PLEC DE CLÀUSULES TÈCNIQUES

Contracte relatiu al **Subministrament de llicències de EDR 2025-2028** per Ferrocarril Metropolità de Barcelona, SA; Transports de Barcelona, SA. (en conjunt, TMB).

CPV 48730000-4 Paquetes de software de seguridad

Expedient número: 16076419
Procediment obert

Aprovat en data 10 de Desembre del 2024

Transports Metropolitans de Barcelona

Ernest Costa Lluch
Resp. Sistemes de Ciberseguretat

Prescripcions tècniques

1.1. Objecte i Abast

Aquest document constitueix el plec de requeriments tècnics que ha de regir el contracte de Subministrament de llicències de EDR 2025-2028.

1.2. Situació Actual

Davant el creixement continu dels incidents de ciberseguretat es fa necessari ampliar les mesures seguretat desplegades a TMB de la manera més completa possible, així com disposar de capacitats de resposta ràpida que permetin contenir els incidents de forma ràpida i centralitzada.

TMB forma part de la Xarxa Nacional de SOC (RNS) com a empresa pública i participa en l'ús i compartició de IOCs/IACs (indicadors d'Atac o de Compromís), i per tant, requereix d'una solució que pugui gestionar i alimentar aquest tipus d'informació.

Es requereix d'una solució avançada de nova generació de protecció de l'Endpoint, 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.

En l'escenari actual d'incidents de seguretat en entitats públiques i privades ha de manifest que, degut a l'ús de credencials d' usuari o servei obtingudes de forma il·lícita, les capacitats d'atac dels ciberdelinqüents s'han vist potenciades de exponencial, en poder realitzar propagació i desplaçament lateral a les xarxes de la l'organització.

Les credencials d'usuari i servei en l'escenari actual de TMB, en el que existeixen múltiples instàncies de Directori Actiu associades als diferents serveis amb diferents polítiques de gestió, han esdevingudes elements crítics a protegir per garantir la seguretat dels diferents entorns.

Per tot això, es requereix un control de les identitats i per tant, la inclusió d'una solució ITDR que funcioni de manera integrada amb el EDR i les dades puguin ser correlades per la mateixa plataforma. La solució també és necessari que pugui ingestar altres fonts sobretot la de SSE/CASB per poder correlar tota la informació de l'ús que fan els usuaris i relacions entre aquests events i els de EDR i ITDR.

Perquè tant la implementació inicial de la solució com també que durant la vida del contracte es tingui un acompanyament i seguiment, es requereix també un Account Manager del fabricant que també facilitarà i agilitzarà possibles incidents donant-li la prioritat necessària, i per assegurar una correcta implementació.

Per poder fer la integració amb les solucions de les que disposa TMB, caldran Serveis Professionals del fabricant que garanteixin un coneixement expert per realitzar aquesta configuració amb èxit.

I per atendre als casos d´ús d'aplicacions de TMB que necessiten realitzar anàlisi de fitxers en trànsit al núvol, es requereix d'una solució d'escaneig via API per poder enviar peticions i rebre el veredicte de si son legítims o no.

2. Prestacions Objecte del Contracte

L'objecte del present Plec de prescripcions Tècniques (PPT) es la definició del Subministrament de llicències EDR al Núvol.

- **Subscripció a la solució EDR per 5.300 equips** (1.000 servidors i 4.300 equips client) **+ 500 equips XP** des de l'1-Agost-2025 a l'31-Juliol-2028.
- **Subscripció a la solució ITDR en modalitat Detecció** amb capacitats d'auditoria del estat de la configuració del DA i la utilització dels protocols d'autenticació, classificació de credencials privilegiades o no privilegiades, endpoints i valoració de risk per entitat identificada (Postura de seguretat de la identitat i detecció d'amenaces) per **9.000 usuaris** des de l'1-Agost-2025 al 31-Gener-2027 i **Subscripció a la solució ITDR en modalitat Protecció** en temps real davant de l'abús de credencials valides amb motors d'inspecció de comportament habitual i amb accions granulars com la utilització de factors dobles de validació, reseteig de contrasenyes o la inclusió de credencials a llistes de credencials sota sospita **per 9.000 usuaris** des de l'1-Febrer-2027 al 31-Juliol-2028**.**
- **Technical Account Manager (TAM)** del Fabricant que faci un acompanyament durant el desplegament de la solució amb gestió del contracte com de l'aplicació de les bones practiques de configuració inicial. Un cop enllestit el desplegament, el servei de TAM serà el punt de contacte tècnic per els dubtes de l'operació, bones pràctiques i realitzarà comprovacions periòdiques de l'estat de protecció del parc informàtic i la seva configuració com durant tot el contracte des de l'1-Agost-2025 a l'31-Juliol-2028.
- **Serveis Professionals del fabricant (80h)** per poder realitzar la integració d'una font SSE/CASB en la mateixa plataforma repositori de tota la telemetria del EDR amb el ITDR, així com la integració amb el Identity Provider de TMB (Keycloak)
- **15GB diaris amb retenció 6 mesos a la plataforma** per incorporar alertes d'una font SSE/CASB al núvol perquè la plataforma pugui identificar incidents de seguretat correlant la informació amb la del EDR i sobretot del ITDR des de l'1-Agost-2025 a l'31-Juliol-2028.

