Módulo 3. Plataformas de Monitoreo y Seguridad de Red (NDR)

CÓRDOBA CREA FUTURO

Introducción

En un contexto donde las organizaciones enfrentan amenazas cada vez más sofisticadas y persistentes, surge una pregunta inevitable: ¿alcanza con detectar una alerta para decir que comprendemos lo que ocurre en nuestra red? La seguridad actual exige algo más que señales aisladas; requiere **visibilidad profunda, correlación inteligente y capacidad de reconstrucción forense.** En este marco, el monitoreo tradicional evoluciona hacia plataformas integradas de **Detección y Respuesta en Redes (NDR)**, capaces de combinar análisis, evidencia y gobernanza operativa.

En este material se abordará el funcionamiento de las **plataformas de monitoreo y seguridad de red,** con especial foco en la arquitectura basada en **Zeek, Suricata y Arkime**, entendiendo cómo se integran detección, contexto y captura completa de tráfico. Se analizará el rol de los **dashboards y workflows** como herramientas cognitivas que organizan la información y estructuran la investigación. También se estudiarán los **roles y permisos**, fundamentales para garantizar control y

responsabilidad en el acceso a datos sensibles. Finalmente, se des**arrollarán los principios de** salud, actualización, trazabilidad y privacidad, elementos indispensables para que la observabilidad técnica se convierta en una práctica profesional, sostenible y éticamente responsable

Situación profesional

Operador SOC realizando Threat Hunting con consola centralizada NDR

En una entidad financiera que utiliza una arquitectura NDR basada en Security Onion (integrando Suricata, Zeek y Arkime), un operador SOC de nivel 2 realiza tareas de **Threat Hunting proactivo** desde los dashboards centralizados. La infraestructura permite visualizar alertas, consultar logs estructurados y acceder a sesiones completas en PCAP cuando es necesario.

Durante una revisión rutinaria de comportamiento de red, el analista detecta un patrón inusual: un servidor interno crítico establece conexiones HTTPS salientes cada quince minutos hacia un dominio externo que no figura en el histórico habitual de la organización. No existen alertas críticas disparadas por Suricata, lo que obliga al operador a trabajar desde una lógica de análisis comportamental y no basada únicamente en firmas.

El analista inicia el workflow de investigación delimitando un rango temporal específico y correlacionando información en los logs de Zeek. Observa que el dominio fue registrado recientemente y que el tráfico mantiene una periodicidad constante con bajo volumen de datos, características compatibles con un posible canal de comando y control (C2). A partir de esa hipótesis, utiliza Arkime para realizar búsquedas estructuradas sobre los metadatos indexados, filtrando por IP origen y destino hasta identificar las sesiones exactas involucradas.

En este punto surge una decisión crítica: para confirmar la hipótesis es necesario descargar el PCAP completo, pero el servidor involucrado maneja información financiera sensible. El operador debe aplicar el principio de mínimo privilegio y justificar formalmente la extracción, ya que el acceso al contenido completo del tráfico implica consideraciones de privacidad y gobernanza. Tras documentar la investigación y acotar la exportación únicamente a las sesiones pertinentes, procede al análisis forense.

El examen del tráfico confirma la presencia de un patrón compatible con beaconing cifrado. Se determina que el servidor fue comprometido y se activa el procedimiento de contención.

El caso revela varias tensiones estructurales: la detección no surgió de una alerta automática sino del análisis en dashboards; la retención limitada de PCAP podría haber impedido reconstruir el incidente si hubiera comenzado antes; y la ausencia de paneles específicos para detección de periodicidad obligó a un análisis manual. Además, la necesidad de equilibrar visibilidad total con protección de datos evidencia que la arquitectura NDR no es solo un conjunto de herramientas técnicas, sino un sistema que requiere workflows claros, control de roles, trazabilidad y políticas de actualización constantes.

Esta situación permite problematizar cómo el Threat Hunting exige integrar arquitectura técnica, análisis metodológico y gobernanza responsable para transformar la visibilidad de red en capacidad real de defensa.

