Enpresa-Garapenerako Euskal Agentzia
Agencia Vasca de Desarrollo Empresarial
Business Development Basque Agency
www.spri.eus

SPRI-ENPRESA GARAPENEKO EUSKAL AGENTZIA

PRESKRIPZIO TEKNIKOEN AGIRIA

ENDPOINT DETECTION AND RESPONSE (DETEKZIOA ETA ERANTZUNA) SEGURTASUN-ZERBITZUAREN LIZENTZIAK HORNITZEA ETA ZERBITZUA EMATEA

AURKIBIDEA

1. KONTRATUAREN XEDEA 3

2. EGUNGO EGOERA 3

3. ZEHAZTAPEN TEKNIKOAK 3

1 HORNIDURA: EDR eragileen lizentziak urtero hornitzea 3

2 ZERBITZUA: EDR eragileen instalazio- eta mantentze-zerbitzua 4

3 ZERBITZUA: gorabeherak monitorizatzeko, aztertzeko eta haiei eusteko zerbitzua 4

1. KONTRATUAREN XEDEA

SPRI-ENPRESEN GARAPENERAKO EUSKAL AGENTZIAk (aurrerantzean, **"SPRI"**) Endpoint detekzioa eta erantzuna (*Endpoint Detection and Response as a Service* - EDRaaS -) segurtasun-zerbitzuaren hornidurarako kontratu bat du gaur egun, eta kontratu hori 2023ko martxoaren 31n amaituko da.

Lizitazio honen xedea da Endpoint detekzioa eta erantzuna (*Endpoint Detection and Response as a Service* - EDRaaS -) segurtasun-zerbitzua kontratatzea SPRI Taldeko gailuen parkerako, gaur egun duen zerbitzuari jarraipena emateko.

Horretarako, honako hornidura eta zerbitzu hauek hornituko dira (horien deskribapen teknikoa aurreragoko ataletan garatzen da):

- 1 HORNIDURA: EDR eragileen lizentziak urtero hornitzea (aurrerantzean, **"1 HORNIDURA"** edo **"1H"**).
- 2 ZERBITZUA: EDR eragileen instalazio- eta mantentze-zerbitzua (aurrerantzean, **"2 ZERBITZUA"** edo **"2Z")**
- 3 ZERBITZUA: gorabeherak monitorizatzeko, aztertzeko eta haiei eusteko zerbitzua (aurrerantzean, **"3 ZERBITZUA"** edo **"3Z")**

2. EGUNGO EGOERA

SPRI-ENPRESEN GARAPENERAKO EUSKAL AGENTZIAk gaur egun *FireEye (FireEye Endpoint Security Agent*) markako EDR eragile bat (*Endpoint Detection and Response*) du instalatuta lan-ekipoen eta zerbitzarien parkean (ekipo eramangarriak eta mahaigaineko PCak). Guztira 400 ekipo dira.

Norberak erabiltzeko ekipoek eta zenbait zerbitzarik antibirus bat dute (EDR eragilearen osagarri gisa). Zerbitzarien kasuan, egungo antibirusa desinstalatu eta FireEyekin antibirus-modulua aktibatzeko aukera aztertuko da.

Gainera, EDRaaS Zerbitzua dugu, zeinak Endpoint Detection & Response (EDR) teknologia baten hedapena, 7x24 monitorizazioa eta portaeran oinarritutako mehatxuak detektatzen dituen tresnaren eragiketa dituen. Ekipo guztiak fabrikatzailearen kontsolan daude erregistratuta (EDR eragile baten bidez) eta monitorizatuta ((FireEye Hx).

