Consorci
Administració Oberta
de Catalunya

Plec de prescripcions tècniques per l’adquisició i manteniment de solució EDR.

Generalitat
de Catalunya

Consorci de governs locals
per a la societat de la informació

Continguts

1. Introducció 3

2. Infraestructura a protegir 4

3. Detalls de la provisió de la solució EDR 5

4. Requeriments de la solució EDR 6

1. Introducció

El Consorci AOC té un parc informàtic heterogeni:

- diversos DataCenter amb servidors des d'on allotja i ofereix els serveis
- servidors i equips ubicats a oficines amb serveis centralitzats.
- equips d'usuari sobretot portàtils

Per poder donar els serveis amb unes condicions de seguretat adequades, cal que:

- tots els servidors de cada DataCenter
- tots els servidors ubicats a oficines
- i tots els equips d'usuari

disposin d'una solució de seguretat al mateix dispositiu local, capaç d'analitzar i detectar amenaces en temps real amb unes funcionalitats de seguretat avançades.

L'objecte del contracte es:

- L'adquisició/aprovisionament d'una solució EDR, amb el llicenciament necessari durant el període de vigència, incloent el suport per la posada en marxa i la posterior explotació de la solució davant amenaces i events de seguretat.

2. Infraestructura a protegir

La infraestructura a protegir consta de:

- Servidors ubicats a Data Centers de Cloud Public (AWS i Azure).
- Servidors ubicats a Data Centers de Cloud Privat (Nexica i Mediacloud).
- Servidors ubicats a infraestructura d'oficines centrals (Vmware).
- Equips d'usuaris amb plena mobilitat.
- S'estima que en total els dispositius a protegir serien d'uns 500 endpoints.

