Basque CyberSecurity Centre

ZIBERSEGURTASUN INDUSTRIALEKO PROIEKTU-EREDUAK

nformazioaren hartzaileek beren erakundeko kideekin eta ezagutu behar duten bezeroekin eta hornitzaileekin bakarrik partekatu ahal izango dute, beren buruak babesteko edo kalte handiagoak saihesteko.
Bidaltzaileak informazioa partekatzeko murrizketa gehigarriak zehatz ditzake.

Basque CyberSecurity Centre

AURKIBIDEA

Basque CyberSecurity Centre

.01

ESKEMA OROKORRA

1.1 Testuingurua

Zalantzarik gabe, zibersegurtasuna da enpresek gaur egun aurre egin behar dieten erronka nagusietako bat, eta, batez ere, industria-ingurunekoek. Eta ez da zerbait zirkunstantziala. Egunero egiaztatzen ari diren zibereraso ugariek ezaugarri komunak dituzte:

- Oro har, biktima izan daitezkeenen artean helburu finkorik ez duten eraso indiskriminatuak dira, eta, neurri txikiagoan, zuzendutako erasoak.
- Oso gogorrak dira, eta horrek inpaktu handia izan dezake jasaten dituzten erakundeetan, are galera handiak edo ixtea eraginez.
- Onura handiak eskaintzen dizkiete exekutatzen dituzten zibergaizkile-taldeei, eta, beraz, talde horiek gero eta bitarteko eta baliabide gehiago bideratzen ari dira horrelako delituak egitera.

Aurrekoari gehitu behar zaio duela gutxi arte zibereraso bat industria-ingurune batean gertatzea anekdota bat zela, prentsa espezializatuan soilik argitaratzen zena, eta, oro har, enpresa handi edo azpiegitura kritikoetan (Ukrainako sare elektrikoa, Irango zentral nuklearra, etab.) gertatzen zena. Horrek urruneko sentsazio bat eragiten zuen, hain zuzen ere distantziaren eta enpresa-mota zela eta. Baina gaur egun, egia esan, tokiko enpresetan erregistratutako gorabeherak komunikabide jeneralistetan azaltzera pasatu dira; horrenbestez, zibersegurtasunaren inguruko alarma soziala oso handia da.

Zibersegurtasun industrialaren esparruan, esan liteke zibereraso baten eraginak ondorio larriagoak dituela hainbat faktore direla eta:

- Zibersegurtasun-neurriak enpresa batek kudeatzen duen informazioaren babes esklusiboa bilatuz aplikatu dira tradizioz, baina ez da kontuan hartu kontrol industrialerako sistemen eskuragarritasuna, konfidentzialtasuna edo osotasuna bera babestea.
- Hala, kontrol industrialerako sistemak sare korporatiboekin lotzea duela gutxi gertatu da, bere garaian sistema isolatu gisa pentsatu baitziren. Horrek arazo gehigarri bat sortzen du, jatorrizko diseinurako ez baitzen zibersegurtasuna baldintza funtzional gehigarritzat hartu, eta horrek ahalegin handiagoa eskatzen du halakoak behar bezala babesteko.
- Industria-ingurune batean segurtasun-gorabehera bat gauzatzearen ondorioek aurreikusi ezinezko eraginak izan ditzakete, eragindako sistemen tamainarekin zuzenean lotuta daudenak, hainbat arlotan: ekoizpen-sistemen programatu gabeko geldialdiak; fabrikatzeko ezintasuna; eskaeren hornidura ez betetzea; kontratuak ezeztatzea edo zigorrak kontratuetan adostutako zerbitzu-mailak ez betetzearen ondorioz; sektorean eta bezeroengan konfiantza-irudia galtzea; eta abar.

Beraz, eta kontuan hartuz industria-enpresak zibergaizkileen helburu nagusi bihurtu direla, argi dago enpresen biziraupenerako nahitaezkoa dela beren jardueraren arrisku-mailarekin bat datorren segurtasun-maila egokia edukitzea, eta horrek, ezinbestean, behean deskribatutako zibersegurtasun-proiektuak bezalakoak martxan jartzea eskatzen du.

1.2 Egitura

Zibersegurtasun-proiektu batzuen xehetasunak zehaztu nahi dira, modu egituratuan eta argi azaldutako edukiekin. Proiektu horiek industria-eremuko edozein enpresak aurreikusi beharko lituzke uneren batean.

Informazio horrek oinarri bat ematen du industria-enpresek zibersegurtasun-proiektuei ekiteko beharra uler dezaten, eta jakinaren gainean sektoreko enpresa espezialisten lankidetza-ikuspegiak eskatu ahal izan ditzaten. Ikuspegi horiek, gainera, BCSCk argitaratutako "Euskadiko Zibersegurtasunaren Liburu Zuria"n zerrendatuta ageri dira.

Proiektu bakoitza honela dago egituratuta:

- Proiektuaren tipologiaren azalpena, proiektua enpresaren behar posibleen barruan kokatu ahal izateko.
- Proiektua martxan jartzean lortu nahi diren helburuak.
- Proiektua erabat ezartzeak ekarriko lituzkeen onurak. Onuren maila globala ere grafikoki adierazten da, arrisku-maila murrizteari dagokionez.
- Proiektuaren exekuzioa hobetzen duen zibersegurtasunaren neurriak, NISTek (National Institute of Standards and Technology) definitutako zibersegurtasunaren faseak eta nazioarteko erkidegoak erreferentzia gisa onartutakoak erreferentziatzat hartuz: Identifikatzea, Babestea, Detektatzea, Erantzutea eta Berreskuratzea. Proiektuak hobetzen dituen neurriak nabarmentzen dira.
- Proiektua exekutatzeko aurreikusitako denborari buruzko orientazioa. Logikoki, gauzatu beharreko proiektuaren dimentsioari erabat lotuta.
- Enpresa eskatzaileen baliabideen dedikazio-eskakizunak. Proiektuaren barneko langileek proiektuan duten dedikazioa grafikoki adierazi nahi da, kanpoko enpresa espezializatu baten eskutik exekutatzen dela kontuan hartuz.
- Proiektua exekutatzea planteatzerakoan kontuan hartu beharko liratekeen jardunbide egokien zerrenda; kasuren batean mugatzaileak izan daitezke proiektuaren helburuak lortzeko.
- Proiektua exekutatzearekin lotutako zerbitzuak, egin beharreko jardueren tipologiari dagokionez.
- Proiektuarekin lotura estua duten bestelako proiektu batzuk.
- Proiektua kokatzen den Zibersegurtasunaren Euskal Zentroaren (SPRI) zibersegurtasun industrialeko laguntzen programako proiektu-eremu diruz lagungarria, proiektua arautzen duten oinarrietan ezarritakoaren arabera.
- Zerbitzuen edo produktuen enpresa hornitzailearen profila, proiektua exekutatzeaz arduratzen den enpresa espezializatuak aurkeztu beharko lituzkeen gaitasunen arabera adierazpen bat emateko, "Euskadiko Zibersegurtasunaren Liburu Zuria"n erregistratutako kategorizazioaren arabera.

Garrantzitsua da kontuan hartzea adierazitako balorazioak oro har egin direla, eta, beraz, industria-enpresa jakin baten egoera, testuingurua eta beharrak balorazio espezifiko bat izan dezakeela, hemen adierazitakoen desberdina izan daitekeena.

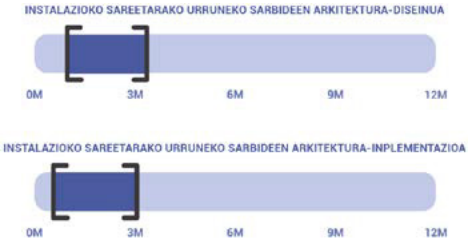
1.3 Garatutako proiektuen xehetasunak

Hona, laburpen gisa, garatutako proiektuen zerrenda.

INDUSTRIA-SAREETAN ARKITEKTURA SEGURUAK DISEINATZEA ETA EZARTZEA

Onurak	Estimatutako exekuzio-denbora	Barneko baliabideen dedikazio-eskakizunak
		

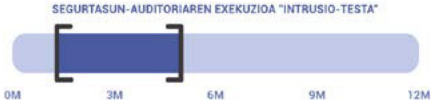
URRUNEKO OT SARBIDEEN SEKURIZAZIOA

Onurak	Estimatutako exekuzio-denbora	Barneko baliabideen dedikazio-eskakizunak
		

INFORMAZIOAREN / DATU INDUSTRIALEN SEGURTASUNAREN EBALUAZIOA

Onurak	Estimatutako exekuzio-denbora	Barneko baliabideen dedikazio-eskakizunak
		

INSTALAZIOETAKO SOFTWARE INDUSTRIALAREN EBALUAZIOA ETA HOBEKUNTZA

Onurak	Estimatutako exekuzio-denbora	Barneko baliabideen dedikazio-eskakizunak
		

PRESTAKUNTZA ETA KONTZIENTZIAZIOA

Onurak	Estimatutako exekuzio-denbora	Barneko baliabideen dedikazio-eskakizunak
		

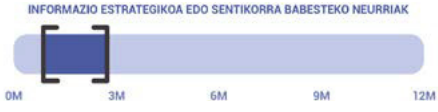
ZIBERSEGURTASUN INDUSTRIALEKO PLANA

Onurak	Estimatutako exekuzio-denbora	Barneko baliabideen dedikazio-eskakizunak
		

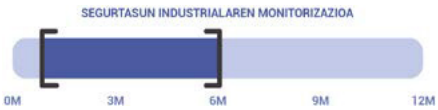
ESTANDARREN JARDUNBIDE EGOKIAK EZARTZEA

Onurak	Estimatutako exekuzio-denbora	Barneko baliabideen dedikazio-eskakizunak
		

INFORMAZIO ESTRATEGIKOA EDO SENTIKORRA BABESTEKO NEURRIAK

Onurak	Estimatutako exekuzio-denbora	Barneko baliabideen dedikazio-eskakizunak
		

SEGURTASUN INDUSTRIALAREN MONITORIZAZIOA

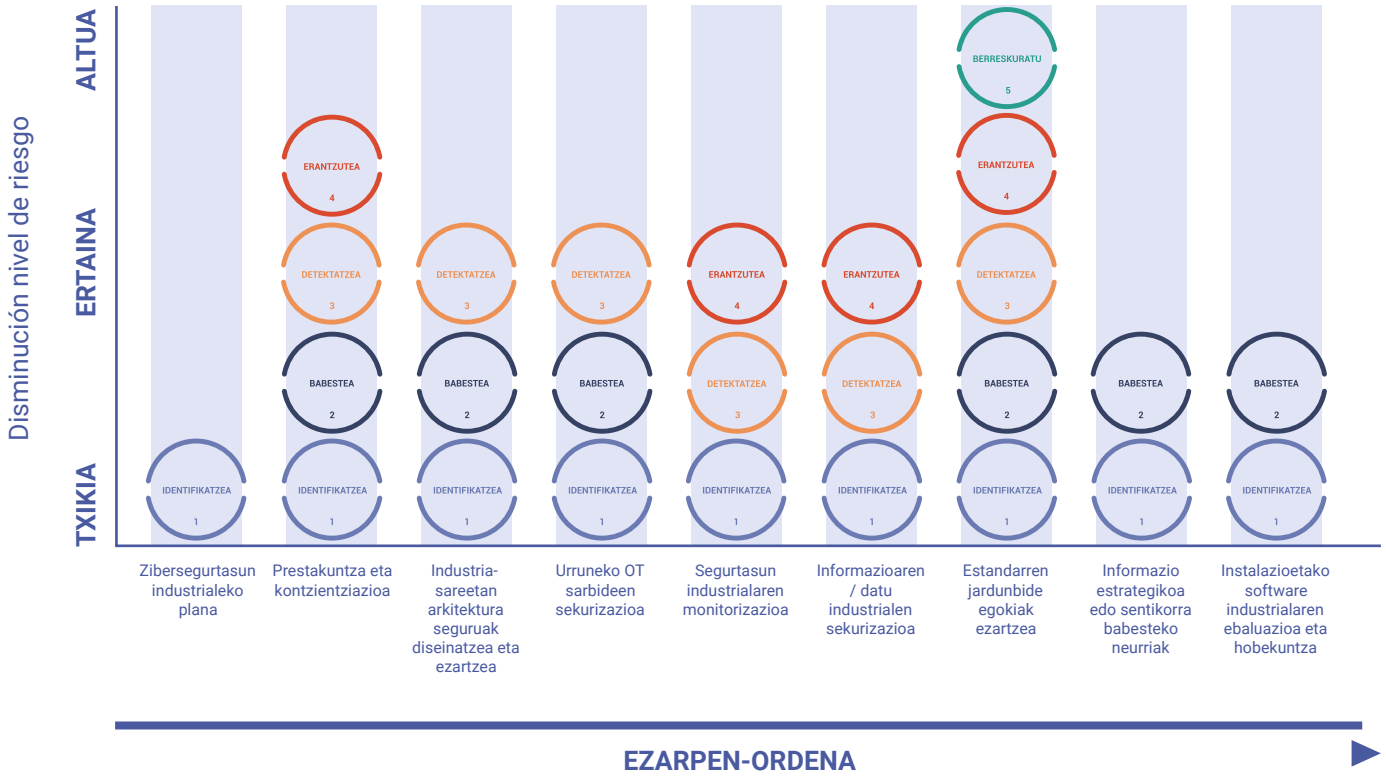
Onurak	Estimatutako exekuzio-denbora	Barneko baliabideen dedikazio-eskakizunak
		

1.4 Zibersegurtasun-proiektuak martxan jartzeko proposamena

Zibersegurtasun-proiektuak egiteko arrazoiak desberdinak izan daitezke:

- Identifikatutako arrisku-maila arintzen edo murrizten duen mehatxu-egoera espezifiko bati erantzuna emateko premia arrazoitua.
- Zibersegurtasun-proiektuei plangintza lehenetsi eta ordenatuaren ikuspegitik heltzen zaien testuinguruan, erakundeak bere gain har dezakeen arrisku-maila lortzeko helburuarekin.
- Bezeroen eta hornitzaileen kontratu-eskakizunak.