CONTINUAR

Unidad 1. Monitoreo de seguridad de red y detección de amenazas con Security Onion

Arquitectura: Zeek + Suricata + Arkime

Una arquitectura NDR basada en **Zeek + Suricata + Arkime** se construye sobre la idea de integrar **detección, contexto y evidencia** dentro de un mismo ecosistema técnico. Cada herramienta cumple un rol específico y complementario, y su valor no está en el funcionamiento aislado, sino en la **correlación operativa** entre ellas.

Suricata actúa como el componente de **detección en tiempo real**. Inspecciona el tráfico mediante reglas y genera **alertas** cuando identifica patrones asociados a amenazas conocidas o comportamientos sospechosos. Es la primera capa de señalización: indica que algo merece atención.

Zeek aporta el plano de **análisis estructurado del comportamiento**. En lugar de centrarse exclusivamente en alertas, transforma el tráfico en **logs detallados por protocolo**, permitiendo entender qué ocurrió, cómo y entre

qué actores. Su fortaleza está en la **contextualización técnica** de la actividad de red.

Arkime, según su documentación oficial, es una plataforma diseñada para la **captura, indexación y búsqueda de tráfico en formato PCAP a gran escala.** Almacena los paquetes completos en disco y envía metadatos a un motor de búsqueda como OpenSearch o Elasticsearch, lo que permite realizar consultas rápidas sobre grandes volúmenes de sesiones. Esto significa que, ante una alerta o evento sospechoso, el analista puede:

- Buscar la sesión correspondiente mediante metadatos indexados.
- Visualizar detalles desde la interfaz web.
- Descargar el PCAP completo para análisis forense.

La arquitectura se organiza entonces en tres niveles integrados: captura de paquetes completos, generación de metadatos indexables y producción de alertas y logs

estructurados. La investigación fluye desde la señal inicial hacia la reconstrucción detallada del tráfico.

Un aspecto clave de Arkime es su diseño distribuido. Cada sensor ejecuta el componente de captura, escribe PCAP en almacenamiento local y envía metadatos al clúster de búsqueda. El componente **viewer** proporciona la interfaz web y gestiona la recuperación de paquetes cuando el analista lo solicita. Esta separación permite **escalar horizontalmente,** distribuir carga y mantener el rendimiento incluso en redes de alto volumen.

Desde una perspectiva estratégica, esta arquitectura permite pasar de una seguridad reactiva a una seguridad basada en evidencia. La alerta no es el final del proceso, sino el punto de partida para un análisis profundo sustentado en datos reales de red.

Dashboards y workflows

En un entorno de **Detección y Respuesta en Redes**, los datos por sí solos no generan valor si no están organizados dentro de una lógica operativa clara. Los **dashboards**

constituyen la capa de visualización que transforma grandes volúmenes de logs y metadatos en información accionable. No se trata simplemente de gráficos, sino de instrumentos estratégicos que permiten al equipo de seguridad comprender el estado de la red en tiempo real y en perspectiva histórica.

Un dashboard eficaz integra información proveniente de **Suricata, Zeek y Arkime**, articulando tres dimensiones distintas: alertas, comportamiento estructurado y sesiones completas. Esto permite que el analista no vea únicamente un evento aislado, sino un **mapa contextual** donde se relacionan IPs, protocolos, dominios, tiempos y severidades.

En términos prácticos, un panel puede mostrar:

- Evolución temporal de **alertas por severidad.**
- Principales direcciones IP o activos más activos.
- Distribución de tráfico por protocolo.
- Indicadores de actividad inusual o picos anómalos.

La clave está en que el dashboard no sea estático. Debe permitir filtrar, pivotear y profundizar sobre los datos. Por ejemplo, una alerta crítica detectada por Suricata puede funcionar como punto de entrada. Desde allí, el analista puede filtrar por IP origen o destino, revisar los logs correspondientes de Zeek para entender el comportamiento asociado y, si es necesario, acceder a Arkime para inspeccionar la sesión completa.

Aquí aparece el concepto de **workflow de investigación.** Un workflow es una secuencia lógica y repetible de pasos que guía al analista desde la detección hasta la resolución o escalamiento del incidente. En un entorno NDR integrado, un flujo típico puede incluir:

- Identificación de la alerta en el dashboard.
- Validación de severidad y contexto mediante logs estructurados.