3. ZEHAZTAPEN TEKNIKOAK

1 HORNIDURA: EDR eragileen lizentziak urtero hornitzea

500 gailutarako *FireEye* lizentziak. Honako hauek dira onartutako bertsioaren gutxieneko baldintzak:

Sistema eragilea	Bertsioa
Windows	Win 10 (32-bit and 64-bit)

	Server 2003 R2 SP2 (32-bit and 64-bit)
	Server 2008 (32-bit and 64-bit)
	Server 2008 R2, R2 SP1, R2 SP2 (64-bit)
	Server 2012 (32-bit and 64-bit)
	Server 2012 R2 (32-bit and 64-bit)
	Server 2016 (32-bit and 64-bit)
Linux	RHEL 6.8+, 7.2+, 8 (64-bit)
	CentOS 6.9+, 7.2+, 8 (64-bit)
	Ubuntu 14.04, 16.04, 18.04, 19.04
	Oracle Linux 6.10, 7.6

Jarraian, hornitu beharreko produktuen fabrikatzailearen *part number* kodeak agertzen dira:

part number	Lizentziaren deskribapena:
EP-E-P-2W-PTM-999-1Y	Endpoint Security Ent Pwr Ed 2- Way w/PTM sppt, per Endpoint
EP-P-C-1Y	Endpoint Security Cloud Power Edition

2 ZERBITZUA: EDR eragileen instalazio- eta mantentze-zerbitzua

Enpresa adjudikazioduna arduratuko da EDR eragileak hedatzeaz, bai eta horiek eguneratzeaz ere. Horretarako, zerbitzu horri ordu-poltsa bat emango zaio (administrazio-baldintzen agirian deskribatutako baldintzetan).

2. atalean ("EGUNGO EGOERA") deskribatu den bezala, ekipoak fabrikatzailearen kontsola bakar batean daude erregistratuta (EDR eragileen bidez). EDR eragile berrien hedapena, hala badagokio, fabrikatzailearen egungo kontsolan egin behar da.

Zerbitzari moduko ekipoetan EDR eragilearentzako eskuragarri dagoen antibirus-modulua aktibatzea aztertuko da. Enpresa adjudikaziodunaren ardura izango da gaur egun instalatuta dagoen antibirusa desinstalatzea eta antibirus-modulu berria aktibatzea.

3 ZERBITZUA: gorabeherak monitorizatzeko, aztertzeko eta haiei eusteko zerbitzua

Instalatutako EDR FireEye eragileetan gorabeherak monitorizatzeko, aztertzeko eta haiei eusteko zerbitzua hornitu beharko da. Honako hauek dira gutxieneko baldintzak:

- FireEye Hx Cloud fabrikatzailearen kontsolatik kudeaketa zentralizatua egitea (ez da onartuko enpresa lizitatzailearen hodeian hedatzea).
- Aktibo guztien 24x7 monitorizazioa (500 *endpoints* arte).
- Ekipo kritikoen multzoa definitzea, 24x7 aztertzeko.

- Aktibo guztien 8x5 azterketa (gutxienez 20 azterketa).
- Aktibo kritikoen 24x7 azterketa (gutxienez 2 azterketa aktiboen % 10entzat gutxienez).
- Mehatxu batek kaltetutako gailuei zerbitzuaren irismenean eustea, eta aktibo ez kritikoen euste automatikoa 5 minutuan baino gutxiagoan.
- Adimen espezifikoa txertatzea:
    - IOCak (konpromiso-adierazleak) txertatzea FireEye Hx-ren kontsolan.
    - Ikerketetatik eratorritako IOC propioak kentzea.
- Mehatxu eta *malware*en azterketa proaktiboa.
- Tiketen gorabeherak, eskabideak eta jarraipena kudeatzea Segurtasun Eragiketen Zentro (ESZ) baten bidez.

Gutxienez, honako jarraipen-jarduera hauek gauzatu beharko dira:

- Zerbitzuen txosten teknikoak hilero.
- Zerbitzuaren jarraipena egiteko bilerak hilero.
- Lan-bilera teknikoak hiru hilean behin, zerbitzuarekin lotutako gaiak jorratzeko. SPRIk zehaztuko ditu bilera horiek.