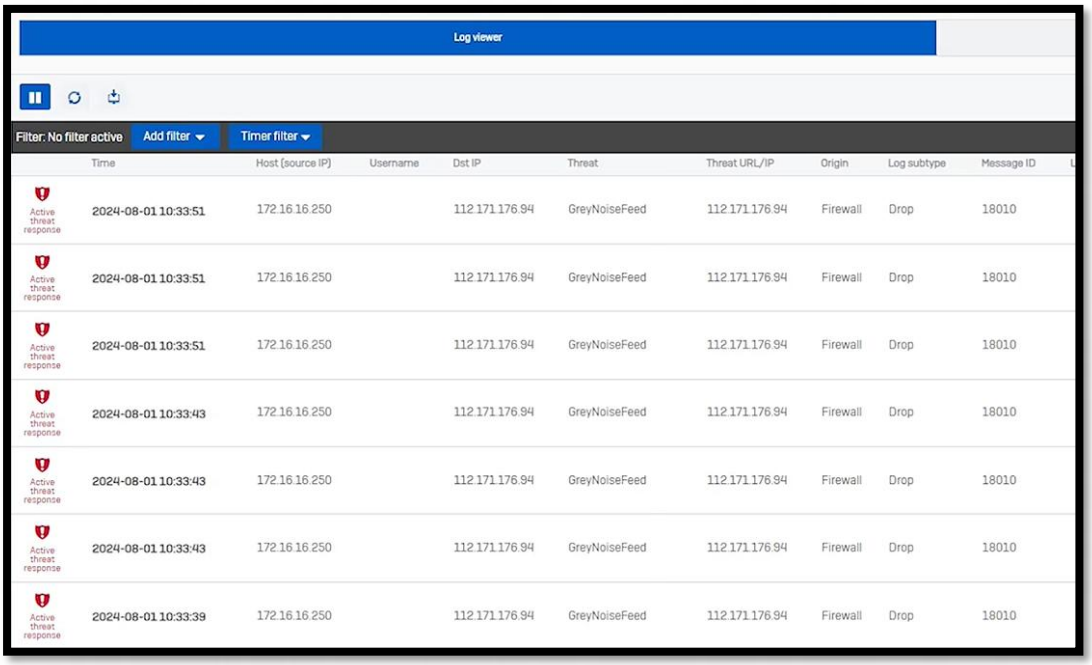
شکل۱۱.مشاهده لاگ

در این حالت با انتخاب گزینه Active threat response می توان لاگ های آن را مشاهده کرد .



شکل۱۲.مشاهده لاگ

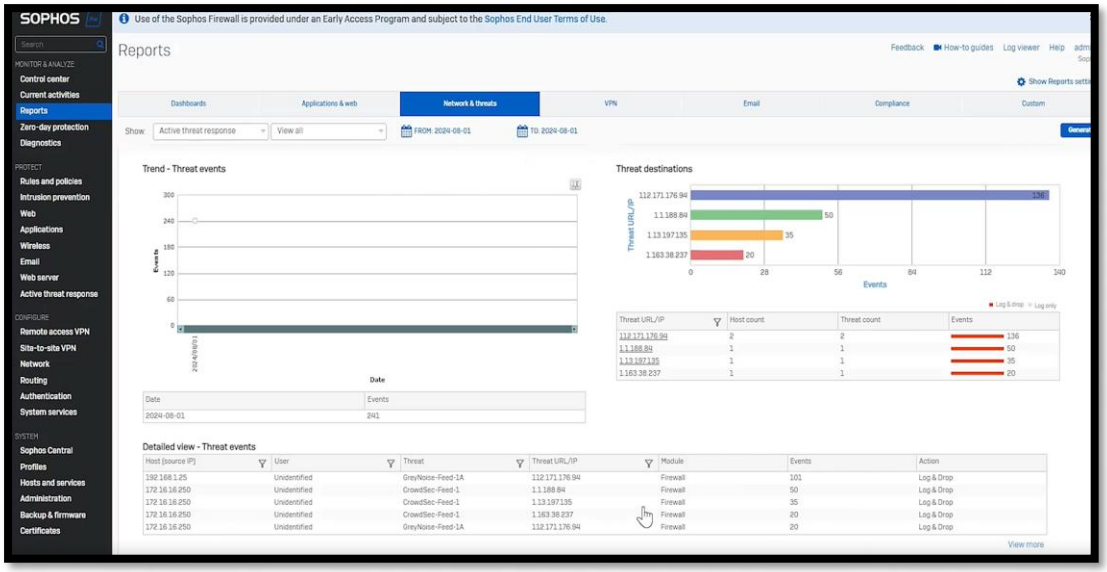
همان طور که در عکس زیر مشخص است، سیاست ایجاد شده در فایروال ترافیک به مقصد آدرس feed را مسدود کرده است.