- Correlación con otras actividades del mismo host o usuario.

- Recuperación de evidencia en PCAP si se requiere confirmación técnica.

El objetivo es reducir el **tiempo medio de detección (MTTD)** y el **tiempo medio de respuesta (MTTR)** mediante procesos claros y herramientas que faciliten la correlación. Sin dashboards adecuados, el analista queda expuesto a revisar datos de manera fragmentada; con dashboards bien diseñados, la información se organiza alrededor de preguntas operativas concretas.

Además, los dashboards no solo sirven para la respuesta reactiva. Son fundamentales para el **threat hunting proactivo.** Permiten identificar patrones que, aunque no hayan disparado una regla específica, pueden revelar comportamientos anómalos. Por ejemplo, conexiones periódicas a dominios poco frecuentes o incrementos inusuales en tráfico cifrado hacia destinos externos.

Desde el punto de vista organizacional, los workflows también aportan **estandarización**. Cuando los pasos de análisis están definidos y soportados por paneles claros, se

reduce la variabilidad entre analistas y se mejora la consistencia de las investigaciones. Esto es especialmente relevante en equipos SOC donde trabajan distintos turnos y perfiles.

En definitiva, dashboards y workflows no son componentes accesorios. Son la interfaz cognitiva del sistema NDR. Traducen datos técnicos complejos en decisiones operativas, conectan señal con evidencia y convierten una arquitectura técnica en una práctica de seguridad efectiva y sostenida en el tiempo.

Roles y permisos

En una arquitectura NDR que integra **Zeek, Suricata y Arkime**, la gestión de **roles y permisos** no es un aspecto administrativo menor, sino un componente estructural de la seguridad del sistema. Estamos hablando de plataformas que almacenan **tráfico completo de red**, metadatos de sesiones, registros de comportamiento y alertas potencialmente sensibles. Sin un modelo de control de

acceso claro, el riesgo no solo es técnico, sino también legal y organizacional.

El principio rector debe ser el de **mínimo privilegio:** cada usuario accede únicamente a las funciones y datos necesarios para desempeñar su rol. Esto implica diseñar un esquema de **control de acceso basado en roles (RBAC)** que se articule tanto en la interfaz de Arkime como en el motor de indexación subyacente (OpenSearch o Elasticsearch).

En un entorno operativo típico pueden distinguirse distintos perfiles:

Administrador del sistema, —

con capacidad para configurar sensores, gestionar índices, administrar almacenamiento y definir políticas de retención.

Analista SOC, —

con permisos de consulta, filtrado y visualización de sesiones, pero sin acceso a configuraciones críticas.

Investigador forense, —

con posibilidad de exportar PCAP completos y generar evidencia técnica para reportes.

Auditor o perfil de solo lectura, —

limitado a dashboards y métricas agregadas.

La diferencia entre visualizar metadatos y descargar tráfico completo es sustancial. Permitir la exportación de PCAP implica acceso a contenido potencialmente confidencial, por lo que debe estar restringido y auditado. Arkime, por ejemplo, permite controlar el acceso a través de autenticación segura y gestionar permisos sobre qué usuarios pueden acceder a determinadas funcionalidades, integrándose además con mecanismos de autenticación externos o del propio motor de búsqueda.

Un aspecto clave es la **segmentación por datos**. En organizaciones grandes, puede ser necesario que ciertos analistas solo accedan a tráfico de determinadas redes, zonas o clientes. El modelo de permisos debe contemplar filtros y restricciones que eviten la exposición transversal innecesaria de información.

Además del acceso a datos, también deben regularse los permisos sobre acciones operativas. No es lo mismo consultar un dashboard que:

- Modificar reglas de detección en Suricata.
- Cambiar scripts o configuraciones en Zeek.
- Alterar políticas de retención en Arkime.
- Borrar índices históricos.

Estas acciones tienen impacto directo en la capacidad de detección y en la integridad de la evidencia. Por eso, una arquitectura madura incluye **trazabilidad de acciones,** registros de auditoría y separación clara entre funciones operativas y funciones analíticas.

