MITRE MARKOAN OINARRITUTAKO BARNE ETA KANPO ESPOSIZIOAREN EBALUAZIO-ZERBITZURAKO PRESKRIPZIO TEKNIKOEN AGIRIA (ESP. ZIUR2026002)

I. XEDEA ETA ZERBITZUAREN IRISMENA

Lizitazio honen **helburua** ATT&CK/ATLAS eta threat intelligence eguneratuak, kanpoko esposizioaren analisia eta emaitzen itzulketa argia konbinatzen dituen zerbitzu kudeatu bat lortzea da, Gipuzkoako industria-enpresei erresilientzia ebaluatzen, inbertsioak orientatzen eta ikusgarritasun objektibo eta neurgarria ematen laguntzeko.

Zibermehatxuak azkar eta etengabe bilakatzen dira. Taktikak, teknikak eta prozedurak aldatzen dituzte, eraso-azalera handitzen dute eta mendekotasun teknologiko berriak ustiatzen dituzte. Horregatik, erakunde askok ez dute zibersegurtasun-jarreraren ikuspegi objektiborik eta eguneraturik: ez dakite ziberkriminalen zein teknikek detektatu edo arindu dezaketen, non dauden arrisku handienak (*bai barne-mailan, bai kanpo-azaleran*) eta zer ekintzek emango luketen segurtasun-itzulera handiagoa baliabide mugatuekin. Gainera*, threat intelligence* informazioa sakabanatuta egon ohi da, eta zaila da erakundeen artean alderagarriak diren erabaki operatibo eta metrikoetan islatzea.

Ildo horretan, MITRE ATT&CK-ek teknika eta azpiteknika mailan mehatxuak eta defentsa-gaitasunak mapeatzeko hizkuntza komuna eskaintzen digu, bai Enterprise inguruneetan, bai ingurune industrialetan (ICS), eta MITRE ATLASek ikuspegi hori IA duten agertokietara zabaltzen du. Esparru horietan oinarritzeak aukera ematen du modu estandarizatuan ebaluatzeko, erreferentzia-agertokiak sortzeko, hobekuntzak lehenesteko eta denboran egindako aurrerapenak neurtzeko.

II. PRESTAZIOAREN DESKRIBAPENA

Proiektuaren helburua betetzeko, zibersegurtasuneko plataforma bat kudeatutako zerbitzu bat eduki nahi da, zerbitzuan sartutako erakundeen zibersegurtasuneko jarrera ebaluatu eta hobetzeko eta, oro har, honako hauek eskaintzeko:

- Mehatxuen aurrean hautemateko eta babesteko gaitasunen ebaluazioa, MITRE ATT&CK-en gainean kalkulatutako rating batekin eta threat intelligence txosten eguneratuekin haztatuta.
- Threat intelligence-n oinarritutako eta MITRE ATT&CK-en mapeatutako eraso-agertokiak sortzea, erakunde bakoitzarentzat garrantzitsuak direnak, detekzio proaktiboa aktibatuta maila definitutako erosotasun-atalasearen azpitik dagoenean.
- Kanpoko esposizioaren gainazalarekiko segurtasun-jarrera mapeatzea (web-domeinuak bereziki), denbora errealean eguneratuta, etengabeko analisiaren bidez eta threat intelligence txostenekin eta datuen analisiarekin korrelazioaren bidez.
- Hobetzeko aukerak identifikatzea eta lehenestea, baliabideak eta inbertsioa optimizatzeko eta zibersegurtasunaren jarrera handitzeko.
- Txosten global anonimizatua, Gipuzkoako industria-ingurunearen segurtasun-maila zehazteko aukera emango duena, hainbat motatako erakundeen lagin adierazgarri gisa, zerbitzua indarrean dagoen bitartean hobetzeko aukerak hartzearen ebaluazioa barne.

III. METODOLOGIA

Enpresa esleipendunak ZIUR Fundazioari lanen garapenari dagozkion ikuskapen- eta kontrol-funtzioak betetzea erraztu beharko du, jasotzen dituen ohar eta gomendioak zorrotz betez.

ZIUR Fundazioak, lanen garapena eta jarraipena errazte aldera, zerbitzuaren beharren arabera, enpresa esleipendunari eskatu ahal izango dio beharrezkotzat jotzen dituen dokumentu guztiak aurkez ditzala eta zerbitzua behar bezala garatzeko egokitzat jotzen dituen lan- edo informazio-bilera guztietara joan dadila. Hori guztia modu presentzialean eta/edo telematikoan egin ahal izango da, esleipendunaren aukeran.

Nolanahi ere, ZIUR Fundazioaren esku geratuko da jarraipena egiteko modua aldatzea (bilerak, aktak, txostenak...), beharrezkotzat jotzen badu.

