Módulo 4. Proyecto integrador

Ha quedado claro que los ciberataques evolucionan de manera dinámica en sus métodos. Esta característica puede dejar vulnerables a los mecanismos de protección estáticos, ya que carecen de la capacidad necesaria para detectar cambios en los vectores de ataque durante su ejecución. En este contexto, la inteligencia artificial, a través de algoritmos de machine learning y deep learning, permite analizar comportamientos variables en miles de peticiones y accesos simultáneos, una tarea que resultaría inviable mediante enfoques tradicionales.

Las organizaciones actuales pueden combinar distintos tipos de detección y tomar acciones de respuesta ante eventos. Estos se conocen con el nombre de:

- EDR: Endpoint Detection and Response.
- MDR: Managed Detection and Response.
- NDR: Network Detection and Response.
- XDR: Extended Detection and Response.

1. EDR (Endpoint Detection and Response)

2. Managed Detection and Response (MDR)

3. Network Detection and Response (NDR)

4. XDR: Extended Detection and Response

1. EDR (Endpoint Detection and Response)

¿Qué es un *endpoint*?

Un *endpoint* es cualquier dispositivo final que se conecta a una red:

- Computadoras de escritorio
- *Notebooks*
- *Servidores*
- Máquinas virtuales
- Dispositivos móviles (según la solución)

Nota: son el principal punto de entrada de ataques (*phishing*, *ransomware*, *exploits*).

EDR

El *Endpoint Detection and Response* (EDR) es una solución de ciberseguridad avanzada diseñada para monitorear, detectar y responder a amenazas en dispositivos finales *(endpoints*) como *laptops*, servidores y móviles en tiempo real. A diferencia de los antivirus tradicionales que se basan en firmas de virus conocidos, el EDR utiliza análisis de comportamiento e inteligencia artificial para identificar ataques sofisticados, como el *ransomware* o ataques "*fileless*" (sin archivos).

Funciones principales

Monitoreo continuo: —

registra toda la actividad del sistema (procesos, conexiones de red, cambios en registros) para detectar anomalías.

Detección de amenazas: —

identifica comportamientos sospechosos comparándolos con patrones de ataques reales (frecuentemente alineados con el marco MITRE ATT&CK).

Respuesta automatizada: —

puede aislar dispositivos infectados de la red, bloquear procesos maliciosos o revertir cambios automáticamente para contener el ataque.

Análisis forense: —

almacena datos históricos que permiten a los equipos de seguridad investigar el origen y alcance de un incidente (*Threat Hunting).*

¿Por qué el antivirus tradicional no es suficiente?

Tabla 1. Antivirus tradicional vs. EDR

Característica	Antivirus Tradicional	EDR
Enfoque	Basado en firmas conocidas.	Basado en comportamiento.
Detección	Reactivo.	Proactivo.

Visibilidad	Limitada al escaneo de archivos.	Visibilidad total de procesos y red.
Respuesta	Elimina/pone en cuarentena el archivo.	Aísla el equipo y permite una investigación profunda.
Amenazas	*Malware* común.	*Ransomware*, *zero-day*, APT.
Análisis	No analiza eventos.	Registra todos los eventos.

Fuente: elaboración propia.

Componentes principales de una solución EDR

Agente en el *endpoint*: se instala en cada equipo. Recolecta eventos del sistema:

- Procesos
- Accesos a archivos
- Conexiones de red
- Cambios en el registro

Motor de análisis: analiza los datos recolectados. Aplica:

- Reglas
- *Machine Learning*
- Heurística
- Análisis de comportamiento

Consola central: interfaz de gestión. Permite:

- Visualizar alertas
- Analizar incidentes

- Ejecutar respuestas

¿Cómo funciona un EDR? (flujo paso a paso)

1. El usuario ejecuta una acción (ej. abrir un archivo).
2. El agente EDR registra el evento.
3. El motor analiza el comportamiento.
4. Se detecta una anomalía.
5. Se genera una alerta.
6. Se inicia una respuesta (manual o automática).

