SOPHOS

Sophos Network Detection and Response

Mejore las operaciones de seguridad con Sophos Network Detection and Response (NDR)

Monográficos de Sophos. Abril 2023

Introducción

En el panorama actual de amenazas en constante cambio, las organizaciones deben adoptar un enfoque proactivo para identificar y responder a posibles ciberataques. La tecnología de detección y respuesta de red (NDR) desempeña un papel fundamental en esta estrategia.

Esta tecnología se sirve del análisis de Deep Learning, la coincidencia basada en reglas tradicional y estadísticas de flujo basadas en riesgos para analizar el tráfico de red sin procesar e identificar actividad sospechosa y potencialmente maliciosa en la red. Esto permite a los equipos de seguridad tomar medidas proactivas para evitar los ciberataques y minimizar su impacto.

Sin embargo, el elevado índice de falsos positivos es un reto habitual asociado a la tecnología NDR. Sophos NDR solventa esta limitación por medio de una tecnología patentada de agrupación y puntuación que combina pruebas de diversos motores de detección de amenazas.

Si bien la tecnología NDR lleva disponible desde los noventa, su complejidad y precisión varían de un proveedor a otro. Es crucial que las organizaciones se planteen incorporar una solución NDR robusta como Sophos NDR, que ofrece unos niveles avanzados de detección de amenazas y permite identificar amenazas con precisión minimizando los falsos positivos. En este monográfico, profundizaremos en las funciones y ventajas de Sophos NDR y explicaremos por qué debe ser un componente fundamental de las operaciones de seguridad de cualquier organización.

Contenido

Evolución de la supervisión de la seguridad de red: cronología de la tecnología NDR

Sophos NDR es un componente crítico de las operaciones de seguridad modernas, pero el origen de la NDR se remonta a los años 90, cuando surgieron los sistemas de detección de intrusiones basadas en red (NIDS). Los primeros sistemas NIDS se centraban en la identificación y el bloqueo de los ataques en la red, pero no podían correlacionar distintos eventos ni detectar amenazas avanzadas que abarcaban múltiples sistemas.

A principios de los 2000, la tecnología NDR evolucionó para resolver estas limitaciones. En lugar de simplemente identificar ataques individuales basados en la red, las soluciones NDR empezaron a analizar el tráfico de red y a correlacionar eventos entre varios sistemas a fin de identificar amenazas avanzadas. Sophos NDR es una solución NDR líder que se sirve del análisis de Deep Learning, la coincidencia basada en reglas tradicional y estadísticas de flujo basadas en riesgos para identificar actividad sospechosa y potencialmente maliciosa en la red.

Con el tiempo, la tecnología NDR se ha vuelto más sofisticada, ya que proporciona visibilidad casi en tiempo real de la actividad de la red y se integra perfectamente con otras soluciones de seguridad. La siguiente cronología muestra los principales hitos en la evolución de la tecnología NDR:

AÑO	HITO
1980-89	Empiezan a aparecer los productos de seguridad de red, con una amplia adopción de la tecnología de firewall.
1990-99	Aparecen los sistemas de detección de intrusiones basadas en red (NIDS), lo que marca el inicio de la supervisión de la seguridad de red.
2000-09	La tecnología de detección y respuesta de red (NDR) evoluciona y pasa a analizar el tráfico de red y a correlacionar eventos en distintos sistemas.
2010-19	Se integran algoritmos avanzados de Machine Learning en las soluciones NDR para poder identificar amenazas complejas y reducir los falsos positivos.
2016	La red de bots Mirai, que utiliza dispositivos IoT, lanza uno de los ataques de denegación de servicio distribuidos (DDoS) más importantes de la historia, lo que subraya la necesidad de una seguridad de red avanzada.
2019	Gartner introduce el término «detección y respuesta de red (NDR)» para reemplazar el término anterior «análisis de tráfico de red (NTA)».
Desde 2020	Las soluciones NDR ofrecen visibilidad en tiempo real y opciones de despliegue flexibles para que las organizaciones puedan incorporarlas en cualquier entorno.

Las soluciones NDR como Sophos NDR permiten a las organizaciones detectar y responder de manera efectiva a las amenazas avanzadas.

Sophos NDR: supervisión de redes avanzada para amenazas modernas

Sophos NDR es una solución de supervisión de redes avanzada diseñada para responder al complejo y cambiante panorama de amenazas.

A diferencia de las soluciones NDR tradicionales, Sophos NDR combina distintos motores de detección propios y el análisis de Deep Learning, lo que proporciona información procesable en tiempo real sobre una amplia variedad de amenazas de red.

Los motores de detección propios de Sophos NDR clasifican el tráfico de red en función de más de 330 protocolos, 50 riesgos de flujo y miles de indicadores de peligro (IoC). Estos motores también incorporan predicciones de múltiples modelos de Deep Learning, lo que ofrece un nivel de precisión sin precedentes en la detección de amenazas al tiempo que minimiza los falsos positivos.

Ventajas clave de Sophos NDR:

NDR TRADICIONAL	SOPHOS NDR	MEJORA
Cobertura de protocolos limitada	Más de 330 protocolos de red	Sophos NDR clasifica el tráfico usando más de 330 protocolos para obtener una visión más amplia del tráfico de red, lo que es crucial para identificar amenazas nuevas y emergentes. Consulte la lista completa de protocolos en el Apéndice B.
IoC básicos	Miles de IoC	Sophos NDR utiliza miles de indicadores de peligro (IoC) para mejorar la precisión de la detección de amenazas.
Identificación mínima de riesgos de flujo	50 riesgos de flujo	Sophos NDR incorpora 50 riesgos de flujo en sus motores de detección propios para poder detectar más amenazas complejas que podrían pasar desapercibidas a otras soluciones NDR. Consulte la lista completa de riesgos de flujo en el Apéndice A.
Coincidencia basada en reglas	Análisis de Deep Learning	Sophos NDR utiliza análisis de Deep Learning para ofrecer un nivel de precisión sin precedentes en la detección de amenazas al tiempo que minimiza los falsos positivos.
Altos índices de falsos positivos	Tecnología patentada de agrupación y puntuación	Sophos NDR utiliza una tecnología patentada de agrupación y puntuación para reducir los falsos positivos, lo que proporciona información procesable sobre una amplia variedad de amenazas de red.