Desde una perspectiva pedagógica y profesional, comprender los roles y permisos en NDR implica reconocer que la seguridad no solo se aplica hacia afuera, frente a amenazas externas, sino también hacia adentro, en la gestión responsable del acceso a la información. Un sistema técnicamente robusto puede volverse vulnerable si no existe una gobernanza adecuada sobre quién puede ver, modificar o exportar los datos.

En definitiva, los roles y permisos constituyen el marco de control que sostiene la arquitectura. Sin ellos, la visibilidad se convierte en exposición; con ellos, la visibilidad se transforma en capacidad estratégica de análisis bajo criterios de seguridad, responsabilidad y cumplimiento normativo.

Salud y actualización

En un entorno de **Detección y Respuesta en Redes**, la arquitectura puede estar correctamente diseñada y aun así fallar si no se sostiene una política rigurosa de **salud operativa** y **actualización continua**. La eficacia de Zeek,

Suricata y Arkime no depende únicamente de su configuración inicial, sino de su capacidad para mantenerse estables, sincronizados y vigentes frente a un entorno de amenazas dinámico.

La **salud del sistema** se refiere a la condición técnica y funcional de cada componente. En términos prácticos, implica verificar que los sensores estén capturando tráfico sin pérdida significativa de paquetes, que los procesos de análisis estén funcionando correctamente y que la indexación de metadatos no presente retrasos. Si un sensor deja de capturar tráfico o si la ingestión hacia OpenSearch se detiene, el sistema puede seguir "aparentemente activo" mientras en realidad está ciego.

En el caso de **Arkime,** es fundamental monitorear tanto el almacenamiento local donde se guardan los PCAP como el estado del motor de búsqueda que indexa los metadatos. La retención de paquetes depende directamente del espacio disponible en los discos de los sensores, mientras que la retención de metadatos depende del dimensionamiento del clúster de OpenSearch/Elasticsearch. Una saturación en cualquiera de estos niveles impacta directamente en la capacidad de investigación histórica.

Desde el punto de vista de Zeek y Suricata, la salud implica comprobar que:

- Los procesos estén activos y sin errores.
- No existan colas acumuladas de procesamiento.
- Las alertas y logs se estén generando con normalidad.
- Los relojes de los sistemas estén correctamente sincronizados.

La sincronización temporal es particularmente crítica, porque la correlación entre alertas, logs y sesiones depende de marcas de tiempo coherentes.

La **actualización** es el segundo pilar. En seguridad, la obsolescencia es una forma de vulnerabilidad. Suricata depende de reglas que deben mantenerse al día frente a nuevas amenazas. Zeek evoluciona con scripts y mejoras que

permiten interpretar protocolos actualizados o detectar comportamientos emergentes. Arkime publica versiones que incorporan mejoras de rendimiento, compatibilidad y seguridad.

No actualizar puede generar múltiples problemas: pérdida de capacidad de detección, incompatibilidades con versiones nuevas del motor de búsqueda o exposición a vulnerabilidades conocidas. Sin embargo, actualizar sin planificación también puede afectar la estabilidad. Por eso es necesario definir una política que incluya:

- Pruebas en entornos de staging antes de pasar a producción.
- Ventanas de mantenimiento programadas.
- Documentación de versiones y cambios implementados.
- Planes de reversión ante fallos.

La salud y la actualización no deben considerarse tareas aisladas del área técnica, sino parte del **ciclo de vida del sistema NDR**. Una arquitectura madura incorpora métricas

de rendimiento, alertas internas sobre el estado de los componentes y revisiones periódicas de configuración.

Finalmente, mantener la salud del sistema no es solo una cuestión técnica, sino estratégica. Un NDR que no se monitorea a sí mismo puede generar una falsa sensación de seguridad. En cambio, cuando se implementan controles continuos de funcionamiento y políticas de actualización disciplinadas, la organización asegura que la capacidad de detección y respuesta se mantenga efectiva en el tiempo, acompañando la evolución de la infraestructura y del panorama de amenazas.

CONTINUAR

Lección 3 de 5

Unidad 2. Captura y el análisis de paquetes de red con Arkime

Captura/índice de pcap

En una arquitectura NDR, la **captura completa de tráfico** es el nivel más profundo de visibilidad. Arkime está diseñado para realizar **full packet capture**, almacenando el tráfico en **formato PCAP estándar** mientras construye un sistema de **indexación eficiente** que permite buscar ese tráfico posteriormente sin necesidad de abrir archivos manualmente.

