[ESTADO: INCIDENTE EN CURSO]

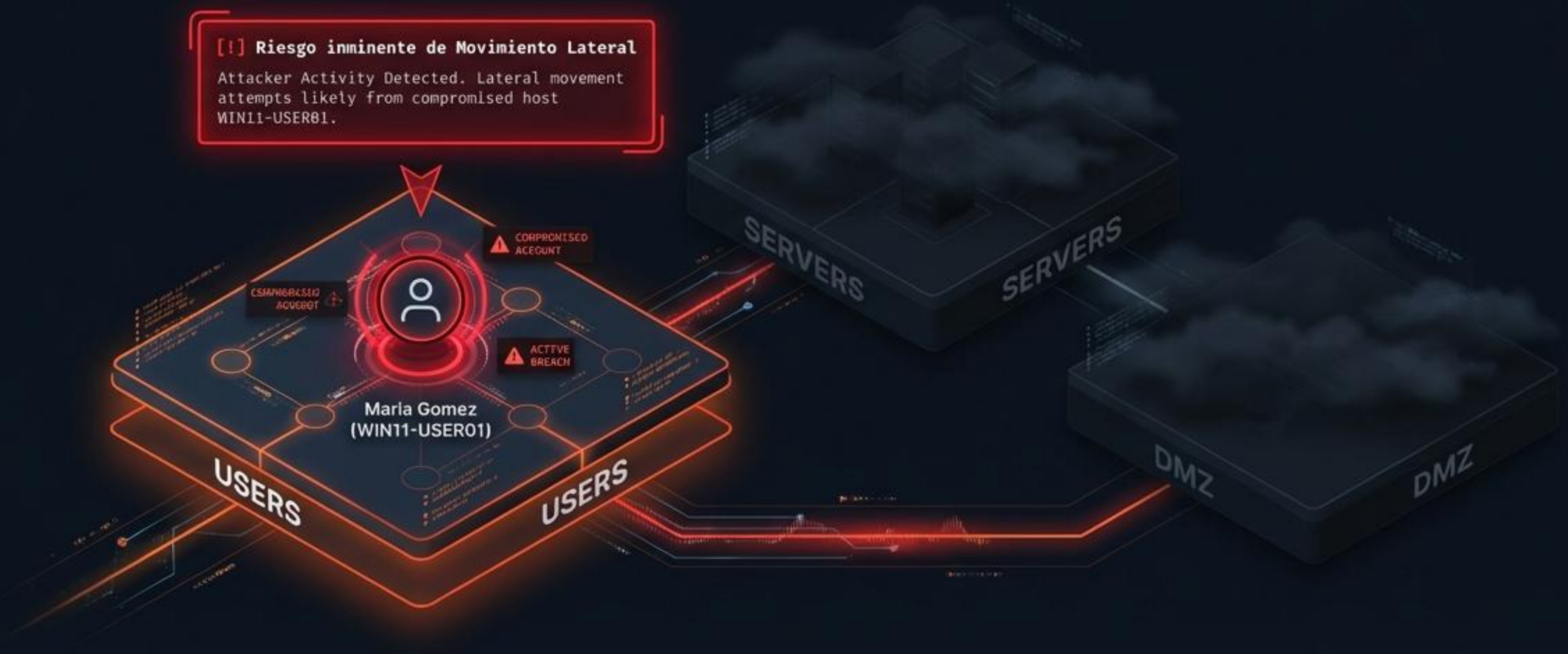
Sesión 03 | Reconocimiento y Escaneo de Red

Detectando a BlackCedar en las sombras de la red corporativa.

CLASIFICACIÓN: TLP:RED | DESTINATARIO: BLUE TEAM ANALYST | ENTORNO: SECURITY ONION

Situación Actual: El enemigo está dentro, pero está ciego.

BlackCedar ha comprometido las credenciales de Maria Gomez. Tienen una cabeza de playa en la subred 10.60.10.0/24. Desconocen la ubicación del Controlador de Dominio (DC01) y de los datos médicos sensibles. Para avanzar, necesitan mapear el terreno.