Garatutako zibersegurtasun-proiektuak martxan jartzeko ibilbide logikoa zein izango litzatekeen argitzeko, abiapuntua esparru horretan inolako ekimenik egin ez duen eta modu ordenatuan martxan jarri behar duen enpresa bat da. Beraz, proposamena hau izango litzateke:



Zalantzarik gabe, baliteke aurreko grafikoan azaldutako ezarpen-ordena bat ez etortzea enpresa bakoitzaren berezitasun eta inguruabar zehatzekin, eta, beraz, orientazio gisa bakarrik hartu behar da.

.02

PROIEKTUEN XEHETASUNAK

2.1 Industria-sareetan arkitektura seguruak diseinatzea eta ezartzea

PROIEKTUAREN AZALPENA

Duela gutxi arte ohikoa zen IT eta OT sareak ez egotea ez fisikoki ez logikoki konektatuta; baina, egia esan, gaur egun bi ingurune horien arteko elkarreragingarritasuna industria-prozesuen ohiko eragiketarako beharrezkoa den premia bihurtu da kasu askotan.

Ildo horretan, IT eta OT sareetako elementu bereizgarriak sare logiko berean aldi berean egotea ikusgarritasuna eta elkarren arteko elkarrekintza-gaitasuna emateko oinarrizko sarea ezartzearen ondorioa da, eta halakoetan ez dira kontuan hartu zibersegurtasunaren premisak ez diseinuari dagokionez, ez eta inplementazioari dagokionez ere. Eredu hau barne-sareen erabateko konfiantzan oinarritu da, kontuan hartuz barne-trafikoa fidagarria dela, "Zero trust" ereduaren gaur egungo praktika ohikoenetik oso urrun (halakoetan, erakundeen barneko sareek –bai IT eta bai OT sareek– kanpoko sareek edo sare publikoek –adibidez, Internetek– duten arriskuaren aurrean izan dezaketen kontsiderazio bera dute).

Era berean, kontuan hartu behar da OT sareetako elementuak arrisku-maila altuan egoten direla haien gainean hedatutako segurtasun-neurririk ez dagoelako. Kasu askotan, beren antzinatasunarekin lotutako gabeziak, konfigurazio erlaxatuak, eguneratze-falta edo -ezina, sistema eragile zaharkituak... direla eta, eta baita ingurune horretako komunikazio-protokolo bereizgarrien erabileragatik ere, zibersegurtasuna ez zelako kontuan hartu haien diseinuan, eta, beraz, muturren arteko autentifikaziorik gabeko komunikazioek edo komunikazioetan zifraturik ez egoteak, adibidez, nahiko erraz konprometitzea eragiten dute.

Azkenik, garrantzi handikoak dira hirugarren batzuek (ingeniaritzek, fabrikatzaileek, etab.) egungo industria-sistemei euskarria eta/edo mantentzea emateko behar dituzten konektagarritasun-eskakizunak, bai eta instalazioan datuak lortzearekin –produkzio-prozesuak, ekoizpen-mantentzeak eta abar hobetzeko ustiatzeko asmoz– lotutako proiektuetarako beharrezkoak diren konektagarritasun-beharrak ere.

Oinarri nagusia, beraz, sareko eta segurtasuneko arkitektura bat edukitzean datza, hauek ahalbidetuko dituena:

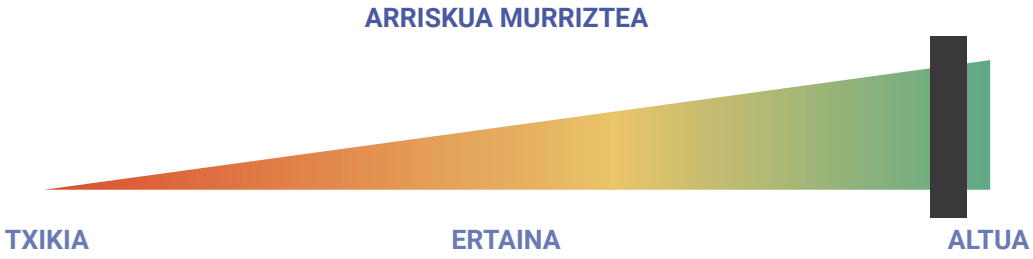
- IT/OT inguruneak bereiztea sareko elektronikaren konfigurazio egoki baten bidez, bai eta segurtasun-elementuak (suebakiak) erabiltzea ere, bi ingurune horien artean gertatzen diren komunikazioak mugatzeko eta monitorizatzeko.
- OT sareen segmentazioa egitea, ingurune horietako bakoitzaren barruan sare gehigarriak (edo "eremuak") definituz, hauek egiteko aukera emango dutenak: 1) eremu horietan funtzionaltasun edo helburu komun bat partekatzen duten elementuak sartzea; eta 2) komunikazioak (edo "hodiak") esplizituki baimendutako trafikoetara mugatzea.

HELBURUAK

Proiektu honek helburu hauek lortu nahi ditu:

- IT/OT sareko arkitektura seguru baten diseinua egitea, IT eta OT inguruneak bereizi ahal izateko beharrezkoak diren neurri guztiak kontuan hartuz, bai eta eremu eta hodi egokiak definitzea ere, sareko elektronikan konfigurazioen bidez, suebakiak erabiliz, trafikoa ikuskatuz, eta abar.
- Aurrez definitutako sare seguruaren diseinu batetik abiatuta, hura ezartzea, ingurune bakoitzerako beharrezkoak eta egokiak diren segurtasun-elementuak eskuratuz eta martxan jarriz.

ONURAK



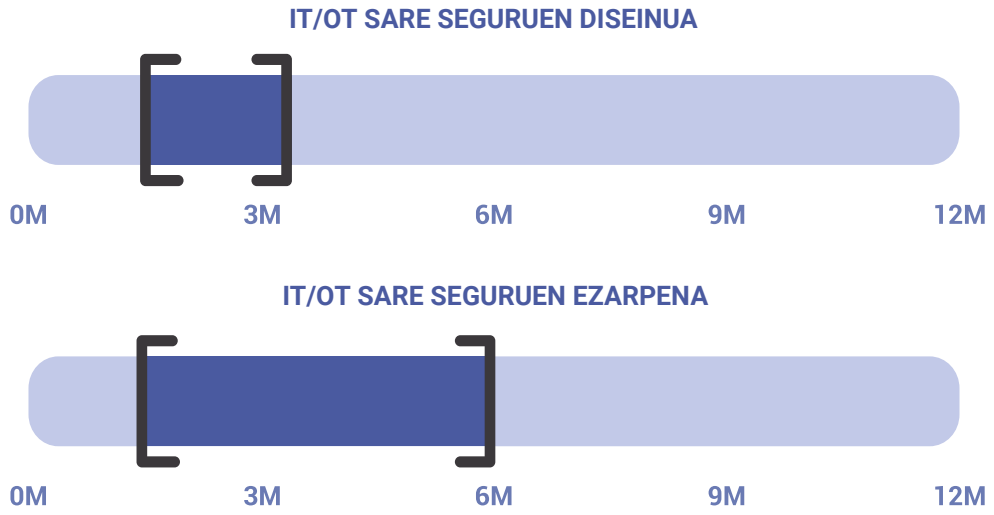
Hauek izango lirateke proiektua martxan jartzeak ekarriko lituzkeen onurak:

1. Negozioaren jarraipena bermatzen laguntzea.
2. Zibermehatxuen aurkako erresilientzia-maila hobetzea.
3. Komunikazioak eta halakoak sortzen dituzten elementuak identifikatzea, behar-beharrezkoak direnak ahalbidetuz.
4. Gaur egungo trafikoaren azterketa egitea eta erakunde barruan lehendik dauden anomaliak detektatzea.
5. Sare-diseinu egokia, eskalagarria eta kudeagarria izatea segurtasun-gobernantzaren ikuspegitik.
6. Segurtasun-gorabehera bat gauzatzeak erakundean izango duen inpaktua murriztea, eremuak eta hodiak behar bezala ezartzeak eragindako eremura mugatuko bailuke.
7. Sare barruan industria-aktiboek duten esposizio- eta ikusgarritasun-maila murriztea.
8. Eremu arteko sareko trafikoaren monitorizazioa izatea, eta baimendu gabeko trafikoa identifikatzea, haren kausak eta izaera aztertu ahal izateko.
9. Eremuen eta inguruneen artean sor daitekeen trafiko gaiztoa (IDS) detektatzeko aukera, eta erreakzio- edo babes-arau automatizatuak (IPS) inplementatzeko aukera.
10. Sare korporatiboetarako hirugarrenen sarbide seguruen arkitektura ezartzeko aukera ematea, kanpo-konexioetarako eta jauzi-eremuetarako eremu espezifikoak sortuz.

PROIEKTUAREN EXEKUZIOA HOBETZEN DUEN ZIBERSEGURTASUNAREN DIMENTSIOAK

ESTIMATUTAKO EXEKUZIO-DENBORA

Horrelako proiektuak exekutatzeko aurreikusitako denborak orientazio gisa bakarrik adierazten dira, hainbat faktoreren mende baitaude: sarearen tamaina eta konplexutasuna, definitu beharreko eremu- eta hodi-kopurua, ingurunearen egungo egoeraren ezagutza, etab.



ENPRESA ESKATZAILEEN BALIABIDEEN DEDIKAZIO-ESKAKIZUNAK

JARDUNBIDE EGOKIAK PROIEKTUA EXEKUTATZEAN

Horrelako proiektuak behar bezala gauzatzeko, alderdi garrantzitsu batzuk hartu behar dira kontuan:

- IT/OT lankidetza: sareak diseinatzeko proiektuek ITko nahiz OTko langileen parte-hartze aktiboa eskatzen dute normalean, batzuetan sarearen "jabetzaren" mugak lausotuta egon baitaitezke bi inguruneetan. Beraz, funtsezkoa da proiektuan aktiboki parte hartzea bai IT Arloko sare-teknikariak eta bai Ekoizpen/Mantentze/Eragiketa/... Arloko langileek, dagoen azpiegiturari buruzko informazioa eta ezagutza eman ahal izateko. Diziplina anitzeko lantaldeak erabiltzea gomendatzen da.
- Industria-testuingurua: instalazio bateko sareko arkitektura diseinatzeko, zehatz-mehatz ezagutu behar da bertako kontrol industrialeko sistemen funtzionamendu-eredua, bai eta integrazio-mailaren arabera OT edo IT ingurunean egon daitezkeen beste elementu batzuekiko interkonexio-beharrak ere.
- Aktiboen inbentarioa: zaila da sare-eredu bat aztertzea eta diseinatzea eredu horrekin zer dagoen konektatuta jakin gabe; beraz, inbentario bat –oinarrizkoa besterik ez bada ere– da industria-testuinguruaren eta mundu fisikoaren arteko harremana ezartzeko aukera ematen duen abiapuntua. Era berean, garrantzitsua da identifikatzea halakoek beste ekipo eta sistema korporatibo batzuekin ezartzen dituzten komunikazioak, bai instalazioetan, bai Cloud plataformetan hedatutakoak.

Aktiboen kritikotasuna: ezaugarri honek industria-prozesu baten barruko aktiboen kritikotasunaren arabera edo eragiten duten arrisku-mailaren arabera kontuan hartu beharreko babes-maila zehazten du, eta baliteke sare-eremu batzuetan beste batzuetan baino segurtasun-maila altuagoa ezarri behar izatea.

Kontrol industrialeko sistemetan aldaketak egiteko aukera: ohikoa da instalazio-sare bat berriro diseinatzeak elementu jakin batzuen helbideratzeetan aldaketak egitea, baina kontuan hartu behar da ezin direla beti egin: aldaketen inpaktu ekonomikoa, funtzionamendu-ziurgabetasuna, aldaketak egiteko ordutegi-leihoak, espresuki eragozten duten hirugarrenekiko kontratuak... faktore horiek mugatzaile posibletzat hartu behar dira, eta sarearen diseinua dauden aukeretara egokitu behar da.

LOTUTAKO ZERBITZUAK

IT/OT sareko arkitektura seguruak diseinatzeko:

- Industria-inguruneetan espezializatutako aholkularitza-zerbitzuak.

IT/OT sareko arkitektura seguruak ezartzeko:

- Segurtasun-ekipamendua hornitzea, instalatzea, konfiguratzea eta martxan jartzea: suebakiak, belaunaldi berriko suebakiak (NGFW).

- Sare-azpiegitura instalatzeko, konfiguratzeko eta martxan jartzeko zerbitzuak (switchak, sarbide-puntuak, etab.)

LOTUTAKO BESTE PROIEKTU BATZUK

- Urruneko sarbideen arkitektura seguruak diseinatzea eta/edo inplementatzea.

ZIBERSEGURTASUN INDUSTRIALEKO LAGUNTZEN PROGRAMAKO PROIEKTU DIRUZ LAGUNGARRIAREN ARLOA

- Zibererasoen aurrean IT / OT inguruneetarako (Information Technology / Operational Technology) babes-sistemak bateratzea eta integratzea. Arkitektura seguruen diseinua eta exekuzioa, eta, hala badagokio, industria-sareen segmentazioa gauzatzea.