Nota: a diferencia del antivirus, no espera a que exista una firma conocida.

Tipos de detecciones que realiza EDR

- Ejecución de procesos anómalos
- Uso sospechoso de PowerShell
- Movimientos laterales
- Elevación de privilegios
- Persistencia (tareas programadas, claves de registro)
- Comunicación con servidores C2
- Técnicas MITRE ATT&CK

Respuesta ante incidentes (Response)

Un EDR puede:

🔒 Aislar un endpoint de la red.

❌ Finalizar procesos maliciosos.

🗑️ Eliminar archivos.

🔄 Revertir cambios.

📊 Capturar evidencias forenses.

📌 Todo sin intervención directa del usuario.

EDR y MITRE ATT&CK

EDR utiliza el framework MITRE ATT&CK para:

- Clasificar técnicas de ataque.
- Entender la cadena de intrusión (Kill Chain).
- Facilitar el análisis y la respuesta.

Ejemplo:

- T1059 → Command and Scripting Interpreter.
- T1021 → Remote Services.

Beneficios del EDR

- Detección de amenazas avanzadas
- Visibilidad total del *endpoint*

- Respuesta rápida a incidentes
- Reducción del tiempo de permanencia del atacante
- Mejora en tareas forenses

Limitaciones de EDR

- Requiere personal capacitado
- Genera gran volumen de eventos
- No reemplaza una estrategia integral
- Necesita integrarse con otras herramientas

Ejemplos de soluciones EDR

- Microsoft Defender for Endpoint
- CrowdStrike Falcon
- SentinelOne

- VMware Carbon Black
- Sophos Intercept X

CONTINUAR

2. Managed Detection and Response (MDR)

El *Managed Detection and Response* (MDR), o detección y respuesta gestionadas, es un servicio de ciberseguridad que combina tecnología avanzada con experiencia humana para supervisar, detectar y responder a amenazas en tiempo real las 24 horas del día.

A diferencia de los servicios tradicionales que solo generan alertas, el MDR se enfoca en la acción directa para contener y neutralizar ataques antes de que causen daños significativos.

Componentes y proceso clave

El funcionamiento de un servicio MDR suele seguir cinco etapas fundamentales:

Priorización: —

se utiliza inteligencia artificial y análisis humano para filtrar miles de alertas diarias, separando falsos positivos de amenazas reales.

Búsqueda proactiva (Threat Hunting): —

analistas expertos buscan activamente señales sutiles de intrusión que las herramientas automáticas suelen pasar por alto.

Investigación: —

se analiza el alcance del ataque, determinando qué sistemas fueron afectados y cómo ocurrió la brecha.

Remediación y respuesta: —

el equipo toma medidas directas, como aislar dispositivos infectados, bloquear tráfico malicioso o eliminar malware de los registros.

Recuperación y análisis de causa raíz: —

se restaura el sistema a su estado original y se analiza el origen del ataque para prevenir futuras recurrencias.

Introducción: del EDR al MDR

Las organizaciones modernas disponen de herramientas avanzadas de seguridad como EDR, SIEM, firewall, IDS/IPS, etc.

Sin embargo, muchas no cuentan con el personal, el tiempo ni la experiencia para:

- Analizar alertas 24/7.
- Investigar incidentes avanzados.
- Responder correctamente ante ataques reales.

Nota: MDR surge como la evolución operacional de EDR: no solo tecnología, sino personas + procesos + tecnología.

Definición de *Managed Detection and Response* (MDR)

MDR es un servicio de seguridad gestionado que combina:

- Herramientas de detección (EDR, XDR, SIEM, NDR).
- Analistas humanos expertos en ciberseguridad.

- Monitoreo continuo (24/7).
- Investigación y respuesta a incidentes.

Nota: MDR es la detección y respuesta ante amenazas realizada por un equipo externo especializado, en nombre de la organización.