Estas mejoras son especialmente relevantes para la NDR porque permiten que Sophos NDR identifique y responda con precisión a las amenazas de red sin generar un número excesivo de falsos positivos. Sophos NDR destaca por su velocidad, precisión y capacidad de gestionar el tráfico cifrado sin tener que descifrarlo, lo que lo convierte en un componente esencial de cualquier estrategia de seguridad integral.

Sophos NDR ofrece a las organizaciones una solución de supervisión de redes avanzada diseñada para detectar y responder eficazmente a un panorama de amenazas en constante cambio. Al combinar varios motores de detección propios con el análisis de Deep Learning, Sophos NDR proporciona información procesable que es tanto precisa como relevante para las amenazas modernas de hoy.

Arquitectura conceptual del sensor de NDR

Sophos NDR se despliega como solución de supervisión pasiva del tráfico que escucha en un puerto SPAN o espejo y que no añade latencia al tráfico de red ni crea un punto de error en la red si se sobrecarga o está desconectada.

A medida que los datos fluyen hacia el sensor, se recopilan metadatos y los detalles de los flujos de red se envían a una serie de motores de detección antes de agruparse y puntuarse. Los resultados de los flujos de red agrupados se envían a Sophos Data Lake y se presentan en el panel de detecciones de Central.

Procesamiento de paquetes de red (NPP)

Para garantizar el buen funcionamiento de las soluciones NDR, es fundamental recopilar metadatos de los flujos de red de forma efectiva. Este proceso implica consolidar los paquetes de red en una única comunicación o flujo y recopilar metadatos de cada paquete de red mediante la inspección detallada de paquetes (DPI). A continuación, los metadatos recopilados se complementan con información de geolocalización y otras métricas, como destinos menos habituales, periodicidad y dinámicas de paquetes. La fase final consiste en detectar indicadores de riesgo como información de TLS incorrecta, tráfico unidireccional, paquetes DNS de gran tamaño y otros.

Para comprender mejor los datos de encabezado de paquete y de capa de aplicación que se recopilan en esta fase, en las siguientes tablas se incluyen ejemplos de lo que se puede determinar a partir de cada categoría y por qué son importantes para la búsqueda de amenazas.

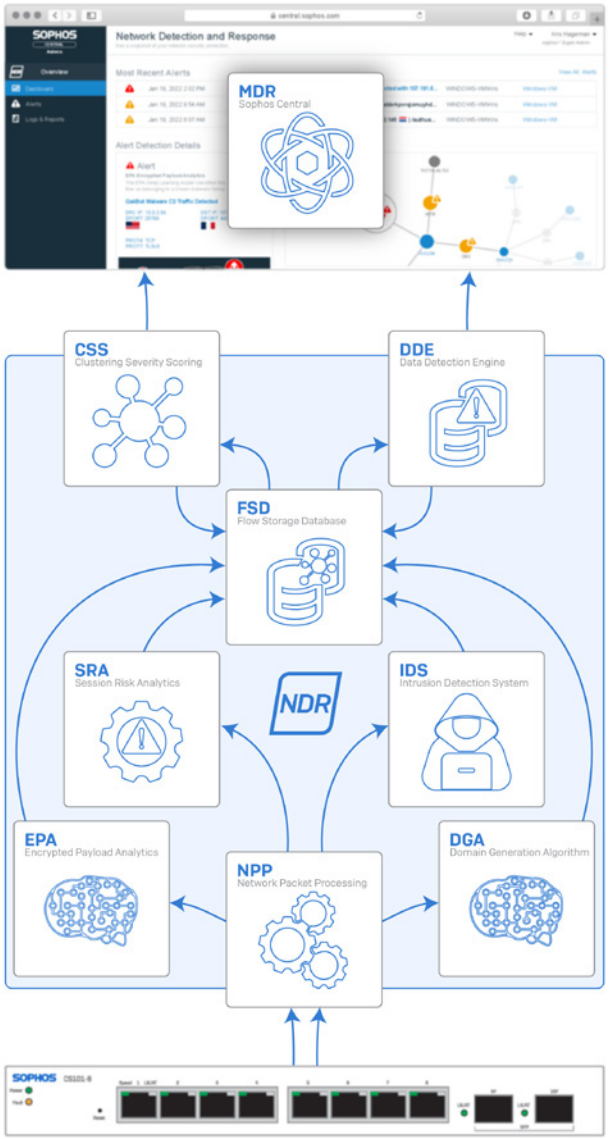

Figura 1: Diagrama de la arquitectura de Sophos NDR

NPP: datos de encabezado de paquete

Los datos de encabezado de paquete proporcionan información sobre la comunicación de red, como las direcciones de origen y destino, el protocolo de transporte, la duración y el tamaño. Ayudan a las soluciones NDR a identificar el origen de la comunicación y la amenaza que podría suponer. A continuación se indica alguna de la información que se puede obtener a partir de los datos de encabezado de paquete:

