MEMBER OF
BASQUE RESEARCH
& TECHNOLOGY ALLIANCE

t. +34 94 657 40 00
info@azti.es | **www.**azti.es

Lizitazio iragarkia

Sukarrieta, 2022ko martxoaren 28a

1. XEDEA

AZTI Fundazioak iragartzen du lehiaketa publiko bidezko lizitazio prozedura bat ireki duela **FUNDACIÓN AZTI – AZTI FUNDAZIOAren parke informatikoko ekipo guztiak (erabiltzaileen eta zerbitzarien lanpostuak) detektatzeko, malwarea desinfektatzeko eta babesteko zerbitzua berritzeko, PANDA ACTIVE DEFENSE 360 delakoaren bidez**.

Zerbitzu horri esker, lanpostuan exekutatzen den software guztia sailkatu ahal izango da, haren portaera monitorizatuko da, software fidagarri eta ez-fidagarriaren identifikazioa ziurtatuko du eta software ez-fidagarriaren exekuzioa blokeatuko du.

Ekipoak kudeatzeko eta mantentzeko zerbitzu bat ere sartu behar da, ekipoen egoera kontrolatzeko eta politikak aplikatu eta urrunetik instalatu ahal izateko.

Hauek izango dira kontratatu beharreko zerbitzuak:

- Adaptive defense 360 Aether Platform.
- Panda Systems Management.
- Panda patch management

2. ZERBITZUAREN IRAUPENA

Zerbitzua **gutxienez 24 hilabetekoa (2 urte)** eta **geienez 36 hilabetekoa (3 urte)** izango da, kontratua sinatzen den egunetik aurrera. Jasotako eskaintzen arabera erabakiko da epe hori.

3. ESKAINTZA EKONOMIKOA

Lizitazio honetarako onartuko den gehieneko eskaintza ekonomikoa **hirurogeita hamar eurokoa da (70,00€)** lizentzia bakoitzeko 24 hilabeteetarako, zergak barne hartu gabe. AZTIk, gutxienez 380 lizentzia erostea bermatzen du.

Fakturazioa kontratua sinatzen denean egingo da, eta jaulki eta hurrengo 60 egunetan ordainduko da faktura.

MEMBER OF
BASQUE RESEARCH
& TECHNOLOGY ALLIANCE

4. PROPOSAMENAK BALORATZEKO IRIZPIDEAK

Jasotako proposamenak irizpide hauen arabera baloratuko dira:

Eskaintza ekonomikoa	%70
Ziurtagiri teknikoak	%20
Hobekuntzak	%5
Gizarte Erantzukizun Korporatiboko Politikak	%5

5. PROPOSAMENAK AURKEZTEA

Lizitatzaileek Irati Velezi aurkeztu ahal izango dizkiote proposamenak ivelez@azti.es helbide elektronikoan eta AZTIren edozein zentrotan, iragarki hau AZTI Fundazioaren webgunean argitaratzen denetik **2022ko apirilaren 25eko 12:00ak arte**.

Lizitatzaileek helbide honetara jo ahal izango dute **informazio tekniko** gehigarria jasotzeko:

AZTI

Norentzat: Cesar Idokiliz

Tel. 34 656 784 978

Mail: cesar@azti.es

6. ESLEIPENA

Eskaintzak aurkezteko adierazitako egunean jaso ondoren, 15 laneguneko epean, AZTI Fundazioaren webgunean argitaratuko da lizitazioaren emaitza.

