1. Erronka proposatzen duten erakundeak

UPTEK: IBARMIA, LANTEK, LOIRE, ONA, ZAYER

2. Erronka

Nola bihur ditzakegu seguru makinak eta haien softwareek sortzen dituzten datuak? Nola hobe dezakegu zibersegurtasuna gure aktiboen kudeaketa globalean?

3. Balizko konponbide aplikagarriak

- Zibersegurtasuna: aktiboen/datuen segurtasuna eta ziber-adimena
- Software eta hardwarearen segurtasun-ingeniaritza
- Segurtasunaren kudeaketa eta *threat intelligence*: mehatxuen monitorizazioa eta korrelazioa
- Arrisku-auditoretza edo -mapak
- Urruneko sarbideak indartzeko teknologiak
- Nortasun digitalen eta sarbideen kudeaketa (IAM)

4. Testuingurua

M-H sektoreko zibersegurtasuna merkatuan eskaintzen diren produktuei, izan makinak (Ibarmia, Loire, Ona eta Zayer) edo softwarea (Lantek) eta enpresaren ekoizpen- eta lan-prozesuei aplikatzen zaie. Izan ere, eskainitako makina eta produktuek beste makina eta sistemekiko konexio ugari dituzte, eta bezeroari arriskurik gabeko konexio segurua ziurtatu behar zaio une oro. Horrez gain, konpainiak gai izan behar du ziurtatzeko haren prozesuak ere seguruak direla. Testuinguru horretan, erronka proposatzen duten enpresek zenbait arazo eta interes dituzte:

- Batzuek urteak daramatzate Internet bidez konektatzeko web-aplikazioak eskaintzen, eta haiek zenbait zerbitzaritako hodeiaren bidez sartzen dira horietan. Beraz, urruneko sarbide seguru ziurtatu behar dute. Alde horretatik, konponbideak zenbait bezerotan ezarri direnez, garrantzitsua da konexioen kudeaketa globala izatea, mehatxuak monitorizatu eta horiei erantzuteko.
- Beste batzuek arazoak dituzte modu seguruan sartzeko eta bezeroaren makinetatik datuak ateratzeko urrunetik.
- Halaber, saldutako makina batzuek bigarren salmenta edo hirugarrenen erabilera okerra izan ditzakete, eta, beraz, planteatzen da mugimendua eta lokalizazioa kontrolatzea, edo makina erabili ahal izateko hatz-aztarnak erabiltzea.

Testuinguru horretan, enpresa bakoitzak behar dituen segurtasun-estandarrak zehaztuko dituzten startupen laguntza behar da, eta horiek lortzeko konponbideak aplikatu behar dira, ziurtatzeko horiek teknologia-hornitzaile gisa merkatuan egiten dituzten proposamenak seguruak direla bezeroentzat, eta lehiakide gisa kokatzen dituztela egungoaren gaineko mailan.

5. Azpierronkak eta helburuak

Aurrekoa ikusita, eta aintzat hartuta, gainera, sektoreko ekipamenduek ahultasun ugari dituztela beste ekipamendu, sistema periferiko eta SW tresnekiko konexioan, enpresek makinaren eta haren konexioen segurtasuna hobetu behar dute, hau da, makinaren babesa bermatu behar dute, bai barruan eta bai kanpoan.

Beraz, parte hartu duten ETE-ek 2 azpierronka planteatzen dituzte erronka honekin lotuta:

1. **Datuaren segurtasuna hobetzea:** izan ere, gaur egun, zibersegurtasunaren arloko arazo nagusietako bat datuaren "esfiltrazioa" da, hau da, gorde nahi den ingurunetik ihes egitea. Mehatxu zibernetikoak geroz eta ohikoagoak dira, eta askotan ez dute datua lapurtzen, baizik eta faltsutu. Beraz, proposatzen da **datuaren jatorriaren ziurtapena balioztatu eta kudeatzeko erronka bat** jorratzea.
2. Bestalde, ikuspuntu integralago batetik, enpresek konponbideak behar dituzte **euren aktiboak modu globalean kudeatzeko, monitorizatzeko eta mehatxuei erantzun koordinatua emateko.** Horretarako, interesgarria izango litzateke, lehenik eta behin, prozesu osoan zehar laguntzeko startup bat, **aktibo eta konexioen segurtasun globala ziurtatzeko**: horretarako, lehenik, gailu/protokolo/konexioen zibersegurtasun-**analisi digital forentseak** egingo dira, arrisku-mapa bat sortzeko eta jarduketak lehenesteko, eta, bigarrenik, **zibersegurtasun-eragiketen zentro bat finkatzeko, gorabeherak prebenitzeko, zuzenean monitorizatzeko eta mehatxuei erantzuteko.**

Amaitzeko, enpresek merkatuan egiten dituzten galderetako batzuk erakusten dira, testuinguruan jartzeko goiko 2 azpierronkekin erakutsi nahi diren <u>arazoetako</u> batzuk:

- Monitoriza eta aktiba daiteke mehatxuen aurreko erantzun automatiko bat modu koordinatuan eta globalean, erakundearen eskutik?
- Nola artikula daitezke babes-mekanismoak bezeroari produktuan eskainitako konexio-zerbitzuetan?
- Alerta- eta blokeo-mekanismoak gara daitezke makinen mugimendua hautemateko?
- Nola ziurta daitezke erakundearen sarerako konexio seguruak langileak kanpotik konektatzen direnean?