DATOS DE ENCABEZADO DE PAQUETE	DESCRIPCIÓN	IMPORTANCIA PARA LA BÚSQUEDA DE AMENAZAS DE NDR
IP de origen	Dirección IP del remitente.	Identifica el origen de la comunicación, que puede utilizarse para hacer un seguimiento de la actividad sospechosa o localizar hosts infectados.
Dirección MAC de origen	Dirección Media Access Control (MAC) del remitente.	La dirección MAC puede usarse para identificar el dispositivo físico asociado al tráfico de red y utilizarse con información de otros sensores para correlacionar alertas de múltiples sensores en un dispositivo específico.
Puerto de origen	Puerto utilizado por el remitente para la comunicación.	Ayuda a identificar el servicio o la aplicación específicos asociados a la comunicación, lo que se puede utilizar para detectar actividad sospechosa o no autorizada.
IP de destino	Dirección IP del receptor.	Ayuda a identificar el destino de la comunicación, lo que puede utilizarse para identificar el origen de amenazas externas.
Dirección MAC de destino	Dirección MAC del receptor.	Ayuda a identificar el dispositivo físico asociado a la comunicación, que puede utilizarse para hacer un seguimiento de la actividad sospechosa o localizar hosts infectados.
Puerto de destino	Puerto utilizado por el receptor de la comunicación.	Ayuda a identificar el servicio o la aplicación específicos asociados a la comunicación, lo que se puede utilizar para detectar actividad sospechosa o no autorizada.
Etiquetas TCP	Indica el estado de una conexión TCP, como SYN, ACK, FIN, RST, etc.	Se puede utilizar para detectar actividad de red sospechosa o ataques, como el escaneado de puertos o ataques de denegación de servicio.
Duración de la comunicación	Tiempo que ha durado la comunicación.	Ayuda a identificar actividad sospechosa, como conexiones que duran más de lo esperado, conexiones inusualmente cortas y comunicaciones periódicas relacionadas con la señalización.
Bytes recibidos	Cantidad de datos recibidos durante la comunicación.	Se puede utilizar para detectar actividad sospechosa o ataques, como la exfiltración de datos o las descargas de malware.
Protocolos de Capa 3 (red) y Capa 4 (transporte)	Protocolos utilizados para la comunicación, como IP, OSPF, ICMP, TCP y UDP.	Ayuda a identificar el tipo de tráfico y servicios asociados, lo que se puede utilizar para detectar actividad sospechosa o no autorizada.
ID de VLAN (red de área local virtual) de la red	Etiqueta VLAN asociada a la comunicación.	Ayuda a identificar el segmento de red específico asociado a la comunicación.

NPP: datos de capa de aplicación

Los datos de capa de aplicación proporcionan información clave sobre el contenido de la comunicación de red, lo que permite a las soluciones NDR identificar posibles amenazas que puedan esconderse en ella. Ofrece información sobre las aplicaciones y los servicios utilizados en la comunicación de red y ayuda a identificar nombres de usuario y contraseñas en texto sin cifrar. A continuación encontrará ejemplos de la información que se puede obtener a partir de los datos de capa de aplicación.

DATOS DE CAPA DE APLICACIÓN	EXPLICACIÓN	IMPORTANCIA PARA LA BÚSQUEDA DE AMENAZAS DE NDR
Protocolo de capa de aplicación	Protocolo que se utiliza en la capa de la aplicación, como HTTP, TLS o SMB (bloque de mensajes del servidor).	Conocer el protocolo de capa de aplicación que se está utilizando puede ayudar a identificar tráfico potencialmente malicioso y comportamientos anormales para ese protocolo.
Nombres de host de origen y destino	Nombres de host asociados a las direcciones IP de origen y destino, resueltos mediante DNS u otros medios.	Puede ayudar a identificar tráfico potencialmente malicioso y comportamientos anormales asociados a hosts o dominios.
Tipo de contenido HTTP	Tipo de contenido que se está transfiriendo mediante HTTP, como texto, imagen o vídeo.	Puede ayudar a identificar tráfico potencialmente malicioso y comportamientos anormales asociados a tipos de contenido.
Código de respuesta	Código de estado de HTTP devuelto por el servidor en respuesta a una solicitud HTTP.	Puede ayudar a identificar tráfico potencialmente malicioso y comportamientos anormales asociados a códigos de respuesta concretos, como 404 No encontrado o 500 Error interno del servidor.
URL	URL completa que se solicita o a la que se accede.	Puede ayudar a identificar tráfico potencialmente malicioso y comportamientos anormales asociados a URL dominios.
Agente de usuario	Agente de software utilizado por el cliente para realizar la solicitud, como un navegador web o una app móvil.	Puede ayudar a identificar tráfico potencialmente malicioso o comportamientos anormales asociados a agentes de usuario, como los asociados a software malicioso conocido.
Nombres de usuario y contraseñas en texto sin cifrar	Cualquier nombre de usuario o contraseña transmitidos en texto sin cifrar, como una solicitud HTTP no cifrada.	Puede ayudar a identificar posibles problemas de seguridad e intentos de acceso no autorizado.
Información del certificado TLS	Información sobre el certificado TLS utilizado en una conexión segura, incluidos los hashes JA3.	Puede ayudar a identificar certificados potencialmente maliciosos o falsificados, además de arrojar luz sobre la naturaleza del tráfico cifrado.
Cliente y servidor SSH, método HASSH	Método con huella digital para identificar clientes y servidores SSH.	Puede ayudar a identificar posible tráfico SSH malicioso o detectar intentos de acceso SSH no autorizado.
Encapsulación CAPWAP	Protocolo de control y aprovisionamiento de puntos de acceso inalámbricos (CAPWAP), utilizado para gestionar puntos de acceso inalámbricos.	Puede ayudar a identificar intentos de acceso inalámbrico potencialmente maliciosos o no autorizados y actividad inusual en la red inalámbrica.

En conclusión, la recopilación de metadatos de los flujos de red es un componente esencial de las soluciones NDR que ofrece visibilidad sobre la comunicación de red y permite detectar posibles amenazas. Los datos de encabezado de paquete y de capa de aplicación proporcionan una información valiosa que permite identificar el origen, el tipo y el posible riesgo de la comunicación. Sirviéndose de esta información, las soluciones NDR pueden detectar y responder de manera efectiva a las amenazas de red.

