Endpoint Security LATAM

¿Qué es la Detección y Respuesta de Red o Network Detection and Response (NDR)?

TABLA DE CONTENIDO

¿Cómo funciona la detección y respuesta de red?

Aprendizaje automático

Heurística

Análisis estadístico

Firmas

Fuentes de inteligencia de amenazas

Beneficios de NDR

Deficiencias de NDR

Mejore la detección y respuesta de la red con Heimdal®

 © 2026 antivirusthor.com



A principios de la década de 2010, se desarrolló la tecnología de detección y respuesta de red (NDR) para detectar y contrarrestar las amenazas de red evasivas que eran difíciles de detener utilizando firmas o patrones de ataque conocidos.

NDR, también conocido como análisis de tráfico de red (NTA), supervisa el tráfico de red y crea una línea base de actividad mediante el aprendizaje automático y el análisis de comportamiento. Posteriormente, pueden identificar actividades sospechosas vinculadas a malware, abuso interno y comportamiento peligroso o ataques dirigidos.

Con las soluciones de NDR, las empresas pueden identificar el tráfico irregular que podría estar relacionado con malware, movimiento lateral, comando y control o exfiltración.

¿Cómo funciona la detección y respuesta de red?

Las soluciones de detección y respuesta de red (NDR) monitorean continuamente la red de una empresa, recopilando todo el tráfico de red, empleando análisis de comportamiento, aprendizaje automático e inteligencia artificial para identificar amenazas cibernéticas y comportamiento inusual, y tomando las medidas apropiadas contra estas amenazas, ya sea directamente o integrándose con otras herramientas de ciberseguridad.

Las soluciones de NDR van más allá de la mera detección de amenazas; también permiten la respuesta a amenazas en tiempo real mediante controles nativos o una variedad de integraciones con otras herramientas y soluciones de ciberseguridad, como orquestación, automatización y respuesta de seguridad (SOAR).

Las herramientas y técnicas más comunes que utilizan las herramientas NDR son el aprendizaje automático, la heurística, el análisis estadístico, las firmas y las fuentes de inteligencia de amenazas. Aquí hay más detalles sobre ellos:

Aprendizaje automático

Para analizar grandes conjuntos de datos y generar predicciones más precisas, el aprendizaje automático utiliza la potencia informática. Cuando se trata de soluciones NDR, los modelos de aprendizaje automático pueden usar análisis de comportamiento para encontrar amenazas de red desconocidas. Los algoritmos que utilizan el aprendizaje automático pueden identificar amenazas cibernéticas inminentes y permitir una clasificación y reparación más rápidas. Además, las amenazas potenciales se reevalúan continuamente mediante modelos de aprendizaje automático basados en resultados reales.

Heurística

Al examinar los datos en busca de características sospechosas, el análisis heurístico contribuye a la detección de amenazas. En las soluciones NDR, las heurísticas se utilizan para mejorar la eficacia de las técnicas de detección basadas en firmas al mirar más allá de las amenazas actuales y detectar atributos sospechosos en las nuevas, así como en versiones alteradas de amenazas conocidas.

Análisis estadístico

El análisis estadístico es una técnica de comportamiento útil, que puede incluir cualquier cosa, desde un análisis sencillo de valores atípicos (como la identificación de URL que no han sido visitadas por un grupo de dispositivos) hasta análisis bayesianos básicos de patrones de tráfico de red. Por lo general, el análisis estadístico incluye un componente de muestreo para establecer una línea de base que luego se usa para detectar qué actividad se aparta de los usos regulares del tráfico, lo que permite a los SOC caracterizar el tráfico de red típico y mostrar un comportamiento inusualmente sospechoso.

Firmas

Para reconocer una amenaza conocida en el futuro, las técnicas de detección basadas en firmas utilizan un identificador de indicador de compromiso (IOC) específico. Este método ha perdido gran parte de su eficacia en un mundo donde los ataques como la repetición de credenciales, el malware personalizado y los kits de herramientas de malware son la norma.

Fuentes de inteligencia de amenazas

Los flujos de datos llamados feeds de inteligencia de amenazas brindan información sobre amenazas en línea previamente identificadas. La inteligencia de amenazas puede ayudar a las soluciones de NDR a identificar amenazas conocidas y ofrecer información contextual adicional para clasificar una anomalía de red detectada por riesgo si es oportuno y factible. La necesidad de obtener, administrar y seleccionar de forma activa los datos de amenazas para garantizar que la información esté actualizada y sea relevante es una limitación de las fuentes de inteligencia de amenazas.

Beneficios de NDR

una solución de detección y respuesta de red:

- Puede ampliar la visibilidad de los ataques para evitar falsos negativos; literalmente pueden ver todas las actividades de red que experimenta un atacante, incluidas las últimas etapas de un ataque, además de las operaciones de movimiento lateral y exfiltración.
- No tiene huella de red cuando utiliza análisis proporcionados por la nube. Las herramientas modernas de detección y respuesta de red se proporcionan a través de la nube, lo que agiliza las operaciones al eliminar la necesidad de que los equipos de TI configuren nuevos servidores de registro en el sitio para recopilar y analizar datos de red.

Las plataformas NDR avanzadas también pueden recopilar registros de red de herramientas de seguridad de red que ya están en uso, como firewalls de red, lo que elimina la necesidad de sensores de red dedicados. Con una interacción mínima, los sistemas NDR brindan visibilidad completa y detección de amenazas.

Deficiencias de NDR

Aunque las soluciones NDR impulsadas por IA son automáticas y aumentan significativamente las detecciones de seguridad y la efectividad del centro de operaciones de seguridad (SOC), las herramientas NDR también tienen inconvenientes:

- Solo pueden monitorear y rastrear registros de red; no pueden rastrear ni monitorear eventos de puntos finales como información de procesos, modificaciones del registro o comandos del sistema.
- No pueden ver la identidad o los datos de la nube u otras fuentes importantes de información de seguridad.
- Las soluciones NDR pueden ser costosas de implementar y mantener, pueden dar lugar a posibles puntos ciegos y pueden necesitar cambiar entre consolas para que los analistas de seguridad recopilen el contexto.

Mejore la detección y respuesta de la red con Heimdal®

Al proporcionar una búsqueda de amenazas única y una visibilidad completa en toda su red, la solución Red de Prevención de Amenazas de Heimdal® puede ayudarlo a mejorar la seguridad del DNS del perímetro de la red de su empresa.

Independientemente del dispositivo o sistema operativo, obtendrá protección de la A a la Z: al aprovechar el aprendizaje automático en el dispositivo a la infraestructura, Heimdal® Threat Prevention Network detecta y detiene los ataques que los firewalls no pueden ver, bloqueando el contenido web malicioso, evitando la fuga de datos y filtrando el tráfico localmente en cualquier entorno.

Heimdal también puede ayudarlo a abordar el desafío de múltiples consolas: nuestro software de red de prevención de amenazas también se puede usar en combinación con otras soluciones líderes en el mercado (punto final de prevención de amenazas, administración de parches, administración de acceso privilegiado, control de aplicaciones, Protección de cifrado de ransomware y Next- Gen Antivirus) de nuestra cartera, agrupados en nuestros servicios EDR / XDR, brindándole seguridad de punto final unificado de primera clase.

Puede encontrar el artículo original en este link.