ZERBITZUEN EDO PRODUKTUEN ENPRESA HORNITZAILEAREN PROFILA

Mota honetako proiektuetan sartutako zerbitzuak emateko gaitasuna duten enpresak, “Euskadiko Zibersegurtasunaren Liburu Zuria”n erregistratuta daudenak, kategorizazio honetan sartuta daudenak dira:

Gaitasuna	Konponbidearen kategoria	Konponbidearen kategoria
BABESTEA	Babes-teknologia	Wireless segurtasuna Urruneko sarbidea/VPN Hurrengo belaunaldiko suebakia / Suebakia Mehatxuen kudeaketa bateratua (UTM)

2.2 Urruneko OT sarbideen sekurizazioa

PROIEKTUAREN AZALPENA

Kontrol industrialeko sistemek (KIS) enpresen sare korporatiboekiko gero eta konektagarritasun handiagoa izateak zerbitzuak emateko modu berri bat sortzen laguntzen ari dira, bai enpresetako barne-langileen aldetik, bai hornitzaileen aldetik.

KISekin urruneko konexioak ezartzeko aukerak hirugarrenek eskainitako zerbitzuaren kalitatea handitzea errazten du, hainbat ikuspegitatik:

- Funtzionamendu txarrei edo gorabeherei erantzuteko denborak hobetzen dira.
- Instalazioan presentzia fisikorik eskatzen ez duten esku-hartzeetarako baliabideak optimizatzen dira.
- KISetako datuak atzitzeko aukera ematen da prebentziozko mantentzearekin eta industria-prozesuen optimizazioarekin eta hobekuntzarekin –besteak beste– zerikusia duten zereginetarako.
- Teknikari eta langile espezializatuen joan-etorrien kostuak murrizten dira.

Bestalde, eta telelanaren agertokien gorakada kontuan hartuz, bertako langileen urruneko konexioek funtsezko garrantzia hartu dute ohiko funtzioak behar bezala garatzeko.

Alde horretatik, eta bertako langileen konexioei dagokienez, ohikoa bada ere konexioak VPN korporatiboen bidez ezartzea, OT ingurunean normala izaten da ingeniaritza edo fabrikatzaile bakoitzak –instalazio berean aurki ditzakegun askotarikoetatik– urruneko sarbiderako bitarteko propioak izatea eta:

- Kasurik onenean, gailu edo sistema horiek instalazioaren jabe den enpresak ezagutzea, nahiz eta enpresa horrek ez kudeatu.
- Baliteke sare korporatiboa nahitaez erabili behar ez izatea urruneko konexioak ezartzeko, sare mugikorrak baizik (4G, etab.).
- Elementu horien segurtasun-konfigurazioa ez ezagutzea, eta, beraz, erlaxatutako politikek aukera ematea hornitzailearen erantzukizunpeko elementuak nahiz sare korporatiboetako gainerako elementuak ere gehiegi bistaratzeko.
- Azken enpresak konexioen kudeaketarik ez duenez, konexioen ezarpenari buruzko oinarrizko hiru galderen erantzuna ez jakitea: nork, noiz eta zertarako.
- Era horretako sarbideen kontratu-erregulaziorik ez egoteak zailtzen du erantzukizunak esleitzea bitarteko horren bidezko segurtasun-gorabehera bat gertatzen eta gauzatzen bada, hornitzaile bati egotz dakiokeenean.

Azken batean, kontuan hartu behar da instalazioen bihotzerako urruneko sarbiderako bitartekoak egotea sare korporatiboen segurtasunarentzako arriskua bihur daitekeela, baldin eta behar bezala diseinatuta, instalatuta eta kudeatuta ez badaude. Konexioetan segurtasun- eta kontrol-neurririk ez egoteak egoera hauek eragin ditzake:

- Urruneko sarbideen segurtasun-politika erlaxatua edo ez oso murriztailea baimenik ez duen hirugarren batek erabiltzea enpresaren barne-sareak konprometitzeko; horrek, gauzatuz gero, ondorio larriak eragin ditzake.
- Gure hornitzailearen segurtasun-gorabehera bat gure azpiegiturara zabaltzea. Hori da hornidura-katearen bidezko erasoa.

HELBURUAK

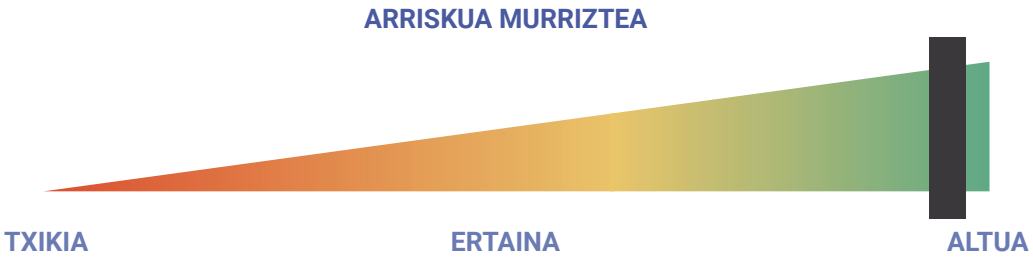
Proiektu honek helburu hauek lortu nahi ditu:

OT ingurunerako urruneko sarbideen eredu bat ezartzea, enpresak behar dituen baliabideak izan ditzan barne-langileek nahiz hirugarrenek ezarritako konexioen gaineko kudeaketa eta ikusgaitasun osoa mantentzeko.

Segurtasunaren eta eraginkortasunaren artean oreka egokia izateko aukera emango duen arkitektura teknologikoa zehaztea, langile propioen nahiz mantentze-zerbitzuen enpresa hornitzaileen urruneko sarbidea egokitzat jotzen diren segurtasun-neurriek kaltetu ez dezaten.

OT ingurunerako urruneko sarbideen arkitektura-eredu bat ezartzea –bai ikuspegi teknikotik bai antolamendu-ikuspegitik–, halakoak behar bezala kudeatzeko beharrezkoak eta egokiak diren politikak, protokoloak eta prozedurak definituz.

ONURAK



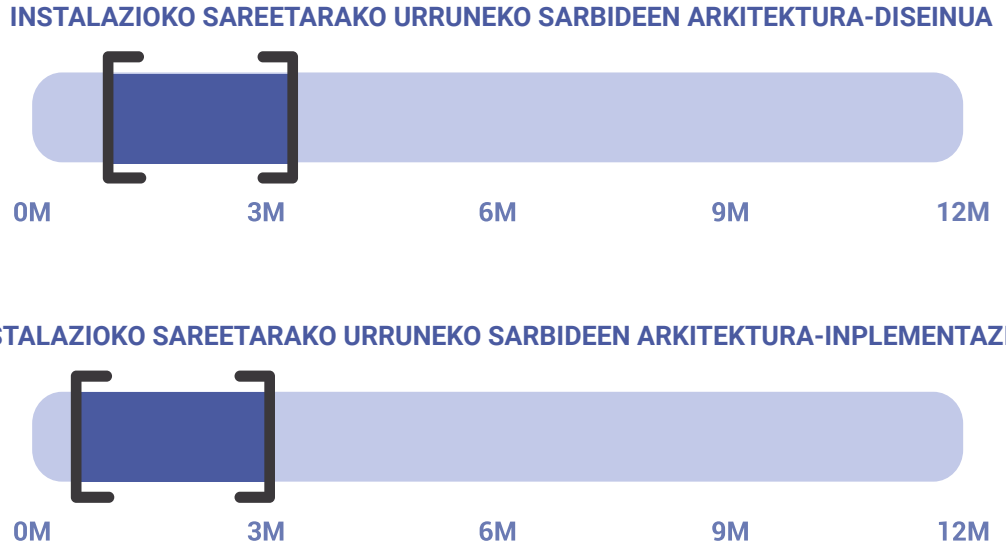
Hauek izango lirateke proiektua martxan jartzeak ekarriko lituzkeen onurak:

1. Negozioaren jarraipena bermatzen laguntzea.
2. Zibermehatxuen aurkako erresilientzia-maila hobetzea.
3. Sare korporatiboen kanpoaldetik egindako OT inguruneko sareetarako konexioek eragindako arrisku-maila murriztea, bai barneko bai kanpoko langileenak.
4. Hornidura-katearen bidez erasoak egiteko probabilitatea murriztea.
5. Instalazioko sareetarako sarbide guztien kontrola eta kudeaketa mantentzea, sare horien bidez egiten ari diren segurtasun-gertaerak identifikatu ahal izateko.
6. Konexioen segurtasuna handitzera bideratutako neurri teknikoak ezartzea ahalbidetzea.
7. Gure hornitzaileen urruneko konexioak ezartzeko kontratu- eta prozedura-esparrua arautzea, segurtasun-gorabehera bat gauzatzen denerako erantzukizunak argi eta garbi ezarriz.
8. Komunikazio-fluxuetan konfidentzialtasuna bermatzea.

PROIEKTUAREN EXEKUZIOA HOBETZEN DUEN ZIBERSEGURTASUNAREN DIMENTSIOAK

ESTIMATUTAKO EXEKUZIO-DENBORA

Horrelako proiektuak gauzatzeko aurreikusitako denborak orientazio gisa bakarrik adierazten dira, eta hainbat faktoreren mende daude: sarearen tamaina eta konplexutasuna, definitu beharreko eremu- eta hodi-kopurua, etab.



ENPRESA ESKATZAILEEN BALIABIDEEN DEDIKAZIO-ESKAKIZUNAK

JARDUNBIDE EGOKIAK PROIEKTUA EXEKUTATZEAN

Horrelako proiektuak behar bezala gauzatzeko, alderdi garrantzitsu batzuk hartu behar dira kontuan:

- Hornitzaileen inbentarioa: Ekoizpen/Mantentze/Eragiketa/... Arloko langileen laguntza eduki behar da, urruneko sarbidea behar duten hornitzaileak identifikatu ahal izateko, zein egoeratan, zein diren gaur egun erabiltzen ari diren bitartekoak (ezagutzen badira) eta urruneko sarbideen indarraldia (urteko euskarria, bi urtekoa, 24x7x365; 8x5; eta abar); eta aldizka berritu behar da.
- Urruneko sarbiderako gailuen inbentarioa: sarea aztertzea urruneko sarbideak ezartzeko erabil daitezkeen gailu inbentariatu gabeen bilaketarako.
- Lehendik dagoen sareko arkitektura-eredua: segmentatu gabeko OT sare batek eragozten du sarbidea soilik behar duten elementuetara urruneko sarbideak mugatzeko eremuak eta hodiak ezartzea.
- Segurtasun-azpiegitura egokia: segurtasun-elementu egokirik ez egoteak edo halakoen konfigurazio eskasak izugarri zaildu dezake enpresa bakoitzaren zirkunstantzia zehatzetara egokitutako urruneko sarbide-ereduak ezartzea.

LOTUTAKO ZERBITZUAK

OT sareetarako urruneko sarbideen arkitektura-eredua diseinatzeko:

- Aholkularitza-zerbitzuak.

Urruneko sarbideen arkitektura-ereduak ezartzeko:

- Segurtasun-ekipamendua hornitzea, instalazioa, konfiguratzea eta martxan jartzea urruneko konexio seguruak ezartzeko funtzionaltasun egokiak dituena: suebakiak, belaunaldi berriko suebakiak (NGFW).
- Urruneko konexioak ezartzeko elementu espezifikoak instalatzeko, konfiguratzeko eta martxan jartzeko zerbitzuak (behar izanez gero).

LOTUTAKO BESTE PROIEKTU BATZUK

- IT/OT sareko arkitektura seguruak diseinatzea eta/edo inplementatzea.
- Industria-sistema kritiko bateko elementuen inbentarioa.

ZIBERSEGURTASUN INDUSTRIALEKO LAGUNTZEN PROGRAMAKO PROIEKTU DIRUZ LAGUNGARRIAREN ARLOA

Urruneko OT sarbideen sekurizazioa ekoizpen-instalazioko industria-ekipamenduekiko, ekipoa mantentzeko, halakoak kontrolatzeko eta eragiteko beharrezkoak direnak; horrelako lanak gero eta maizago egiten dira urrunetik.

ZERBITZUEN EDO PRODUKTUEN ENPRESA HORNITZAILEAREN PROFILA

Mota honetako proiektuetan sartutako zerbitzuak emateko gaitasuna duten enpresak, “Euskadiko Zibersegurtasunaren Liburu Zuria”n erregistratuta daudenak, kategorizazio honetan sartuta daudenak dira:

Gaitasuna	Konponbidearen kategoria	Produktu- / zerbitzu-multzoa
BABESTEA	Babes-teknologia	Wireless segurtasuna Urruneko sarbidea/VPN Hurrengo belaunaldiko suebakia / Suebakia Mehatxuen kudeaketa bateratua (UTM)

2.3 Informazioaren / datu industrialen segurtasunaren ebaluazioa

PROIEKTUAREN AZALPENA

Zalantzarik gabe, informazioa da enpresen jardueraren aktibo nagusia. Bezeroei, eskaerei, pertsonalari eta abarri buruzko daturik gabe, ezinezkoa izango litzateke erakundean ezarritako negozio-prozesuak kudeatzea.

