PRESKRIPZIO TEKNIKO PARTIKULARREN BALDINTZA AGIRIA, ZIUR FUNDAZIOAREN ZIBERSEGURTASUN BEHATOKI JARRAITUAREN ZERBITZUA ESKAINTZEKO (THREAT INTELLIGENCE ETA THREAT HUNTING) (ESP.: ZIUR2023-018)

I.- ZERBITZUAREN XEDEA ETA IRISMENA

Kontratu honen helburua da bi zerbitzu jarraitu martxan jartzea ZIUR Fundazioaren Zibersegurtasun Behatokiaren barruan. Hauek dira sortu beharreko edukiak:

- **Cybercrime Threat Intelligence** teknologia txertatzea, Gipuzkoako industria sektoreko enpresa eta aktibo adierazgarrienak etengabe monitorizatzeko eta balizko aktibo konprometituak detektatzeko.

- **Deception** teknologia txertatzea, makina birtualak eta iruzur amuak automatikoki ezartzearen poderioz fabrikatutako engainu sare bat sortzeko, helburu gisa harturik etengabe aztertzea ea Gipuzkoako industria sektoreko enpresak zuzendutako erasoen xede ote diren ala ez.

II.- ZERBITZUAREN DESKRIBAPENA

1. sorta: Cybercrime Threat Intelligence teknologia txertatzea

Proposamenak elementu hauek jaso behar ditu:

1. Mehatxuetarako adimen soluzio automatizatu bat ematea, mehatxuak aztertzeko eta testuinguruan kokatzeko gai izango dena; horretarako, zibergaizkileen ikuspegitik behatu beharko du eraso azalera, bai eta Interneteko ziberdelituen iturri nagusiak monitorizatu ere.
2. Lizitatzailearen kontura izango dira hardware eta software lizentzia guztiak, hau da, aplikazioa eta haren osagai guztiak xede enpresan hedatzeko eskatzen direnak.
3. ZIUR Fundazioak izendatzen dituen pertsonak tresna erabiltzeko trebatzea.
4. ZIUR Fundazioari laguntza ematea zerbitzuak irauten duen bitartean, tresna erabiltzen duten industria enpresetan erreminta hori hedatzeko lanetan.

Lizentziak kontratuaren indarraldi osoan izango du balioa, eta barnean hartuko ditu haren funtzionalitate guztiak, baita erabiltzeko eta mantentzeko beharrezko elementu guztiak ere.

2. sorta: Deception teknologia eskuratzea, makina birtualen eta iruzur amuen inplementazio automatikoaren bidez fabrikatutako engainu sare bat sortzeko.

Proposamenak elementu hauek jaso behar ditu:

1. Deception soluzio bat hornitzea, makina birtualen eta iruzur amuen inplementazio automatikoaren bidez fabrikatutako engainu sare bat sortu ahal izateko.
2. Lizitatzailearen kontura izango dira hardware eta software lizentzia guztiak, hau da, aplikazioa eta haren osagai guztiak xede enpresan hedatzeko eskatzen direnak.
3. ZIUR Fundazioak izendatzen dituen pertsonak tresna erabiltzeko trebatzea.
4. ZIUR Fundazioari laguntza ematea tresna erabiltzen den industria enpresetan tresna hedatzeko, zerbitzuak irauten duen bitartean.

Lizentziak kontratuaren indarraldi osoan izango du balioa, eta barnean hartuko ditu haren funtzionalitate guztiak, baita erabiltzeko eta mantentzeko beharrezko elementu guztiak ere.

III.- METODOLOGIA

1. sorta: Cybercrime Threat Intelligence teknologia txertatzea

Enpresa adjudikaziodunak erraztu egin beharko ditu ZIUR Fundazioari dagozkion lanak ikuskatzeko eta kontrolatzeko eginkizunak, eta zorrotz bete beharko ditu jasotzen dituen oharrak eta gomendioak.