- **Anàlisis immediat de fitxers via API** per a fins 25.000 fitxers al mes des de l'1-Agost-2025 a l'31-Juliol-2028.

La contractació és per una **durada de 3 ANYS** (**1-Agost-2025 al 31-Juliol-2028**).

La oferta haurà d'incloure qualsevol altre element no descrit expressament en la licitació i que sigui necessari per al correcte funcionament del programari subministrat.

Tots els requisits de seguretat del Plec, han de ser coberts per un únic fabricant de seguretat, una única plataforma, un únic repositori d'informació i una única consola en modalitat cloud. És a dir, la solució proposada ha de facilitar l'accés a totes les funcionalitats des d'una consola amb un únic portal web al núvol que reculli totes les capacitats.

EDR

Requeriments ENS sobre el producte:

- La solució haurà de ser un producte certificat per a compliment d'ENS nivell ALT en el Catàleg de Productes de Seguretat de les Tecnologies de la Informació i la Comunicació, Guia de Seguretat de les TIC CCN-STIC 105 de la Familia EDR.

- La solució haurà de ser un producte certificat per a compliment d'ENS nivell ALT en el Catàleg de Productes de Seguretat de les Tecnologies de la Informació i la Comunicació, Guia de Seguretat de les TIC CCN-STIC 105 de la Familia EPP (Endpoint Protection Platform)

Requeriments de compliment:

- Els serveis en el cloud públic del fabricant (el seu proveïdor d'infraestructura al núvol) han d'estar allotjats en datacenters de la Unió Europea i disposar de la certificació de ENS nivell ALT. Addicionalment, es requereix pel fabricant, disposar de la certificació "CSA-STAR level 2 ", vinculada a garantir la seguretat de la solució EDR en cloud pública.

- La solució haurà d'estar posicionada en el quadrant de líder en l'últim Gartner® Magic Quadrant™ for Endpoint Protection Platforms (actualment de Juliol 2024). D'aquesta manera es demostra que es tracta d'una solució avançada i de referència en el mercat.

Descripció de la solució d'EDR que 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 [] 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. Aquesta execució ha de ser capaç de demanar confirmació humana per correu, teams o slack per dur a terme les accions si així es requereix.

- 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 temporal de connectivitat amb els servidors d'administració i/o recursos basats en el núvol.

- S'ha de poder gestionar equips que no tinguin accés directe a Internet i per tant amb la consola SaaS del producte.

- 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).
- 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 permetre connectar només dispositius de confiança (registrant la seva activitat), així com configurar polítiques d'actuació per categories de dispositius, per fabricant o per identificador únic(SN) que permetin la prevenció immediata d'interacció amb altres dispositius connectats per USB desconeguts amb possible contingut maliciós o que permetin extreure informació de manera no autoritzada.
- Scripts: s'ha de detectar i impedir l'execució de scripts maliciosos (almenys PowerShell, Cscripts, macros d'Office), així com evitar que un procés iniciï 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 neutralitzats als dispositius, recopilant informació com fitxers i connexions de xarxes realitzades, mòduls carregats, processos executats, etc. i tota la informació forense de rellevància que permeti a l'equip de CSIRT investigar les causes, vies d'entrada, atribució, etc, vinculades a l'atac de manera que pugui aplicar mesures a futur per evitar noves ocurrències.

- 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, severitat, finestra de temps, nom de màquina, atribució d'adversari, etc.