El componente **capture** monitorea el tráfico en tiempo real, escribe los archivos PCAP en disco local y, al mismo tiempo, extrae **metadatos de sesión** que envía al motor de búsqueda basado en **OpenSearch/Elasticsearch**. Esta separación entre **evidencia cruda** (PCAP) y **metadatos indexados** es el principio estructural del sistema.

Desde el punto de vista operativo, esto significa que el analista puede trabajar en dos niveles distintos:

Nivel de consulta rápida, —

utilizando búsquedas sobre metadatos indexados.

Nivel de evidencia forense, —

recuperando el PCAP completo cuando necesita validar una hipótesis.

La captura conserva el tráfico en almacenamiento local de cada sensor, lo que permite definir políticas de retención diferenciadas según la capacidad de disco. En cambio, la retención de metadatos depende del dimensionamiento del clúster de búsqueda. Esta distinción es estratégica: puede existir un histórico de consultas más amplio que el período disponible de PCAP completo.

La indexación transforma grandes volúmenes de tráfico en información consultable. El sistema permite filtrar por dirección IP, protocolo, rango temporal u otros campos extraídos durante el parsing. Así, la investigación deja de ser un proceso manual sobre archivos y pasa a ser una **búsqueda estructurada sobre sesiones**.

Además, la arquitectura es **distribuida y escalable.** Cada sensor ejecuta la captura y envía metadatos al clúster de búsqueda, mientras el componente viewer gestiona la interfaz web y la entrega de paquetes cuando se solicitan. Si el volumen de tráfico crece, pueden agregarse nuevos sensores, manteniendo la coherencia del índice central.

En términos estratégicos, la captura e índice de PCAP permiten que la detección no dependa exclusivamente de alertas o logs derivados. La posibilidad de volver al tráfico real y reconstruir exactamente lo ocurrido es lo que convierte a NDR en una disciplina basada en evidencia y no solo en señales.

Búsqueda y extracción controlada

En un entorno NDR, la **búsqueda** no es simplemente una funcionalidad técnica, sino el mecanismo que transforma la captura masiva de tráfico en **capacidad investigativa real.** Arkime utiliza un motor de búsqueda basado en **OpenSearch/Elasticsearch**, donde se almacenan los **metadatos de sesión** generados durante el proceso de captura. Esto permite realizar consultas estructuradas sobre grandes volúmenes de tráfico sin necesidad de acceder directamente a los archivos PCAP.

La búsqueda se apoya en campos indexados como direcciones IP, puertos, protocolos, tiempos de inicio y fin de sesión, entre otros atributos extraídos durante el parsing. Esta indexación habilita consultas rápidas y precisas, fundamentales para reducir el tiempo de análisis en contextos de incidente.

Desde la práctica operativa, el analista suele comenzar con una hipótesis o con un indicador concreto, por ejemplo una dirección IP sospechosa o un rango temporal asociado a una alerta. A partir de allí, la búsqueda permite:

- Delimitar el **intervalo temporal exacto** del evento.
- Identificar todas las **sesiones relacionadas** con un host específico.
- Correlacionar comunicaciones entre múltiples actores.
- Detectar patrones repetitivos o conexiones inusuales.

La potencia de esta capa radica en que convierte terabytes de tráfico en un espacio consultable y navegable.

Extracción controlada de evidencia

La búsqueda es solo la primera etapa. Cuando el análisis requiere validación profunda, entra en juego la **extracción controlada**. Arkime permite recuperar los **PCAP completos** asociados a sesiones específicas a través del componente viewer o mediante sus **APIs,** que también pueden exportar datos en formato JSON.

Aquí aparece un principio fundamental: no toda investigación necesita el tráfico completo. Muchas veces el análisis de metadatos es suficiente para tomar una decisión operativa. La extracción de PCAP debe reservarse para los casos donde es necesario confirmar contenido, reconstruir cargas útiles o generar evidencia técnica formal.