ZIUR Fundazioak, lanen garapena eta jarraipena errazteko, enpresa adjudikaziodunari eskatu ahal izango dio aurkez ditzala beharrezkotzat jotzen dituen dokumentu guztiak, zerbitzuaren beharren arabera, eta eskatu ahalko dio, orobat, joan dadila zerbitzua behar bezala garatzeko egokitzat jotzen dituen lan edo informazio bilera guztietara. Horiek aurrez aurre eta/edo bide telematikoz egin ahal izango dira, adjudikaziodunak aukeratu bezala.

Nolanahi ere, ZIUR Fundazioaren irizpidearen arabera geratuko da jarraipena egiteko modua aldatzea (bilerak, aktak, txostenak, prozedurak...), baldin eta beharrezkotzat jotzen badu.

Kontratu honen barruan garatutako dokumentuak eta ekintzak ZIUR Fundazioaren nortasun korporatiboaren eskuliburuak dioena aintzat harturik egingo dira.

Nolanahi ere, adjudikaziodunak prestazio hauei ekin beharko die:

1. Aldez aurreko lanak eta erremintaren hedapena.
2. ZIUR Fundazioari tresnaren erabilerari buruzko prestakuntza ematea
3. ZIUR Fundazioari laguntza eta mantentze lanak bermatzea, kontratua indarrean dagoen bitartean.

2. sorta: Deception teknologia eskuratzea, makina birtualen eta iruzur amuen inplementazio automatikoaren bidez fabrikatutako engainu sare bat sortzeko.

Enpresa adjudikaziodunak erraztu egin beharko ditu ZIUR Fundazioari dagozkion lanak ikuskatzeko eta kontrolatzeko eginkizunak, eta zorrotz bete beharko ditu jasotzen dituen oharrak eta gomendioak.

ZIUR Fundazioak, lanen garapena eta jarraipena errazteko, enpresa adjudikaziodunari eskatu ahal izango dio aurkez ditzala beharrezkotzat jotzen dituen dokumentu guztiak, zerbitzuaren beharren arabera, eta eskatu ahalko dio, orobat, joan dadila zerbitzua behar bezala garatzeko egokitzat jotzen dituen lan edo informazio bilera guztietara. Horiek aurrez aurre eta/edo bide telematikoz egin ahal izango dira, adjudikaziodunak aukeratu bezala.

Nolanahi ere, ZIUR Fundazioaren irizpidearen arabera geratuko da jarraipena egiteko modua aldatzea (bilerak, aktak, txostenak, prozedurak...), baldin eta beharrezkotzat jotzen badu.

Kontratu honen barruan garatutako dokumentuak eta ekintzak ZIUR Fundazioaren nortasun korporatiboaren eskuliburuak dioena aintzat harturik egingo dira.

Nolanahi ere, adjudikaziodunak prestazio hauei ekin beharko die:

1. Aldez aurreko lanak eta erremintaren hedapena.
2. ZIUR Fundazioari tresnaren erabilerari buruzko prestakuntza ematea
3. ZIUR Fundazioari laguntza eta mantentze lanak bermatzea kontratua indarrean dagoen bitartean, industria enpresentzat gauzatzen diren inguruneak hedatzerakoan. ZIUR Fundazioko langileek aukeratuko dituzte enpresa horiek.
4. Zerbitzuak ematen diren bitartean, enpresa bakoitzaren gaineko txostenak egitea, tresnak hedapen bakoitzerako eskaintzen dituen emaitzak oinarri harturik.
5. ZIUR Fundazioarentzako azken txostena prestatzea, egindako hedapen guztien laburpenarekin.

Txosten guztiak gaztelaniaz eta euskaraz aurkeztu beharko dira.

IV.- ERREMINTAREN BALDINTZA TEKNIKOAK

1. sorta: Cybercrime Threat Intelligence teknologia txertatzea

Teknologiak plataforma batean oinarrituta egon behar du. Plataforma horrek, mehatxuen adimen automatizatua erabiliz, mehatxuak aztertu eta dagokion inguruabarretan kokatu behar ditu, erakundeek zibererasoei aurrea hartu ahal izateko.