MedData
Enterprise SOC Console

Comparativa: Cyber Kill Chain vs. Proceso de Hacking

Proceso de Hacking (Perspectiva del Atacante)

1. Reconocimiento
2. Escaneo y Enumeración
3. Obtención de Acceso
4. Mantenimiento de Acceso
5. Borrado de Huellas

Cyber Kill Chain (Modelo de Defensa)

1. Reconocimiento
2. Armamentización
3. Entrega
4. Explotación
5. Instalación
6. Comando y Control (C2)
7. Acciones sobre los Objetivos

Ambos modelos describen etapas similares, pero la Cyber Kill Chain se enfoca en la detección y disrupción en cada fase, mientras que el proceso de hacking se centra en la ejecución exitosa del ataque.

Reconnaissance	The adversary is trying to gather information they can use to plan future operations.
Resource Development	The adversary is trying to establish resources they can use to support operations.
Initial Access	The adversary is trying to get into your network.
Execution	The adversary is trying to run malicious code.
Persistence	The adversary is trying to maintain their foothold.
Privilege Escalation	The adversary is trying to gain higher-level permissions.
Defense Evasion	The adversary is trying to avoid being detected.
Credential Access	The adversary is trying to steal account names and passwords.
Discovery	The adversary is trying to figure out your environment.
Lateral Movement	The adversary is trying to move through your environment.
Collection	The adversary is trying to gather data of interest to their goal.
Command and Control	The adversary is trying to communicate with compromised systems to control them.
Exfiltration	The adversary is trying to steal data.
Impact	The adversary is trying to manipulate, interrupt, or destroy your systems and data.

¿Qué es MITRE ATT&CK?

Origen y Evolución

Lanzado en 2013 por MITRE Corporation (organización sin fines de lucro).

Nacido del Fort Meade Experiment (FMX) para evaluar telemetría de endpoints.

Lenguaje común entre equipos defensivos (Blue Team) y ofensivos (Red Team).

El Manual del Adversario

Una base de conocimiento global de tácticas y técnicas adversarias basadas en observaciones del mundo real.

No es un simple listado de malware, es un mapa de comportamiento.

Integración nativa con ecosistema STIX/TAXII para automatización de inteligencia de amenazas.

La Arquitectura del Framework: Las Matrices

Mobile

Enfoque: Dispositivos iOS y Android.

Objetivo: Vectores de entrada y exfiltración específicos de smartphones corporativos.

Enterprise (El Núcleo)

Enfoque: Entornos corporativos (Windows, macOS, Linux, Cloud, Redes, Contenedores).

Incluye **PRE-ATT&CK:** Fases de reconocimiento y desarrollo de recursos antes del compromiso.

ICS

Enfoque: Sistemas de Control Industrial e infraestructuras críticas (SCADA, PLC).

Nota: Opera con 12 tácticas (omite Reconocimiento y Desarrollo de Herramientas).

La Arquitectura del Framework: Las Matrices

Mobile

Enfoque: Dispositivos iOS y Android.

corporativos.

Enterprise (El Núcleo)

Enfoque: Entornos corporativos (Windows, macOS, Linux, Cloud, Redes, Contenedores).

y desarrollo de recursos antes del compromiso.