Motores de detección de Sophos NDR

Sophos NDR incorpora cinco motores de detección diferentes para ofrecer una funcionalidad de detección de amenazas exhaustiva. Estos motores de detección funcionan de manera conjunta para identificar y correlacionar varios indicadores de peligro, que después se puntúan y se presentan como información sobre amenazas procesable en Sophos Central a los clientes y analistas.

Para garantizar un mejor rendimiento, los motores de detección con Machine Learning (EPA – Análisis de paquetes cifrados y DGA – Algoritmo de generación de dominios) no se ejecutan en todos los flujos de red, sino que se activan en función de los resultados de otros motores de detección. Permitir la colaboración entre motores de detección para la clasificación es fundamental para mantener el rendimiento y reducir los falsos positivos.

Después, los resultados de los motores de detección se introducen en un algoritmo de agrupación y puntuación de gravedad (CSS) para generar una puntuación global de la amenaza, que se presenta al administrador como una detección en el panel de detecciones de Sophos Central. El registro de detección contiene los resultados del análisis de cada motor.

Motor IDS (Sistema de detección de intrusiones)

Este motor IDS propio es un motor optimizado y más eficiente con la capacidad de identificar indicadores de peligro (IoC) en el tráfico no cifrado. Muchos proveedores de seguridad siguen utilizando sistemas de correspondencia de contenidos excesivamente complicados, incluso cuando la visibilidad se ve limitada debido al cifrado.

Sophos NDR utiliza información sobre amenazas cuidadosamente seleccionada para crear reglas IDS clasificadas en seis grupos, en función del tipo de IoC. Estas son las clasificaciones de las reglas y sus descripciones:

Actividad diversa

Esta clasificación de regla tiene un nivel de gravedad bajo y se utiliza para detectar tráfico de red no asociado a las otras clasificaciones. Algunos ejemplos son el tráfico a servidores DNS públicos, el tráfico a redes de distribución de contenido y el tráfico a servicios en la nube de confianza. Identificar actividad diversa ayuda a establecer una referencia para el tráfico de red normal y señala cualquier desviación de esa referencia.

Infracción de políticas

Esta clasificación de regla tiene un nivel de gravedad bajo y se utiliza para detectar tráfico que puede infringir una política corporativa. Algunos ejemplos son el tráfico a sitios web o servicios no autorizados y el tráfico desde dispositivos no autorizados. Detectar infracciones de políticas ayuda a las organizaciones a hacer cumplir sus políticas de seguridad y a evitar accesos no autorizados y la exfiltración de datos.

Malicioso desconocido

Esta clasificación de regla tiene un nivel de gravedad medio y se utiliza para identificar comunicaciones de red con un destino potencialmente malicioso. Esto puede incluir comunicaciones con una dirección IP o un dominio maliciosos conocidos o comunicaciones con un dominio sinkhole utilizado para redirigir el tráfico a una infraestructura maliciosa. Detectar tráfico malicioso desconocido puede ayudar a identificar endpoints comprometidos y evitar la exfiltración de datos y males mayores.

Descarga de malware

Esta clasificación de regla tiene un nivel de gravedad alto y se utiliza para identificar comunicaciones de red con un origen de distribución de malware conocido. Esto puede incluir comunicaciones con un servidor de comando y control (C2) conocido utilizado para descargar o distribuir malware, o comunicaciones con un sitio de distribución de malware conocido. Detectar descargas de malware ayuda a las organizaciones a identificar e aislar los endpoints infectados para detener la propagación del malware.

Actividad troyana

Esta clasificación de regla tiene un nivel de gravedad alto y se utiliza para identificar comunicaciones con un servidor C2 de malware conocido. Esto puede incluir comunicaciones con un servidor C2 utilizado para el control remoto de un endpoint comprometido, o comunicaciones con un servidor C2 utilizado para exfiltrar datos. Detectar actividad troyana ayuda a las organizaciones a identificar y aislar los endpoints comprometidos y evitar la exfiltración de datos y males mayores.

Lista negra de TLS

Esta clasificación de regla tiene un nivel de gravedad crítico y se utiliza para identificar comunicaciones de red con un atacante conocido en función de la coincidencia del certificado TLS. Esto puede incluir comunicaciones con un dominio malicioso conocido que utiliza un certificado TLS comprometido, o comunicaciones con un dominio malicioso conocido que no utiliza un certificado TLS válido. Detectar tráfico TLS en la lista negra ayuda a las organizaciones a impedir comunicaciones con infraestructuras maliciosas conocidas y a protegerse de los ciberataques.

Motor SRA (Análisis de riesgos de sesiones)

El motor SRA detecta cuándo el tráfico de red se desvía de los estándares de los protocolos documentados, lo que podría indicar actividad de red sospechosa o peligrosa. Esto es importante en la búsqueda de amenazas porque ayuda a identificar comportamientos no estándar que podrían apuntar a un ataque. Cuando el motor SRA observa esta actividad, añade información sobre el comportamiento a los metadatos del flujo. Estos riesgos de flujo no se consideran indicadores de peligro por sí solos, pero cuando se acompañan de detecciones de otros motores, pueden ayudar a identificar actividad maliciosa.