- La retenció de la informació rellevant associada a les Deteccions del EDR haurà de ser de mínim 90 dies. De la mateixa manera que la informació detallada de les activitats enregistrades del dispositiu restarà disponible durant una setmana sencera per permetre cerques d'amenaces.

- Respecte a la informació del inventariat del actius protegits per l'EDR, la informació rellevant de les propietats del dispositius protegits ha d'estar disponible mínim 45 dies en funció de la rellevància de la mateixa. Considerant com essencial els valors identificatius dels dispositius.

- 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.

- Possibilitat de reenviar tota la telemetria relacionada amb la detecció d'un incident, cap a una solució de broker/Kafka instal·lada on-premise a TMB.

- Capacitat per obtenir mitjançant un access remot, de bolcats de memòria de procces o complert, 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 equips físics, com virtuals (i en també VDIs persistents i no persistents).

- Solució amb un únic agent en els equips que proporcioni totes les funcionalitats (activades en el moment del desplegament o si s'activen posteriorment) de les que pugui disposar la solució EDR.

- Compatibilitat de l'agent amb els sistemes operatius Windows següents, amb les mateixes funcionalitats per totes elles:

- Windows Server 2008 R2 SP1, 2012, 2012 R2, 2016, 2019, and 2022
- Windows 7 32bit, 7 64bit, 10, i 11 (versions 32-bit i 64-bit)
- Entorns VDI

- Disposar d'un agent per poder desplegar en equips Legacy (en aquest cas pot ser un agent específic):

- Windows Server 2003 SP2
- Windows XP SP2/SP3, 8, 8.1

- Compatibilitat de l'agent amb els sistemes operatius Linux (com a mínim pels següents), amb les mateixes funcionalitats per totes elles:

- Linux: RedHat Enterprise Linux and CentOS 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

- 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 Mb/dia. L'agent (Windows) ha d'incorporar proteccions anti-tampering, per evitar desactivacions per part tant de l'usuari com d'algun programari maliciós.

- Per garantir que el desplegament de la solució no produeix afectació a la disponibilitat i continuïtat dels serveis productius, Es requereix que la instal·lació completa i les actualitzacions de l'agent en cada lloc de treball o servidors es puguin fer sense reinici i sense intervenció de l'usuari.

- L'agent ha de poder conviure amb la solució microCLAUDIA del CCN, mantenint totes les seves funcionalitats, no produint incompatibilitats o requeriments de desconnexió de capacitats de la solució proposada o de la solució de microCLAUDIA.

- Per simplificar, agilitzar i minimitzar el temps i complexitat de desplegament,i errors durant la instal·lació, Es requereix que l'agent software a desplegar i el seu instal·lador, sigui el mateix per cada família de Sistemes Operatius, entenent families com Windows, Windows Server, Linux excepte IoT (Win XP

- Es requereix que la solució disposi de capacitats de securització basades en tokens o similars per administrar i permetre o bloquejar la desinstal·lació de l'agent en els endpoints.

- L'agent de endpoint ha d'admetre actualitzacions de software controlades per polítiques des de la plataforma en el núvol.

- L' agent ha d'estar habilitat per permetre que es realitzin accions d'alerta i resposta a incidents en temps real quan els usuaris estiguin en itinerància.

- La telemetria dels endpoints així com els detalls forenses, han de poder enviar-se a la plataforma cloud en temps real. En cas de que temporalment no hi hagi connectivitat entre la consola cloud i el endpoint per l'enviament de la telemetria, l'agent instal·lat s'encarregarà de guardar i custodiar aquesta informació fins que retorni aquesta connectivitat i pugui realitzar-se l'enviament a la plataforma cloud.

- La instal·lació de l'agent ha de permetre incloure la parametrització per a arquitectures de xarxa i seguretat basades en proxy.

- Totes les funcionalitats de seguretat han d'estar disponibles independentment de la versió de sistema operatiu i nivell de parches sobre el que es trobi instal·lat l'agent per els sistemes operatius suportats per el sensor.

Gestió de la plataforma:

- La plataforma ha de poder oferir una configuració tipus multi-organisme (multi-tenant) que permeti oferir visibilitat completa i capacitat d'actuació i configuració globals des del tenant principal (tenant pare).

- 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.

- Es requereix la possibilitat d'assignar etiquetes informatives (tags) referents a l'entorn del desplegament en el moment de la instal·lació de l'agent o posteriorment.

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

Es requereix les integracions i casos d'ús amb les eines del CCN-CERT (REYES, LUCIA).