¿Qué problema resuelve MDR?

Tabla 2. Problemas y su solución

Problema	Cómo lo soluciona MDR
Falta de especialistas	Expertos dedicados
Alertas excesivas	Triaging y correlación
Reacción tardía	Respuesta inmediata
Entornos complejos	Gestión integral
SOC costoso	Servicio tercerizado

Fuente: elaboración propia.

Nota: MDR no reemplaza a la empresa, actúa como SOC externo o cogestionado.

Diferencias clave entre EDR y MDR

Tabla 3. Diferencias clave entre EDR y MDR

EDR	MDR
Es una herramienta	Es un servicio
Requiere operación interna	Gestionado por terceros
Detecta y responde	Detecta, investiga y responde
Tecnología	Tecnología + personas
Horario limitado	24/7/365

Fuente: elaboración propia.

Nota: **MDR usa EDR**, pero va mucho más allá.

Componentes principales de un servicio MDR

Tecnología de detección

- EDR / XDR.
- SIEM.
- Telemetría de *endpoints*, red y nube.

Equipo humano

- Analistas SOC Nivel 1, 2 y 3.
- *Threat hunters*.
- Especialistas en respuesta a incidentes.

Procesos

- *Playbooks* de respuesta.
- Investigación forense.
- Gestión de incidentes.

¿Cómo funciona MDR? (flujo operativo)

1. Se recopilan eventos de seguridad
2. Se analizan con herramientas automatizadas

3. Analistas humanos validan la amenaza
4. Se investiga el incidente
5. Se ejecuta la respuesta
6. Se informa al cliente

Nota: el cliente **no recibe ruido**, solo incidentes reales.

Monitoreo 24/7 y *Threat Hunting*

Monitoreo continuo: vigilancia permanente y detección temprana

Threat Hunting

- Búsqueda proactiva de amenazas.
- Identificación de atacantes ya infiltrados.
- Uso del *framework* MITRE ATT&CK.

Respuesta ante incidentes (*Response*)

Un proveedor MDR puede:

🔒 Aislar *endpoints*.

❌ Bloquear procesos.

🧹 Eliminar persistencia.

🔁 Revertir configuraciones.

📊 Realizar análisis forense.

📄 Emitir reportes ejecutivos y técnicos.

Nota: la respuesta puede ser **automática, asistida o aprobada por el cliente**.

MDR y el SOC (*Security Operations Center*)

Tabla 4. SOC interno y MDR

SOC interno	MDR
Alto costo	Costo previsible

Personal propio	Expertos externos
Difícil mantener 24/7	Siempre activo
Infraestructura propia	Plataformas incluidas

Fuente: elaboración propia.

Nota: MDR puede funcionar como:

- SOC externo.
- SOC híbrido.
- Refuerzo del SOC interno.

MDR vs. MSSP vs. XDR

Tabla 5. MDR vs. MSSP vs. XDR

Servicio	Característica
MSSP	Gestión de alertas y dispositivos
MDR	Detección, investigación y respuesta
XDR	Plataforma tecnológica

MDR + XDR	Servicio + herramienta integrada

Fuente: elaboración propia.

Nota: MDR se centra en **amenazas reales**, no solo alertas.

Beneficios del MDR

- Reducción del tiempo de detección (MTTD).
- Respuesta más rápida (MTTR).
- Acceso a expertos especializados.
- Menos carga operativa interna.
- Mayor madurez en seguridad.

Limitaciones del MDR

- Dependencia del proveedor.
- Coste mayor que solo EDR.

- Menor control directo.
- Requiere una buena comunicación.

CONTINUAR

3. Network Detection and Response (NDR)

La detección y respuesta de red (NDR) es una solución de ciberseguridad que emplea inteligencia artificial, aprendizaje automático y análisis de comportamiento para monitorear de forma continua el tráfico de red, detectar anomalías y automatizar la respuesta ante incidentes. A diferencia de las herramientas tradicionales basadas en firmas, NDR permite identificar ataques avanzados que logran evadir otros mecanismos de defensa. Además, proporciona visibilidad en tiempo real, facilita la búsqueda proactiva de amenazas y se integra con otros sistemas de seguridad para lograr una contención de incidentes más rápida, como evolución del análisis tradicional de tráfico de red (NTA).