7. KONTRATAZIORAKO BALDINTZAK

- Hautatutako erakundea, AZTIrekiko zerbitzuak dirauen bitartean, lan, Gizarte Segurantza eta Laneko Segurtasun eta Osasunaren arloan indarrean dagoen araudia bete beharko du, eta, dagokionean, enpresa jarduerak koordinatu beharko

ditu, 171/2004 Errege Dekretuaren arabera, ezarritako prozedura eta espezifikazioei jarraituz (hemen eskuratu daitezke http://www.azti.es/es/coordinacion-de-actividades-empresariales/)

- Hautatutako erakundeak, beste edozein agiri alde batera utzita, zerga betebeharrak eta Gizarte Segurantzarekikoak egunean dituela egiaztatzen duen ziurtagiria aurkeztu beharko du kontratua formalizatu aurretik.
- Hautatutako erakundeak kontratua formalizatzeko behar den dokumentazioa aurkeztu beharko du gehienez 20 eguneko epean, esleipena egiten denetik zenbatzen hasita. Edozein gai gehigarri kontsultatu ahal izango da www.azti.es helbidean argitaratutako Kontratazioaren barne Araudian.
- Baldintza teknikoez eta administratiboez gain, AZTIk positibo baloratuko ditu Kalitate, Segurtasun eta Osasun, Ingurumen, Mugikortasun Jasangarri eta Gizarte Erantzukizun Korporatiboko politikei eusten dietela frogatzen duten hornitzaileei.

  Hornitzaileak politika horiek egiaztatzeko aukera ematen duten dokumentuak edo erregistroak sartuko ditu bere proposamenean (kalitate ziurtagiriak, ingurumenekoak, gizarte erantzukizuneko gaietako jarduerei buruzko dokumentazioa, etab.).

8. DATUAK BABESTEKO ERREGELAMENDU OROKORRA

Arduraduna: Izena: AZTI FUNDAZIOA - IFK: G48939508 Posta helbidea: TXATXARRAMENDI UGARTEA Z.G. SUKARRIETA (BIZKAIA) Telefonoa: 946574000 Helbide elektronikoa: lopd@azti.es.

"AZTI FUNDAZIOAn ematen diguzun informazioa tratatzen dugu, zure eskaera egiteko, zerbitzuak fakturatzeko eta merkataritza harremanak mantentzeko. Zure datu pertsonalen tratamenduaren oinarri juridikoa merkataritza harremanak izateko eta zerbitzuak emateko dugun interes legitimoa da, eta behar-beharrezkoak dira helburu horretarako. Emandako datuak gorde egingo dira merkataritza harremanak dirauen bitartean edo legezko betebeharrak betetzeko behar diren urteetan, eta, harremana amaitu ondoren, erantzukizunak sor daitezkeen neurrian. Datuak ez zaizkie hirugarrenei lagako, legezko betebeharren bat dagoenean izan ezik, ezta zerbitzu tekniko eta informatikoen eta auditoretzaren hornitzaileei ere. Halaber, ez du inola ere zure datu pertsonalen nazioarteko transferentziarik egingo. Eskubidea duzu AZTI FUNDAZIOAn zure datu pertsonalak tratatzen ari garen jakiteko; ondorioz, eskubidea duzu zure datu pertsonaletan sartzeko, datu okerrak zuzentzeko edo ezabatzeko eskatzeko, datuak jada beharrezkoak ez direnean, baita ere aurkaratzeko, mugatzeko eta lekualdatzeko eskubidea ere, datuen babesari buruz aplikatu beharreko araudian xedatutako terminoetan, goian adierazitako

helbidera idatziz jakinaraziz. Halaber, erreklamazioa aurkeztu ahal izango dute kontrolerako agintaritza eskumendunaren aurrean.

9. KLAUSULA TEKNIKO ESPEZIFIKOAK

9.1.- BABESTU BEHARREKO AKTIBOAK

Konponbideak gutxienez 380 ekipo (CPU) babesteko gai izan beharko du.

9.2.- PLATAFORMAREN KOKAPENA

Soluzioa mantentzeko eta ustiatzeko kostuak murrizteko, ez da beharrezkoa izango barne-plataforma bat erabiltzea, cloud-ean oinarritutako soluzio bat behar da. Gutxieneko baldintza da azpiegitura dagoen plataforma gure instalazioetatik kanpo egotea eta soluzioaren fabrikatzaileak erabiltzea cloud eredu batean, betiere plataformaren hazkundean eta eskalagarritasunean eragozpenik ez badago. Instalazioaren nodo-kopurua edozein dela ere, plataformak eraginkortasun-maila berean funtzionatzen duela ziurtatuz. Plataformaren kokalekuak Europar Batasunean egon behar du.

