Diputació Tarragona

Subministrament de subscripcions per una plataforma de ciberresiliència i automatització de la infraestructura de xarxa

Plec de Prescripcions Tècniques

Diputació Tarragona

Índex de continguts

1. OBJECTE DEL CONTRACTE

És objecte del contracte el subministrament de llicències per subscripció per dos anys d'una plataforma de ciberresiliència i automatització per a infraestructura de xarxa.

2. DETALL DEL CONTRACTE

La Diputació de Tarragona disposa d'un parc informàtic extens, amb un nombre elevat de dispositius de xarxa (encaminadors, commutadors...) i elements de seguretat (tallafocs, antispam). Es requereix disposar d'un sistema centralitzat i automatitzat de la gestió de la seguretat, la configuració, el compliment normatiu i el cicle de vida d'aquests dispositius.

2.1 REQUERIMENTS TÈCNICS

Es subministraran llicències per subscripció de programari per a gestionar fins a dispositius de xarxa i equips de seguretat. Aquest programari es desplegarà en forma de màquina virtual a l'hipervisor de la Diputació de Tarragona. La solució proposada haurà de complir, com a mínim, els requeriments tècnics següents:

1) Gestió automatitzada del cicle de vida dels dispositius

- Inventari i descoberta dels dispositius de xarxa.
- Realització automatitzada de còpies de seguretat de configuració.
- Validació de còpies de seguretat i possibilitat de restauració dels dispositius per a una recuperació senzilla i controlada.

2) Gestió multivendor i integracions amb eines corporatives

- La solució ha de suportar la gestió i automatització (inventari, còpia/restauració, verificació, actualització/pegats i execució d'operacions) de dispositius de xarxa de múltiples fabricants, incloent com a mínim els següents fabricants de dispositiu:
  3Com, Allot, Avaya, Barracuda, Blue Coat, Brocade, Check Point, Cisco, Citrix, Dell, F5, Fortinet, HPE, Infoblox, Juniper, NetApp, Oracle i Perle.

- Ha d'existir un mecanisme per afegir nous models (via fabricant) i compromís d'actualització del catàleg.

- La solució ha de disposar de mecanismes d'integració (connector nadiu, API REST i/o exportació d'esdeveniments) amb eines corporatives d'operació i monitoratge, incloent com a mínim: SolarWinds (monitoratge) i Splunk (SIEM/logs), o equivalents.

- El licitador haurà d'aportar documentació oficial amb: el catàleg de dispositius i versions suportats, i la descripció de les integracions disponibles (connectors i/o APIs).

3) Gestió del compliment normatiu i de polítiques

- Execució de verificacions de compliment sobre els dispositius per avaluar la resiliència i detectar desviacions de configuració.

- Capacitat de correcció automàtica (remediació) de configuracions no conformes per alinear-les amb: estàndards normatius del sector, i polítiques i configuracions internes.

4) Integritat i seguretat de la infraestructura de xarxa

- Identificació proactiva d'exposicions actives i mitigació de vulnerabilitats.

- Possibilitat de mitigar mitjançant: canvi de configuració, i/o correcció de la vulnerabilitat mitjançant actualització del programari del dispositiu.

5) Traçabilitat i auditoria d'accessos i accions

- Registre de sessions i d'accions per facilitar la traçabilitat, l'auditoria i la revisió posterior.

Arquitectura i desplegament

6) Arquitectura distribuïda i escalabilitat

- La solució s'ha de proporcionar amb una arquitectura distribuïda, amb possibilitat de separar com a mínim els rols de consola/gestió i processament/execució de tasques (p. ex. workers/proxies/collectors), de manera que permeti l'escalabilitat horitzontal afegint nous nodes quan augmenti el nombre de dispositius gestionats o la càrrega de treball.

- La solució ha de ser escalable tant en capacitat (nombre de dispositius/actius) com en rendiment (execució concurrent de tasques), i ha d'admetre l'ampliació sense interrupcions significatives del servei.

7) Plataforma i format de lliurament

- La solució ha d'estar basada en GNU/Linux, tant pel que fa al sistema operatiu de la plataforma com als seus components principals.

- La solució s'ha de lliurar en forma de màquina virtual preconfigurada (appliance) desplegable en un hipervisor de virtualització de l'organització, i ha d'incloure imatge de desplegament compatible amb entorns de virtualització habituals (OVF/OVA o format equivalent),

- El desplegament ha de ser compatible amb VMware vSphere/ESXi (versió 8 o superior) mitjançant imatge OVA/OVF.

Llicències

Es subministraran llicències per diferents funcionalitats, segons la necessitat i amb la següent quantitat màxima prevista:

Tipus de llicència	Quantitat màxima prevista
Còpia de seguretat equips de xarxa	120
Còpia de seguretat equips de seguretat	15
Accés remot	10
Auditoria de compliment de xarxa	5
Gestió de vulnerabilitats	5

1) Còpia de seguretat equips de xarxa

Llicència per inventariar/fer còpies de seguretat/validar/restaurar dispositius catalogats com a "simples": equips de xarxa amb fluxos de backup/restore més directes com routers i switchos.

2) Còpia de seguretat equips de seguretat

Llicència per inventariar/fer còpies de seguretat/validar/restaurar dispositius catalogats com a "complexos", que són equips de seguretat o serveis amb fluxos de backup/restore i automatitzacions multi-pas: firewalls, proxies, load balancers, VPN, etc.

3) Llicència d'Accés remot

Llicència per connectar al terminal del dispositiu des de la consola de la plataforma (accés interactiu) i executar scripts/comandes des del terminal.

4) Llicència d'Auditoria de compliment de xarxa

Llicència per auditoria/validació de compliment i remediació:

- Definició de regles (estàndards i polítiques internes)
- Biblioteca de regles predefinides (p. ex. CIS, PCI, HIPAA, NIST, STIG, etc.) i capacitat de fer-ne de propis.
- Execució periòdica per detectar no-compliments.

- Remediació: corregir automàticament o bé generar evidència i/o tickets per remediació manual.

5) Llicència de Gestió de vulnerabilitats

Llicència de gestió de vulnerabilitats integrat amb inventari i automatització:

- Correlacionar inventari dinàmic de dispositius amb una font d'intel·ligència de vulnerabilitats.
- Descobriment de vulnerabilitats, prioritzar CVEs segons perfil/risc i establir un flux de remediació (incloent automatitzar nivells de remediació).
- Funcionalitats de seguiment com distingir CVEs obertes vs mitigades i reporting/auditoria associada.

2.2 PROVA DE CONCEPTE DE LA SOLUCIÓ (POC)

La Diputació de Tarragona es reserva el dret a sol·licitar una Prova de Concepte de la solució ofertada, si ho considera necessari, per poder verificar el compliment dels requeriments i funcionalitats demanades.

La prova es realitzarà sobre un entorn de com a mímin10 dispositius 10 fabricants diferents, demostrant:

- Còpia de seguretat massiva + verificació (execució programada i sota demanda)
- Restauració dels dispositius
- Una actualització d'OS/firmware amb pre/post checks i gestió d'errors
- Una comprovació de compliance (baseline(política) i remediació automàtica
- Un informe d'auditoria exportable

El joc de proves s'entregarà em el moment de realitzar la PoC, un cop accedit a l'entorn de demostració, i haurà de ser resolt en el temps que duri la prova que serà de 2 a 4 hores en funció del temps requerit.