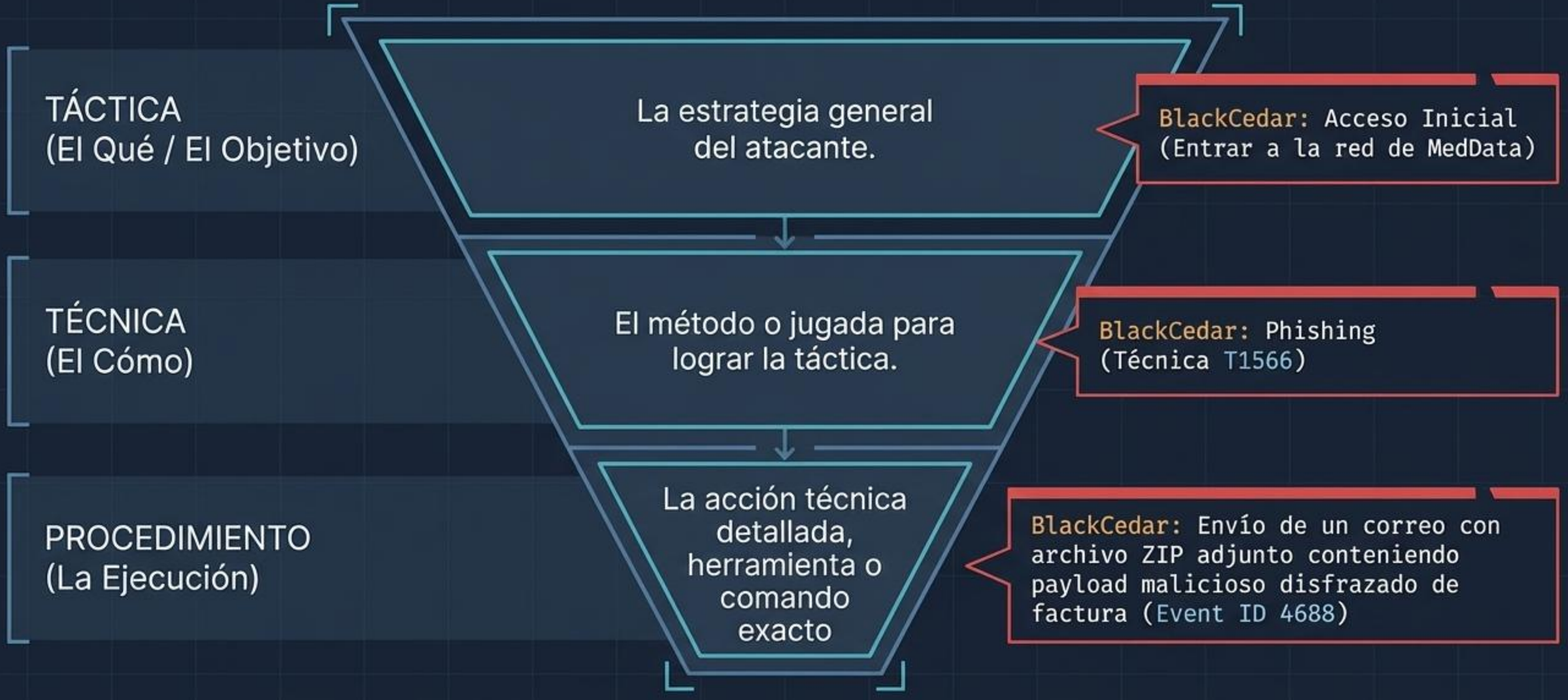
ICS

Enfoque: Sistemas de Control Industrial e infraestructuras críticas

y Desarrollo de Herramientas).

https://attack.mitre.org/

Desglosando el Comportamiento: El Modelo TTP



217.127.200.160

Regular View | Raw Data | Timeline | Whois

// TAGS: vpn

// LAST SEEN: 2026-04-12

General Information

Hostnames	160.red-217-127-200.staticip.**rima-tde.net**
Domains	rima-tde.net
Country	**Spain**
City	**Madrid**
Organization	**Telefonica de Espana SAU (NCC#2001038578)**
ISP	**TELEFONICA DE ESPANA S.A.U.**
ASN	**AS3352**

Open Ports

500 1194

// **500** / UDP 1219566337 | 2026-04-12T10:40:18.924741

```
VPN (IKE)

Initiator SPI: 6b71376e35316239
Responder SPI: 6f69377a74326163
Next Payload: RESERVED
Version: 2.0
Exchange Type: DOI Specific Use
Flags:
    Encryption:     False
    Commit:         False
    Authentication: False
Message ID: 00000000
Length: 36
```

// **1194** / UDP -420209344 | 2026-04-12T13:35:07.046026

```
@\xba\xc3\xb4\x92\t\x9f\x86\x19\x01\x00\x00\x00\x00\xd9\xce:\xbe\xf6\x98\xa5
m\x00\x00\x00\x00
```

El Viaje del Atacante: Las 14 Tácticas Enterprise


```
> SYSTEM ALERT: BlackCedar detectado actualmente en fase 10: Movimiento Lateral.
```

Anatomía de una Maniobra: Técnicas y Subtécnicas

Insight Operativo: Conocer la subtécnica exacta permite configurar el SIEM o Mail Gateway con precisión quirúrgica, reduciendo falsos positivos.