A continuación se incluye una lista con los riesgos de flujo generales, que pueden encontrarse en diversos protocolos, y lo que indican:

TIPO	RIESGO DE FLUJO	DESCRIPCIÓN
General	Posible exploit	Indica que se ha detectado un posible exploit, como Log4J/Log4Shell. Es importante para detectar la actividad de exploits y evitar o mitigar ataques.
General	Protocolo conocido en puerto no estándar	Indica que se está utilizando un protocolo en un puerto no estándar, como HTTP en TCP/8000 en lugar del estándar TCP/80. Es importante para detectar atacantes que utilizan puertos no estándar para eludir la detección.
General	ASN peligroso	Indica que se ha intercambiado tráfico de red con un servidor que pertenece a un ASN (número de sistema autónomo) que se considera de riesgo. Es importante para identificar hosts o redes maliciosos.
General	Tráfico unidireccional	Indica que una sesión es unidireccional, lo que podría indicar actividad de C2 a un servidor que ya no opera en la dirección. Es importante para identificar hosts comprometidos y servidores C2.
General	Sesión de uso compartido de archivos o de escritorio	Indica que el flujo transporta datos de uso compartido de archivos o de escritorio, como TeamViewer o AnyDesk. Es importante para detectar atacantes que utilizan estas herramientas para controlar un host comprometido de forma remota.
General	Protocolo no seguro	Indica que el protocolo utilizado no es seguro y que no debería usarse, como Telnet en lugar de SSH. Es importante para detectar atacantes que pueden interceptar y leer tráfico enviado mediante protocolos no seguros.
General	Credenciales en texto sin cifrar	Indica que se han transmitido credenciales en texto sin cifrar a través de un protocolo conocido, como FTP, HTTP, IMAP, POP3 o SMTP. Es importante para detectar atacantes que pueden interceptar y leer credenciales en texto sin cifrar.
General	Paquete con formato incorrecto	Indica que un paquete tiene un formato inesperado, lo que podría indicar un error de protocolo o la toma de control de un protocolo válido para transportar otro tipo de datos. Es importante para detectar ataques que se sirven de la manipulación de paquetes o hacen un mal uso de los protocolos.
General	Problemas de TCP	Indica que se han encontrado problemas en la configuración de TCP de la sesión de red. Es importante para detectar ciberdelincuentes que aprovechan problemas de TCP en sus ataques para alterar o eludir la detección.
General	Flujo periódico	Indica que la sesión de red se está repitiendo según un intervalo programado, lo que podría indicar actividad de C2 por parte de un troyano o una red de bots. Es importante para detectar atacantes que utilizan comunicaciones periódicas para mantener el control de los hosts comprometidos.

Consulte la lista completa de riesgos de flujo en el Apéndice A.

Motor EPA (Análisis de cargas cifradas) y Machine Learning

El Machine Learning se utiliza cada vez más en las soluciones de detección y respuesta de red (NDR) para detectar tráfico sospechoso en redes empresariales. Las herramientas NDR analizan continuamente el tráfico sin procesar y/o los registros de flujo, como NetFlow, para crear modelos que reflejen el comportamiento de red normal, según Gartner. El Deep Learning lleva más allá esta estrategia al posibilitar la detección de patrones en múltiples atributos, lo que permite realizar detecciones sin información sobre amenazas basada en IoC.

Sophos ha desarrollado una solución específica llamada Análisis de cargas cifradas (EPA) para responder al desafío de detectar amenazas en tráfico cifrado usando tecnologías más antiguas. Los flujos de red se componen de paquetes con datos de encabezado y de carga. Cuando se inspecciona una comunicación cifrada, los datos de carga están cifrados, por lo que no es posible conocer el contenido sin descifrarlo. EPA es un modelo de predicción con Deep Learning multiclase entrenado para detectar patrones en flujos de red en función de la secuencia de longitud de paquete y tiempo entre llegadas (SPLIT). Estos atributos SPLIT son fáciles de calcular y se utilizan para entrenar una red neuronal convolucional (CNN) para la clasificación. Sophos NDR utiliza un proceso patentado para normalizar, transformar y presentar estos datos a la CNN para la clasificación.

Figura 2: Secuencia de longitud de paquete y tiempo entre llegadas

Al utilizar muestras de malware activas, el modelo EPA puede identificar actividad maliciosa en tiempo real, incluidas variantes de malware desconocidas o de día cero y servidores C2, en función de los patrones de los flujos de red entre ellos. El motor EPA también complementa los metadatos del flujo con información de la familia de malware detectada y una puntuación de confianza para reducir el número de falsos positivos. En general, EPA permite a las organizaciones detectar y responder a amenazas cifradas que anteriormente habrían pasado desapercibidas. Este enfoque es especialmente útil cuando los dispositivos endpoint no pueden ejecutar un producto de protección de endpoints tradicional y cuando las comunicaciones de red no deberían descifrarse debido a los requisitos para proteger la información de identificación personal (PII).

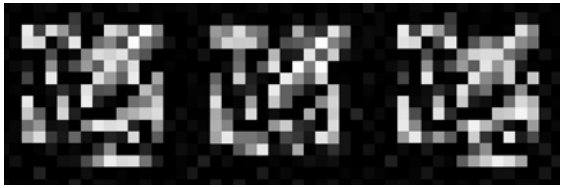

Figura 3: Variante de Cobalt Strike después de procesarla como imagen para la CNN de EPA

El motor EPA (Análisis de cargas cifradas) mejora los metadatos del flujo mediante la identificación de la familia concreta de malware (como Bumblebee, Cobalt Strike, Emotet, Dridex o QakBot) y proporciona una puntuación de confianza de 0 a 100. Para reducir el número de falsos positivos, el modelo también incluye una clasificación de «desconocido».

Motor DGA (Algoritmo de generación de dominios)

Los algoritmos de generación de dominios (DGA) son utilizados por los ciberdelincuentes para generar nombres de dominio que pueden usarse para realizar actividades de comando y control (C2) sin que se les incluya en la lista negra. Por medio de estos algoritmos, el malware puede generar una lista de posibles nombres de dominio en los que podría alojarse el servidor C2. Tras numerosos intentos, el algoritmo encontrará un dominio que exista y establecerá una conexión.