Plataformak funtzionalitate hauek izan behar ditu:

- Iturri bilketa zabala. Soluzioak gai izan behar du sarbide zaileko hainbat iturritako informazioa etengabe biltzeko eta aztertzeko, hala nola foro eta merkatu klandestinoak, berehalako mezularitzako kanal itxiak, eta zibergaizkileek erabiltzen dituzten legez kanpoko beste zerbitzu batzuk.
- Txosten garrantzitsuak. Teknologiak makinaz irakurtzeko moduko adimen txostenak sortu behar ditu automatikoki, eta gai izan behar du, orobat, bere datu baseen, portuen eta sarean ikusgai dauden zerbitzarien, mehatxatutako kontuen edo lapurtutako kreditu txartelen filtrazio potentzialen berri emateko.

- Datuak denbora errealean biltzea. Soluzioak etengabe eta automatikoki bildu behar du ziberdelituaren ekosisteman ezkutatzen diren sarbide zaileko iturri dinamikoen informazioa.
- Irudia aztertzeko funtzio aurreratuak. Proposatutako soluzioak gai izan behar du testua, metadatuak eta irudiak biltzeko iturriak arakatzen diren bitartean, eta irudi analisiak aplikatu behar ditu, adimen kritikoa ateratzeko bilaketarako prestatutako formatuetan.
- Anonimotasuna eta erabateko segurtasuna. Adimen soluzioak modu seguruan eta denbora errealean arakatzeko eta iturrietara sartzeko gai izan behar du, atentzioa eman gabe eta segurtasun politikak urratu gabe.
- Estaldura eleanitza. Soluzioak gai izan behar du prozesatu gabeko datuak 100 hizkuntzatan baino gehiagotan bilatzeko eta atzitzeko, eta emaitza horiek automatikoki itzuli behar ditu, kontsultatu ahal izateko.
- Kontsulta konplexuak. Soluzioak gai izan behar du konplexutasun handiko kontsultak eta bilaketak egiteko, bai eta emaitza garrantzitsuak berehala biltzeko ere. Kontsulta horiek gorde egin behar dira, gero berrerabiltzeko.
- Iturri berriak etengabe sartzea. Soluzioak gai izan behar du iturri klandestinoak iraulita lortutako adimena eskuratzeko, hala nola datu baseak, Telegram taldeak, botnet merkatuak, hacker foroak eta beste hainbat.
- Bilaketa sekurizatuak. Soluzioak ikerketa sekurizatuak egiteko aukera eman behar du, gure xedeak bistaratu gabe, eta zuzenean eskuratu behar ditu prozesatu gabeko datuak gure segurtasun datuen lakutik (Data Leak).
- Denbora errealeko alerta zehatzak. Soluzioak gai izan behar du automatikoki arakatzeko eta berehala jakinarazteko erakundearen aktibo espezifikoen aurkako mehatxuak.
- Datu ikuspegi bakarra. Soluzioak kudeaketa plataforma bakarra izan behar du, datu zentro bateratu batean eskuragarri dagoen adimen guztia integratzeko, eta kanpoko eraso azalera osoaren ikuspegi orokor argia eskaini behar du.
- ZIUR Fundazioko teknikariek plataformara sartzeko erabiliko dituzten kontuek 2FA erabili behar dute.
- Zerbitzu plataformak % 100 hodei ingurunean oinarrituta egon behar du, eta ez da beharrezkoa izango on-premise zerbitzu gehigarririk hedatzea.
- Soluzioak aukera eman behar du 24 hilabeteko historiko batera sartzeko, fabrikatzailearen Data Leaketik.
- Soluzioak dimentsionatuta egon behar du:
    - 2.500 bilaketa soluzioaren adimeneko datu basean.
    - Proposatutako soluzioaren fabrikatzailearen ikerketa taldeak egindako mehatxuen adimenari buruzko txostenak eta azterlanak, hainbat iturritan oinarrituta.
    - 24 x 7 euskarri teknikoa, zerbitzua ematen den bitartean.