- La solució ha de proporcionar la capacitat d'agrupar hosts basats en identificadors de host, OU de Active Directory o etiquetes per l'aplicació de polítiques en el moment de la instal·lació de l'agent o posteriorment.

- Es requereix que la consola mostri una puntuació de risc de les amenaces en temps real. Aquesta puntuació de risc ha de ser dinàmica i evolucionar en temps real en funció de les diferents mètriques que s'utilitzin pel seu càlcul, permetent als administradors, conèixer en tot moment l'estat i severitat de les amenaces i atacs.

Funcionalitats de recerca activa d'amenaces (threat hunting):

La plataforma proposada ha de proporcionar la capacitat de fer recerques d' amenaces (threat hunting) sobre la informació de telemetria generada pels endpoints.

Almenys, ha de disposar de les especificacions i funcionalitats següents:

- La solució proposada ha de supervisar l'activitat de processos dels endpoints enviant de forma contínua i en temps real informació d'esdeveniments i detalls forenses a la plataforma cloud. S'ha de permetre l'exportació de la informació de telemetria recopilada a formats comuns com CSV, XML i raw.

- La solució ha de mostrar informació detallada de cada endpoint pel que fa a processos i serveis, comandaments executats per eines d' administració, activitat de Scripts, activitats relatives a registre, tasques programades i activitats de xarxa.

- La solució ha de proporcionar la capacitat de realitzar una recerca d'esdeveniments sense processar utilitzant un llenguatge de consulta estructurat a través de tota la telemetria de esdeveniments recopilada (apilament de dades). La solució ha de proporcionar consultes predefinides per a totes les activitats relacionades amb l'usuari i el punt final així com artefactes forenses. Les recerques s'han de poder realitzar utilitzant la interfície d' usuari.

Aquestes recerques han de poder incloure, almenys, hashs específics, noms de fitxer, paràmetres de línies de comandaments, adreces IP, dominis, esdeveniments sense processar, claus de registre, etc.

- Ha de permetre les recerques en la informació generada per tota la base sense produir afectació als endpoints o incrementar els consums de recursos maquinari de l'agent instal·lat.

- La solució ha de proporcionar informes de recerca d'amenaces i anàlisis de línies de temps, així com proporcionar un informe per demostrar la línia de temps completa dels esdeveniments que ocorren en un host. La solució ha de proporcionar un informe que demostri la cronologia completa dels esdeveniments d'un procés.

Es requereix les capacitats de la solució per a la realització de la recerca d'amenaces, en concret es requereix la granularitat i varietat dels esdeveniments de telemetria recopilats, les capacitats del motor d'emmagatzematge i recerca en la realització de consultes específiques, regles o recerques predefinides, integració amb les capacitats d'intel·ligència d'amenaces del fabricant.

Es requereix que el número de consultes sobre el repositori d'informació sigui il·limitat.

Les cerques han de poder fer-se sobre les dades en brut directament i no nomes des de dades indexades.

SOAR:

- La plataforma ha d'incloure un SOAR per poder automatitzar tasques de resposta de forma integrada tant d'EDR , d'ITDR i/o Cloud.

- Automatització i orquestració mitjançant la definició de diagrames de flux a la pròpia consola facilitant la resposta automàtica davant els esdeveniments disparadors, planificats o sota demanda.

- El fluxe de treball (workflow) ha de ser personalitzable podent utilitzar les integracions amb altres, tinguent la capacitat de modificar la lògica del fluxe de treball (p.e. demanar un consentiment d'un usuari).

- En cas d'una interacció amb un usuari per una confirmació, s'ha de preveure en el fluxe que l'usauri no respongui passat un temps definit al fluxe.

- Ha de permetre l'automatització de tasques, amb integració amb altres fabricants de l'ecosistema, amb la utilització dels accessos remots als sistemes protegits per recollir fitxers, executar comandes o scripts o mitigar compromisos.

- La solució no pot incorporar restriccions d'execució de workflows, ni límit d'administradors, ni de nombre d'execucions en paral·lel.

- El SOAR ha d'incloure plantilles de casos d'us per realitzar les automatitzacions.

Accés a la plataforma:

- La plataforma ha de disposar de control d'accés amb doble factor d'autenticació, suportar SSO (SAML 2.0) per la seva integració amb els sistemes de gestió d'identitats de TMB, múltiples usuaris i diferents rols per permetre l'accés a diferents àmbits o funcionalitats.