شکل ۱۳.بررسی لاگ

مرحله ۷: بررسی و ایجاد گزارش

در قسمت report با ورود به زیر مجموعه Network & threat می توان از وضعیت آدرس های دریافت شده، میزان ترافیک هرکدام، ارتباط کاربران با این آدرس ها و مواردی مانند آن را در بازه های زمانی مورد نظر مشاهده و گزارش کامل ایجاد کرد.



شکل ۱۴.بررسی وایجاد گزارش

الزامات پیاده‌سازی

برای استفاده صحیح از این قابلیت، موارد زیر باید فراهم باشد:

- Sophos باید به URL معرفی‌شده دسترسی شبکه داشته باشد.
- در صورت استفاده از HTTPS ، گواهی SSL باید معتبر باشد.
- URL معرفی‌شده باید به‌صورت پایدار در دسترس باشد.
- ساختار فایل باید مطابق فرمت مورد انتظار Sophos باشد.

ملاحظات امنیتی

توصیه می‌شود:

- Feed از طریق HTTPS منتشر شود .
- محتوای فایل به‌صورت دوره‌ای بازبینی شود.
- دسترسی به سرور منتشرکننده Feed محدود شود .
- دسترس‌پذیری سرور منتشرکننده به‌صورت مستمر پایش شود.

نحوه ارتباط فایروال با منبع خارجی Threat Feed

توضیحات ارائه‌شده در خصوص استفاده از قابلیت Threat Feed زمانی به‌صورت کامل قابل اجرا است که فایروال سازمان به‌صورت مستمر و مطابق با الزامات امنیتی تعریف‌شده، امکان برقراری ارتباط با اینترنت و دریافت به‌روزرسانی‌های موردنیاز را داشته باشد. در این شرایط، فایروال می‌تواند در بازه‌های زمانی مشخص به منبع Threat Feed متصل شده و آخرین فهرست شاخص‌های تهدید شامل آدرس‌های آی‌پی را دریافت و اعمال نماید.

با این حال، در بسیاری از سازمان‌ها به دلیل الزامات امنیتی، سیاست‌های شبکه و یا ملاحظات حاکمیتی، امکان اتصال مستقیم فایروال به اینترنت وجود ندارد. در چنین شرایطی می‌توان از سناریوهای جایگزین زیر برای بهره‌برداری از Threat Feed استفاده نمود:

سناریوی اول: اتصال موقت و دوره‌ای فایروال به اینترنت

در این روش، فایروال در بازه‌های زمانی مشخص و تحت کنترل تیم امنیت، به‌صورت موقت به اینترنت متصل می‌شود تا آخرین اطلاعات Threat Feed را از منبع موردنظر دریافت نماید. پس از تکمیل فرآیند به‌روزرسانی، دسترسی اینترنت مجدداً قطع خواهد شد.

مزایا:

- پیاده‌سازی ساده و بدون نیاز به زیرساخت اضافی.
- مناسب برای سازمان‌هایی که به‌روزرسانی لحظه‌ای Threat Feed برای آن‌ها ضروری نیست.

محدودیت‌ها:

- فرآیند به‌روزرسانی وابسته به مداخله انسانی است.
- اطلاعات تهدیدات با تأخیر نسبت به حالت برخط دریافت می‌شوند.

سناریوی دوم: استفاده از یک سرور واسط در شبکه داخلی

در این سناریو یک سرور داخلی با دسترسی کنترل‌شده به اینترنت در شبکه سازمان مستقر می‌شود. این سرور به‌صورت دوره‌ای اطلاعات Threat Feed را از دامنه IRANCTI یا منبع تولیدکننده Feed دریافت و در اختیار فایروال قرار می‌دهد.