Perfilando al Enemigo: Grupos APT y Comportamiento

	Ciberdelincuencia Común	Amenazas Persistentes Avanzadas (APT)
Motivación:	Ganancia rápida (Ransomware básico).	Inteligencia estratégica a largo plazo.
Herramientas:	Malware público y scripts comunes.	Exploits Zero-Day y herramientas de élite a medida.
Operación:	Caótica, masiva y oportunista.	Equipos coordinados, sigilosos y altamente financiados.

Panel de Inteligencia

[CONTEXTO] Perfilando a BlackCedar

MITRE ATT&CK asocia grupos públicos con sus TTPs históricos. Rastrear a BlackCedar no requiere buscar su nombre, sino buscar su huella de comportamiento en la matriz ATT&CK.

Traducción Forense: De IoC a TTP

Evidencia		Clasificación ATT&CK
Conexión saliente IP: 185.x.x.x (Maliciosa)	→	Táctica: Comando y Control (TA0011)
Hash MD5: 5e884898... detectado en estación de trabajo	→	Técnica: Ejecución (T1059) → Intento de ejecutar código malicioso
Reporte usuario: Correo de Soporte con archivo invoice.zip	→	Táctica: Acceso Inicial (TA0001) / Técnica: Spear Phishing (T1566)

Insight: Vincular Indicadores de Compromiso (IoCs) a TTPs revela el rompecabezas táctico del atacante y predice su próximo movimiento.

Síntesis: De la Reacción a la Caza Proactiva

Antes - Reactivo

- Perseguir alertas individuales de antivirus.
- Fatiga por indicadores estáticos (IoCs).
- Respuestas ad-hoc y caos operativo.

ATT&CK

Ahora - Proactivo

- Comprender la intención y táctica detrás de cada alerta.
- Generar reglas de detección por comportamiento.
- Simular ataques para anticipar vulnerabilidades.