- Haurà de poder-se integrar amb el gestor d'identitats de TMB (AzureAD/EntraID + Keycloak).

- La plataforma ha de proporcionar un registre d'auditoria de l'activitat dels usuaris, incloses les tasques de gestió i resposta a incidents. Aquesta informació d'auditoria ha de ser accessible des de la pròpia consola o a través de API.

Altres requisits:

- La solució d'EDR ha de poder conviure amb la solució d'AV actual en el moment del desplegament (Trellix ENS+EDR).

- El model de llicenciament EDR ha de ser basat en equips protegits, i no per altres paràmetres com ara el nombre d'usuaris, CPUs, etc.

- Es requereix la inclusió de les capacitats d'automatització i orquestració preferentment en la mateixa consola, essent valorables aquelles solucions que proposin una simplificació en una única consola, entenent-se com a portal web únic en el que es recullin totes les capacitats.

- Es requereix les capacitats i funcionalitats d'automatització, així com la simplificació dels mecanismes de generació i la inclusió d'aquestes funcionalitats en la plataforma única, com poden ser: creació de fluxes de

treball i playbooks d'automatització mitjançant interface visual en la pròpia plataforma i condicions de presa de decisions, entre d'altres.

Funcionalitats preventives i de detecció:

- La solució proposada ha de ser una plataforma de seguretat d'última generació que utilitzi tècniques d'aprenentatge automàtic/machine learning per la prevenció prèvia a la execució de malware conegut i desconegut.

Es requereix que entre les capacitat de detecció i prevenció s'inclogui la detecció de tècniques, tàctiques i procediments i els indicadors d'atac (IoAs) susceptibles de ser utilitzats per agents maliciosos.

- S'ha de permetre posar en quarantena el malware detectat i oferir la possibilitat de restaurar o posar en llista blanca els arxius de quarantena directament des de la plataforma de gestió.

- Es requereix la possibilitat d'enviar arxius per part de l'EDR a un entorn de detonació (sandbox) pel seu anàlisis automàtic mitjançant l'ús d'anàlisis estàtics i dinàmics avançats.

- Ha de disposar de la capacitat per la generació de llistes blanques i negres de hashes d'arxius personalitzables com IOCs.

- La plataforma ha de proporcionar capacitats de detecció basades en l'anàlisi de comportament posterior a l'execució d'un malware, permetent la protecció contra les activitats habituals del ransomware (xifrat d'arxius, eliminació d'arxius shadow, etc.) tenir capacitats de mitigació dels canvis realitzats pel malware.

- Es requereix una detecció i resposta segons l'Indicador d'Atac (IoA) mapejat al marc MITRE ATT&CK o similars.

- La solució ha de ser capaç de prevenir l'ús maliciós de Powershell i els atacs amb scripts.

- La solució ha de proporcionar la capacitat de crear regles de detecció i bloqueig personalitzades basades en artefactes relacionats amb processos, arxius, connexions de xarxa i dominis.

- La solució ha de detectar les tècniques habituals de robatori de credencials.

- La solució ha de facilitar accions de resposta que incloguin l'aïllament del endpoint de la xarxa (persistint la desconnexió després d'un reinici) o la connexió remota interactiva amb el endpoint. Durant aquesta connexió, els administradors han de poder realitzar accions d'anàlisi, contenció, resposta i remediació.

- La solució ha de correlacionar i presentar automàticament la telemetria i les metadades (IoC) relacionades amb l'atac en una línia de temps. Per exemple, arguments de línia de comandes, escriptures d'arxius, sol·licituds DNS, connexions IP, etc.

- La solució ha de suportar la creació de IoC (hashes, IP, dominis i url) via consola que seran utilitzats durant tot el cicle de detecció/resposta de la plataforma.

- La solució ha de proporcionar capacitat per enviar arxius a sistemes remots, executar arxius, executar scripts, matar processos, ajustar claus de registre i altres tasques necessàries durant la resposta a incidents.

- La consola ha d'oferir opcions de filtratge de les deteccions segons diferents criteris, com severitat i data, entre d'altres.

- La solució ha d'oferir la possibilitat d'assignar a un analista, el treball de resposta sobre una detecció.

- Es requereix que la solució permeti integrar informació de tercers relativa als indicadors de la detecció (per exemple, informació a VirusTotal).