Kontratu honetan garatutako dokumentuak eta ekintzak Ziur erakundearen erakunde-nortasunaren eskuliburuaren arabera egingo dira.

Txosten guztiak gaztelaniaz eta euskaraz aurkeztu beharko dira.

IV. ZERBITZUAREN HEDAPENA

Zerbitzua plangintza honen arabera hedatuko da, zerbitzuak irauten duen 12 hilabeteetan:

- 3 kanpaina:
  - Bakoitzak 4 hilabeteko iraupena izango du.
  - Kanpaina bakoitzean gutxienez 5 enpresak parte hartuko dute.
  - ZIUR-eko langileak arduratuko dira kanpaina bakoitzean parte hartuko duten Gipuzkoako industria-enpresak hautatzeaz.

V. PLATAFORMAREN EZAUGARRI TEKNIKOAK

Proposatutako plataforma zerbitzuaren oinarria izango da, eta horren gainean garatuko da proiektua. Soluzioaren hedapena eta datuak eskuratzeko prozesuak errazteko, ezaugarri hauek izan beharko dira gutxienez:

- Adimen artifizialean oinarritutako auditoria duten datuak modu automatizatuan eskuratzea.
- Kanpo-esposizioko gainazalean gaitasunak eta kalteberatasunak detektatzeko sistema bat konfiguratzea.

Bestalde, plataformak, gutxienez, baldintza tekniko eta funtzionaltasun hauek izan behar ditu:

- Lizentziamendua: produktuak behar besteko lizentziak izan beharko ditu zerbitzuko kanpaina bakoitzeko enpresa guztiei euskarria emateko. Lizentziamendua pantaila espezifiko batean islatuko da, ZIUR-eko tenant-erako sartutako ezaugarriak argi eta garbi erakusteko.

- Irisgarritasuna eta bateragarritasuna: soluzioa *responsive* izango da, eta aplikazio mugikor gisa instalatu ahal izango da, ahal dela Progressive Web App (PWA) formatuan, idazmahaiko gailuetatik, tabletetatik eta mugikorretatik sarbidea errazteko.
- Arkitektura: soluzioak ZIUR-erako tenant espezifiko bat eskainiko du. Tenant horretatik, irismeneko enpresekin egin beharreko proiektu bakoitzaren instantziak konfiguratuko dira, erakunde bakoitzaren pribatutasuna eta segregazioa bermatuz.
- Erabiltzaileen kudeaketa: tresnari esker, baimenen kudeaketa xehatua egin ahal izango da, administrazio orokorretik hasi eta proiektu bakoitzeko irakurketa hutsera arte, gutxienez honako rol hauek barne hartuta:
    - Administratzaile globala: administrazio osoa tenant guztietan.
    - Irakurketa globala: irakurketa osoko sarbidea tenant guztietan.
    - Tenant-en administratzailea: esleitutako tenant-aren administrazioa.
    - Tenant irakurgailua: irakurketa osoa esleitutako tenantean.
    - Proiektu-administratzailea: esleitutako proiektuen administrazioa.
    - Proiektuen irakurlea: esleitutako proiektuen irakurketa.
- Segurtasuna:
    - Aplikaziora sartzeko, faktore anitzeko autentifikazioa beharko da, eta TOTP estandarrarekin bateragarriak diren tresnak onartuko dira (Google Authenticator, Microsoft Authenticator, DUO Mobile, etab.).
    - Irtenbidea SaaS moduan eskainiko da, Europan kokatutako zerbitzariekin eta agenterik hedatu beharrik gabe.
- Bistaratzea, jakinarazpenak eta txostenak:
    - Aplikazioak jakinarazpen-pantaila bat izango du, posta elektronikoz eta push bidez bidalita.
    - Informazio garrantzitsua PDFko txosten gisa esportatu ahal izango da.
    - Administrazioa panel intuitibo baten bidez egingo da, funtzionalitateen eta gaitasunen kontrol aurreratua ahalbidetzeko.
    - ZIUR-ek parte hartzen duten erakundeen arteko datu konparatiboak ikusteko aukera emango duten pantailak izango dira, aztertutako ekosistemaren zibersegurtasun-egoerari buruzko ikuspegi orokor agregatua lortu ahal izateko.
- Hizkuntzak
    - Plataformaren interfaze osoak erabiltzaile bakoitzeko hizkuntza hautatzeko aukera emango du, eta, gutxienez, euskara eta gaztelania izango ditu. Horrela, menu guztiak aurrez hautatutako hizkuntzan aurkeztuko dira.
    - Kanpoko esposizio-azalerari buruzko adierazleak euskaratuta egon beharko dira interfazearen barruan.
    - Plataformak automatikoki sortzen dituen txosten guztiak, gutxienez, euskaraz eta gaztelaniaz aurkeztu behar dira.
    - OHARRA: Plataformako menuak nolakoak izango liratekeen argi eta garbi aurkeztea eskatzen da, bai gaztelaniaz bai euskaraz.