Ikuspegi industrial hutsetik, ondoriozta daiteke negozioarentzat kritiko gisa katalogatu daitekeen informazioa ere badagoela, besteak beste:

- Hirugarren batek emandako informazioaren konfidentzialtasuna babesteko beharra; esate baterako, gure bezero batek pieza bat fabrikatzeko emandako planoak.
- Jabetza intelektuala, industria-patenteei, diseinuei eta abarri dagokienez, gure negozioaren faktore diferentziala osatzen dutenak eta lehiakideentzat balio handia izan lezaketenak.
- Instalazioan ekoizten ari diren kontrol industrialeko sistemen osagaietan exekutatzen ari diren kodeak, programak...; halakoak alteratzeak eragiketak etetea ekar dezake.
- Industria-jardueratik bertatik ateratako datu operazionala, haren analisiaren bidez ekoizpen-prozesuak optimizatzea ahalbidetzen baita.

Industria-arloko informazioa, beraz, eta enpresan egon daitekeen bestelako informazio konfidentziala bezala, babestu behar da, negozioari balio ukaezina ematen diolako. Hala ere, ez da ohikoa aurreko agertokietarako egokiak diren babes-neurriak topatzea.

Alde horretatik, dagoen informazioa bi alderditatik jar daiteke arriskuan:

- Baimendu gabeko datu-esfiltrazioak, erakundeetako barne-langileek gauzatutakoak.
- Une jakin batean informazioa atzi dezaketen hirugarrenek informazioa lapurtzea, modu bideratuan nahiz bideratugabean.

Erakundeak esparru horretan duen sendotasuna frogatzeko bideetako bat da segurtasun-auditoretzak egitea, industria-informazioaren babesaren arloan gabeziak identifikatzeko eta jada hedatuta dauden neurrien eraginkortasuna ebaluatzeko nahiz egokitzat jotzen direnak proposatzeko.

Mota horretako segurtasun-auditoriak edo intrusio-probak ("Hacking Etiko" ere esaten zaio) exekutatzeko formularik ohikoenak hauek dira:

- Bere aldetik iturri publikoen bidez enpresari buruz lor dezakeen informazioa eta sarbidea besterik ez duen eta helburu gisa barne-sare korporatiboetan sartzea eta informazio konfidentziala lortzea dituen erasotzaile baten jarduera simulatzea.
- Konprometitutako sare-postu baten edo erabiltzaile baten kredentzialen lapurretatik abiatutako agertoki bat simulatzea hortik aurrera hirugarren erasotzaile batek egingo lituzkeen ekintzak aurrera eramateko.

Sare korporatiboko postu bat konprometitzera iristeko erabil daitezkeen teknikak dira, besteak beste, kalteberatasunak ustiatzeko neurriak; izaera tekniko hutseko segurtasun-hutsegiteak; eta erabiltzailearen beraren bidez sarbidea lortzen saiatzen diren gizarte-ingeniaritzako teknikak.

HELBURUAK

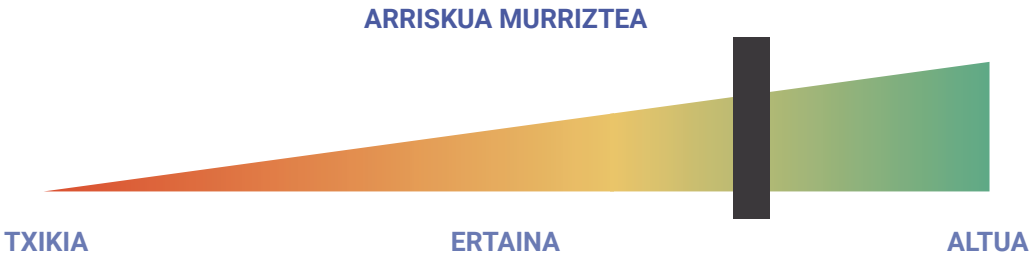
Proiektu honek helburu hauek lortu nahi ditu:

- Erakundeak kanpoko erasotzaile baten ikuspegitik duen esposizio-, babes- eta erresilientzia-maila zehaztea.
- Negoziorako industria-informazio kritikoaren irisgarritasun-maila identifikatzea, bai barneko erabiltzaileen aldetik, bai baimendu gabeko hirugarrenen aldetik.

- Erakundeko erabiltzaileen zibersegurtasunaren arloko kontzientziazio-maila ebaluatzea gizarte-ingeniaritzako teknikak erabiltzen dituzten erasoen aurka.

- Informazioaren konfidentzialtasuna babesteko babes-neurri egokiak zehaztea.

ONURAK



Hauek izango lirateke proiektua martxan jartzeak ekarriko lituzkeen onurak:

1. Negozioaren jarraipena bermatzen laguntzea.

2. Zibermehatxuen aurkako erresilientzia-maila hobetzea.

3. Zibersegurtasunaren gobernantza arduratsuaren atal gisa inplementatu beharko liratekeen neurriak identifikatzea.

4. Erabiltzaileen zibersegurtasunaren arloko prestakuntzari eta kontzientziazioari buruz hartu ahal izan diren neurrien eraginkortasuna egiaztatzea.

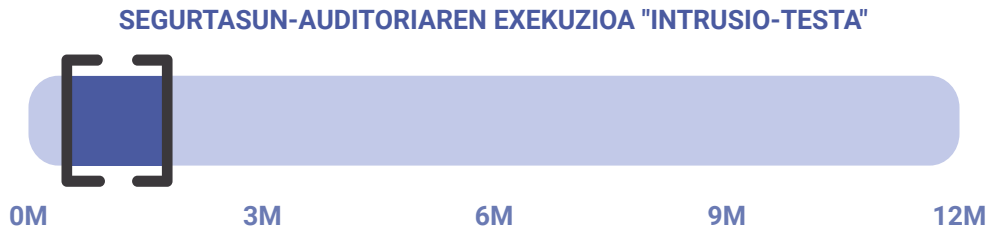
5. Teknikariek mehatxuak detektatzeko eta haiei erantzuteko duten gaitasuna ebaluatzea, benetan eraso-egoera bat simulatzen ari delako.

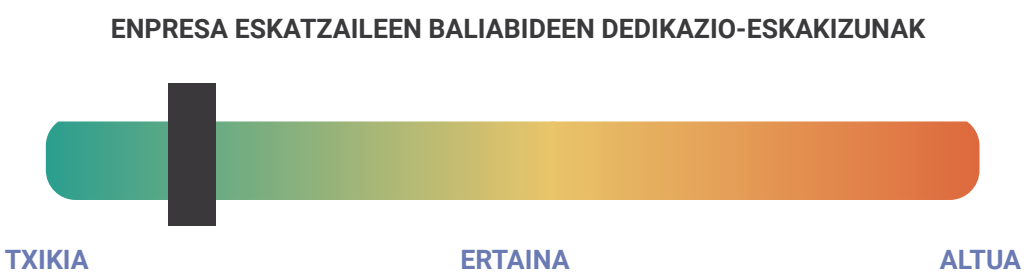
6. Informazio konfidentzialaren une horretako babesa handitzera bideratutako neurri teknikoak definitu edo optimizatu ahal izatea.

PROIEKTUAREN EXEKUZIOA HOBETZEN DUEN ZIBERSEGURTASUNAREN DIMENTSIOAK

ESTIMATUTAKO EXEKUZIO-DENBORA

Horrelako proiektuak exekutatzeko aurreikusitako denborak orientazio gisa bakarrik adierazten dira.





JARDUNBIDE EGOKIAK PROIEKTUA EXEKUTATZEAN

Horrelako proiektuak behar bezala gauzatzeko, alderdi hauek hartu behar dira kontuan:

- Ordutegi-leihoak ezartzea: erakundeak egokitzat jotzen badu, testak exekutatzeko ordutegi-leihoak definitu behar dira; hala ere, kontuan hartu behar da benetako erasotzaile batek ez duela ordu-mugarik eraso bat egiteko.
- Testak kanpoko hornitzaileei jakinaraztea: horrelako ariketak berariaz onartu edo baimendu behar diren neurrian soilik, batez ere komunikazio-hornitzaileen kasuan edo erakundeari urruneko sarbide-zerbitzuak eskaintzen dizkiotenen kasuan.
- Testak teknikariei ez jakinaraztea: horrela, modu praktikoan ebaluatu ahal izango dira gorabeherak detektatzeko, jakinarazteko eta haiei erantzuteko ezarritako prozedurak.
- Kontratu-akordioak egitea: proben ondorioz lor daitekeen informazioa behar bezala tratatzeko, eta bereziki, informazio hori suntsituko dela bermatzeko, ezartzen diren baldintzen arabera.

LOTUTAKO ZERBITZUAK

Horrelako proiektuak behar bezala gauzatzeko, alderdi hauek hartu behar dira kontuan:

- Hacking Etikoan espezializatutako eta industria-inguruneari eta -teknologiari buruzko ezagutza duen lantalde baten aholkularitza-zerbitzuak.

LOTUTAKO BESTE PROIEKTU BATZUK

- Informazio estrategikoa edo sentikorra babesteko neurriak.

ZIBERSEGURTASUN INDUSTRIALEKO LAGUNTZEN PROGRAMAKO PROIEKTU DIRUZ LAGUNGARRIAREN ARLOA

- Informazioaren / datu industrialen sekurizazioa. Erakundetik kanpoko pertsonek egindako erasoen auditoriak eta simulazioak, eta barne-profilei buruzko auditoriak, konpainiaren datuetarako sarbide-maila desberdinekin.

ZERBITZUEN EDO PRODUKTUEN ENPRESA HORNITZAILEAREN PROFILA

- Mota honetako proiektuetan sartutako zerbitzuak emateko gaitasuna duten enpresak, "Euskadiko Zibersegurtasunaren Liburu Zuria"n erregistratuta daudenak, kategorizazio honetan sartuta daudenak dira:

Gaitasuna	Konponbidearen kategoria	Produktu- / zerbitzu-multzoa
BABESTEA	Mantentzea	Intrusio-testa / Red Teaming

2.4 Instalazioetako software industrialaren ebaluazioa eta hobekuntza

PROIEKTUAREN AZALPENA

Kontrol industrialeko sistemak, ekoizpenaren kontrola eta abar kudeatzen dituen softwarea ez da garatu, oro har, segurtasun-neurriak diseinutik aplikatuz; horregatik, oso ohikoa da gabezia asko izatea, hirugarren erasotzaile baten aurrean oso kaltebera egiten dutenak.

Batzuetan, softwarearen antzinatasunagatik, edo enpresa hornitzaileek garapen seguruko sistemetara ez egokitzeagatik, egia da ez dela ohikoa garapen seguruko frameworkak erabiltzea kalteberatasun klasikoen aurkako (SQL Injection, Cross Site Scripting, etab.) neurriak inplementatzeko, baita fuzing, DoS, eta abarretan oinarritutako erasoen aurkako neurriak ere.

Mota honetako proiektuen eremuan, jarduera hauek egin daitezke:

- Industria-eremuko softwarearen/sistemen aurkako kalteberatasunen analisia egitea.
- Sarearen beraren eremuan sistemen eskuragarritasuna eta osotasuna ebaluatzeko probak egitea.
- Programen iturburu-kodea berrikustea eta ikuskatzea, softwarean bertan dauden oinarrizko gabeziak identifikatuz.

Zalantzarik gabe, baimendu gabeko hirugarren batek industria-prozesuak gobernatzen eta erabiltzen dituzten sistemak konprometitzeak oso inpaktu larria izan dezake enpresan; horregatik, softwarearen zibersegurtasuna bermatzea –nahiz eta batzuetan konplexua izan– hobekuntza-neurri garrantzitsua da zibersegurtasunaren arloan.

Nabarmendu behar da softwarearen zibersegurtasunaren hobekuntza oso lotuta egongo dela software-hornitzailearen beraren gaitasunei, seguru asko. Alde horretatik, eta ezin direnez adabakiak edo eguneratzeak garatu eta/edo aplikatu, bestelako konpentsazio-neurri batzuk (edo virtual-patching) planteatu beharko dira.

HELBURUAK

Proiektu honek helburu hauek lortu nahi ditu:

Izaera industrialeko aplikazioen segurtasuna aztertzea eta baimendu gabeko sarbideen aurka duten arrisku maila zehaztea.

Softwareari lotuta dagoen industria-prozesuaren kritikotasunari egokitutako babes-maila izateko hedatu beharreko neurriak ebaluatzea eta ezartzea.

ONURAK

Hauek izango lirateke proiektua martxan jartzeak ekarriko lituzkeen onurak:

Industria-prozesuen jarraipena bermatzen laguntzea eragiten dituen softwarea sekurizatuz.

Zibermehatxuen aurkako erresilientzia-maila hobetzea.

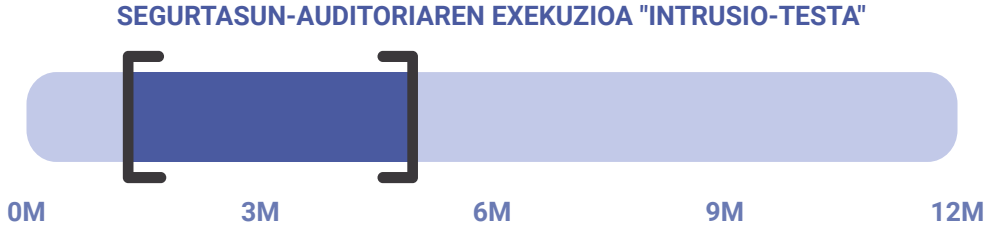
Industria-inguruneko softwarearen esposizio-maila eta kalteberatasunak identifikatzea.

Softwarearen esparruan industria-prozesuen jarraipena bermatzeko hedatu beharko liratekeen neurriak zehaztea.