El Verbo Clave: Threat Hunting

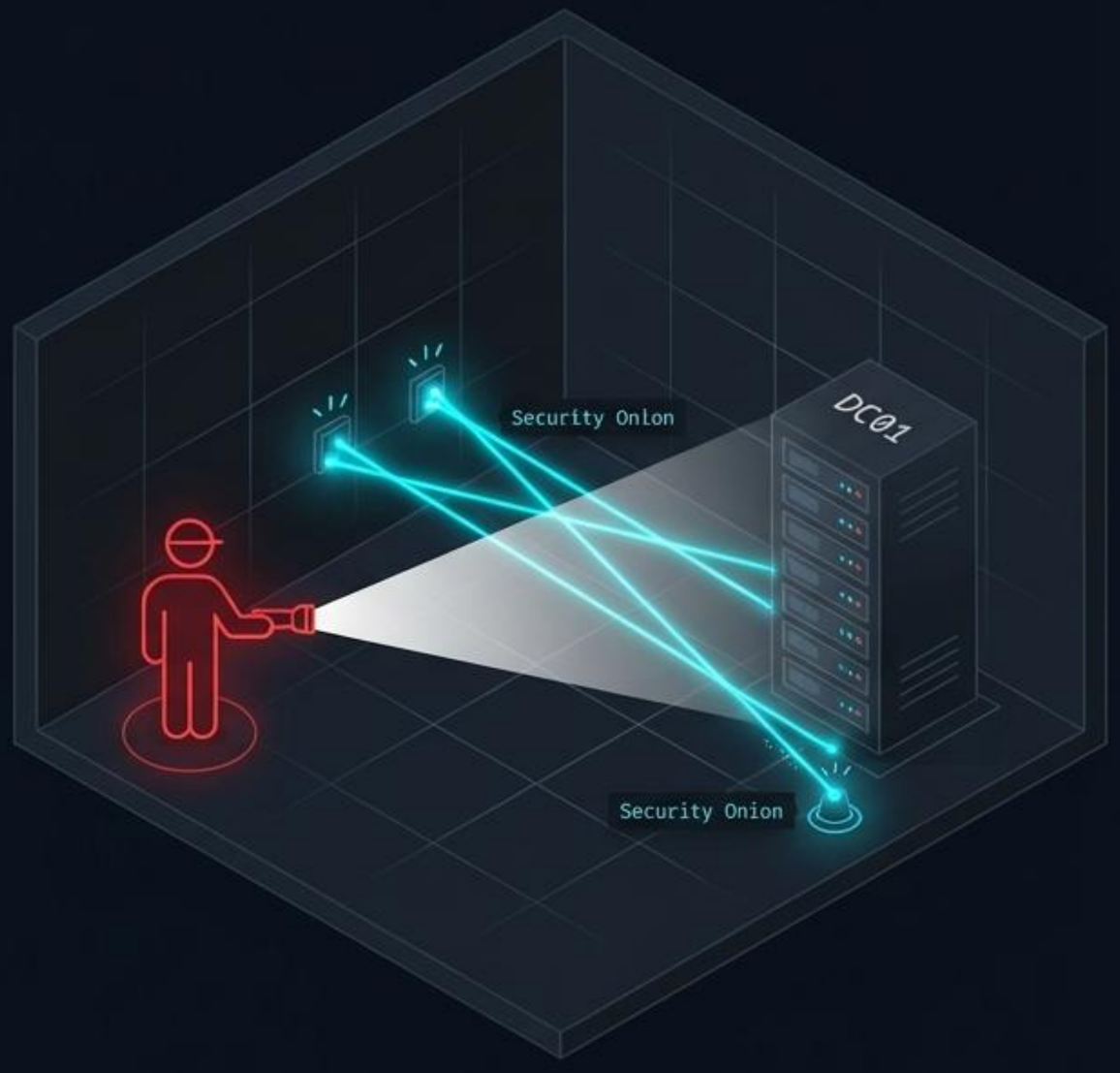
Usar MITRE ATT&CK no como un diccionario estático, sino como el manual operativo para sobrevivir y cazar a BlackCedar.

MedData
Enterprise SOC Console

El Dilema del Atacante: Reconocimiento Activo

En esta fase de la Kill Chain, el atacante asume el mayor riesgo. Al interactuar directamente con nuestra infraestructura para descubrir hosts y servicios, genera ruido.

Objetivo SOC:
Nuestro objetivo no es evitar que enciendan la linterna, sino detectar su luz antes de que encuentren una puerta abierta.



CURSO SOC

LABORATORIO PRÁCTICO

Acceded a la pestaña Alerts de Security Onion e investigad la actividad sospechosa reciente para responder:

IDENTIFICACIÓN DEL ATACANTE

¿Cuál es la IP del atacante? ¿Interna o externa?

OBJETIVOS DEL ESCANEO

¿Qué sistemas han sido escaneados?

HERRAMIENTAS DETECTADAS

¿Qué herramientas se han detectado?

SERVICIOS WEB BUSCADOS

¿Qué servicios web intentó encontrar el atacante?