Nodo batzuk hainbat egoitzatan banatuta daude, baita mugikortasunean ere; horregatik, horiek cloud azpiegituraren erabilgarritasuna baliatuko dute soluzioaren konfigurazioan eta eguneratzean erabat integratuta egon daitezen.

Kudeaketa-plataformak ziurtapen-maila nagusiak estali behar ditu, hala nola: ISO 27001, eta positiboki baloratuko da azpiegiturak duen beste edozein ziurtagiri.

9.3.- ZERBITZUAREN OSAGAIAK

9.3.1. Cloud azpiegitura

Esleipendunak zerbitzarien, datu-baseen eta zerbitzuarekin lotutako informazioa tratatzeko prozesuen multzoa hornituko du hodeitik. Bezeroek harrapatutako prozesuak hodeian tratatuko dira, sistema korporatiboen gaineko inpaktua ahalik eta txikiena izan dadin. Ekipoen kudeaketa hodeitik egingo da, kokapen desberdinetan ekipoak kudeatu ahal izateko, baita mugikortasunean ere.

9.3.2. Agentea, ekipoetan hedatu beharrekoa.

Zabaldutako agenteak antibirus tradizionalaren babesa, prozesu ezezagunen babesa eta ekipoekiko urrutiko konexioa komunikatu eta kudeatzeko aukera emango du.

Gertaerei eta horiek sortzen dituzten osagaiei buruzko informazioa jasoko du, informazioa eta erabiltzaile-dokumentuak bildu gabe. Parkeko gailuen gaineko inpaktuak PUZ, memoria eta diskoaren errendimenduaren % 5 baino txikiagoa izan beharko du.

Agenteak gai izan behar du mahai gaineko ekipoak eta ekipo eramangarriak sistema eragile hauen bidez babesteko:

- Microsoft Windows 7tik Microsoft Windows 11ra.

Zerbitzari-ekipoak sistema eragilearen bertsioekin babestu beharko ditu:

- Microsoft Windows 2012 R2tik Microsoft Windows 2022ra.

Babesaren desinstalazioa pasahitz bidez babestu beharko da.

Soluzioa isilean hedatu ahal izango da mekanismo hauen bidez: IP helbidearen arabera, IP helbideen mailaren arabera, makinaren izenaren arabera eta Microsoften Direktorio Aktiboko taldeen arabera, domeinu-politiketan oinarrituta.

9.3.3. Web kontsola

Esleipendunak interfaze bat emango du datuak denbora errealean kontsultatzeko, txostenak/alertak deskargatzeko, konfiguraziora eta politiketara sartzeko eta eragileen eguneratzeak izateko.

Zerbitzuaren administratzaileek kontsola bakar batetik eta modu zentralizatuan kudeatu ahal izango dituzte, edozein web-nabigatzaileren bidez, Windows zerbitzari eta lan-estazio guztien segurtasuna eta produktibitatea, ordenagailu eramangarriak eta urruneko bulegoak barne.

9.4.- BABESA

Eskatutako babesa hiru zatitan banatuko da:

- Endpoint Protection Platform (EPP)
- Endpoint detection and response (EDR)
- Remote Monitoring & Management (RMM)

Lehenengo bi zatiak konbinatuta eta bateratuta egon behar dira konfigurazio-mailan, funtzionaltasun-mailan bakarrik egongo dira banatuta. Eta eragile bakar batek eta irtenbide bakar batek osatzen dute. Ezin izango dira hainbat osagai erabili. Mehatxu ezezagunen aurkako babesa lortzeko, antibirus tradizionalak babes aurreratuarekin lagunduko duena.