La “extracción controlada” implica tres dimensiones:

1. **Primero, acotamiento técnico.** Se deben exportar únicamente las sesiones pertinentes, evitando descargas masivas innecesarias.
2. **Segundo, gobernanza de acceso.** Solo ciertos roles deberían poder descargar PCAP completos, dado que pueden contener información sensible.
3. **Tercero, trazabilidad.** Cada extracción debería poder asociarse a un caso o investigación específica, manteniendo coherencia entre la búsqueda realizada y la evidencia obtenida.

Equilibrio entre agilidad y protección

Uno de los desafíos en NDR es equilibrar la rapidez de respuesta con la protección de datos. La arquitectura de Arkime favorece este equilibrio al mantener los PCAP en los sensores y entregar los datos bajo demanda. La indexación central permite buscar ampliamente sin mover evidencia innecesaria, y la recuperación se realiza solo cuando el analista lo solicita.

Este diseño reduce exposición y optimiza recursos. Además, cuando la extracción se realiza mediante APIs, puede integrarse en workflows automatizados, siempre bajo controles

definidos.

En síntesis, la **búsqueda estructurada** convierte el tráfico en conocimiento operativo, y la **extracción controlada** convierte ese conocimiento en evidencia verificable. Juntas, ambas funciones permiten que la investigación en NDR sea eficiente, rigurosa y gobernada por criterios de proporcionalidad y seguridad.

Trazabilidad de casos

En un entorno de **Detección y Respuesta en Redes**, la trazabilidad no es un aspecto administrativo secundario, sino un requisito esencial para que la investigación tenga **validez técnica, coherencia metodológica y valor probatorio.** La arquitectura de Arkime, basada en la separación entre **PCAP almacenado y metadatos indexados**, ofrece una base sólida para sostener esa trazabilidad de manera estructurada.

Cuando hablamos de trazabilidad en NDR, nos referimos a la capacidad de reconstruir con precisión qué ocurrió en la red, cómo se investigó y qué decisiones se tomaron a partir de la evidencia. Esto implica que cada caso debe poder responder, al menos, tres preguntas fundamentales: qué señal originó la investigación, qué sesiones fueron analizadas y qué evidencia concreta respalda la conclusión.

La indexación en **OpenSearch/Elasticsearch** permite que cada sesión tenga atributos consultables, lo que facilita

documentar búsquedas reproducibles. Un caso bien trazado no se limita a afirmar que “se observó tráfico sospechoso”, sino que especifica:

- El **rango temporal exacto** analizado.
- Los **criterios de búsqueda** aplicados.
- Los **identificadores de sesión** relevantes.
- Los **artefactos exportados** (PCAP o JSON) asociados al análisis.

Esta lógica transforma la investigación en un proceso verificable. Si otro analista repite la consulta con los mismos filtros y en el mismo intervalo temporal, debería obtener resultados equivalentes. Esa reproducibilidad es uno de los pilares de la trazabilidad.

Continuidad entre señal, contexto y evidencia

La trazabilidad también implica mantener una continuidad clara entre la **señal inicial, el análisis contextual y la evidencia final.** En un entorno integrado, la investigación puede comenzar con una alerta o hipótesis, continuar con búsquedas sobre metadatos indexados y culminar con la recuperación de un PCAP específico.

Cada uno de estos pasos debe poder vincularse entre sí. Si se exporta un PCAP, debe quedar claro por qué se seleccionó esa sesión y no otra. Si se descarta una hipótesis, deben quedar documentados los criterios que llevaron a esa conclusión. La trazabilidad no solo protege la calidad técnica del análisis, sino que también protege al analista y a la organización ante auditorías o revisiones posteriores.

Dimensión organizacional y probatoria

En muchos contextos, especialmente cuando hay implicancias legales o regulatorias, la trazabilidad adquiere un valor adicional. El tráfico capturado puede constituir **evidencia digital,** y la forma en que se buscó, filtró y extrajo debe poder justificarse. Arkime facilita este proceso al permitir búsquedas estructuradas y recuperación puntual de sesiones, evitando manipulaciones innecesarias sobre grandes volúmenes de datos.