در این حالت فایروال به جای اتصال مستقیم به اینترنت، صرفاً به سرور داخلی متصل شده و فایل‌های Threat Feed را از آن دریافت می‌کند.

برای اینکار می توان از بزارهایی مانند curl و lynx و ... کمک گرفت . به عنوان مثال:

```
Curl threathunt.irancti.ir/ioc/malicious-ip .txt  -o ip_list.txt
```

در این روش آدرس ها در یک فایل text ذخیره می شوند . به منظور اتصال سوفوس به سرور و دریافت فایل لازم است روی پورت ۸۰ یک http server داخلی راه اندازی شود.

به عنوان مثال :

```
Sudo python3 –m http.server 80
```

سپس در قسمت تنظیمات مربوط به feed در سوفوس ، در قسمت external url آدرس سرور داخلی را قرار می دهیم .

مزایا:

- حذف نیاز به اتصال مستقیم فایروال به اینترنت.
- امکان اعمال کنترل‌های امنیتی، ثبت رویدادها و پایش فرآیند دریافت داده‌ها.
- کاهش سطح ریسک دسترسی اینترنتی برای تجهیزات امنیتی.

نکات و ملاحظات:

با توجه به اینکه سوفوس فایل آی‌پی ها را از سرور واسط دریافت می کند باید موارد امنیتی را در این سرور رعایت نمود تا از آلوده شدن آن جلوگیری شود.

توصیه می‌شود:

- دسترسی سرور داخلی باید محدود باشد .
- ترافیک های ورودی و خروجی سرور داخلی محدود و کنترل شده باشد .
- در صورت امکان از ابزار های DPL یا FIM جهت بررسی فایل استفاده شود .

سناریوی سوم: معماری دو مرحله‌ای (DMZ / Staging Server)

در سازمان‌هایی با الزامات امنیتی سخت‌گیرانه‌تر می‌توان از معماری دو سروری استفاده کرد.

در این روش:

۱. سرور اول دارای دسترسی محدود و کنترل‌شده به اینترنت بوده و اطلاعات Threat Feed را از دامنه IRANCTIدریافت می‌کند.

۲. سرور دوم هیچ‌گونه دسترسی مستقیمی به اینترنت ندارد و اطلاعات را صرفاً از سرور اول دریافت و ذخیره می‌کند.

۳. فایروال تنها به سرور دوم متصل شده و اطلاعات Threat Feed را از این سرور دریافت می‌نماید.

در این معماری، فایروال هیچ ارتباط مستقیمی با اینترنت یا حتی با سرور متصل به اینترنت نخواهد داشت و کلیه تبادل داده‌ها از طریق یک لایه واسط انجام می‌شود.

مزایا:

- بالاترین سطح جداسازی و کنترل امنیتی.

- کاهش ریسک انتقال تهدیدات از محیط اینترنت به تجهیزات امنیتی.
- مناسب برای سازمان‌های حساس، زیرساخت‌های حیاتی و محیط‌های دارای الزامات انطباقی سخت‌گیرانه.

نکات و ملاحظات:

- دسترسی هر دو سرور داخلی باید محدود باشد .
- ترافیک های ورودی و خروجی سرورها محدود و کنترل شده باشد .
- در صورت امکان، سرور آفلاین تنها با سوفوس و سرور اول در ارتباط باشد و تمام ترافیک های دیگر مسدود شود .
- از ابزار های DPL یا FIM جهت بررسی فایل استفاده شود .
- جهت ارتباط امن برای جابه جایی فایل بین ۲ سرور از روش ها و ابزارهایی مانند SSH tunneling و VPN وSTunnel و ... استفاده شود .

سناریوی چهارم: انتقال آفلاین Threat Feed

در سازمان‌هایی که هیچ‌گونه ارتباط مستقیم یا غیرمستقیم با اینترنت مجاز نیست، اطلاعات Threat Feedمی‌تواند توسط یک سامانه مجاز در خارج از محیط عملیاتی دریافت و پس از انجام کنترل‌های امنیتی لازم، به‌صورت آفلاین به شبکه داخلی منتقل شود. در این روش فایل‌های Threat Feed بر روی یک مخزن یا سرور داخلی بارگذاری شده و فایروال اطلاعات موردنیاز را از همان منبع داخلی دریافت می‌کند.