PROIEKTUAREN EXEKUZIOA HOBETZEN DUEN ZIBERSEGURTASUNAREN DIMENTSIOAK

ESTIMATUTAKO EXEKUZIO-DENBORA

Horrelako proiektuak exekutatzeko aurreikusitako denborak orientazio gisa bakarrik adierazten dira.



ENPRESA ESKATZAILEEN BALIABIDEEN DEDIKAZIO-ESKAKIZUNAK

JARDUNBIDE EGOKIAK PROIEKTUA EXEKUTATZEAN

Horrelako proiektuak behar bezala gauzatzeko, alderdi hauek hartu behar dira kontuan:

- Ordutegi-leihoak ezartzea testak egiteko: erakundeak egokitzat jotzen badu, testak exekutatzeko ordutegi-leihoak definitu behar dira; hala ere, kontuan hartu behar da benetako erasotzaile batek ez duela ordu-mugarik eraso bat egiteko.

- Iturburu-kodearen atzigarritasuna: batzuetan ezin izango da atzitu aplikazioen iturburu-kodea; beraz, ezin izango da mota horretako auditoretzarik egin.

- Segurtasun-hutsegiteak software-hornitzaileei jakinaraztea: segurtasun-arrakalak identifikatzen diren neurrian, hornitzaileari komunikatu beharko litzaizkioke lehenbailehen konpon ditzan, bai gure enpresaren ingurunerako, bai hirugarrenen gainerako instalazioetarako. Alde horretatik, garrantzitsua da hornitzaileak horrelako gertaeren aurrean emandako erantzuna ebaluatzea, hedatu beharreko neurrien kritikotasuna kontuan hartuta.

LOTUTAKO ZERBITZUAK

- Hacking Etikoan espezializatutako eta industria-inguruneari eta -teknologiari buruzko ezagutza duen lantalde baten aholkularitza-zerbitzuak.

- Softwarearen garapenari aplikatutako zibersegurtasunaren ezagutza aurreratuak dituen pertsonal espezializatuaren aholkularitza-zerbitzuak.

LOTUTAKO BESTE PROIEKTU BATZUK

- Industria-sareetan arkitektura seguruak diseinatzea eta ezartzea.

- Estandarren jardunbide egokiak ezartzea.

ZIBERSEGURTASUN INDUSTRIALEKO LAGUNTZEN PROGRAMAKO PROIEKTU DIRUZ LAGUNGARRIAREN ARLOA

- Industria-softwarearen zibersegurtasuna ebaluatzea ekoizpen-instalazioetan eta hura hobetzea.

ZERBITZUEN EDO PRODUKTUEN ENPRESA HORNITZAILEAREN PROFILA

Mota honetako proiektuetan sartutako zerbitzuak emateko gaitasuna duten enpresak, “Euskadiko Zibersegurtasunaren Liburu Zuria”n erregistratuta daudenak, kategorizazio honetan sartuta daudenak dira:

Gaitasuna	Konponbidearen kategoria	Produktu- / zerbitzu-multzoa
BABESTEA	Mantentzea	Intrusio-testa / Red Teaming
	Informazioa babesteko prozesuak eta prozedurak	Static Application Security Testing (SAST) Aplikazioen segurtasuna

2.5 Prestakuntza eta kontzientziazioa

PROIEKTUAREN AZALPENA

Zalantzarik gabe, enpresetan hedatutako babeserako neurri teknikoen eraginkortasuna handitu ahala, erasotzaile batek arrakasta izateko dituen aukerak proportzio berean murrizten dira. Horregatik, mehatxuen gaur egungo panorama pertsonen erabilerara bideratua dago sistema baten konpromisoa lortzeko bitarteko gisa.

Agertoki horretan, giza naturarekin lotutako berezko kalteberatasunek garrantzi handiagoa hartzen dute, eta, beraz, ezagutza eta entrenamendu egokiak eskaini behar dira halakoak ustiatzen saiatzen diren mehatxuen aurka behar bezala erreakzionatu ahal izateko.

Zibersegurtasunaren arloan erabiltzaileak prestatzea eta kontzientziatzea jarduera iraunkortzat hartu beharko litzateke, hauek barnean hartuko dituen prestakuntza-programa bat garatuz:

Profil zehatzei zuzendutako prestakuntza espezifikoa. Barnean hartzen ditu, besteak beste, Goi-zuzendaritzarako prestakuntza-saio espezifikoak nahiz erakundearen zibersegurtasunaren arloan erantzukizun desberdinak dituzten profiletarako alderdi arauemaile, tekniko edo legal egokiagoak garatzen dituzten ikastaroak.

Kontzientziazio orokorreko prestakuntzak zibersegurtasunaren arloan, erakundeko enplegatuei begira.

Erakundeko erabiltzaileak aldiro-aldiro alertan mantenduko dituzten abisuak, aholkuak, informazio-pilulak... zibersegurtasunaren alderdi zehatzei edo gaurkotasun-albisteei dagokienez.

Erabiltzaileen gaitasun-maila ebaluatzeko eta neurtzeko, oso gomendagarria da ariketa praktikoak egitea pertsonei zuzendutako erasoak simulatuz, horrelakoetan prestakuntza-planaren garapenarekin lortutako helburuei buruzko ondorioak eta hobekuntza-alderdiak lortzen baitira. Era horretako ariketak garatzeko erabiltzen diren gizarte-ingeniaritzako teknikek ez dute arlo teknologikora mugatu behar (phishing, identitatea ordeztea...): mundu fisikoan oinarritutako beste teknika-mota batzuk ere praktikan jarri behar dituzte (instalazioetarako intrusio fisikoa, gizarte-ingeniaritza, identitatea ordeztea telefonoz nahiz presentzialki, etab.).

HELBURUAK

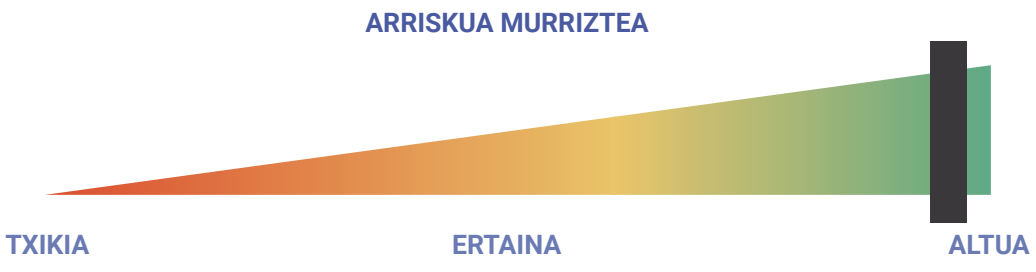
Proiektu honek helburu hauek lortu nahi ditu:

Erakundearen segurtasun globalari laguntzea, langileak zibersegurtasunaren arloan eta, zehazki, industria zibersegurtasunaren arloan prestatuz eta trebatuz.

Bitartekoak eskaintzea erabiltzaileek beren lanpostuaren araberako zibersegurtasun-ezagutzak izan ditzaten, gainerako erakundearentzat izan ditzakeen arriskuez jabetu ahal izateko.

Erabiltzaileak alertan eta "tentsioan" etengabe edukitzea nazioartean nahiz ingurune hurbileneko antzeko enpresetan gerta daitezkeen mehatxuen eta gorabeheren egoerari dagokionez.

ONURAK



PROIEKTUAREN AZALPENA

Hauek izango lirateke proiektua martxan jartzeak ekarriko lituzkeen onurak:

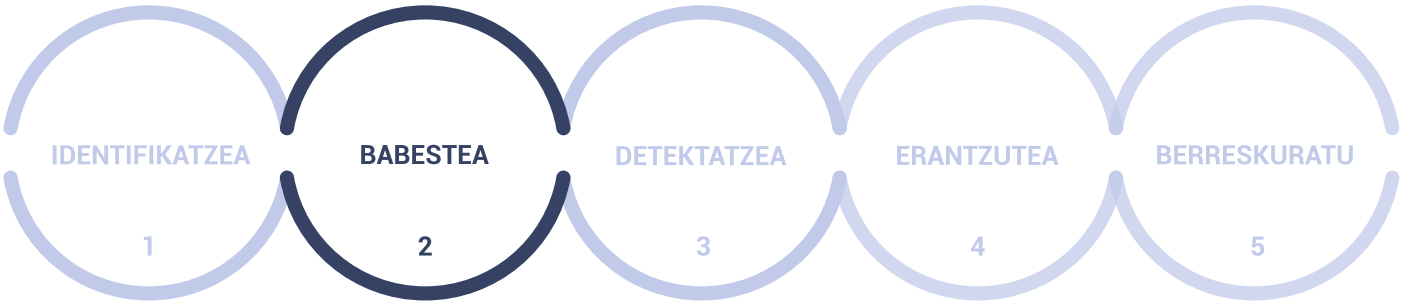
Enpresako langileen gaitasunak eta trebetasunak garatzea haien lan-inguruneari aplikatutako zibersegurtasunarekin zerikusia duten ezagutzak eta trebetasunak eskuratzeko, erakundearen babeserako geruza gehigarri gisa balio dezaten.

Langileak etengabe alertan edukitzea enpresan segurtasun-gorabeherak saihesteko.

Segurtasun fisikoarekin lotutako prozesuetan gertatzen den bezala (esate baterako, sute-simulakroak), kontrolatuta esperimentatzea langileek mehatxu simulatu baten aurka dituzten erreakzioak.

Segurtasun-gorabeherak jakinarazteko bitartekoek behar bezala funtzionatzen dutela egiaztatzea.

PROIEKTUAREN EXEKUZIOA HOBETZEN DUEN ZIBERSEGURTASUNAREN DIMENTSIOAK



ESTIMATUTAKO EXEKUZIO-DENBORA

Horrelako proiektuak exekutatzeko aurreikusitako denborak orientazio gisa bakarrik adierazten dira.

ENPRESA ESKATZAILEEN BALIABIDEEN DEDIKAZIO-ESKAKIZUNAK

JARDUNBIDE EGOKIAK PROIEKTUA EXEKUTATZEAN

Horrelako proiektuak behar bezala gauzatzeko, alderdi hauek hartu behar dira kontuan:

- Prestakuntza pertsonalizatua: prestakuntza bat benetan eraginkorra izan dadin, enpresaren espezifikotasunen arabera diseinatu behar da, bertako langileak prestakuntzan zehar ikusgai dauden erabilera-kasuetan eta adibideetan batez ere islatu ahal izan daitezen.

- Harridura-faktorea: gizarte-ingeniaritzako testak kudeatzen dituzten langileei bakarrik komunikatu behar zaie, harridura-faktorea baliatu ahal izateko langileen erreakzioak ebaluatzeko. Halaber, horretan sartzen dira, bereziki, Goi Zuzendaritzako kideak; horiekin, izan ere, ekintza horiek areagotu beharko lirateke.

- Emaitzen anonimizazioa: prestakuntza-plana garatzean eskuratutako ezagutzei buruz egin daitezkeen testen edo ebaluazioen emaitzak ez dira jendaurrean ikusgai jarri behar pertsona jakin batzuk seinalatuz. Ondorioek orokorrak izan behar dute, baita horiek aztertu ondoren identifikatzen diren indartze- edo hobekuntza-jarduerek ere.

LOTUTAKO ZERBITZUAK

- Prestakuntza eta gaitasun espezifikoko zerbitzuak.

LOTUTAKO BESTE PROIEKTU BATZUK

- Intrusio-testak egitea gizarte-ingeniaritzako teknikak erabiliz.

ZIBERSEGURTASUN INDUSTRIALEKO LAGUNTZEN PROGRAMAKO PROIEKTU DIRUZ LAGUNGARRIAREN ARLOA

- Industria-enpresako plantilla zibersegurtasunaren arloan kontzientziatzeko ekimenak.

ZERBITZUEN EDO PRODUKTUEN ENPRESA HORNITZAILEAREN PROFILA

Mota honetako proiektuetan sartutako zerbitzuak emateko gaitasuna duten enpresak, “Euskadiko Zibersegurtasunaren Liburu Zuria”n erregistratuta daudenak, kategorizazio honetan sartuta daudenak dira:

Gaitasuna	Konponbidearen kategoria	Produktu- / zerbitzu-multzoa
BABESTEA	Kontzientziazioa eta prestakuntza	Prestakuntza-saioak Cyber Ranges
	Mantentzea	Intrusio-testa / Red Teaming

2.6 Zibersegurtasun industrialeko plana

PROIEKTUAREN AZALPENA

Orain arte, industria-inguruneetako zibersegurtasuna, zoritxarrez, ez da kontuan hartu enpresa askotan normaltasunez.

Egoera hori ez da kasualitatea, eta industria osoan gertatzen diren baldintza batzuen ondorioa da:

- Zibersegurtasuna diseinuaren ikuspegitik kontuan ez hartzea; horrek esan nahi du ez dagoela segurtasun-kontrolik edo -neurririk.
- Lehendik dauden kontrol industrialeko sistemen arkitekturaren eta osagaien ezagutza xehaturik eza, askotan enpresa hornitzaileetan soilik dagoena.
- Industria-sareetara konektatutako elementuen antzinatasuna, askotan fabrikatzaileen laguntza teknikoaren epetik kanpo eta segurtasun-kalteberatasun ezagunak dituztenak. Horrek esan nahi du zuzenean proportzionala dela sareko gainerako elementuekiko esposizioa.
- Sare-arkitektura egokirik ez egotea segurtasun-irizpide onargarrien arabera.
- Segurtasun-neurri jakin batzuk martxan jartzeko esku-hartzerako leiho egokiak izateko ezintasuna, 24x7 ekoizpenek edo programatutako mantentze-aldiek baldintzatuak.