- La solució ha d'oferir una vista que permeti observar l'arbre de processos relacionat amb una detecció.

- La solució ha d'oferir a un analista capacitats d'inclusió de comentaris relatius a les tasques realitzades de resposta a una detecció.

- La solució ha d'oferir detecció d'amenaces basada en comportament i intel·ligència d'amenaces que permeti alertar i bloquejar amenaces i que addicionalment ofereixi informació relativa a:

    - Vector d'entrada utilitzat per l'atacant.
    - Comprensió de les tàctiques i tècniques utilitzades per l'atacant.
    - Període temporal en el que s'enmarca l'amenaça.
    - Actius compromesos.
    - Contextualització dels processos seguits per l'atacant al llarg de la cadena d'atac.

ITDR

La solució ITDR ha de complir les característiques mínimes següents:

S'ha de poder integració amb Keycloak i Azure AD/Entra ID.

- Ha de proporcionar la salut de la configuració de seguretat del DA/bastionat:
    - Nivell de risc del DA
    - Riscos per severitat
    - Riscos amb probabilitat d'explotació (per prioritzar)
    - Recomanació de cada risc
- Identitats privilegiades
    - Atributs per cada identitat que mostrin diferents riscos/característiques
    - Nivell de risc per identitat
    - Passwords compromesos "en temps real" que han estat filtrats
- Polítiques de protecció en temps real bloquejant certes accions:
    - MFA challenge
    - Llista sospitosos
    - Block
- Detectar intents de inclusió d'usuaris en grups d'administradors del sistema operatiu.

Funcionalitats de la solució ITDR de protecció contra atacs basats en identitat:

Atesa l'especial rellevància dels mecanismes de gestió d'identitats en el control, detecció, contenció i prevenció d'incidents de seguretat Es requereix els requisits següents:

- Es requereix funcionalitats de seguretat específiques orientades a la protecció de identitats. Específicament capacitats de seguretat vinculades a la protecció de entorns de Directori Actiu, així com detecció d'atacs basats en vulnerabilitats de protocols d'autenticació. Així com funcionalitats que permetin detectar i bloquejar l'ús il·lícit de credencials, intents de suplantació d'identitat, propagació lateral, d'accés a recursos i actius crítics. Així mateix, Es requereix que les capacitats de detecció i prevenció puguin aplicar-se en arquitectures de Directori Actiu en format on-premise (infraestructura, serveis de directori actiu i controladors de domini en entorns propis de TMB), cloud (serveis i infraestructura de Directori Actiu ubicats en entorn de núvol públic EntraID) o híbrids (convivència de les dues modalitats anteriors).

- Es requereix que les capacitats de seguretat contra atacs basats en identitat utilitzin el mateix agent únic que en la resta de les funcionalitats demanades (mateix agent que el EDR). No seran vàlides solucions que requereixin el desplegament de solucions addicionals que requereixin la instal·lació de serveis, servidors o entorns addicionals en l'àmbit de TMB o en entorns de núvol públic.

- Es requereix que la solució proposada pugui permetre la definició i implantació polítiques de detecció, bloqueig o accés condicional basades en desviació de comportament respecte a la línia base de comportament d' usuari. Així mateix, es requereix que la solució disposi de funcions d'aprenentatge automàtic de l'entorn, permeti fer seguiment dels comportaments al llarg del temps i aplicar polítiques flexibles que puguin adaptar-se automàticament a mesura que canviïn les circumstàncies de l'entorn.

- Es requereix que la solució proposada inclogui capacitats de descobriment de objectes de directori actiu mostrant informació sobre comptes d' usuari, de servei, comptes privilegiats, etc. facilitant l'aplicació de polítiques i bones pràctiques de l'administració del Directori Actiu. Així mateix, es requereix les capacitats de descobriment i la riquesa de la informació recopilada per la solució. També que la solució faciliti una puntuació de risc processable per a cada objecte/entitat del directori (usuari, compte, dispositiu) que permeti representar la probabilitat d'exposició a una bretxa o un incident, així com informació sobre la postura de seguretat de l'entorn.

- Es requereix que la solució proposada pugui enriquir les capacitats de threat hunting permetent realitzar consultes en la informació de telemetria relacionades amb atributs i esdeveniments del tràfic d'autenticació, atributs d'usuaris, dispositiu, mètodes d'accés, canvis en el compte, etc. Es requereix les capacitats afegides per aquestes funcionalitats d'enriquiment de les funcionalitats de threat hunting.