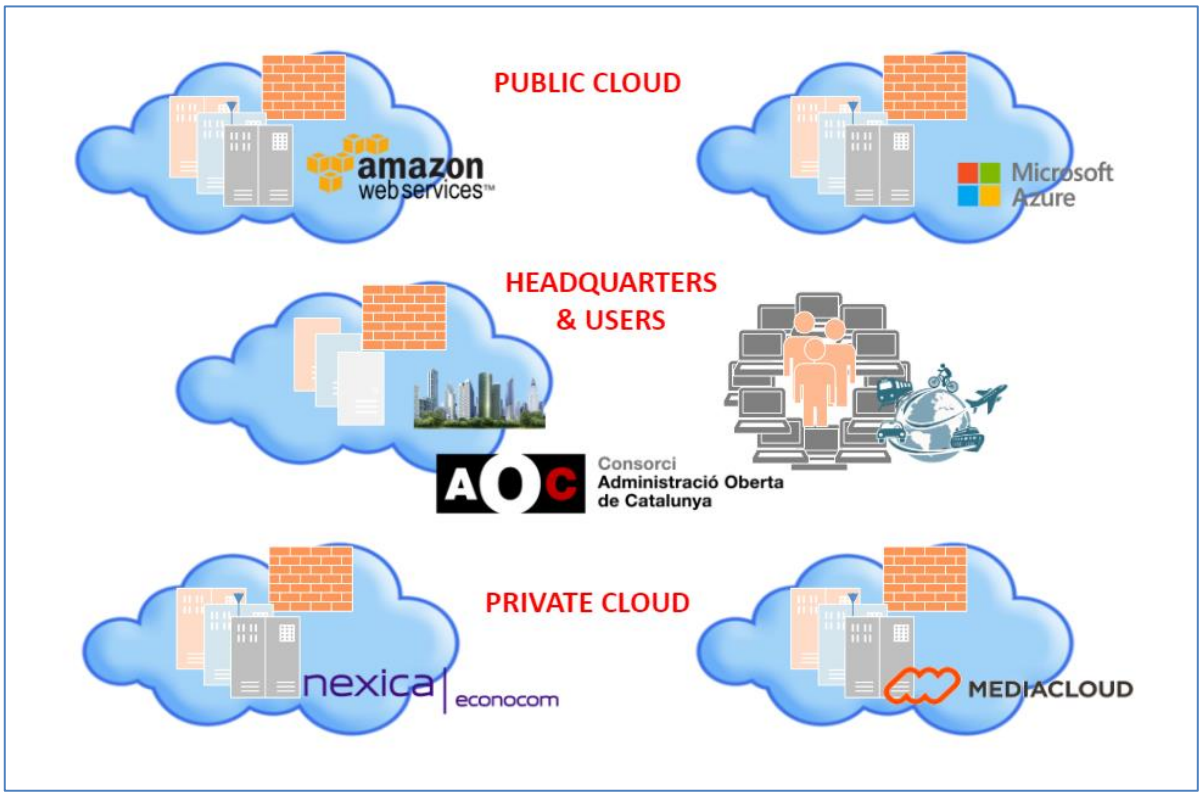


Diagrama orientatiu.

3. Detalls de la provisió de la solució EDR

El fabricant tecnològic de la solució haurà de:

- Aprovisionar la infraestructura necessària per disposar dels quadres de comandament de la solució.
- El llicenciament necessari per protegir fins a un total de 500 dispositius/endpoints.
- Donar el suport necessari per desplegar tots els agents amb una configuració (setup) inicial per tal de deixar la solució treballant en un estat òptim, havent treballat prèviament tots i cadascun dels casos i events detectats en la fase de creació del "*baseline*" o comportament habitual de la infraestructura.
- Proveir el suport proactiu davant d'amenaces i events de seguretat:
    - Monitoratge i resposta en format 27 hores els 7 dies de la setmana (24x7)
    - Incloent triatge i revisió forense en cas necessari
    - Creació de polítiques que calguin per donar resposta
    - Establir els escalats que es puguin acordar entre client i proveïdor

  La finalitat és que hauran d'analitzar, respondre, contenir i corregir incidents de seguretat per reduir el temps de resolució per limitar el seu impacte.
- El suport el tindrà que donar exclusivament el fabricant tecnològic de la solució ja que tindran que ser analistes sènior per completar el nostre servei de SOC.

4. Requeriments de la solució EDR

Es requereix una solució avançada de nova generació de protecció de l'end-point, que analitzi en temps real i de manera automàtica el lloc d'usuari i servidors, mitjançant una aproximació no basada en firmes sinó en l'anàlisi de comportaments, per bloquejar codi maliciós i exploits tant coneguts com desconeguts.

Ha d'incorporar funcionalitats tant de detecció com de resposta automatitzada davant les amenaces, constituint una solució d'Endpoint Detection and Response (coneguda pel seu acrònim EDR).

La solució ha de contemplar 500 llicències entre llocs d'usuari i servidors per una vigència establerta de 3 anys.

La solució d'EDR ha de complir les característiques mínimes següents:

- Capacitat de detecció en temps real davant d'activitats potencialment malicioses, fins i tot quan l'equip no està connectat a la xarxa, incloent-hi el monitoratge de processos en execució, inicis i aturades, i interaccions entre processos, canvis maliciosos al registre, connexions de xarxa i activitats sospitoses associades a fitxers DLL.

- Capacitats de prevenció (preexecució) i desactivació (postexecució) d'amenaces, prevenint l'execució de fitxers, DLLs i aplicacions malicioses, i evitant l'establiment de connexions malicioses. Ha de permetre la definició de llistes blanques i negres per personalitzar -mitjançant exclusions- aquestes proteccions (per hash, nom i/o ruta d'arxiu, o per aplicació, incloent dades de versió i fabricant), així com marcar fàcilment, tant manual com automàticament, determinada activitat com a fals positiu, evitant a més que hi hagi deteccions similars. Addicionalment, s'han de poder definir “llistes blanques” d'aplicacions, processos i fitxers considerats com a segurs, de manera que no disparin esdeveniments de seguretat.

- Capacitat de resposta automatitzada en temps real davant d'incidents, basada en conjunts d'accions orquestrades, per permetre com a mínim: interrompre processos, eliminar fitxers, restaurar la configuració base (com registres del sistema modificats), i aïllar de la xarxa processos individuals o el dispositiu de manera completa.