Beraz, eta neurri zehatzak abian jartzen hasi aurretik –agian lehentasunezkoenak edo egokienak ez direnak– zibersegurtasun industrialaren "ibilbide-orria" definitzeko jarduera logikoak hauek dira:

- Enpresaren zibersegurtasun industrialaren arloko gaur egungo egoera ezagutzea, puntu ahulak eta indartsuak identifikatzeko aukera emango duen diagnostiko baten bidez, balizko mehatxu-agertokiekiko arriskua baloratuz eta erakundeak arrisku-maila onargarria (eta ezaguna) lor dezan egin beharreko jarduerak zehaztuz.
- Plan bat ezartzea, erakundeak bere gain onar ditzakeen denbora-tartearekin eta baliabide-esleipenarekin (pertsonak, ekonomikoak), zehaztu diren zibersegurtasun-proiektuei modu egituratu eta lehenetsian ekin ahal izateko.

Arrisku-maila zehazteko, arriskuen analisi bat egiten da. Jarduera hori zenbait metodologiaren bidez gauza daiteke, merkatuko estandarretan (Magerit, etab.) nahiz antzeko emaitzak lortzeko aukera ematen duten faktura propiokoetan oinarrituta. Azterketak ahalik eta esparru gehien hartzeko erabil daitezkeen informazio-iturriak edo -jatorriak hauek izan daitezke:

- Segurtasun-esparru edo -estandarrekin kontrastatzea, hala nola ISA/IEC 62443, ISO27002, NIST eta abar.
- Intrusio-testak egitea modalitate desberdinetan, instalazioko hari gabeko komunikazioen analisia barne.
- Kalteberatasunak identifikatzeko analisiak egitea.

Arriskuen analisia egitearen ondorioz identifikatzen diren jardueren zerrendak aukera emango du dagokion ekintza-plana ezartzeko.

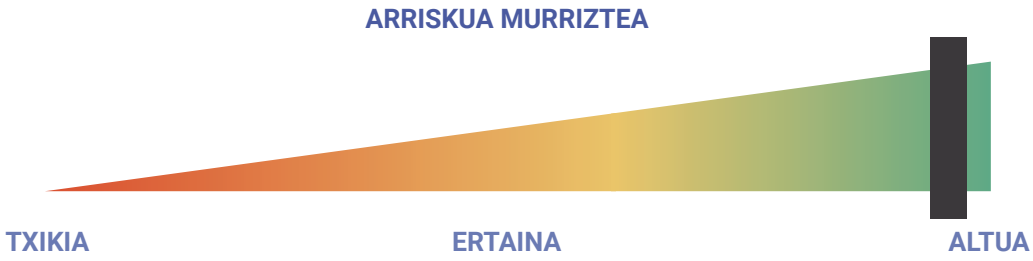
HELBURUAK

Proiektu honek helburu hauek lortu nahi ditu:

- Erakundeak industria zibersegurtasunaren arloan duen arrisku-maila identifikatzea, kuantifikatzea eta agerian jartzea.
- Identifikatutako arriskuak arintzen, transferitzen edo ezabatzen dituzten jarduerak zehaztea.

- Proiektuak exekutatzeko egutegi bat ezartzea, erakundeak aurrera eramatea erabaki duen aurreko puntuko jarduerak jasoko dituena, haren arrisku-gosean oinarrituta.
- Enpresako Goi Zuzendaritzari jakinaraztea, proiektu-plana aurkeztuz, balidatuz, babestuz eta hari jarraipena eginez.

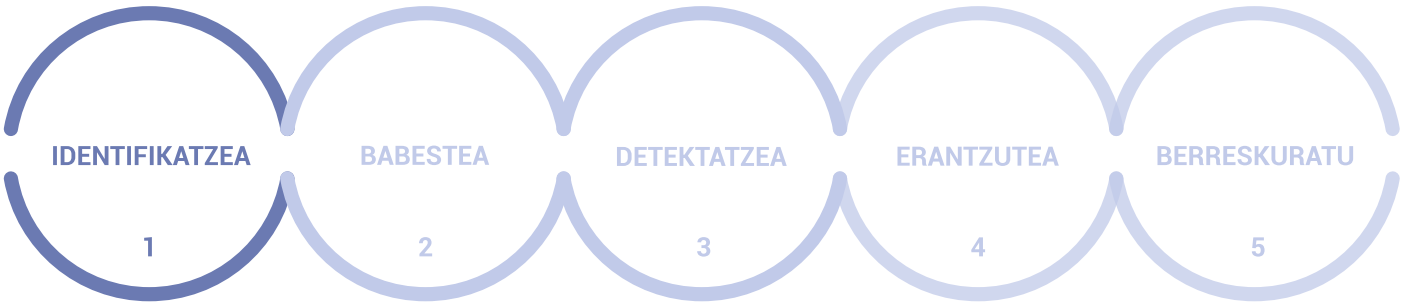
ONURAK



Hauek izango lirateke proiektua martxan jartzeak ekarriko lituzkeen onurak:

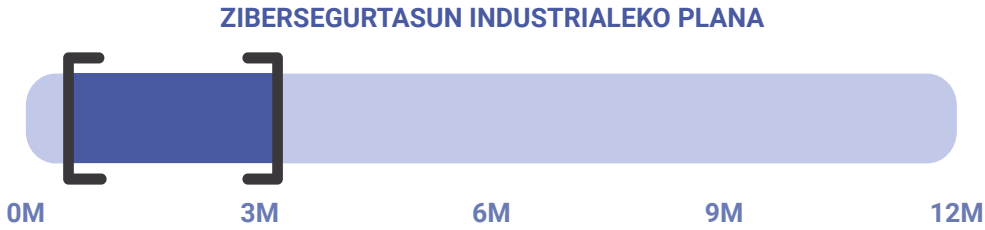
1. Erakundeak onar ditzakeen mugetara eramateko behar diren arrisku-maila eta jarduerak ezagutzea, negozioaren jarraipena bermatzen laguntzeko.
2. Kostuen eta inbertsioen egutegi bat izatea, finantza-funtzioa planifikatzeko hitzartutako denbora-epe gertagarri batean heldu beharreko segurtasun-proiektuei dagokienez.
3. Enpresako Goi Zuzendaritzari jakinaraztea negozioak jasan ezin dituen inpaktuak eragingo dituzten eta espero ez diren etenak eragin ditzaketen arrisku-agertokien aurka jarduteko beharra.

PROIEKTUAREN EXEKUZIOA HOBETZEN DUEN ZIBERSEGURTASUNAREN DIMENTSIOAK



ESTIMATUTAKO EXEKUZIO-DENBORA

Horrelako proiektuak exekutatzeko aurreikusitako denborak orientazio gisa bakarrik adierazten dira.



ENPRESA ESKATZAILEEN BALIABIDEEN DEDIKAZIO-ESKAKIZUNAK

TXIKIA ERTAINA ALTUA

JARDUNBIDE EGOKIAK PROIEKTUA EXEKUTATZEAN

Horrelako proiektuak behar bezala gauzatzeko, alderdi hauek hartu behar dira kontuan:

- Goi Zuzendaritzaren laguntza: goi-zuzendaritzak ekimenean parte hartzen ez badu, aukera dago proiektuak planaren diseinuaren fasetik harago aurrera ez egiteko. Garrantzitsua da laguntza hori bermatzea eta, batez ere, Planaren balidazio formala bilatzea.

- Konfiantza eta gardentasuna: batzuetan –eta proiektuaren sustatzailearen arabera–, litekeena da informazio jakin bat emateko unean erreparoak izatea edo errealitatearen arabera modu fede-emailean ez transmititzea. Kontuan hartu behar da zibersegurtasunaren arloan erakundeak guztiz sendotu gabe dituen alderdiak agerian jartzeak plan honen bidez alderdi horiek hobetzeko aukera ematen duela.

LOTUTAKO ZERBITZUAK

- Aholkularitza-zerbitzuak.

LOTUTAKO BESTE PROIEKTU BATZUK

- Industria-sistema kritiko bateko elementuen inbentarioa.

- Intrusio-test industrial bat egitea.

- Hari gabeko industria-komunikazioen auditoriak.

ZIBERSEGURTASUN INDUSTRIALEKO LAGUNTZEN PROGRAMAKO PROIEKTU DIRUZ LAGUNGARRIAREN ARLOA

- Industriaren zibersegurtasun industrialaren arloko gaur egungo egoeraren diagnostikoa egitea eta zibersegurtasuna hobetzeko ekintza-plana lantzea. Arrisku industrialaren eta kalteberatasun industrialaren analisia. Industria-sistema kritiko bateko elementuen inbentarioa. Intrusio-test industrial bat egitea. Web-aplikazioetako kalteberatasunen analisia. Hari gabeko industria-komunikazioen auditoriak.

ZERBITZUEN EDO PRODUKTUEN ENPRESA HORNITZAILEAREN PROFILA

- Mota honetako proiektuetan sartutako zerbitzuak emateko gaitasuna duten enpresak, "Euskadiko Zibersegurtasunaren Liburu Zuria"n erregistratuta daudenak, kategorizazio honetan sartuta daudenak dira:

Gaitasuna	Konponbidearen kategoria	Produktu- / zerbitzu-multzoa
IDENTIFIKATZEA	Negozioaren ingurunea	Negozioko inpaktuaren analisia
	Gobernantza eta arriskuaren kudeaketa	Betetzea, arriskua eta gobernantza
	Arriskuaren analisia	-
	Arriskua kudeatzeko estrategia	-
	Arriskuaren kudeaketa hornidura-katean	-

2.7 Estandarren jardunbide egokiak ezartzea

PROIEKTUAREN AZALPENA

Tradizioz, informazioaren segurtasunaren gobernantza ahalbidetu duten kudeaketa-sistemak ezarri izan dira –batez ere ISO27001 arauan oinarrituta–; aspaldi honetan, erreferentzia-estandarrak eta -esparruak sortu dira industria-eremu hutsean antzeko funtzioa inplementatzeko aukera emateko, hala nola: ISA/ IEC 62443, NIST CSF, etab.

Informazioaren segurtasuna eta eragiketa-prozesuena batera kudeatzeak erakunde osoaren zibersegurtasunaren kudeaketa sistema bakar batean integratzea dakar. Hala eta guztiz ere, industriak, gaur egun, industria-sektore gehienetan aplika daitekeen IT eta OT zibersegurtasuna kudeatzeko esparru bakar bat identifikatzeko premia du. Izan ere, gabezia horren aurrean, araudi sektorialak garatu dira (baita enpresa bakar baten esparru esklusiboak ere), oro har lehen aipatutako araudien eta estandarren birformulazioak besterik ez direnak.

Alde horretatik, askotan enpresek estandar horietan zehaztutako jardunbide egokiak abian jarri direla ohartarazten dute, zibersegurtasunaren kudeaketa beste helburu osagarririk gabe hobetzeko bide gisa; baina beste kasu batzuetan beharra hirugarrenen (normalean bezeroen) eskakizunetatik dator, halakoek eskatzen dutelako enpresak zibersegurtasuna modu arduratsuan kudeatzen duela frogatzeko, ziurtagiri jakin batzuk lortzeko betebeharra barne.

Erreferentzia-esparru edo -estandar horiek erakundeak ezarri beharko lituzkeen segurtasun-kontrolen multzo bat ezartzen dute, erakundearen ezaugarri zehatzetan oinarrituta aplikagarriak diren ala ez kontuan hartuta, eta zibersegurtasunarekin lotutako alderdi guztiak hartzen dituzte barnean: pertsonak, prozesuak eta teknologia.

Zibersegurtasun industrialaren irismenari edo aplikagarritasunari dagokionez, ISA/IEC 62443 arauak segurtasun-kontrolen multzo osoa eskaintzen du hainbat rol edo ikuspegitatik: instalazioen jabea, sistemen integratzailea edo osagaien fabrikatzailea. Osagaien fabrikatzailearen rolaren kasuan, estandar horrek erreferentzia-esparru bat ezartzen du osagaien garapen segururako (ISA/IEC 63442-4-1), bai eta inplementatu beharreko segurtasun-kontroletarako ere (ISA/ IEC 62443-4-2), lortu beharreko segurtasun-maila objektiboaren arabera.

Beraz, etorkizun hurbilean alderdi hauek barneratu, inplementatu eta, batzuetan, erakunde ziurtagiri-emaile independente batek emandako ziurtagiri bidez frogatu beharko dira:

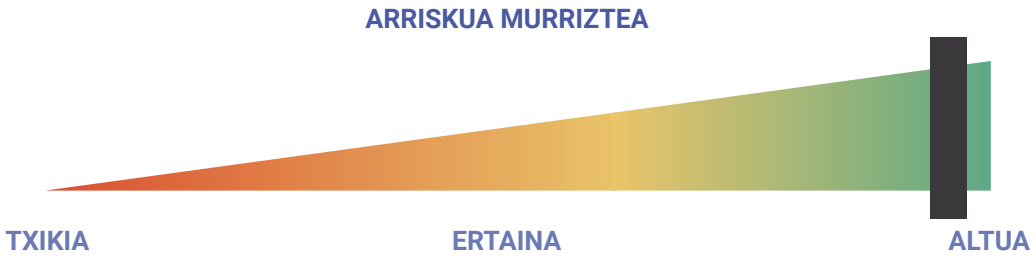
- Zibersegurtasuna industria-inguruneetan kudeatzea (IT eta OT inguruneak modu integratuan barnean sartuz), erakundearen prozesu korporatibo gisa tratatuz.
- Osagai batean inplementatutako zibersegurtasunaren arloko diseinuan, garapenean eta funtzionaltasunetan segurtasuna izatea.