- Es requereix, considerant la rellevància i criticitat especial de les infraestructures de sistemes que sustenten els sistemes d'identitat de Directori Actiu (Controladors de Domini), l'impacte en el rendiment d'aquests sistemes provocat per aquestes funcionalitats específiques de seguretat orientades a la protecció d'identitats

- Es requereix que les funcionalitats demandades en aquest apartat siguin accessibles, preferentment, des de la mateixa interfície única des de la qual es presten totes les funcionalitats de seguretat, entenent-se aquesta com un únic portal web en el qual es recullin totes les capacitats.

A efectes de valoració de la interfície o consola única, no es consideraran valorables aquelles solucions que requereixin vincular, enllaçar o integrar diferents plataformes o aplicacions web, dominis o consoles per cobrir les funcionalitats requerides o aquelles que integrin aquestes consoles en un portal d' aplicacions.

ANÀLISI IMMEDIAT DE FITXERS VIA API

Solució per fer anàlisi dinàmic "on the fly" mitjançant integració API abans de ser el fitxer emmagatzemat a l'infraestructura de TMB. L'anàlisi dels fitxers ha de produir-se en segons (quasi temps real amb un màxim de 2 segons) i sense latències.
Eina que permeti integrar-se a les aplicacions o a la protecció de correu mitjançant crides API.
Les verificacions s'han de realitzat tant de forma estàtica com dinàmica.
La plataforma ha de poder permetre l'enviament sota demanda via API de fins a 25.000 escanejos de fitxers al mes.
La solució ha de ser auto-escalable i adaptable a les necessitats de possible creixement a TMB.

SERVEIS PROFESSIONALS DEL FABRICANT

Els Serveis Professionals del fabricant seran per poder fer la integració a la plataforma del Identity Provider de TMB (Keycloack) amb la solució ITDR, creació de dashboards personalitzats i per poder configurar la recepció de logs de la font SSE/CASB per poder correlar amb la telemetria del EDR i ITDR en la mateixa plataforma i millorar la detecció d'incidents. També haurà de col·laborar en la arquitectura/configuració d'enviament de logs cap al Kafka on-premise de TMB.

SUPORT TAM DEL FABRICANT

El TAM haurà de donar suport no només durant el onboarding, supervisant tota la configuració i desplegament necessaris, sinó també amb revisions, actualitzacions i noves funcionalitats, etc. per assegurar que TMB treu tot el profit de la plataforma. Recomanacions de casos d'ús a tenir en compte en el ITDR, la compartició de nous Dashboards, i atendre a les peticions del SOC respecte a dubtes sobre la utilització o malfuncionament de la plataforma (com a pas previ a obrir un cas a suport).

SUPORT TÈCNIC DEL FABRICANT

Amb suport 24x7 per qualsevol incidència del producte i per poder escalat possibles casos oberts amb el fabricant. L'àmbit serà sobre tota la plataforma i solucions contractades (EDR i ITDR),

INGESTA 15GB DIARIS DE FONTS EXTERNES

La plataforma haurà de tenir la capacitat d'emmagatzemar tota la telemetria dels productes EDR i ITDR, però també poder ingestar logs d'altres eines (i sobretot de SSE/CASB) amb una capacitat màxima de 15GB/dia i una retenció de 6 mesos per les fonts externes.

3. Condicions de servei

El proveïdor haurà de demostrar amb un certificat emès pel fabricant, que és Partner del fabricant de la solució que proposa en la oferta.

4. Seguretat i Confidencialitat

L'adjudicatari s'obliga a no difondre i guardar el més absolut secret de tota la informació a la qual tingui accés en compliment de l'actual servei, i a subministrar-la solament al personal autoritzat per TMB.

L'adjudicatari serà responsable de les violacions del deure de secret que es puguin produir per part del personal sota el seu càrrec. Tan mateix, s'obliga a aplicar les mesures necessàries per garantir l'eficàcia dels principis de mínim privilegi i necessitat de conèixer, per part del personal que participi en el desenvolupament del servei.

Un cop finalitzat el present servei, l'adjudicatari es compromet a destruir amb les garanties de seguretat suficients o retornar tota la informació facilitada per TMB, així com qualsevol altre producte obtingut com a resultat del present contracte.

El proveïdor ha de complir amb la Política y Cos Normatiu de Seguretat Tecnològica i de la Informació de TMB.