Características técnicas: CARMEN

CARMEN (Centro de Análise de Rexistros e Minaría de Eventos)

- Subministración e implantación dun appliance, así como, da licenza de explotación non exclusiva de CARMEN.
    - Subministración de appliance CARMEN e posta en funcionamento, contará con: Log de navegación (HTTP), DNS, SMTP e NetBIOS, en particular, Named Pipes e Mail slots
    - O modulo applicance debe entregarse cun servidor para rack cunha altura de 2U. cun mínimo de 2 procesadores de 2,4 GHz (10 cores/20 fíos), 64 GB de RAM, capacidade de retención de 350 GB de logs; 8 interfaces de rede de 1 Gbps de cobre e fonte de alimentación redundante.

- Consultoría, integración, parametrización e posta en marcha da plataforma.
- A licenza de uso non exclusivo por tratarse dunha administración pública debe ser gratuita.

CARMEN ofrecerá unha protección avanzada ante ameazas na organización vixiada, de forma que tanto os tráficos de rede saíntes e internos da organización como os tráficos de rede entrantes son adquiridos, procesados e analizados para a defensa desta: a existencia de usos indebidos, a detección de anomalías ou os intentos de intrusión son identificados, organizados e representados para facilitar o desempeño do equipo de seguridade. Disporá dunha ferramenta que permite cubrir as principais vías de comunicación destas ameazas co exterior (navegación web, consultas DNS e correo electrónico) así como diferentes mecanismos de comunicación interna na rede comprometida.

CARMEN permitirá a análise automática, semiautomático e manual do tráfico de rede da organización para a detección de usos indebidos e, especialmente, para a detección de anomalías significativas neste tráfico: estatísticas, series temporais. A Detección poderá realizarse mediante a execución manual de analizadores ou ben mediante a programación periódica de análises automáticas da información adquirida para cada un dos protocolos considerados. Identificará intrusións, detectará intrusos, mediante unha rede de intelixencia compartida.