Figura 4: Ejemplo de dominio DGA

Históricamente, DGA se ha utilizado en diversos ataques de gran repercusión. Por ejemplo, en el ataque del gusano Conficker de 2008, se utilizó DGA para generar una lista de más de 50 000 nombres de dominio todos los días que podían utilizarse como servidores C2. Debido a esto, los investigadores de seguridad tuvieron enormes dificultades para desactivar la red C2 del gusano. En otro caso, el malware Gameover Zeus también utilizó DGA para generar hasta 1000 nombres de dominio por día con el objetivo de establecer un servidor C2. La red de bots Gameover Zeus llegó a robar más de 100 millones USD a víctimas de todo el mundo.

El motor de detección DGA de Sophos NDR es crucial para identificar actividad maliciosa en tiempo real. El motor de detección DGA de Sophos NDR está respaldado por una red neuronal de memoria a corto-largo plazo (LSTM) de Deep Learning que evalúa cada nombre de dominio que se consulta y al que se accede. Es importante destacar que no toda la actividad de DGA es maliciosa, ya que muchos servicios legítimos utilizan DGA habitualmente. Por lo tanto, Sophos NDR no genera una alerta cada vez que se detecta un DGA. En lugar de ello, se añade una puntuación de confianza (0-100) a los metadatos del flujo, que es utilizada por el motor de agrupación y puntuación de gravedad (CSS) para determinar si la actividad relacionada con las detecciones de DGA es en efecto maliciosa.

Motor de detección de datos (DDE)

El motor de detección de datos (DDE) es un componente de Sophos NDR que se ejecuta en cada sensor. Es un motor de correlación ligero que aprovecha el almacenamiento de base de datos incorporado de los flujos de red y los grupos de flujos. El DDE lleva a cabo actividades programadas de extracción de datos en esta información para identificar amenazas de red complejas como actividades de enumeración. Después, esta información se envía a Sophos Central y se utiliza para generar informes sobre la red.

Además, los datos recopilados por el DDE pueden correlacionarse con datos de los sensores de endpoints de Sophos XDR (detección y respuesta ampliadas) para identificar recursos no gestionados en la red. Esta correlación tiene lugar en Sophos Data Lake y ofrece una vista completa de la red, lo que permite a los administradores identificar posibles riesgos de seguridad y tomar las medidas necesarias. Es importante destacar que el DDE realiza actividades de extracción de datos según una programación establecida y no en tiempo real.

Agrupación y puntuación de gravedad (CSS)

La función de agrupación y puntuación de gravedad (CSS) es una parte esencial de las capacidades de detección de amenazas de Sophos NDR. Durante las sesiones de red entre clientes y servidores, el sistema observa una amplia gama de indicadores de amenazas. Estos indicadores, al analizarse solos, pueden no representar de forma precisa un problema o actividad maliciosa. Por esta razón, Sophos NDR se sirve de un proceso patentado para agrupar estos indicadores a lo largo del tiempo y ofrecer así un mayor nivel de confianza a la hora de identificar amenazas.

Mediante este proceso, se agrupan los flujos de red en función de información de red básica, como la IP/puerto de origen y destino y el protocolo. Al agrupar múltiples flujos ocurridos a lo largo del tiempo, el sistema puede generar una vista más completa de la actividad sospechosa, además de consolidar los flujos de red relacionados en un único evento de detección en el que la correlación entre flujos ayude a entender la actividad sospechosa.

Una vez creados estos grupos, se puntúan de acuerdo con la información recopilada por cada uno de los motores de detección. El algoritmo CSS evalúa todas las actividades de cada grupo para proporcionar contexto adicional, lo que mejora la precisión y reduce los falsos positivos.

El sistema de puntuación de CSS se basa en varios factores, incluidos los niveles de gravedad y los indicadores de amenazas identificados por los distintos motores de detección. Combinando toda esta información, Sophos NDR asigna una puntuación a cada grupo, la cual refleja el posible riesgo que acarrea la actividad de red. Este sistema de puntuación proporciona a los administradores de red información valiosa sobre las posibles amenazas para que puedan priorizar sus respuestas en función de la gravedad del riesgo.

APÉNDICES

APÉNDICE A: Riesgos de flujo de SRA

PROTOCOLO	RIESGO DE FLUJO	DESCRIPCIÓN
GENERAL	Posible exploit	Se ha detectado un posible exploit (p. ej., Log4J/Log4Shell).
GENERAL	Protocolo conocido en puerto no estándar	Se está utilizando un protocolo en un puerto no estándar (p. ej., HTTP en TCP/8000 cuando el estándar es TCP/80).
GENERAL	ASN peligroso	Se ha intercambiado una sesión de red con un servidor que pertenece a un ASN (número de sistema autónomo) de riesgo.
GENERAL	Tráfico unidireccional	La sesión es unidireccional. Esto podría indicar actividad de C2 a un servidor que ya no opera en la dirección.
GENERAL	Sesión de uso compartido de archivos o de escritorio	El flujo transporta datos de uso compartido de archivos o de escritorio (p. ej., TeamViewer o AnyDesk).
GENERAL	Protocolo no seguro	El protocolo utilizado no es seguro y no debería usarse (p. ej., Telnet en lugar de SSH).
GENERAL	Credenciales en texto sin cifrar	Se han transmitido credenciales en texto sin cifrar a través de un protocolo conocido (p. ej., FTP, HTTP, IMAP, POP3 o SMTP).
GENERAL	Paquete con formato incorrecto	El paquete de red tiene un formato inesperado. Esto podría indicar un error de protocolo o la toma de control de un protocolo válido para transmitir otro tipo de datos.
GENERAL	Problemas de TCP	Se han encontrado problemas en la configuración de TCP de la sesión de red.
GENERAL	Suscriptor anónimo	La dirección IP de origen se ha anonimizado y no se puede utilizar para identificar al suscriptor (p. ej., flujo generado por un nodo de salida del relay privado de iCloud).
GENERAL	Flujo periódico	La sesión de red se está repitiendo según un intervalo programado. Esto podría indicar actividad de C2 por parte de un troyano o una red de bots.
TLS, HTTP, DNS	Dominio DGA sospechoso	El nombre de dominio podría ser un DGA, que se utiliza para generar nombres de dominio usados frecuentemente por malware.
TLS, HTTP, DNS	Dominio peligroso	Se ha producido tráfico de red en un dominio que se considera de riesgo.
TLS, HTTP, DNS	Caracteres no válidos	El protocolo descodificado contiene caracteres no permitidos en ese protocolo (p. ej., un nombre de host DNS solo puede contener un subconjunto de todos los caracteres imprimibles).
TLS, HTTP, DNS	IDN Punycode	Se ha observado un nombre de dominio en el formato IDN. Los dominios IDN Punycode podrían indicar un ataque de phishing homógrafo.

