CONSORCI SANITARI DEL MARESME

INFORME DE NECESSITATS PER LA CONTRACTACIÓ D'UN SERVEI GESTIONAT DE DETECIÓ I RESPOSTA D'AMENACES AVANÇADES (MDR) AL CONSORCI SANITARI DEL MARESME

Descripció de la necessitat

Actualment al CSdM estem utilitzant el programari d'antivirus convencional (basat en signatures) que ajuda a detectar i bloquejar amenaces conegudes. El principal problema d'aquest tipus d'antivirus és que no protegeix d'amenaces no conegudes o de noves variants. Per aquest motiu, aquesta no és una solució efectiva davant l'alt volum d'amenaces avançades o amenaces zero-day que apareixen a diari.

En l'actualitat hi ha eines preventives basades en intel·ligència artificial que analitzen els comportaments dels equips i les aplicacions que s'executen, i son capaços de detectar irregularitats i per tant aplicar mesures per bloquejar i revertir les accions. També permeten la contenció dels equips infectats, quan no es possible una remediació automatitzada, per evitar la propagació a més equips de la xarxa. Aquestes eines es denominen EDR (Endpoint Detection and Response).

Des del CSdM hem analitzat el mercat i revisat les comparatives d'empreses reconegudes mundialment (com Gartner, Forester o Mittre) i hem fet proves de concepte amb els 3 EDRs millor posicionats en prestacions i efectivitat en la detecció d'amenaces.

Aquest productes són ideals per la detecció avançada, però també es necessari disposar d'una monitorització 24x7 de les alertes generades i d'un recolzament de professionals experts en ciberseguretat, que davant d'un incident de ciberseguretat facin accions immediates per aturar o mitigar l'atac, realitzar recomanacions davant nous tipus d'atac i donar suport a la presa de decisió davant d'una determinada situació. El coneixement d'experts és vital per fer front a la gran quantitat de tipus d'atacs i la seva constant sofisticació. Per tant no només és dotar-se d'unes eines de detecció avançada si no que també són necessaris un serveis de monitorització i resposta 24x7x365 per una àgil detecció i bloqueig.

El darrers any hem estat fent una prova pilot de desplegament de la solució que hem analitzat com a més completa, així com el serveis gestionats de 24x7x365. Després de la valoració positiva volem extendre una solució i servei d'aquest tipus al conjunt d'estacions de treball i servidors del CSdM. Amb aquesta acció també es donaria conformitat al requisit del nou pla de ciberseguretat de l'Agència de Ciberseguretat de Catalunya pels centres assistencials del SISCAT.

L'**objectiu** del contracte és la contractació de:

- Llicenciament d'ús d'una solució MDR en modalitat SaaS per la protecció contra amenaces avançades en **1.700 estacions de treball i 240 servidors** del CSdM, completament gestionats per l'adjudicatari.
- **Servei de SOC** per donar resposta al compliment dels requeriments d'aquest plec tècnic per la monitorització i resposta a alertes, gestió de la plataforma, actualitzacions, intel·ligència d'amenaces i funcionalitats avançades de detecció i resposta en modalitat 24x7x365.
- Manteniment i suport de la solució.
- **Subministrament, instal·lació, configuració i posada en marxa** d'una solució MDR per al CSdM**.**

Sr. Xavier Roca Ysarn
Cap d' Informàtica
Mataró, 4 d'agost de 2025

Sr. Francesc Moya Olvera
Director Sistemes Informació