- Zibersegurtasuneko framework-ak: soluzioa MITRE ATT & CK (Enterprise eta ICS geruzak) markoan oinarrituko da, eta MITRE ATLAS IA erabiltzen duten erakundeentzat erabiltzeko gaitasuna izango du.
- Funtzionaltasun orokorrak:
    - Erakunde bakoitzaren segurtasun-jarrera zehaztea, MITRE ATT&CK-ren arabera.
    - Erakundeak portafolioen arabera antolatzea, zehaztutako portafolio bakoitzean hura osatzen duten erakundeen multzoaren rating agregatua lortu ahal izateko.
    - Zibersegurtasun-jarrera zehazteko garaian, organizazioetako hornitzaile desberdinen cloud inguruneetara ere hedatu ahal izan behar da. Soluzioa bateragarria den CLOUD hornitzaileen zerrenda zehaztu behar da.
    - Intereseko threat intelligence agertokien zerrenda eguneratua (softwarea, talde kriminalak, kanpaina aktiboak, sektoreak, kokapen geografikoa, etab.).
    - MITRE ATT&CK matrize pertsonalizatuen bidez gaitasunak aztertzea, MITRE ATT&CK Navigatorrekin bateragarriak eta JSON-en esportagarriak.
    - MITRE ATT&CK tridimentsionalen matrizeak sortzeko aukera, erakunde bakoitzaren segurtasun-jarrera, teknikatik teknikora, zehaztean inplikatutako aldagaiak ulertzen laguntzeko.
    - Aurrez definitutako katalogo batetik abiatuta, erakundeek dituzten zibersegurtasuneko produktuak hautatzea, gaitasunen mapaketa erraztuz.
    - Lehenetsitako hobekuntza-aukeren zerrenda bisuala eta testuala.
    - Zerbitzuaren ikuspegi zentralizatuko pantaila, timeline orokorrarekin eta dokumentu-kudeatzailearekin, beharrezkoa denean dokumentazioa trukatzeko.
    - Zerbitzuarekin lotutako zibersegurtasuneko albiste hautatuetarako sarbidea.
    - Erakundeen kanpo-esposizioko azaleraren (web-domeinuak) mailan monitorizazioa konfiguratzea eta segurtasun-jarrera zehaztea.
    - Kanpo-azalerako moduluak aurkitutako arazoak MITRE ATT&CK lan-esparruan sortutako agertokietatik iragazi ahal izango dira, erakundeak benetan interesgarriak diren mehatxuetara bideratu ahal izateko.
    - Kanpo-esposizioko gainazal-moduluak (EASM) erakundearen aztarna digital bat sortu beharko du, ekarritako eta aurkitutako aktiboetan oinarrituta, eta hainbat modutan grafikoki irudikatu ahal izango da: mapa geografikoa, sare-diagrama, sunburst diagrama eta sankey diagrama.
    - Kanpo-esposizioko azaleraren moduluak (EASM) adierazleen katalogo bisual bat izan beharko du, kanpo-esposizioko azalerarako estalitako adierazleak eta detekzioak une oro ezagutzeko aukera emango duena. Honako hauek eskainiko ditu: detekzio bakoitzaren deskribapen xehatua, hobekuntza-ekintzak, mapaketa MITRE ATT&CK-rekin, araudia betetzeko esparru desberdinak dituen mapaketa eta informazioa zabaltzeko intereseko orrietarako estekak.

- Konponbidea hedatzea: esleipenduna arduratuko da zerbitzua indarrean dagoen bitartean datuak konfiguratzeaz eta abiarazteaz, eskuratzeaz eta beharrezko mantentze-lanez.