Una práctica madura de trazabilidad implica:

- Asociar cada búsqueda y extracción a un **caso formal** o ticket.
- Mantener coherencia entre filtros aplicados y conclusiones alcanzadas.
- Preservar la integridad de los artefactos exportados.
- Evitar descargas masivas que no estén justificadas por el análisis.

Trazabilidad como disciplina metodológica

Más allá de la herramienta, la trazabilidad es una disciplina. Significa investigar con método, documentar decisiones y sostener la lógica de cada paso. En NDR, donde el volumen de datos es enorme, esta disciplina evita conclusiones apresuradas y reduce el riesgo de interpretaciones sesgadas.

En definitiva, la **trazabilidad de casos** convierte la observabilidad técnica en un proceso formal de investigación. Sin trazabilidad, el análisis es una serie de consultas aisladas; con trazabilidad, se transforma en un relato técnico coherente, reproducible y defendible.

Consideraciones de privacidad

En un entorno de **Detección y Respuesta en Redes,** la privacidad no es un elemento accesorio ni una cuestión meramente legal: es una dimensión estructural del diseño. Cuando se implementa una solución de **full packet capture** como Arkime, se está almacenando tráfico completo en **formato PCAP**, lo que puede incluir contenido sensible, credenciales, datos personales, información comercial estratégica y comunicaciones privadas. Esta capacidad técnica, que fortalece la investigación forense, también amplifica la responsabilidad institucional.

Arkime está concebido para almacenar los PCAP en los sensores y exponerlos a través del componente **viewer** o mediante **APIs**, lo que ya introduce una separación entre almacenamiento físico y acceso analítico. Esa arquitectura es un primer paso hacia la protección, pero no es suficiente por sí sola. La privacidad debe abordarse desde varios niveles.

Minimización y proporcionalidad

Uno de los principios fundamentales es la **minimización de datos.** Capturar todo el tráfico es técnicamente posible, pero debe evaluarse si es proporcional a los objetivos de seguridad definidos por la organización. Las políticas de **retención de PCAP** y de **retención de metadatos indexados** deben responder a un análisis de riesgo y no a una acumulación indiscriminada de información.

La retención prolongada de tráfico completo incrementa la superficie de exposición. Por ello, es necesario definir horizontes temporales claros y alineados con necesidades reales de investigación, auditoría o cumplimiento normativo.

Control de acceso y segregación de funciones

La privacidad también depende de la correcta implementación de **roles y permisos.** No todos los analistas deberían tener acceso irrestricto a la descarga de PCAP completos. La extracción de tráfico completo debe limitarse a perfiles autorizados y asociarse siempre a un caso formal.

En este punto es clave la **segregación de funciones:** quien administra el almacenamiento no necesariamente debe ser quien realiza análisis forense, y quien consulta dashboards agregados no debería poder exportar contenido detallado. Esta separación reduce riesgos internos y mejora la gobernanza.

Además, el acceso al entorno debe protegerse mediante mecanismos robustos de autenticación, cifrado de comunicaciones (HTTPS) y, cuando sea posible, integración con sistemas de identidad centralizados. Estas medidas no son opcionales cuando se gestionan datos de red a nivel de paquete.

Auditoría y trazabilidad del acceso

La privacidad no solo se protege limitando accesos, sino también registrándolos. La **auditoría de acciones** es esencial en un sistema que maneja evidencia digital. Debe poder saberse quién accedió, qué buscó y qué descargó. Esta trazabilidad protege tanto a la organización como a los propios analistas.

Cuando se exporta un PCAP, ese artefacto debe tratarse como material sensible. Su almacenamiento posterior, transferencia y eventual eliminación deben regirse por políticas claras. La evidencia digital no puede circular informalmente ni almacenarse en dispositivos personales sin control.

Equilibrio entre seguridad y derechos

Un entorno NDR profesional debe sostener un equilibrio entre la necesidad de visibilidad y el respeto por los derechos de las personas cuyos datos circulan por la red. Esto implica adoptar principios como:

- Necesidad legítima de acceso.
- Limitación del propósito de uso de la información capturada.
- Protección contra reutilización indebida del tráfico almacenado.