HELBURUAK

Proiektu honek helburu hauek lortu nahi ditu:

- Negozioaren jarraipena bermatzea, bertako zibersegurtasunaren kudeaketan oinarrituta.
- Erakunderen arriskua ez ezagutzearen ondoriozko segurtasun-gorabehera bat gauzatzeko probabilitatea murriztea.
- Erakundeak zibersegurtasunaren arloan duen arrisku-mailaren ikuspegi iraunkorra izatea.
- Zibersegurtasuna prozesu korporatibo gisa txertatzeko egiturazko eta etengabeko sistematika bat ezartzen laguntzea.
- Erakundeak onargarritzat jotzen dituen mugen barruan arrisku-mailari eusteko bitarteko eta baliabide egokiak esleitzea.

ONURAK



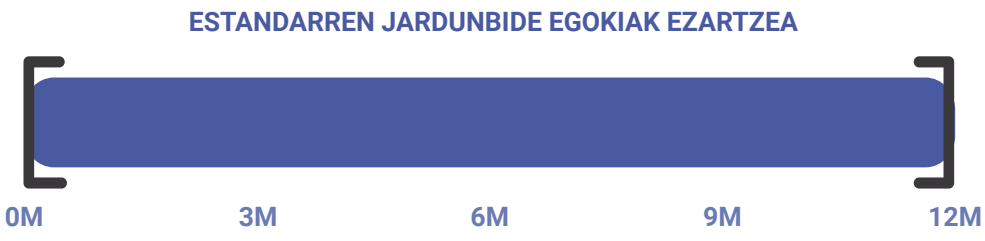
Hauek izango lirateke proiektua martxan jartzeak ekarriko lituzkeen onurak:

1. Zibersegurtasunaren beharraren kultura bultzatzea negozioaren jarraipena bermatzeko funtsezko oinarri gisa.
2. Zibersegurtasuna kudeatzeko prozesu formal korporatiboak ezartzea, halakoen eraginkortasuna kontrolatzeko eta hari jarraipena egiteko neurriak ezartzeko aukera emanez.
3. Zibersegurtasunaren arloko rolak eta erantzukizunak zehaztea eta esleitzea, batez ere askotan IT eta OT inguruneen arteko mugak oso lausoak direnean.
4. Zibersegurtasuna diseinutik txertatzea kontrol industrialeko sistemak martxan jartzean enpresen instalazioetan bertan.
5. Osagaiak zibersegurtasunaren ikuspegitik garatzeko aukera ematea.
6. Erakundeari berari edo merkaturatzen diren produktuei aplikatutako zibersegurtasunaren arloan baimendutako ziurtagiri-erakunde independenteek egiaztatutako aitorpena lortzea.
7. Bezeroek eta hornitzaileek eskakizun berriak betetzea arrisku teknologikoen murrizketari, informazioa baliatzeari eta hornidurak bermatzeari dagokienez, besteak beste.

PROIEKTUAREN EXEKUZIOA HOBETZEN DUEN ZIBERSEGURTASUNAREN DIMENTSIOAK

ESTIMATUTAKO EXEKUZIO-DENBORA

Horrelako proiektuak exekutatzeko aurreikusitako denborak orientazio gisa bakarrik adierazten dira.



ENPRESA ESKATZAILEEN BALIABIDEEN DEDIKAZIO-ESKAKIZUNAK

TXIKIA ERTAINA ALTUA

JARDUNBIDE EGOKIAK PROIEKTUA EXEKUTATZEAN

Horrelako proiektuak behar bezala gauzatzeko, alderdi hauek hartu behar dira kontuan:

- Goi Zuzendaritza proiektuaren sustatzaile gisa: IT eta OT segurtasuna kudeatzeko sistema bat ezartzeak nahitaez enpresako Arlo ia guztien parte hartzea eta baliabideak bideratzea eskatzen duenez, proiektua Goi Zuzendaritzak egindako eskaera gisa sortu behar da, hark lortu nahi duen helburua ezta hura gauzatzeko erabili beharreko baliabideak ere zalantzan jarri ahal izan ez daitezen.
- Aldaketaren kudeaketa: prozesu berriak ezartzeak edo zibersegurtasun-eskakizunen arabera egiteko moduetan aldaketak egiteak aldaketaren kudeaketa ona eskatzen dute, erakundeak modu positiboan eta naturalean aldaketak bere gain hartu ahal izan ditzan denbora-tarte labur batean.

LOTUTAKO ZERBITZUAK

- Aholkularitza-zerbitzuak.

LOTUTAKO BESTE PROIEKTU BATZUK

- Zibersegurtasun industrialaren arloko araudietara edo sektore- eta enpresa-eskakizunetara egokitzea.
- Segurtasunaren Eskema Nazionala –SEN– betetzeko egokitzea (3/2010 Errege Dekretua).
- PIC Erregelamendura egokitzea (704/2011 Errege Dekretua).

ZIBERSEGURTASUN INDUSTRIALEKO LAGUNTZEN PROGRAMAKO PROIEKTU DIRUZ LAGUNGARRIAREN ARLOA

- Zibersegurtasun industrialeko estandarretan (ISA/IEC 62443 edo baliokideetan) edo Zibersegurtasuna kudeatzeko bestelakoetan (ISO 27001 edo baliokideetan) jasotako jardunbide egokiak txertatzea. Segurtasunaren Eskema Nazionala (3/2010 Errege Dekretua), PIC Erregelamendua (704/2011 Errege Dekretua) betetzeko egokitzea. Zibersegurtasunaren kudeaketa-prozesua etengabe hobetzea, neurri espezifikoak hedatuz edo neurri horiek lehendik zeudenetara baino heldutasun-maila altuagoetara eramanez.

ZERBITZUEN EDO PRODUKTUEN ENPRESA HORNITZAILEAREN PROFILA

Mota honetako proiektuetan sartutako zerbitzuak emateko gaitasuna duten enpresak, “Euskadiko Zibersegurtasunaren Liburu Zuria”n erregistratuta daudenak, kategorizazio honetan sartuta daudenak dira:

Gaitasuna	Konponbidearen kategoria	Produktu- / zerbitzu-multzoa
IDENTIFIKATZEA	Negozioaren ingurunea	Negozioko inpaktuaren analisia
	Gobernantza eta arriskuaren kudeaketa	Segurtasun-ziurtagiria Betetzea, arriskua eta gobernantza
	Arriskuaren analisia	-
	Arriskua kudeatzeko estrategia	-
	Arriskuaren kudeaketa hornidura-katean	-

2.8 Informazio estrategikoa edo sentikorra babesteko neurriak

PROIEKTUAREN AZALPENA

Informazioa ezinbesteko aktiboa da enpresentzat. Negozio-prozesu guztiak garatzeko aukera ematen du, eta prozesu horiek galtzeak edo atzitzerik ezak ondorio garrantzitsuak izan ditzake negozioaren jarraipenean.

Informazioa hainbat leku eta modutan aurki daiteke: paperean nahiz euskarri digitalean, datu-baseetan, fitxategi ofimatikoen zerbitzarietan, hodeiko biltegiratze-sistemetan, etab.; egia esan, gaur egun, industria-ingurune batean prozesu zehatz baten oinarri gisa erabiltzen den paperezko informazio-kantitatea gero eta txikiagoa da (eta, kasu askotan, hutsala).

Beraz, bitarteko digitaletan dagoen informazioa ziurtatzeak berekin dakar, berez, enpresaren funtzionamendua bermatzea. Hala ere, informazio digitalaren babes egokia lortzeak berekin dakar hainbat gai planteatzea, eta horiek erronka handi bihur daitezke:

- Enpresak ba al daki non dauden informazio korporatiboa biltzen duten biltegiak?
- Gai al gara daukagun informazioaren kritikotasuna zehazteko?
- Gai al gara informazioaren balioa zehazteko eta informazio hori galtzeak, atzitu ezin izateak edo hirugarrenei baimendu gabe transmititzeak –esate baterako– zer eragingo lukeen aurreikusteko?
- Ezagutzen al ditugu gaur egun informazioaren baimenik gabeko tratamenduak prebenitzeko aplikatzen ari diren segurtasun-neurriak? Eta halakoen eraginkortasun erreala?

Azken finean, informazioa babesteko neurriak planteatzea dokumentu-kudeaketako alderdi orokorrak –lehen aipatutakoak, besteak beste– kontuan hartu gabe neurri eraginkorra izan daiteke, baina kasu askotan ez oso efizientea.

Beraz, eta enpresak negoziorako informazio kritikoena edo konfidentzialena gutxienez identifikatua duelako oinarritik abiatuta, beharrezkoa izango da babes-maila egokia lortzeko antolamendu- eta prozedura-neurri nahiz neurri tekniko batzuk ezartzea. Neurri teknikoen artean, hauek azpimarra ditzakegu, besteak beste:

- Fitxategi korporatiboen zerbitzarietako karpetetarako sarbide-baimenen bidezko kontrola.
- IRM (Information Rights Management) konponbideak hedatzea informazioaren kontrola mantentzeko, biltegiratuta dagoen lekua kontuan hartu gabe.
- DLP (Data Loss Prevention) sistemak martxan jartzea, sare korporatiboetatik datuak transmititzeko bide ohikoenen bidez informazioaren baimenik gabeko ihesak prebenitzeko neurriak ezartzeko aukera ematen dutenak.
- Hodeiko sistemetan dagoen informazioaren segurtasuna kudeatzea, CASB (Cloud Access Security Broker) konponbideen bidez, halako inguruneetan dauden baliabideetako segurtasun-politikak aplikatzeko aukera ematen dutenak.

HELBURUAK

Proiektu honek helburu hauek lortu nahi ditu:

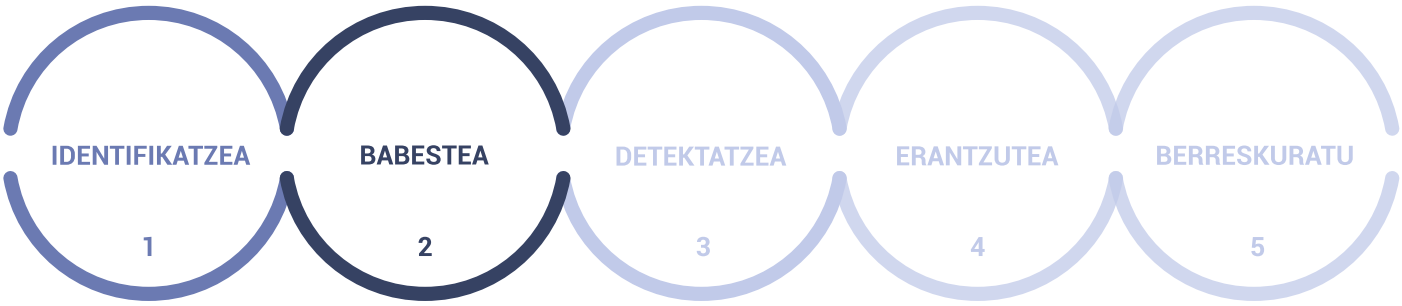
- Enpresarentzat kritikoa den informazioaren konfidentzialtasuna bermatzea, bai hirugarrenen aurrean, bai baimendu gabeko barneko langileen aurrean.
- Enpresari laguntzea Industria Jabetzaren Legea betetzen, bertako informazioa babestuz.

ONURAK

Hauek izango lirateke proiektua martxan jartzeak ekarriko lituzkeen onurak:

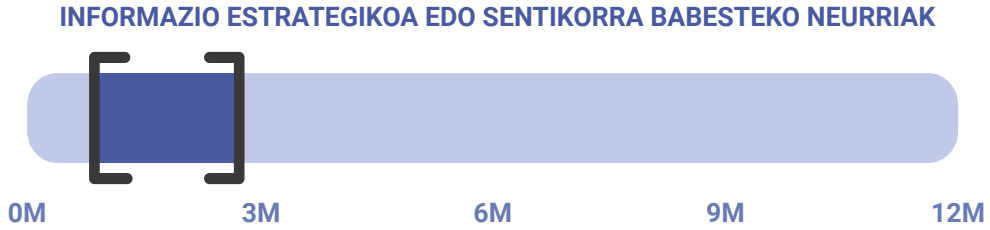
1. Negozioaren jarraipena erraztea, informazioa ziurtatuz.
2. Informazio korporatiboko biltegiak eta bertako informazioaren konfidentzialtasun-maila identifikatzea.
3. Dokumentazio konfidentzialari buruzko kontrol zorrotza izatea informazio horren tratamendu jakin bat nork, noiz eta nola egin duen jakiteko.
4. Baimenik ez duten pertsonei informazio konfidentziala eskuratzea oztopatzea.

PROIEKTUAREN EXEKUZIOA HOBETZEN DUEN ZIBERSEGURTASUNAREN DIMENTSIOAK



ESTIMATUTAKO EXEKUZIO-DENBORA

Horrelako proiektuak exekutatzeko aurreikusitako denborak orientazio gisa bakarrik adierazten dira.



ENPRESA ESKATZAILEEN BALIABIDEEN DEDIKAZIO-ESKAKIZUNAK

JARDUNBIDE EGOKIAK PROIEKTUA EXEKUTATZEAN

Horrelako proiektuak behar bezala gauzatzeko, alderdi hauek hartu behar dira kontuan:

- Informazio-biltegiak identifikatzea: beharrezkoa izango da informazioa biltzean oinarritutako teknikak aplikatzea erakundearen arlo desberdinetako erabiltzaileekin egindako elkarrizketen bidez, bai eta aurkikuntza-lanetarako tresna automatizatuak erabiltzeko aukera ere. Lehen aipatu den bezala, hori da, oro har, erakunde batek aurre egin beharreko lehen erronka.