- Compliance: Plataformak erakundearen egungo egoera mapeatzeko aukera eman behar du, egungo zibersegurtasuneko konplizeen eskakizunen arabera, hala nola: ISO27001, NIS2, etab.
- Alertak: Plataformak aukera eman behar du alerta automatikoen sorrera pertsonalizatzeko.
- Datuak eskuratzea:
    - Datuen eskuratze automatizatua ("auto-enrollment" motakoa) adimen artifizialean oinarritutako auditoretzarekin.
    - Zerbitzuan parte hartzen duten erakundeek beren auditoriak modu autonomoan egiteko aukera izan behar dute, sistema automatizatu hau erabiliz, bisualki chatbot gisa aurkeztua eta barnean integratua, banakako auditoria bakoitzaren datu egituratuekin
    - Sistema horrek aukera eman behar du kasu zehatz bakoitzera egokitzen diren galderak dituen sistema bat sortzeko, aurrez definitutako formulario estatikoak erabili beharrean.
    - Kanpo-esposizioko gainazalean gaitasunak eta kalteberatasunak detektatzeko sistema bat konfiguratzea, erakunde bakoitzaren domeinuak zehaztuz, eta horiei eragin diezaieketen mehatxuak denbora errealean detektatuz.
- Euskarri teknikoa: esleipendunak euskarri tekniko eraginkorra bermatuko du eragiketari, erabilgarritasunari eta errendimenduari buruzko gorabehera eta kontsultetarako, bai eta erabilerari eta gaitasunei buruzko zalantza funtzionaletarako ere. Honako hauek izan beharko ditu:
    - Euskarri-posta elektronikoa.
    - Euskarri-telefonoa.
    - Help desk sistema.
    - Oinarrizko erabilera-arazoak konpontzeko plataforman integratutako IAren laguntzailea.
- Integrazioak: irtenbideak kanpoko tresnekin eta beste marko batzuekin integratzeko gaitasuna izatea baloratuko da, hala nola MITRE CAR, MITRE D3FEND eta NISTren CPE datu-basea.
- API REST: soluzioak API REST dokumentatu bat izan beharko du, beharrezkoa denean, erabiltzaile-interfazetik haragoko informazioa eta emaitzak lortzeko aukera emango duena, erabiltzaile bakoitzeko autentifikazio-gako bakarren bidez eskura daitekeena.

VI. ZERBITZUAREN BALDINTZAK

Zerbitzua baldintza hauetan oinarrituta eman behar da:

1. Zerbitzua konfiguratzea eta martxan jartzea: esleipendunak plataformaren hasierako konfigurazioa egingo du, proiektu bakoitzaren parametrizazioa egingo du eta kanpaina hasteko beharrezko datuak eskuratuko ditu.
    - Erakundeei alta ematea eta dagozkien proiektuak sortzea.
    - Erabiltzaileak eta baimenak konfiguratzea.
    - Datuak automatikoki eskuratzeko eta IA-rekin ikuskaritza egiteko mekanismoak aktibatzea, bai eta kanpo-esposizioko gainazalaren monitorizazioa ere.
2. Kanpaina bidezko hasierako prestakuntza: hasierako prestakuntza-saio bat emango da kanpaina bakoitzaren hasieran, tresnaren erabilera eta ZIUR-i eta erakunde parte-hartzaileei zerbitzua emateko prozesua azaltzeko.

3. Zerbitzuaren kudeaketa operatiboa erakunde bakoitzarekin: esleipendunak harremana eta lan-zikloa kudeatuko ditu, eta emaitzak jakinarazi eta itzuliko direla ziurtatuko du.
    - MITRE ATT&CK-en oinarritutako gaitasun rating-a itzultzea eta threat-intel bidez haztatzea.
    - Kanpo-esposizioaren analisiaren aurkezpena (aurkikuntzak, lotutako arriskuak eta bilakaera).
    - Hobetzeko aukerak identifikatzea eta lehenestea, eta kanpainan zehar horien ezarpenaren jarraipena egitea.
    - ATT & CK matrize pertsonalizatuak ematea (JSONen esportagarriak) eta threat-inteleko agertoki garrantzitsuak eguneratzea.
    - Jarraipen-bilerak (gutxienez hilean behin) eta ekintzen egoeraren eta adierazleen aldaketaren berri ematea.

4. Laguntza teknikoa zerbitzuan zehar: kanpainan zehar intzidentzietarako eta kontsulta funtzional/teknikoetarako euskarria izatea, posta elektroniko, telefono, help desk eta plataforman dagoen IA agentearen bidez. SLAk (erantzun- eta ebazpen-denborak kritikotasun-mailen arabera) ZIURen eta esleipendunaren artean adostuko dira, eta aldizka jakinaraziko dira.

5. Amaierako txostena eta txosten global anonimizatua: zerbitzu osoa amaitzean, txosten orokor bat emango zaio ZIUR-i, metrika erantsiekin anonimizatua. Honako hauek jaso beharko ditu: rating-aren bilakaera erantsia, mapatutako tekniken estaldura, azaleraren murrizketa eta aurkikuntza garrantzitsuak, ekintza lehenetsien onarpen- eta itxiera-maila, joerak, eten komunak eta enpresa-sarea hobetzeko proposamen estrategikoak.

Donostian,

ZIUR FUNDAZIOKO ZUZENDARI NAGUSIA

Firmado por PENILLA AZCUENAGA, MARIA (FIRMA) el día 12/04/2026 con un certificado emitido por AC DNIE 004

María Penilla Azcuenaga