En contextos regulatorios exigentes, la captura de tráfico puede estar sujeta a marcos legales específicos sobre protección de datos. Por ello, la arquitectura técnica debe alinearse con la política institucional y con el marco normativo aplicable.

Privacidad como parte del diseño, no como corrección

La enseñanza clave para ustedes, como futuros profesionales, es que la privacidad no se agrega después de implementar la herramienta. Debe formar parte del **diseño arquitectónico inicial:** definición de retención, segmentación de acceso, controles de autenticación, auditoría y manejo seguro de evidencia.

Cuanto mayor es la capacidad de observación que ofrece una solución como Arkime, mayor es la responsabilidad en su uso. La potencia técnica sin gobernanza adecuada puede transformarse en riesgo. En cambio, cuando la captura, la indexación, la búsqueda y la extracción se gestionan bajo principios de privacidad y control, el sistema se convierte en una herramienta poderosa y legítima para la defensa de la red.

Cierre

El estudio de las Plataformas de Monitoreo y Seguridad de Red (NDR) permite comprender que la detección y respuesta en redes no depende de una herramienta aislada, sino de una arquitectura integrada, metodológicamente gestionada y estratégicamente gobernada. La articulación entre Suricata, Zeek y Arkime evidencia cómo la detección en tiempo real, el análisis estructurado del comportamiento y la captura completa de tráfico se complementan para construir un modelo de seguridad basado en evidencia.

La arquitectura técnica constituye el soporte, pero el verdadero valor emerge cuando esa infraestructura se organiza mediante dashboards claros y workflows definidos. La visibilidad por sí sola no garantiza seguridad; lo que la transforma en capacidad operativa es la posibilidad de correlacionar señales, contextualizar eventos y reconstruir sesiones con rigor metodológico. En este sentido, el operador SOC deja de ser un simple receptor de alertas para convertirse en un analista que formula hipótesis, valida evidencias y toma decisiones fundamentadas.

Asimismo, la gestión de roles y permisos introduce una dimensión de gobernanza imprescindible. El acceso a metadatos y, especialmente, a tráfico completo en formato

PCAP implica responsabilidades técnicas, legales y éticas. El principio de mínimo privilegio, la trazabilidad de acciones y la segregación de funciones no son elementos administrativos secundarios, sino condiciones estructurales para que la visibilidad no se transforme en exposición indebida.

La captura e indexación de PCAP, junto con la búsqueda estructurada y la extracción controlada, consolidan el carácter probatorio del NDR. La posibilidad de reconstruir exactamente lo ocurrido en la red convierte a la disciplina en un modelo de investigación reproducible y verificable. Sin embargo, esta capacidad debe sostenerse en políticas claras de retención, actualización y monitoreo de la salud del sistema, ya que una arquitectura desactualizada o mal dimensionada puede generar una falsa sensación de seguridad.

Finalmente, las consideraciones de privacidad atraviesan todo el diseño. La capacidad de observar en profundidad el tráfico de red exige un equilibrio entre defensa y respeto por los derechos y datos de las personas. La privacidad no debe entenderse como un límite externo, sino como un criterio de diseño que orienta la implementación, el acceso y la gestión de la evidencia.

En síntesis, el NDR se configura como una práctica integral donde tecnología, metodología y gobernanza convergen. La eficacia en la detección y respuesta no reside únicamente en capturar más datos, sino en organizar esa visibilidad bajo principios de evidencia, trazabilidad, proporcionalidad y actualización continua. Solo así la arquitectura técnica se convierte en una verdadera capacidad estratégica de defensa organizacional.

CONTINUAR

Referencias

Arkime. (s. f.). *Settings* (Configuración del sistema Arkime) [Página web]. https://arkime.com/settings

Arkime. (2025). *README.md* (Repositorio Arkime). GitHub. https://github.com/arkime/arkime/blob/main/README.md

Locked Dorr Security. (28 de julio de 2022). *Install Arkime for PCAP Analysis* [Entrada de blog]. Medium. https://medium.com/@LDS_Cyber/install-arkime-for-pcap-analysis-6adc61e972e2

CONTINUAR

Lección 5 de 5

Descarga en PDF

PDF

modulo-3-plataformas-de-monitoreo-y-seguridad-de-red-ndr.pdf

788.7 KB