9.4.1.- Endpoint Protection Platform

EPP (Endpoint Protection Platform) soluzio bat behar da, funtzionalitate hauekin:

- Fitxategietarako, postarako eta webgunerako antibirusak. Edozein mehatxu mota detektatzeko eta desinfektatzeko aukera emanez. Portaeraren araberako malwarea detektatzen. Postak POP3n detektatuko du. Web babesari dagokionez, elementu

maltzurrak dituzten webguneetara sartzeko saiakerak detektatuko dira, eta blokeatu egingo dira.

- Lokalean edo web-kontsolatik modu zentralizatuan kudeatutako firewall pertsonala.

  Aukera eman behar du:

  - Blokeatu nahi dituzun aplikazioetako sarrerako eta/edo irteerako konexioak
  - Sarguneen prebentzioa
  - Firewall arauak sortzea nahi dituen makinen sarrerako/irteerako noranzkoan trafikoa baimentzeko/ukatzeko, nahi dituen protokolo/portuetarako.

- Gailu espezifiko guztiak blokeatzea (biltegiratze-unitate ateragarriak, irudiak hartzeko gailuak, CD/DVD unitateak, USB modemak, Bluetooth, etab.), malwarea sartzea eta informazio-ihesak eragotziz. Gailu mota bakoitzerako hainbat ekintza definitzea ahalbidetuz (blokeoa, sarbidea, irakurketa/idazketa).

- Nahi ez diren webguneetarako sarbidea blokeatzea. Kategorietan oinarritutako babes hori konfiguratu ahal izango da, baina baimendutako gune eta domeinuen zerrenda zuriak eta beltzak ere gehitu ahal izango dira.

9.4.2.- Endpoint detection and response

EDR motako soluzio bat behar da (endpoint detection and response), honako mehatxu hauetatik babesteko:

- Malware aurreratua
- PUP (potential unwanted programs)
- Ransomware motako zeroday mehatxuak
- Belaunaldi berriko troiarrak, antibirusek detektatu ezin dituztenak.

Konponbide horrek ahalik eta gehien saihestu beharko ditu infekzioak modu proaktiboan, inoiz ez erreaktiboan. Irtenbideak honako hauek ez diren kontraneurriak izan behar ditu:

- Tokiko sinadurak, etengabe eguneratu beharrekoak
- Motor heuristikoak, PUZ erabili behar dutenak eta positibo faltsuak eragin ditzaketenak.
- Zerrenda zurien sistemak, ez baitugu horrelako sistemak emateko langile nahikorik.
- Baliabideak kontsumitzen dituen eta malwareak saihets ditzakeen sandboxing-sistemak.

Babes-sistemak makinetan gauzatutako prozesuen % 100 sailkatzeko gai izan behar du, malware edo goodware sailkapena sortuz.

Baldintza bat da prozesu ezezagunak blokeatzea, makinak eskura ditzakeen datuak (nahi ez den zifratzea, adibidez) edo datuak lapurtzea edo eskuratzea saihesteko.

Anti-Exploit sistema bat izan behar du, esploits ezagun edo ezezagunen erabilera detektatzeko eta blokeatzeko aukera ematen duena.

Blokeo-maila desberdinak ezartzeko aukera izan behar da (gutxi-asko murriztaileak), bai eta sistemak blokeatutako prozesuak banaka desblokeatu ahal izateko erabiltzaileen gaitasun-maila desberdinak ere.

Soluzioak administratzaileak nahi duen izenaren eta hash-aren araberako aplikazioak blokeatzeko aukera barne hartu behar du.

9.4.3.- Mehatxuen alerta-zerbitzua (Threat Hunting)

Ekipamenduen parkean aurrez ikuskatutako portaera normalean oinarritutako jarduera anomaloa detektatzen denean, zerbitzu bat behar da, neurri zuzentzaile egokiak hartzeko.

Zerbitzu hori EDR soluzioaren fabrikatzaileak eskaini beharko du teknikari espezializatuek, auzitegi-auditorian jasotako datuak erabiliz.