2. sorta: Deception teknologia eskuratzea, makina birtualen eta iruzur amuen inplementazio automatikoaren bidez fabrikatutako engainu sare bat sortzeko.

1. Inguruneen hedapena kudeatzeko sistema nagusiak appliance formatua izan behar du, eta fundazioak bere bulegoetan duen datuak prozesatzeko zentroan (DPZ) hedatuko da.

2. Amuak automatikoki hedatu behar dira abian jarritako ingurune bakoitzean, batez ere tresnan dauden sareko aktiboen inbentarioan oinarrituta. Soluzioak aldaketak egiteko aukera eman behar du, amu automatiko horietan oinarrituta, enpresa bakoitzaren inguruneetara egokitzeko.
3. Erremintak MITRE ICSrekin integratuta egon behar du, eta haren matrizeak erabili behar ditu; hala, hedatutako inguruneetara iristen diren erasotzaileen profila egin behar du, erasotzaile horiek erabiltzen dituzten teknikei dagokienez.
4. Tresnak kudeaketa plataforma zentral bat izan behar du, eta han kudeatuko dira hedatutako ingurune guztiak.
5. Tresnak gai izan behar du detekzio goiztiar eta zehatzarekin eta alerta prozesagarriekin jarduera eta elkarreragina azaltzeko. Erasotzaileen alboko mugimendua arakatzeko eta erlazionatzeko aukera ematen du, eta jakinaren gainean ipintzen ditu segurtasun administrariak web interfazea, posta elektronikoa, SNMP TRAP, erregistroak eta gertaerak baliatuz, SYSLOG/CEF bidez. Informazioaren azterketa forentsea egiteko aukera ematen digu, eta, haren bidez, erasotzaileen alboko mugimenduak eta jarduerak zehaztu ditzakegu, bai eta gertakarien eta kanpaina erasotzaileen informazioa erlazionatu ere.
6. Tresnak gai izan behar du 2. geruzako erasoak detektatzeko, hala nola MITM, Responder, ICMP swiping eta abar.
7. Soluzioak gai izan behar du amu makinek harrapatutako malwarearen analisi sakona egiteko, Sandbox soluzioekin eta Virus Total tresnekin integratuta.
8. Soluzioak gai izan behar du gertaeren alertei buruzko txosten osoak sortzeko PDF/CSV formatuan, barnean harturik alertak posta elektronikoz bidaltzeko aukera.
9. Soluzioak aukera eman behar du gertaerak eta kanpainak monitorizatzeko eta erlazionatzeko, eta alderdi hauei buruzko informazioa eman behar du:
    a. saioaren hasiera eta amaierak;
    b. alboko mugimenduen jarraipena;
    c. amu makinetan exekutatutako, erantsitako, aldatutako edo ezabatutako artxiboak.
10. Tresnak honako hauetarako dimentsionatuta egon behar du:
    a. 500 IP helbide jasan behar ditu, zabaldutako amuei loturik betiere.
    b. 20 amu jasan behar ditu (VM gainean oinarrituta), bai eta 128 VLAN ere.
11. Sistemak gai izan behar du makina, sistema eragile, protokolo eta zerbitzu birtual hauek jasateko, zabaldutako inguruneetan amu gisa erabiltzeko:
    - Windows (SO eta lotutako zerbitzuak)
    - VPN
    - Linux
    - IoT (Gauzen Internet)
    - Cloud
    - SCADA zerbitzuak
        - HTTP
        - FTP
        - TFTP
        - MODBUS
        - S7COM

  - BACNET
  - IPMI
  - TRIXONEX
  - GUARDIAN-AST
  - IEC 60870-5
  - DNP3
  - TRICONEX
  - SRTP
  - PROFINET
- SIEMENS
- SCHNEIDER
- RODWALL
- TRIDIUM
- VERTIV
- GENERAL ELECTRIC
- PHOENIX CONTACT

Donostia, 2023ko irailaren 29a.

ZIUR FUNDAZIOKO ZUZENDARI NAGUSIA



Koldo Peciña Txintxurreta