¿Por qué mirar la red?

Aunque las organizaciones utilicen antivirus / EDR, *firewalls* y sistemas de autenticación, muchos ataques se mueven y se esconden dentro de la red.

La red es el lugar donde:

- Los atacantes se desplazan lateralmente.
- Se comunican con servidores externos.
- Se exfiltran datos.

Nota: si no se monitorea la red, el ataque es invisible.

Cómo funciona NDR

- **Monitorea el tráfico de red**: analiza todo el tráfico de red, norte-sur (Internet) y este-oeste (dentro de la red) en tiempo real.
- **Establece líneas de base**: utiliza IA/ML para comprender el comportamiento "normal" de la red.
- **Detecta anomalías**: señala desviaciones de la línea de base, lo que indica posibles amenazas como la exfiltración de datos, ataques de día cero o dispositivos comprometidos.
- **Respuesta automática**: activa acciones automatizadas, como el bloqueo de

conexiones sospechosas o el aislamiento de amenazas, a menudo mediante la integración con otras herramientas (como SOAR).

¿Qué problema resuelve NDR?

Tabla 6. Problemas que resuelve NDR

Problema	Cómo lo resuelve NDR
Tráfico cifrado	Análisis de metadatos.
Amenazas internas	Detección de anomalías.
Movimiento lateral	Visibilidad Este-Oeste.
Ataques sin malware	Análisis de comportamiento.
Dispositivos no gestionados	Observación pasiva.

Fuente: elaboración propia.

Nota: NDR no depende de agentes y detecta qué comportamiento es anormal.

Características y beneficios clave

- **Detección avanzada de amenazas**: detecta amenazas desconocidas que las herramientas basadas en firmas pasan por alto.
- **Búsqueda de amenazas**: proporciona contexto y herramientas para que los analistas de seguridad busquen proactivamente amenazas ocultas.
- **Respuesta a incidentes**: agiliza las investigaciones y ayuda a contener los incidentes más rápidamente.
- **Visibilidad**: ofrece información detallada sobre la actividad de la red y los riesgos potenciales.

¿Por qué es importante?

Las redes modernas son complejas y grandes, lo que crea escondites ideales para los atacantes. Las defensas perimetrales tradicionales (firewalls, antivirus) suelen ser insuficientes contra amenazas sofisticadas.

La detección y respuesta de red (NDR) cubre esta deficiencia al proporcionar monitoreo continuo y análisis inteligente del comportamiento de la red.

Componentes principales de NDR

Captura de tráfico

- SPAN / Mirror ports.
- TAP de red.
- Flow logs (NetFlow, IPFIX).

Análisis

- Machine Learning.
- Behavioral analytics.
- Reglas heurísticas.
- Detección de anomalías.

Consola de gestión

- Visualización de alertas.
- Mapas de comunicación.
- Timeline de incidentes.

¿Cómo funciona NDR? (flujo didáctico)

- Se captura el tráfico de red
- Se extraen metadatos
- Se construyen líneas base
- Se detecta una anomalía
- Se genera una alerta
- Se recomienda o ejecuta una respuesta

Nota: no interfiere con el tráfico (modo pasivo).

Tipos de amenazas que detecta NDR

- Comunicaciones con C2
- Movimiento lateral
- Escaneo de red
- Exfiltración de datos
- *Beaconing*
- Ataques internos
- Uso anómalo de protocolos

Respuesta (Response) en NDR

Un NDR puede:

🔔 Generar alertas.

🔌 Integrarse con firewalls.

❌ Bloquear IP o dominios.

🔒 Aislar segmentos.