Neurri zuzentzaileak alertan jartzeko eta EDR sistemaren adimenean sartzeko aukera izan behar dute.

9.4.4.- Monitoring & Management sorta

RMM (remote monitoring and management) motako soluzio bat behar da helburu hauek lortzeko:

- Hardware eta softwareari buruzko informazio zentralizatua lortzea.
- Erabilitako lizentzien kontrola
- Inbentarioan lortutako informazioaren arabera iragazkiak egiteko gaitasuna
- Hardware edo software mailan ekipoan sortutako aldaketen erregistroa.
- Prozesuak, zerbitzuak, memoria, PUZ, erregistroa, fitxategien tamaina edo karpetak monitorizatzea
- Monitore pertsonalizatu berriak sortzeko aukera
- Sareko gailuak monitorizatzea.
- Zereginak automatikoki egiteko gaitasuna, monitore batean gertaera jakin bat gertatzen denean.
- Microsoften adabakiak kudeatzea, ekipoa edonon dagoela ere.
- Hirugarrenen softwarea instalatzea, desinstalatzea eta adabakiak jartzea.
- Atazak automatizatzeko scriptak urrutitik gauzatzea
- Urrutiko kontrola Internetera konektatutako ekipoei, edonon daudela ere.
- Erabiltzailearekin txat bidez komunikatzeko sistema.
- Smartphone eta tableten kontrola, gailua ezabatzeko, blokeatzeko eta lokalizatzeko gutxieneko funtzionaltasunarekin.

Funtzionalitate horiek guztiak agente bakar baten zati gisa integratuko dira, eta kudeaketa eta urrutiko kontrola ahalbidetuko ditu.

9.5.- SEGURTASUN ESKEMA NAZIONALA

Soluzioak nahitaez egon behar du Informazioaren eta Komunikazioaren Teknologien Segurtasun Produktuen Katalogoan. (CPSTIC) CCNk (Zentro Kriptografiko Nazionala) argitaratua, lanpostua KUALIFIKATU gisa babesteko familiaren barruan.

Cloud Teknologia Publikoa, derrigorrezkoa da kategoria altuko ENSrekiko adostasun-ziurtagiria izatea.

9.6.- INFORMAZIOA

Sistemak ekipo bakoitzarekin lotutako auzitegi-informazioa sortu behar du, ondoren ustiatu ahal izateko. Sistemak txosten bat izan beharko du, hautemandako mehatxuari buruzkoa, prozesuak egin dituen ekintzekin edo bilduta egon den testuinguruarekin lotuta; adibidez, Internetetik deskargatu den edo fitxategi konprimitu batetik atera den. Ingurune atsegina eta jarraitzeko erraza baloratuko da, mehatxu aurreratuen ezagutza handirik eskatu gabe. Gainera, babesen egoerari, malware-detekzioei eta txosten exekutiboren bati buruzko txostenak jaso behar ditu, informazio globalaren laburpenarekin.

Txostenak berehala lortu ahal izango dira datuekin, denbora errealean, baita aldizka ere, posta elektronikoz eta hainbat formatutan, ondoren tratatzeko.

9.7.- EUSKARRI TEKNIKOA 24X7X365

Erakundeko postu eta zerbitzari guztietan funtzionamendu egokia ziurtatzeko mantentze-lanak eta laguntza teknikoa ezarriko dira. Honela:

- Fabrikatzaileak telefonoz eskaintzen duen euskarri-zerbitzua, gaztelaniaz.
- Service Packs eta hotfixes: produktuaren hobekuntza teknikoetarako sarbidea zerbitzua aktibatzen den bitartean
- Euskarri-webgunea: foroetarako sarbidea, blogak, azken mehatxuei buruzko informazioa, birusen entziklopedia,
- 24x7x365 posta elektronikoko euskarri teknikoa, inplementatutako soluzioan ziurtatutako teknikariek emana
- Ezkutuko birusen online analisietarako sarbidea
- Helpdeskera mugarik gabe sartzea: gorabeherarik gabe