

Detección de ataques avanzados / APT



¿Qué es Carmen?

Carmen es la solución de identificación de **Amenazas Persistentes Avanzadas** (APT). Esta solución adquiere, procesa y analiza información para la elaboración de inteligencia a partir del tráfico de una red interna. De este modo, es capaz de detectar anomalías y movimientos laterales y externos dentro de la red, así como de analizar malware mediante sandboxing avanzado.



¿Por qué usar Carmen?

Protege la información sensible, la propiedad intelectual y los activos críticos de la organización.

Evita daños en la reputación corporativa y en las marcas de la organización.

Reduce el impacto económico derivado de los robos de información.

Obtiene **visibilidad completa** y consciente del movimiento de información no legítimo de la organización.

Propiedades

Protección eficaz contra el compromiso por APT

Detección de amenazas no conocidas

Detección a medida de amenazas dirigidas

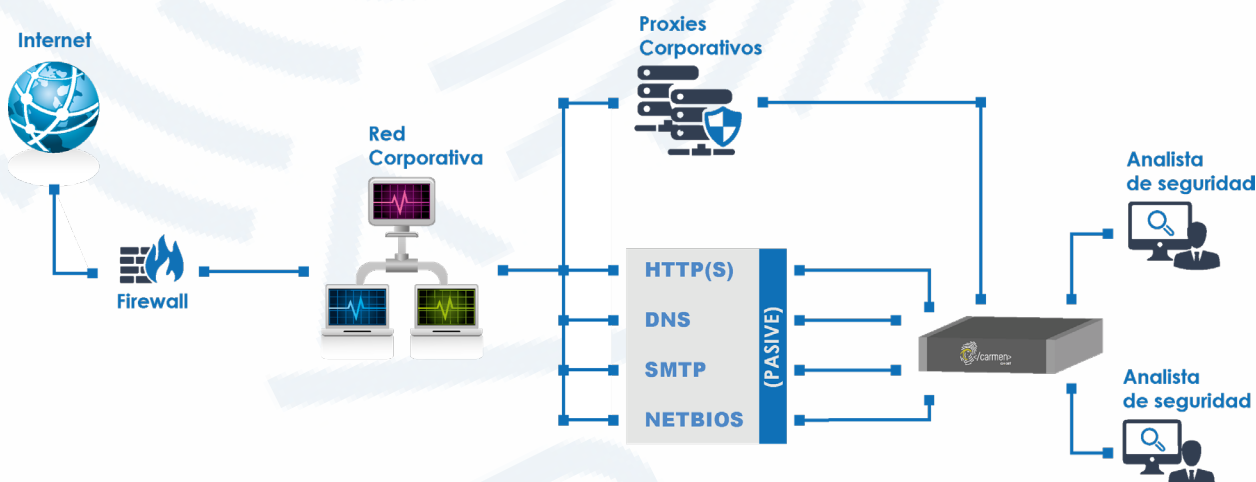
Acelera los ciclos de investigación

Obtiene visibilidad completa e informada

Instalación rápida, sencilla y no intrusiva

¿Cómo funciona?

Carmen pone el foco en el procesamiento y el análisis de tráfico de red salientes (Command & Control y exfiltración) de la organización vigilada con el objetivo de **identificar exfiltraciones o comunicaciones** con sistemas C2 en protocolos como HTTP, DNS o SMTP (los más habituales para este tipo de comunicaciones), así como mecanismos habituales de mantenimiento de persistencia o robo de información en la red corporativa (movimiento lateral).



Para ello, se adquiere la información de estos tráfico tanto de forma pasiva (vía sniffing y disección del protocolo, por ejemplo Passive Proxy) como mediante la recepción de registros (por ejemplo, proxy HTTP), se normaliza y se almacena. A partir de entonces, puede comenzar el análisis automático, semiautomático y manual, convirtiéndose Carmen en una solución de apoyo a la toma de decisiones que permita a un analista de seguridad encontrar la aguja en el pajar; priorizando los elementos a analizar de entre todo el volumen de datos adquiridos.

Integración con otras soluciones CCN-CERT



Intercambio de información de
ciberamenazas



Gestión de ciberincidentes



carmen@ccn-cert.cni.es

www.ccn-cert.cni.es