این سناریو بیشترین سطح جداسازی از اینترنت را فراهم می‌کند، اما فرآیند به‌روزرسانی وابسته به اقدامات دستی بوده و معمولاً برای محیط‌های بسیار حساس و زیرساخت‌های با الزامات امنیتی سخت‌گیرانه مورد استفاده قرار می‌گیرد.

سناریوی پنجم: بارگذاری دستی شاخص‌های تهدید در فایروال

در سازمان‌هایی که امکان استفاده از Threat Feed و یا استقرار زیرساخت واسط برای توزیع اطلاعات تهدید وجود ندارد، می‌توان شاخص‌های تهدید (IOC) را به‌صورت دستی یا از طریق اسکریپت‌های کنترلی در فایروال بارگذاری نمود.

در این روش، اطلاعات Threat Feed توسط دامنه IRANCTI دریافت شده و پس از انجام بررسی‌های امنیتی و تأیید صحت داده‌ها، فهرست آدرس‌های آی‌پی به‌صورت دستی و یا از طریق API در قالب Address Objectو Address Group در فایروال ثبت می‌شوند.

مزایا :

- عدم نیاز به اتصال فایروال به اینترنت.
- عدم نیاز به سرور واسط یا زیرساخت توزیع Feed
- امکان اعمال کنترل و تأیید کامل بر روی داده‌های واردشده.

محدودیت‌ها:

- فرآیند به‌روزرسانی وابسته به اقدامات دستی یا اجرای اسکریپت‌های مدیریتی است.
- با افزایش تعداد شاخص‌های تهدید، مدیریت و نگهداری اطلاعات دشوارتر خواهد شد.
- امکان تأخیر در اعمال آخرین تغییرات و به‌روزرسانی‌های Threat Intelligence وجود دارد.

این روش معمولاً در سازمان‌هایی مورد استفاده قرار می‌گیرد که به دلیل محدودیت‌های عملیاتی یا الزامات امنیتی، امکان استفاده از مکانیزم‌های خودکار دریافت و به‌روزرسانی Threat Feed را ندارند و ترجیح می‌دهند تمامی داده‌های ورودی پیش از اعمال در تجهیزات امنیتی مورد بررسی و تأیید قرار گیرند.

جمع‌بندی

قابلیت Third-Party Threat Feeds در Sophos روشی استاندارد، کارآمد و منعطف برای دریافت و اعمال خودکار شاخص‌های تهدید از منابع خارجی محسوب می‌شود. در این روش تنها با تعریف آدرس منبع Feed ، فایروال می‌تواند به‌صورت دوره‌ای اطلاعات موردنیاز را دریافت کرده و از آن‌ها در سیاست‌های امنیتی، مکانیزم‌های مسدودسازی و فرآیندهای دفاعی سازمان استفاده نماید. این قابلیت ضمن کاهش فعالیت‌های دستی، سرعت واکنش به تهدیدات را افزایش داده و مدیریت متمرکز و به‌روزرسانی مستمر داده‌های امنیتی را تسهیل می‌کند.

با این حال، نحوه پیاده‌سازی و به‌روزرسانی Threat Feed باید متناسب با الزامات امنیتی، سطح حساسیت دارایی‌ها و سیاست‌های حاکم بر شبکه سازمان انتخاب شود. اگرچه اتصال مستقیم فایروال به اینترنت ساده‌ترین روش بهره‌برداری از این قابلیت است، اما سازمان‌ها می‌توانند با استفاده از سرورهای واسط، معماری‌های چندلایه، انتقال آفلاین داده‌ها یا حتی بارگذاری دستی شاخص‌های تهدید، ضمن حفظ الزامات امنیتی خود از مزایای Threat Intelligence بهره‌مند شوند. در تمامی این سناریوها، رعایت اصل حداقل دسترسی (Least Privilege)، کنترل و اعتبارسنجی داده‌های دریافتی، ثبت رویدادها و پایش مستمر ارتباطات از الزامات اساسی برای حفظ امنیت و اطمینان از صحت عملکرد سامانه خواهد بود.