📤 Notificar al SOC o MDR.

Nota: la respuesta suele ser integrada con otras herramientas. NDR ve lo que EDR no puede ver. NDR detecta el patrón anómalo.

Ejemplos de soluciones NDR

Son varias las aplicaciones que se mencionan: Darktrace, Vectra AI, ExtraHop, Cisco Secure Network Analytics, Corelight, Plixer.

CONTINUAR

4. XDR: Extended Detection and Response

La detección y respuesta extendidas (XDR) es una plataforma de ciberseguridad unificada, basada en inteligencia artificial, que integra herramientas de seguridad en endpoints, redes, cargas de trabajo en la nube y correo electrónico con el objetivo de proporcionar visibilidad integral y detección automatizada de amenazas multicapa. Esta tecnología evolucionó a partir de la detección y respuesta en endpoints (EDR) para enfrentar ataques cada vez más sofisticados mediante la centralización de datos, la reducción de los tiempos de investigación y la habilitación de respuestas más rápidas y coordinadas.

En la actualidad, las organizaciones modernas utilizan múltiples herramientas de seguridad, lo que genera un problema de visibilidad fragmentada al operar soluciones como EDR, NDR, seguridad de correo, seguridad en la nube, firewalls, IDS y sistemas SIEM. En este contexto, el principal desafío no radica en la falta de datos, sino en la dispersión y falta de correlación de la información. XDR surge para

unificar y correlacionar estos datos, permitiendo detectar y responder de manera eficaz a amenazas complejas que atraviesan distintos dominios, y ampliando la detección más allá del endpoint para ofrecer una visión integral del ataque.

Extended detection and response (XDR) es una plataforma unificada de detección y respuesta que:

- Integra telemetría de múltiples fuentes
- Correlaciona eventos automáticamente
- Reduce alertas aisladas (*noise)*
- Prioriza incidentes reales
- Permite respuesta coordinada

¿Qué problemas resuelve XDR?

Tabla 7. Problemas que resuelve XDR

Problema	Solución XDR
Alertas desconectadas	Correlación automática.

Falta de contexto	Visión de ataque completa.
Tiempo elevado de análisis	Incidentes consolidados.
Herramientas aisladas	Plataforma unificada.
SOC sobrecargado	Prioridad basada en riesgo.

Fuente: elaboración propia.

Diferencia entre EDR, NDR y XDR

Tabla 8. Diferencia entre EDR, NDR y XDR

Tecnología	Alcance
EDR	Endpoint.
NDR	Red.
XDR	Endpoint + Red + Correo + Nube + Identidad.

Fuente: elaboración propia.

XDR no reemplaza a EDR o NDR: los integra. Un XDR moderno puede integrar:

- EDR (procesos, archivos, memoria).
- NDR (flujos y comportamiento de red).
- Email Security (*phishing*).
- Identidad (AD, Azure AD, IAM).
- Cloud (SaaS, IaaS).
- *Firewalls* y *proxies*.

Arquitectura general de XDR

- **Recolección**: Agentes, API, *Logs* y sensores de red.
- **Análisis**: *Machine Learning*, correlación de eventos, detección basada en comportamiento. MITRE ATT&CK.
- **Respuesta**: automatizada, orquestada y manual asistida.

Respuesta en XDR (*Response*)

XDR puede ejecutar:

🔒 Aislar endpoints.

❌ Bloquear usuarios comprometidos.

📧 Eliminar correos maliciosos.

🌐 Bloquear IP y dominios.