MedData
Enterprise SOC Console

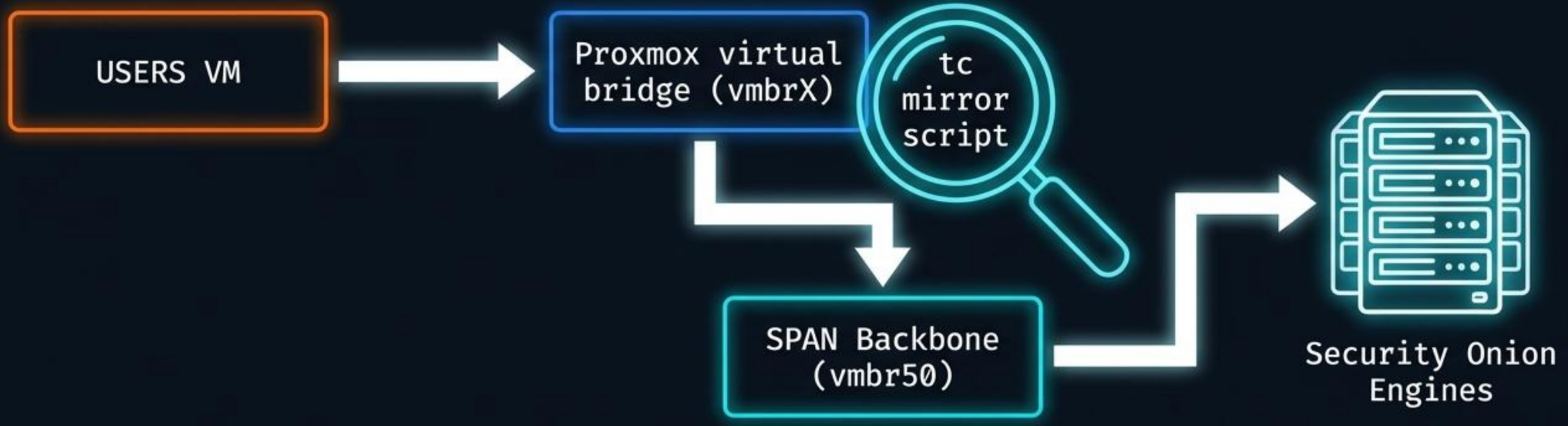
El Arsenal Ofensivo: Firmas de Reconocimiento

Herramienta	Objetivo Principal	Técnica	Nivel de Ruido en el SOC
Nmap (-sS)	Encontrar puertas abiertas en el DC01 (`10.60.20.10`)	Escaneo de puertos TCP SYN (Stealth). Evita completar la conexión TCP.	**Moderado-Alto** (Ráfagas de paquetes SYN sin ACK)
Nikto	Buscar archivos peligrosos y misconfigurations en WEB01 (`10.60.30.10`)	Escaneo de vulnerabilidades web (Metralladora HTTP).	**Extremo** (Generación masiva de tráfico web anómalo)

Nuestro Arsenal: Arquitectura NDR y Visibilidad

¿Cómo escuchamos los pasos del atacante en el tráfico East-West?

MedData
Enterprise SOC Console
58:53
23
CPU RAM Disk



Suricata (IDS)

Detección por Firmas. Busca patrones conocidos como el Nmap Scripting Engine. (Acción determinista).

Zeek (NDR)

Telemetría neutral. Genera logs detallados de red (conn.log, http.log) para ver todo el tráfico lateral, incluso si no hay una firma que haga saltar la alarma.

MedData

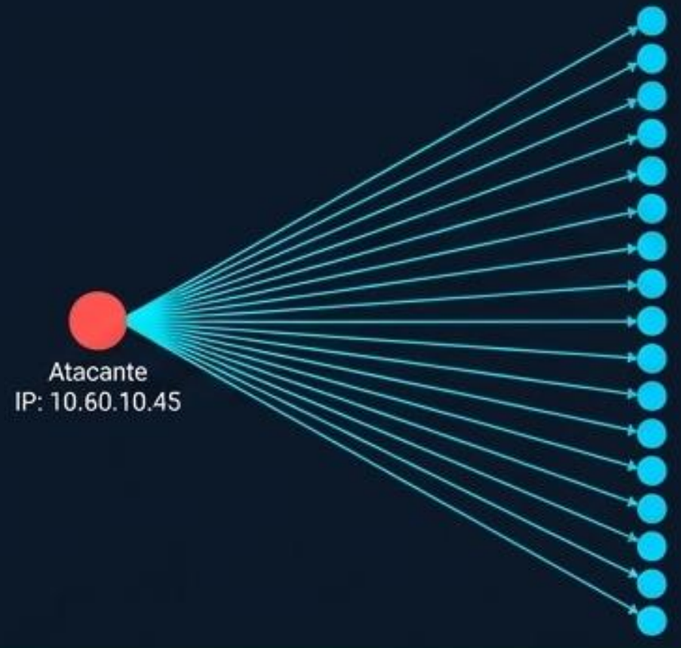
Síntesis de Comportamiento: El Patrón del Escáner

