PLEC DE PRESCRIPCIONS TÈCNIQUES
EXP-LIC-2023-82503

CONTRACTE RELATIU AL SUBMINISTRAMENT DE LLICÈNCIES DE TIPOLOGIA EDR/EPP PER A ESTACIONS DE TREBALL I SERVIDORS

Índex

1. Objecte

L'objecte del present plec de prescripcions tècniques és definir i regular les especificacions tècniques de la contractació per a l'adquisició d'una solució d'EDR/EPP (Endpoint Detection and Response, Endpoint Protection Platform) per a les estacions de treball (Windows i MacOS) i els servidors (Windows).

2. Volumetria

R0. **Mínim de llicències per plataforma**:

Desktop Windows	5000
Desktop MacOS	500
Servidor Windows	400

3. Requisits generals

R1. **Compatibilitat**: la solució d'EDR ha de ser compatible amb els sistemes operatius següents:

- Estacions de treball: Windows i MacOS
- Servidors: Windows

R2. **Desplegament desatès**: la solució d'EDR ha de permetre un desplegament desatès del client EDR en les estacions de treball i servidors, integrant-se amb les eines de gestió de dispositius comunes.

Específicament, en el cas de dispositius Windows, la solució ha de ser compatible amb el

Directori Actiu, Microsoft System Center Configuration Manager, Intune, etc.

R3. **Integració amb altres eines de seguretat**: la solució d'EDR ha de ser capaç d'integrar-se amb altres eines de seguretat de la institució, com ara tallafocs, SIEMs o altres sistemes de gestió de seguretat.

R4. **Consola de gestió al núvol i programari client**: la solució d'EDR ha de disposar d'una consola de gestió centralitzada basada en el núvol, que permeti als administradors de seguretat monitorar, gestionar i configurar els endpoints de manera remota i en temps real. La consola de gestió al núvol ha de complir amb les normatives de seguretat i protecció de dades aplicables, garantint la confidencialitat, integritat i disponibilitat de la informació.

La solució d'EDR ha d'incloure un programari client lleuger i eficient per a les estacions de treball, que sigui compatible amb els sistemes operatius especificats. Aquest programari client serà l'únic component que caldrà instal·lar a les estacions de treball, i serà responsable de la comunicació amb la consola de gestió al núvol, així com de l'execució de les tasques de detecció, prevenció i resposta a les amenaces. El programari client ha de requerir un mínim d'impacte en el rendiment dels equips i haurà de ser actualitzat automàticament a través de la consola de gestió al núvol.

El client haurà de poder funcionar de manera autònoma si perd puntualment la connexió amb la xarxa o la consola de gestió centralitzada.

R5. **Escalabilitat**: la solució d'EDR ha de ser escalable per adaptar-se al creixement de l'organització i a l'augment del nombre d'estacions de treball i servidors.

R6. **Actualitzacions**: la solució d'EDR ha de proporcionar actualitzacions periòdiques de seguretat i millores de rendiment per garantir la protecció efectiva dels endpoints.

R7. **Certificació**: la solució d'EDR ha d'estar inclosa en el Catàleg de Productes Certificats del Centro Criptológico Nacional (CCN) (guía CCN STIC 105). Aquest requisit garanteix que la solució d'EDR compleix amb els estàndards de seguretat i qualitat establerts pel CCN per a la protecció de les infraestructures crítiques i sistemes d'informació.

R8. **Gestió delegada:** la solució ha de permetre la gestió delegada, tant de grups d'administradors com d'equips (pot ser amb capacitat multitenant o bé amb gestió d'administradors amb visió limitada per grups d'equips).

En cas de suport multitenant, s'ha de permetre també la visió única de tots el tenants i l'establiment de polítiques comuns.

4. Requisits funcionals

R9. **Inventari en temps real**: la solució d'EDR ha de permetre mantenir un inventari en temps real del desplegament, incloent-hi la identificació de les estacions de treball i servidors que tenen el client EDR instal·lat, la versió del client, l'estat de la seva connexió i qualsevol altra informació pertinent. Aquesta funcionalitat és essencial per a una gestió eficient dels dispositius i per assegurar que la solució d'EDR estigui correctament desplegada i actualitzada a tota la infraestructura.

R10. **Detecció i anàlisi de les amenaces**: la solució d'EDR ha de ser capaç de detectar i analitzar de manera eficient les amenaces avançades, com ara malware, ransomware, APTs i altres tipus d'atacs dirigits.

R11. **Prevenció i resposta**: la solució d'EDR ha de proporcionar mecanismes de prevenció i resposta a les amenaces detectades, incloent-hi la possibilitat de contenir i eliminar el malware i restaurar els sistemes afectats.

R12. **Monitoratge i alertes**: la solució d'EDR ha de proporcionar una interfície de monitoratge centralitzada que permeti als administradors de seguretat visualitzar l'estat dels endpoints i rebre alertes en temps real en cas d'incidents de seguretat.

R13. **Polítiques de seguretat i conformitat**: la solució d'EDR ha de permetre la creació i aplicació de polítiques de seguretat específiques per a cada tipus d'endpoint, així com garantir

el compliment de les normatives de seguretat aplicables a la institució.

R14. **Capacitat de manteniment d'històric de dades**: la solució d'EDR ha de ser capaç de mantenir un històric de dades d'un mínim de 30 dies, incloent-hi registres d'activitat, incidents de seguretat, actualitzacions i altres esdeveniments rellevants.

5. Formació i suport

R15. **Formació**: El proveïdor de la solució d'EDR ha de proporcionar formació als administradors de seguretat de la institució per garantir el correcte funcionament i manteniment del sistema.

- Formació genèrica: Es requereix un mínim de 10 hores de formació genèrica (online) sobre les funcionalitats de la plataforma.
- Formació específica: Es requereix un mínim de 20 hores de suport i ajuda a la implantació específica de la nostra instal·lació.

R16. **Suport 24x7**: Es requereix suport 24x7 preferiblement directe del fabricant. El suport pot ser en anglès tot i que es pot valorar que en certes franges horàries es pugui proporcionar suport en castellà i/o català.

6. Presentació de l'oferta tècnica

L'oferta tècnica ha de contenir:

- Una taula amb els requeriments numerats (del R0 al R16) i una explicació de les evidències del compliment de cadascun dels requeriments amb un màxim de 250 caràcters.
- Com a evidències es poden aportar documents addicionals o annexes, en cas de contradicció prevaldrà com a evidència del compliment del requisit la descripció en la taula que haurà d'anar signada com a declaració responsable.

7. Consultes sobre els plecs

L'adreça de contacte per a consultes o aclariments sobre aquesta licitació és: licitacions@upcnet.es