- Les capacitats de resposta han d'incloure la possibilitat de definir scripts personalitzats per a la interacció amb qualsevol element (via API, per exemple), amb independència del fabricant. Aquests scripts de resposta s'han de poder seleccionar en funció de la severitat de l'esdeveniment de seguretat detectat i des de la mateixa secció de la consola on es configurin la resta de respostes automatitzades.

- S'ha de proporcionar una resposta eficaç en la prevenció d'exploits i codi maliciós (malware) fins i tot en condicions d'absència de connectivitat amb els servidors d'administració i/o recursos basats en el núvol.

- Avaluació de vulnerabilitats i parxejat virtual, amb capacitat per al descobriment d'aplicacions vulnerables mitjançant l'anàlisi de les comunicacions, incloent-hi la classificació de reputació i el detall dels codis CVE aplicables, i de parxejat virtual, inhabilitant l'accés a la comunicació amb l'exterior d´aplicacions vulnerables.

- Ha d'oferir protecció almenys davant dels escenaris d'atac següents:
    - Escalada de privilegis, com per exemple per substitució de programes legítims del Sistema Operatiu, escalada de privilegis del nucli (evitant que un atacant utilitzi la informació d'un altre procés amb més privilegis per executar un procés maliciós amb permisos del sistema), o intents de inclusió d'usuaris en grups d'administradors del sistema operatiu.
    - Malware conegut (a través d'executables o l'obertura de documents maliciosos, fins i tot sense coneixement previ dels mateixos ni deteccions anteriors) i desconegut, així com intents d'explotació de vulnerabilitats de dia 0, detectats a través del seu comportament, que en permeti la aplicació immediata de mesures de remediació.
    - Ransomware: s'han de bloquejar i aplicar de manera immediata mesures de remediació davant la detecció de comportaments de tipus ransomware, com ara processos que llegeixen o escriuen massa fitxers en un període de temps molt curt, i/o que en modifiquin els valors d'entropia (mitjançant la seva compressió o xifratge, per exemple).
    - Dispositius USB: s'han de poder permetre dispositius de confiança (registrant la seva activitat), així com configurar polítiques d'actuació (com la prevenció immediata d'interacció) amb altres de maliciosos o desconeguts.
    - Scripts: s'ha de detectar i impedir l'execució de scripts maliciosos (almenys PowerShell, Cscripts, macros d'Office), així com evitar que un procés inicïi un

procés legítim que es pugui fer servir amb fins maliciosos (com els motors de scripts).
  - Robatori de contrasenyes, protegint els processos on l'atacant pot fer servir eines per obtenir les credencials.

Investigació d'incidents:

- Proporcionar anàlisis forenses detallats sobre les amenaces detectades i atacs desactivats als dispositius, recopilant informació com fitxers i URIs accedits, mòduls carregats, processos executats, etc.

- Mapeig dels comportaments maliciosos detectats conforme a la matriu ATT&CK de MITRE, possibilitat de fer cerques avançades en funció d'aquests comportaments, a més d'altres paràmetres com ara fitxers, processos, etc.

- Període de retenció mínim de 6 mesos per als esdeveniments de seguretat en desplegaments a cloud.

- Possibilitat de recollir tota la telemetria de l'endpoint, amb independència que estigui o no relacionada amb esdeveniments de seguretat, incloent-hi les activitats relacionades amb processos, fitxers, claus de registre i la xarxa.

- Obtenció de logs tipus syslog disponibles per a integració amb un SIEM o SOAR.

- Capacitat per obtenir imatges instantànies o bolcats de memòria, per exemple per a l'estudi de codi maliciós de tipus file-less, així com la recuperació des de l'endpoint de fitxers relacionats amb esdeveniments de seguretat.

- Arquitectura del servei: la solució d'EDR haurà de poder-se desplegar tant en format on-prem com en cloud, valorant-se favorablement l'opció de desplegament mixt per a una protecció òptima dels dispositius tant des de dins de la xarxa corporativa com a fora.