¿Cómo confirmamos que una IP es hostil? Un usuario corporativo normal hace peticiones específicas. Un atacante hace esto:

Datos Crudos: Log de Zeek (conn.log)

	ts	uid	id.orig_h	id.resp_h	id.resp_p
2	16892…	CHg8…	10.60.10.45	10.60.20.1	445
3	16892…	C7uL…	10.60.10.45	10.60.20.2	445
4	16892…	C92a…	10.60.10.45	10.60.20.3	445

Visualización: Escaneo Secuencial



Un atacante en fase de reconocimiento toca cientos de IPs secuenciales (10.60.20.1 al 10.60.20.254) en milisegundos, buscando respuestas. Es una huella digital inconfundible en los logs de Zeek.

MedData

Objetivos de Inteligencia (Triaje)

Paso 1: Clasificación del Origen (¿Es un escaneo autorizado?)

Si es interno y autorizado: Marca como "Falso Positivo" y cierra.
Si es desconocido: Continúa al Paso 2.

Paso 2: Análisis del Objetivo (¿Qué están buscando?)

Identificar la Aplicación: ¿A qué servidor y puerto se dirigen? Analizar la Petición HTTP: Si la alerta es de Nmap (NSE), busca el http.uri. ¿Están intentando acceder a carpetas sensibles como /admin, /config, o buscando archivos .env o .php?

Códigos de Respuesta: Revisa el http.status_code.

- 404: El escaneo falló (no encontró nada).
- 200 / 301 / 401: El escaneo tuvo éxito o encontró algo ¡Atención aquí!

MedData

Objetivos de Inteligencia (Triaje)

Paso 3: Determinar la Magnitud (¿Es un ataque dirigido o masivo?)

Frecuencia y Patrón:
Alcance: ¿Esa misma IP está escaneando a otros servidores de nuestra red o solo a uno?
Alertas Relacionadas: Busca si esa IP ha disparado otras alertas en las últimas 24 horas (ej. intentos de fuerza bruta en SSH o Telnet).

Paso 4: Búsqueda de Éxito y Persistencia (¿Han entrado?)

Conexiones Establecidas: Busca conexiones con estado SF (establecida/finalizada).
Actividad en el Host: Si tienes telemetría de endpoint, comprueba si hay procesos sospechosos (CommandLine) en el momento del escaneo.

Contención Estructural: El Valor de la Segmentación

¿Cómo minimizamos el impacto de este reconocimiento?

Defense in Depth: BlackCedar está en **10.60.10.x**. No pueden hacer un escaneo ARP mágico para descubrir la red **10.60.20.x** porque están en diferentes dominios de broadcast. Todo el tráfico se ve obligado a subir y atravesar el firewall, dándonos el punto de estrangulamiento perfecto para nuestro SPAN virtual.

Punto de Decisión: Respuesta Inicial (IR)

Como analista **junior** en el turno de guardia, has confirmado la IP atacante. ¿Qué haces?

¿Cortamos su acceso de inmediato, avisando al atacante de que estamos mirando?

¿Aislamos lógicamente y observamos sus movimientos para entender su objetivo final antes de que cambien de táctica?

MedData

Reporte de Fin de Turno

Status	Intruso (BlackCedar) detectado con éxito en la fase de reconocimiento activo.
Systems Check	Nuestra telemetría de red (Suricata/Zeek) y el flujo del SPAN virtual están validados y operativos.
Próxima Guardia (Sesión 04)	**El atacante ya sabe dónde está el DC01. Preparad las defensas de Identidad. El intento de Escalada de Privilegios y Movimiento Lateral es inminente.**