PROTOCOLO	RIESGO DE FLUJO	DESCRIPCIÓN
HTTP, DNS	Código de error detectado	Se ha detectado un error en el protocolo.
DNS	Tráfico sospechoso	Se ha observado un tipo de registro DNS inesperado u obsoleto.
DNS	Paquete grande	El paquete DNS sobre UDP ha superado el límite de tamaño de 512 bytes. Esto podría indicar la exfiltración o tunelización de DNS.
DNS	Fragmentado	DNS sobre UDP fragmentado. Esto podría indicar la exfiltración o tunelización de DNS.
SSH	Cifrado o versión de cliente obsoletos	El cliente SSH ha utilizado una versión de protocolo obsoleta o cifrados no seguros.
SSH	Cifrado o versión de servidor obsoletos	El servidor SSH ha utilizado una versión de protocolo obsoleta o cifrados no seguros.
SMB	Versión no segura	Se ha observado una versión de SMB no segura (p. ej., SMBv1).
ICMP	Entropía sospechosa	Se ha observado una entropía sospechosa en los paquetes ICMP. Esto podría indicar una exfiltración de datos a través de ICMP.
TLS	Certificado autofirmado	Se ha utilizado un certificado autofirmado.
TLS	Certificado SHA1 malicioso	Se ha encontrado el certificado TLS observado en un certificado malicioso.
TLS	Certificado no coincidente	El certificado TLS no coincide con el nombre de host al que se está accediendo.
TLS	Falta SNI	Falta el SNI del servidor al que se está accediendo.
TLS	Uso de ESNI sospechosa	Se ha observado una SNI cifrada. Esto podría indicar un ataque de enmascaramiento de dominio.
TLS	No transporta HTTPS	El flujo TLS no se estaba usando para transportar HTTPS.
TLS	Huella digital JA3 maliciosa	Se ha encontrado una huella digital JA3 en una lista negra de JA3 maliciosas.
TLS	Extensión sospechosa	El nombre de dominio en la extensión SNI no era imprimible.
TLS	ALPN inusual	Se ha observado una extensión ALPN inusual en el flujo TLS (p. ej., HTTP/1.1).
TLS	Certificado caducado	El certificado TLS utilizado en el flujo ha caducado.
TLS	Certificado con caducidad inminente	El certificado TLS utilizado en el flujo está a punto de caducar.
TLS	Validez de certificado demasiado larga	El certificado TLS utilizado en el flujo tiene una duración superior a 13 meses.
TLS	Versión obsoleta	La versión TLS es anterior a 1.1.
TLS	Cifrado débil	Se ha utilizado un cifrado TLS no seguro en la configuración del flujo.

PROTOCOLO	RIESGO DE FLUJO	DESCRIPCIÓN
TLS	Alerta grave	El protocolo TLS ha emitido una alerta grave en el flujo.
HTTP	Host IP numérico	Se ha accedido al servidor web utilizando su dirección IP en lugar del nombre de host.
HTTP	URL sospechosa	La URL de acceso es sospechosa. (Ejemplo: http://127.0.0.1/msadc/..%255c../..%255c../winnt/system32/cmd.exe.).
HTTP	Encabezado sospechoso	El encabezado HTTP contiene entradas sospechosas que no se esperan en un encabezado HTTP. (Ejemplo: UUID, versión de TLS, nombre de SO).
HTTP	Agente de usuario sospechoso	La cadena del agente de usuario contenía caracteres o un formato sospechosos. (Ejemplo: <?php something ?>).
HTTP	Contenido sospechoso	El flujo HTTP transportaba contenido en un formato inesperado. (Ejemplo: el encabezado HTTP indica que el contexto es texto/html, pero el contenido no se puede leer porque son datos binarios).
HTTP	Transferencia de aplicación binaria	Se está descargando o cargando una aplicación binaria. Los archivos detectados incluyen binarios de Windows, ejecutables de Linux, scripts de Unix y apps de Android.
HTTP	Posible XSS en la URL	Se ha observado un posible ataque de XSS (scripts entre sitios).
HTTP	Posible inyección de SQL en la URL	Se ha observado un posible ataque de inyección de SQL.
HTTP	Posible inyección de RCE en la URL	Se ha observado un posible ataque de RCE (ejecución remota de código).
HTTP	Bot rastreador	Se ha detectado un rastreador/bot/robot.
HTTP	Servidor obsoleto	Se ha detectado una sesión de red con un servidor Apache o Nginx obsoleto.