- Compatibilitat de l'agent amb els sistemes operatius i entorns següents:
  - Windows XP SP2/SP3, 7, 8, 8.1, 10, and 11 (32-bit and 64-bit versions)
  - Windows Server 2003 SP2, R2 SP2, 2008 SP2, 2008 R2 SP1, 2012, 2012 R2, 2016, 2019, and 2022

  - MacOS: El Capitan (10.11), Sierra (10.12), High Sierra (10.13), Mojave (10.14), Catalina (10.15), Big Sur (11.x), and Monterey (12.x)
  - Linux: RedHat Enterprise Linux and CentOS 6.x, 7.x, and 8.x, Ubuntu LTS 16.04.x, 18.04.x, 20.04.x server, 64bit only Oracle Linux 7.7+ and 8.2+, Amazon Linux AMI 2 SuSE SLES 15.1
  - Entorns VDI: VMware Horizons 6 and 7 i Citrix XenDesktop 7

- Desplegament, manteniment i requisits de l'agent: els agents s'actualitzaran sense intervenció de l'usuari, i sense necessitat d'interrompre l'activitat del lloc de treball o servidor, i tindran una empremta o impacte molt baix en el rendiment de l'equip, amb una càrrega de CPU inferior al 2%, consumint menys de 120MB de RAM i 100MB d'espai en disc, i amb un consum de trànsit de xarxa no superior als 20 kbps. L'agent ha d'incorporar proteccions anti-tampering, per evitar desactivacions per part tant de l'usuari com d'algun programari maliciós.

Gestió de la plataforma:

- La gestió de la solució ha de poder realitzar-se íntegrament amb un navegador web, sense ser necessari, en cap cas, la instal·lació de programari addicional.

- Ha de proporcionar quadres de comandament que mostrin tant l'estat de seguretat i les amenaces, com la "salut" dels diferents elements de la plataforma.

- Configuració granular de perfils d'accés amb privilegis diferents, així com l'assignació d'usuaris a aquests perfils.

- La plataforma ha de suportar per disseny el login i l'operació en format multi-tenancy (RBAC/Role-Based Access Control).

- Suport RestFull API per desenvolupar les integracions addicionals que es requereixin.

Accés a la plataforma:

- Cal que l'accés tingui mecanismes d'autenticació recolzats en tecnologies MFA/2FA.

- Haurà de poder-se integrar amb el gestor d'identitats del Consorci AOC (AzureAD).

Altres requisits:

- La solució d'EDR ha de poder conviure amb la solució d'AV actual en el moment del desplegament.
- Ha de poder complementar la seguretat global de la solució amb l'execució de fitxers sospitosos/maliciosos en un sandbox per assegurar-ne l'exactitud de l'anàlisi i proporcionar un veredicte addicional.
- El model de llicenciament ha de ser basat en equips protegits i no per altres paràmetres com ara el nombre d'usuaris, CPUs, etc.
- Capacitació a l'eina per part del equip del adjudicatari i/o fabricant al equip designat pel Consorci AOC.

Solvència de fabricant:

- El fabricant propietari de la solució haurà de comptar al seu portfoli global de solucions amb productes certificats per a compliment d'ENS alt en almenys 4 categories del Catàleg de Productes de Seguretat de les Tecnologies de la Informació i la Comunicació, Guia de Seguretat de les TIC CCN-STIC 105.
- El fabricant propietari de la solució haurà de comptar a la seva cartera global de solucions amb productes certificats per ICSA labs en almenys 4 categories.
- El fabricant propietari de la solució haurà de comptar al seu portfoli global de solucions amb productes posicionats entre els tres primers llocs del quadrant màgic de Gartner en almenys 2 categories.

Rafael Carrasco Caballero - DNI 43447713T (TCAT)

Firmado digitalmente por Rafael Carrasco Caballero - DNI 43447713T (TCAT)
Fecha: 2023.07.03 15:19:32 +02'00'

Barcelona, 23 de Març de 2023.
Rafael Carrasco Caballero
Cap de Projectes de Seguretat