- Informazioaren konfidentzialtasun-maila ezartzea: horretarako, gomendatzen da informazioari balio ekonomiko bat ezartzea edo, gutxienez, informazio hori galtzeak, atzitu ezin izateak edo lapurtzeak erakundean eragingo lukeen inpaktua kualitatiboki ezartzea, ondoren konfidentzialtasun-maila jakin bakoitzerako kontuan hartzen diren babes-neurriak aplikatzea justifikatu ahal izateko.

- Informazioaren babes-maila zehaztea: informazio horri aplikatu beharreko neurriak zehaztuko ditu .

LOTUTAKO ZERBITZUAK

- Aholkularitza-zerbitzuak.

- Softwarea hornitzea, instalatzea, konfiguratzea eta martxan jartzea informazio konfidentziala edo sentikorra babesteko.

LOTUTAKO BESTE PROIEKTU BATZUK

- Segurtasun-kopien sistemak egokitzea.

ZIBERSEGURTASUN INDUSTRIALEKO LAGUNTZEN PROGRAMAKO PROIEKTU DIRUZ LAGUNGARRIAREN ARLOA

- Informazio estrategikoa edo sentikorra babesteko neurriak, hala nola jabetza intelektuala, I+G+b estrategiak, eraikinen edo produktuen diseinuaren planoak, DBEOk edo negozioaren lehiakortasunarekin eta jasangarritasunarekin zuzenean lotutako beste edozeinek eragindako informazioa (neurrien adibidea: biltegiratzea zifratzea, sarbide-kontrola, kopia-banaketaren kontrola, ezabaketa segurua, etab.).

ZERBITZUEN EDO PRODUKTUEN ENPRESA HORNITZAILEAREN PROFILA

Mota honetako proiektuetan sartutako zerbitzuak emateko gaitasuna duten enpresak, “Euskadiko Zibersegurtasunaren Liburu Zuria”n erregistratuta daudenak, kategorizazio honetan sartuta daudenak dira:

Gaitasuna	Konponbidearen kategoria	Produktu- / zerbitzu-multzoa
IDENTIFIKATZEA	Gobernantza eta arriskuaren	Betetzea, arriskua eta gobernantza
BABESTEA	Datuaren segurtasuna	Informazio-ihesaren prebentzioa Zifratzea Hodeira sartzeko segurtasuna Sinadura digitala
	Babes-teknologia	Segurtasun-kopiaren segurtasuna eta biltegiratzea

2.9 Industria-segurtasunaren monitorizazioa

PROIEKTUAREN AZALPENA

Industria-sareetan gertatzen denaren ikuspegi osoa, xehatua eta etengabea izatea funtsezko faktorea da segurtasun-gertaerak identifikatzeko eta haiei erantzun egokia emateko enpresentzat ondorio onartezinak dituzten inpaktuak gertatu aurretik.

Industria-sareen monitorizazioak aukera eman beharko luke hauei buruzko informazioa lortzeko:

- Industria-sareetan gertatzen ari diren eraso-patroien identifikazioa, bai IT ingurunearen (zoritxarrez oso ohikoak instalazio-inguruneetan) bereizgarriak direnena, bai OT inguruneko espezifikoena.

- Sareko trafikoa interpretatzean lortutako informazioaren azterketa, ikuspegi operatibo hutsetik (prozesu-aldagaien datuak), dauden industria-protokoloei lotua, lortutako datuen eta kontrol industrialeko sistemen errealitatearekin harreman bat ezartzeko aukera emango duen testuingurua aplikatu ondoren.

- Era berean, eta sarearen monitorizazioak trafiko zirkulatzailearen oso ikusgarritasun handia eskaintzen duenez, sarean dauden industria-aktiboen argazkia lortzea.

Hala ere, monitorizazio-sistema on batek ez ditu berez konpontzen segurtasun-gorabeheren kudeaketarekin lotutako alderdi guztiak, kontuan hartuz sistema horiek ematen duten informazioa aztertu egin behar dela eta, identifikatutako gertaeraren kritikotasunaren arabera beharrezkoa bada, erantzun-ekintza egokiekin jokatu behar dela.

Alde horretatik, oso interesgarria da monitorizazio-sistema industrialetatik lortutako informazioa SIEM (Security Incident and Event Management) konponbide batean sartzea, gertaera-korrelazio handiago baten parte izan daitezen, segurtasun-ekipoei gorabeherak detektatzeko eraginkortasun handiagoa eskainiz.

HELBURUAK

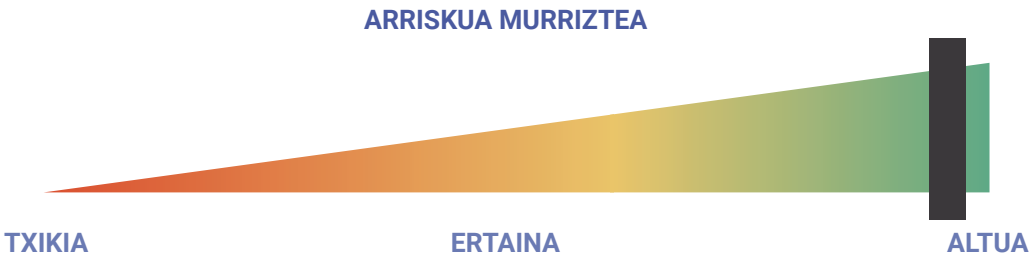
Proiektu honek helburu hauek lortu nahi ditu:

- Sare korporatibo industrialetan segurtasun-gertaerak identifikatzeko gaitasuna izatea.

- Segurtasun-gorabehera bat gauzatzen denean, erantzun-denborak eta, beraz, ekoizpen-sistemetan izandako inpaktua arintzeko bitartekoak eta baliabideak eskaintzea.

- Segurtasun-monitorizazioa kudeatzeko eredu bat ezartzea, neurtu eta hobetu daitekeena.

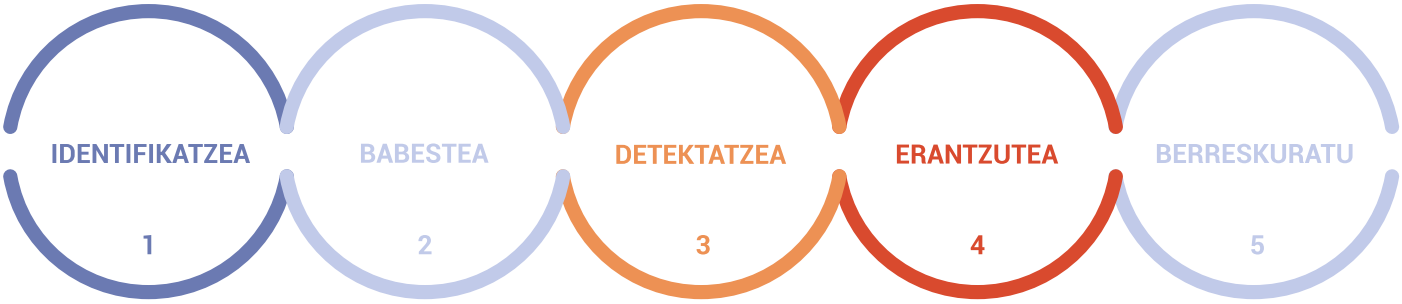
ONURAK



Hauek izango lirateke proiektua martxan jartzeak ekarriko lituzkeen onurak:

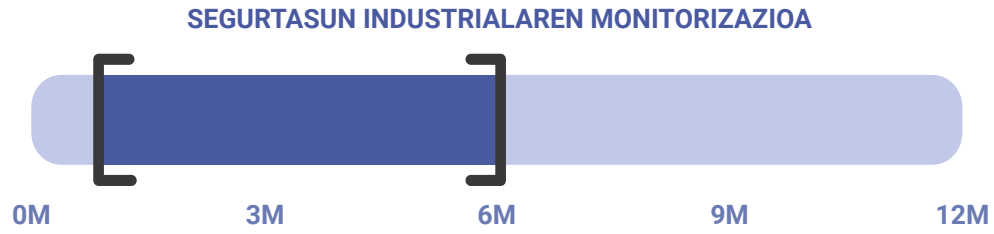
1. Industria-sareetako aktiboen identifikazioa eta inbentarioa.
2. Identifikatutako aktiboei lotutako kalteberatasunen identifikazioa.
3. Industria-sareetako trafikoa bistaratzea.
4. Negozioaren jarraipena bermatzea, IT/OT ohiko eraso-patroietan oinarritutako segurtasun-gorabeheren identifikazio proaktiboari esker.
5. Esanguratsuak izan daitezkeen edo segurtasun-gertaera batekin erlazionatuta egon daitezkeen anomalia operazionalak identifikatzea.
6. Erantzuteko gaitasunak aktibatzeko denborak hobetzea segurtasun-gorabehera bat gauzatuz gero.

DIMENSIONES DE LA CIBERSEGURIDAD QUE MEJORA LA EJECUCIÓN DEL PROYECTO



ESTIMATUTAKO EXEKUZIO-DENBORA

Horrelako proiektuak exekutatzeko aurreikusitako denborak orientazio gisa bakarrik adierazten dira.



ENPRESA ESKATZAILEEN BALIABIDEEN DEDIKAZIO-ESKAKIZUNAK

JARDUNBIDE EGOKIAK PROIEKTUA EXEKUTATZEAN

Horrelako proiektuak behar bezala gauzatzeko, alderdi hauek hartu behar dira kontuan:

- Datu-bilketaren mailak: argi eta garbi zehaztu behar da sareko trafikoa zer mailataraino iritsiko den, kontuan hartuz askotan sare korporatiboan interfaze bakarra duen makina batek barne-sare oso zabala eduki dezakeela. Egoera horrek hurrengo puntuaren garapena baldintzatzen du.

- Monitorizazio-sistemaren arkitektura: industria-inguruneak monitorizatzeko sistema bat hedatzean, zailtasun nagusia sarearen datuak atzitzeko sistemaren dimentsionamendua eta arkitektura da, askotan kudeatu ezin diren komunikazio-elementuak daudelako, zundak behar bezala hedatzea eragozten dutenak.

- Aktiboen identifikazio aktiboa edo pasiboa? Trafikoaren monitorizazioaz gain era horretako konponbideak erabiltzen baditugu gure OT aktiboen inbentarioa hornitzeko, kontuan hartu behar da identifikazio-teknika pasiboak erabiltzeko aukera (lortu beharreko informazioaren xehetasun-maila monitorizazio-sistemak ikusitako trafiko-motaren oso mendekoa da, ez baitago inolako interakziorik azken ekipoekin) eta/edo aktiboak erabiltzeko aukera (azken elementuekiko interakzioa informazio zehatza lortzeko). Teknika aktiboei dagokienez, gomendatzen da konponbideek konexio-protokoloak erabiltzea, galdetutako elementuen funtzionamendu egokia kaltetu edo oztopatu gabe.

- Monitorizazio-sistema kudeatzeko eta ikuskatzeko baliabideak: garrantzitsua da monitorizazio-sistema batetik jasoko den informazioaren tratamenduak dakarren lan-karga gehigarria kontuan hartzea; beraz, beharrezkoa da jarduera hori barnean nahiz hirugarrenen zerbitzuekin indartzeko beharra planteatzea.

LOTUTAKO ZERBITZUAK

- Kudeatutako segurtasun-zerbitzuak eta segurtasun-mehatxuak monitorizatzeko zerbitzuak.

- Industria-inguruneetako segurtasuna monitorizatzeko softwarea hornitzea, instalatzea, konfiguratzea eta martxan jartzea.

LOTUTAKO BESTE PROIEKTU BATZUK

- Sarearen kudeaketa- eta monitorizazio-sistemak hedatzea (NMS – Network Management System).

- Automatizazio industrialeko osagaietan aldaketak monitorizatzeko eta kontrolatzeko sistemak.

ZIBERSEGURTASUN INDUSTRIALEKO LAGUNTZEN PROGRAMAKO PROIEKTU DIRUZ LAGUNGARRIAREN ARLOA

- Perimetroko segurtasun-gailuak eta bestelako gailu industrialak monitorizatzea (switchak, zundak, appliance-ak, suebaki industrialak, PLCak, etab.).

ZERBITZUEN EDO PRODUKTUEN ENPRESA HORNITZAILEAREN PROFILA

Mota honetako proiektuetan sartutako zerbitzuak emateko gaitasuna duten enpresak, “Euskadiko Zibersegurtasunaren Liburu Zuria”n erregistratuta daudenak, kategorizazio honetan sartuta daudenak dira:

Gaitasuna	Konponbidearen kategoria	Produktu- / zerbitzu-multzoa
DETEKTATZEA	Anomaliak eta gertaerak	Intrusioen detekzioa
	Segurtasunaren etengabeko monitorizazioa	SIEM / Gertaera-korrelazioaren konponbidea Cyber Threat Intelligence Segurtasuneko eragiketa-zentroa (SEZ)
ERANTZUTEA	Erantzun-plana	Gorabeheren kudeaketa
	Arintzea	Gorabeherei erantzuteko zerbitzuak (CSIRTaaS)

Basque CyberSecurity Centre

BASQUE CYBERSECURITY CENTRE:

Euskadiko zibersegurtasunaren topalekua

info@bcsc.eus

Albert Einstein 46, 3ª planta Edificio E7
Arabako Teknologi Parkea
01510 Vitoria-Gasteiz

945 236 636