APÉNDICE B: Protocolos NPP

1KXUN	GIT	MICROSOFT_365	SPOTIFY
ACCUWEATHER	GITHUB	MICROSOFT_AZURE	SSDP
ACTIVISION	GITLAB	MINING	SSH
ADS_ANALYTICS_TRACK	GMAIL	MODBUS	STARCRAFT
ADULT_CONTENT	GNUTELLA	MONGODB	STEAM
AFP	GOOGLE	MPEGDASH	STUN
AJP	GOOGLE_CLASSROOM	MPEGTS	SYNCTHING
ALIBABA	GOOGLE_CLOUD	MQTT	SYSLOG
ALICLOUD	GOOGLE_DOCS	MS_ONE_DRIVE	TAILSCALE
AMAZON	GOOGLE_DRIVE	MS_OUTLOOK	TARGUS_GETDATA
AMAZON_ALEXA	GOOGLE_MAPS	MSSQL_TDS	TEAMSPEAK
AMAZON_AWS	GOOGLE_PLUS	MSTEAMS	TEAMVIEWER
AMAZON_VIDEO	GOOGLE_SERVICES	MUNIN	TELEGRAM
AMONG_US	GOTO	MYSQL	TELNET
AMQP	GTP	NATPMP	TENCENT
ANYDESK	GTP_C	NATS	TENCENTVIDEO
APPLE	GTP_PRIME	NEST_LOG_SINK	TEREDO
APPLE_ICLOUD	GTP_U	NETBIOS	TFTP
APPLE_ITUNES	GUILDWARS	NETFLIX	THREEMA
APPLE_PUSH	H323	NETFLOW	TIDAL
APPLE_SIRI	HALFLIFE2	NFS	TIKTOK
APPLESTORE	HANGOUT_DUO	NINTENDO	TINC
APPLETVPLUS	HBO	NOE	TIVOCONNECT
ARMAGETRON	HOTSPOT_SHIELD	NTOP	TLS
AVAST	HPVIRTGRP	NTP	TOCA_BOCA
AVAST_SECUREDNS	HSRP	OCS	TOR
BADOO	HTTP	OCSP	TPLINK_SHP

BGP	HTTP_CONNECT	OOKLA	TRUPHONE
BITTORRENT	HTTP_PROXY	OPENDNS	TUENTI
BJNP	HULU	OPENVPN	TUMBLR
BLOOMBERG	I3D	ORACLE	TUNEIN
CACHEFLY	IAX	PANDORA	TUNNELBEAR
CAPWAP	ICECAST	PASTEBIN	TUYA_LP
CASSANDRA	ICLOUD_PRIVATE_RELAY	PINTEREST	TVUPLAYER
CHECKMK	IEC60870	PLAYSTATION	TWITCH
CISCOVPN	IFLIX	PLAYSTORE	TWITTER
CITRIX	IHEARTRADIO	PLURALSIGHT	UBNTAC2
CLOUDFLARE	IMO	POSTGRES	UBUNTUONE
CLOUDFLARE_WARP	INSTAGRAM	PPSTREAM	ULTRASURF
CNN	IP_EGP	PPTP	USENET
COAP	IP_GRE	PSIPHON	VEVO
COLLECTD	IP_ICMP	QQ	VHUA
CORBA	IP_ICMPV6	QUIC	VIBER
CPHA	IP_IGMP	RADIUS	VIMEO
CRASHLYSTICS	IP_IP_IN_IP	RAKNET	VK
CROSSFIRE	IP_OSPF	RDP	VMWARE
CRYNET	IP_PGM	REDDIT	VNC
CSGO	IP_PIM	REDIS	VUDU
CYBERSECURITY	IP_SCTP	RIOTGAMES	VXLAN
DAILYMOTION	IP_VRRP	RPC	WARCRAFT3
DATASAVER	IPP	RSH	WAZE
DAZN	IPSEC	RSYNC	WEBEX
DEEZER	IRC	RTCP	WEBSOCKET
DHCP	JABBER	RTMP	WECHAT
DHCPV6	KAKAOTALK	RTP	WHATSAPP

DIAMETER	KAKAOTALK_VOICE	RTSP	WHATSAPP_CALL
DIRECTV	KERBEROS	RX	WHATSAPP_FILES
DISCORD	KISMET	S7COMM	WHOIS_DAS
DISNEYPLUS	KONTIKI	SALESFORCE	WIKIPEDIA
DNP3	LASTFM	SAP	WINDOWS_UPDATE
DNS	LDAP	SD_RTN	WIREGUARD
DNSCRYPT	LIKEE	SFLOW	WORLD_OF_KUNG_FU
DOFUS	LINE	SHOWTIME	WORLDOFWARCRAFT
DOH_DOT	LINE_CALL	SIGNAL	WSD
DRDA	LINKEDIN	SIGNAL_VOIP	XBOX
DROPBOX	LISP	SINA	XDMCP
DTLS	LIVESTREAM	SIP	XIAOMI
EAQ	LLMNR	SIRIUSXMRADIO	YAHOO
EBAY	LOTUS_NOTES	SKINNY	YANDEX
EDGECAST	MAIL_IMAP	SKYPE_TEAMS	YANDEX_CLOUD
EDONKEY	MAIL_IMAPS	SKYPE_TEAMS_CALL	YANDEX_DIRECT
ELASTICSEARCH	MAIL_POP	SLACK	YANDEX_DISK
ETHERNET_IP	MAIL_POPS	SMBV1	YANDEX_MAIL
FACEBOOK	MAIL_SMTP	SMBV23	YANDEX_MARKET
FACEBOOK_VOIP	MAIL_SMTPS	SMPP	YANDEX_METRIKA
FASTCGI	MAPLESTORY	SNAPCHAT	YANDEX_MUSIC
FIX	MDNS	SNAPCHAT_CALL	YOUTUBE
FORTICLIENT	MEGACO	SNMP	YOUTUBE_UPLOAD
FTP_CONTROL	MEMCACHED	SOAP	Z3950
FTP_DATA	MERAKI_CLOUD	SOCKS	ZABBIX
FTPS	MESSENGER	SOFTETHER	ZATTOO
FUZE	MGCP	SOMEIP	ZMQ
GENSHIN_IMPACT	MICROSOFT	SOUNDCLOUD	ZOOM

Para obtener más información sobre Sophos NDR, visite es.sophos.com/ndr

2023-03-29 (WP-NP)

SOPHOS