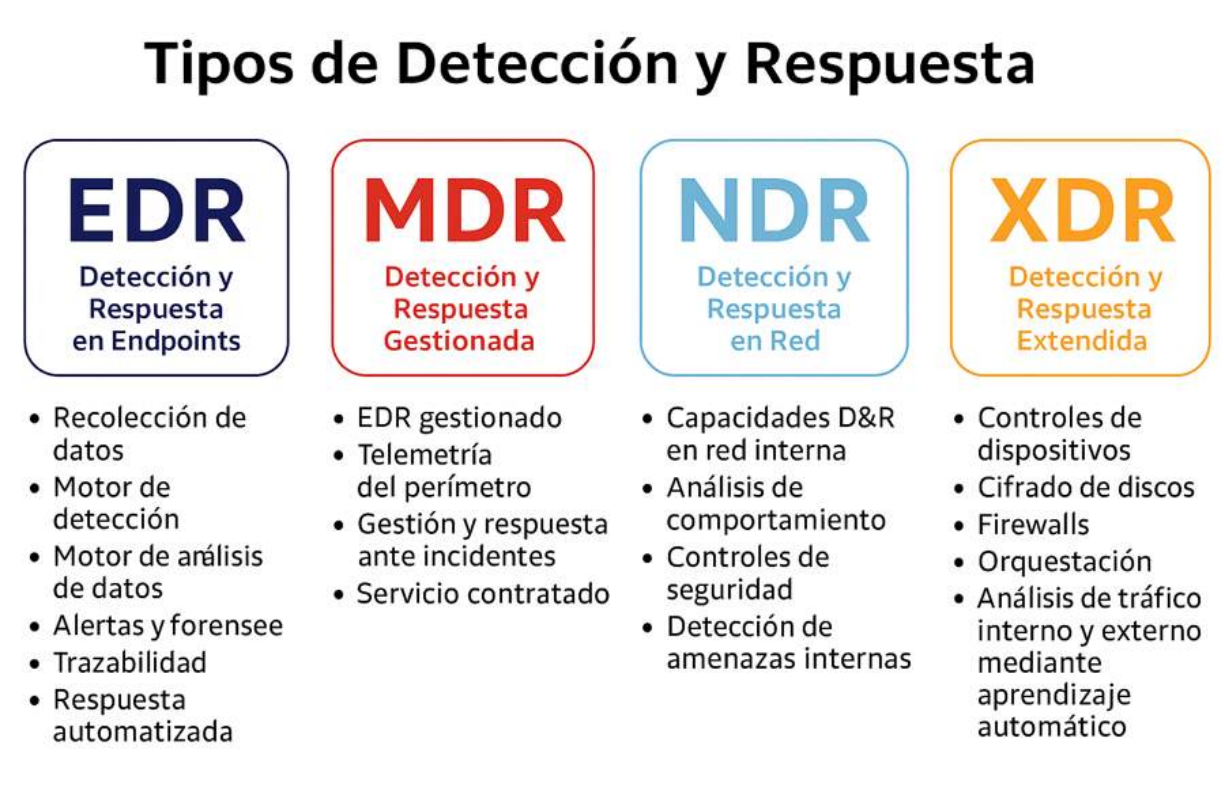
☁️ Suspender cargas en la nube.

📤 Notificar al SOC o MDR.

Ejemplos de plataformas XDR

- Microsoft Defender XDR.
- Palo Alto Cortex XDR.
- Trend Micro Vision One.
- SentinelOne Singularity XDR.
- Sophos XDR.
- VMware Carbon Black XDR.

Figura 1. Tipos de detección y respuesta



Fuente: elaboración propia.

Proyecto integrador

Los conceptos vistos en este curso permitirán tener una base sólida para realizar una aplicación que detecte ciberataques de denegación de servicios usando inteligencia artificial (*Detecting DoS using IA*) que se verá en la parte práctica y se explicó en la primera *masterclass*.

Papers

MITRE Corporation. MITRE ATT&CK® Framework. Disponible en: https://attack.mitre.org.

Este recurso permite comprender el marco central de la detección y respuesta modernas en ciberseguridad. Su enfoque es transversal a EDR, NDR, XDR y MDR, y constituye una base fundamental para el desarrollo de actividades prácticas, el análisis de incidentes, el mapeo de tácticas y técnicas, el estudio de casos y la elaboración del trabajo integrador final.

CONTINUAR