Podpora in vzdrževanje varnostno-operativnega centra – Opis storitev

Predmet razpisa je obratovanje, nadgrajevanje in podpora rešitvi VOC, kar pomeni zagotavljanje nemotenega in stalnega nadgrajevanja in podpore rešitvi VOC, ves čas delovanja rešitve VOC, skladno s pogoji iz razpisne dokumentacije, razen v primeru, če naročnik naroči drugačen režim zagotavljanja nadgrajevanja in podpore rešitve VOC, ki ga omogoča ponudnik.

Natančnejši obseg predmeta javnega naročila bo naročnik objavil v drugi fazi.

Storitev VOC nivo L1, L2 in L3 v režimu 24/7/365

- Stalno spremljanje, preizkušanje, sodelovanje, navzkrižno korelacijo vseh dogodkov, zbranih iz širokega nabora notranjih orodij, zaposlenih ali drugih virov informacij, pa tudi ublažitev in odpravljanje incidentov, ki izhajajo iz dogodkov odkritih na prvi stopnji.
- Kategorizacija, določitev prednostnih nalog in priporočila za zadrževalne ukrepe, določanje vplivov dogodka ter resnosti (kršitev, incident).
- Izdelava načrta za blažitev, sanacijo in reševanje, s ciljem popolne vzpostavitve normalnega stanja. Operativne dejavnosti za odpravo posledic bodo izvedene s strani končnih naročnikov, ponudnik pa zagotovi usmerjanje in koordinacijo aktivnosti.
- Forenzična analiza varnostnega incidenta

Zagotavljanje nemotenega in stalnega nadgrajevanja in podpore rešitvi VOC

Zagotavljanje nemotenega in stalnega nadgrajevanja in podpore rešitvi VOC, skladno s pogoji iz razpisne dokumentacije, razen v primeru, če naročnik naroči drugačen režim zagotavljanja nadgrajevanja in podpore rešitve VOC, ki ga omogoča ponudnik in mora biti predhodno sporočen izvajalcu in implementiran po preteku 60-ih dni od sporočila o spremembi načina vzdrževanja rešitve VOC.

Ponudnik mora nuditi pomoč za:

- upravljanje orodij za zaznavanje in obravnavo kibernetskih dogodkov,
- sistemsko administracijo in natančnejše nastavljanje/prilaganje celotnega sistema,
- nadgradnje/posodabljanje (redne in izredne nadgradnje sistema, posodobitve posameznih gradnikov sistema),
- pri nadzoru nad sistemskimi viri (healthcheck),
- pomoč pri reševanju problemov z drugim/tretjim nivojem IBM podpore,
- reševanje napak pri integraciji z drugimi sistemi,
- izvedba dodatnih storitev po potrebi:
  - vključevanje podprtih virov,
  - vključevanje nepodprtih virov,
  - pregledovanje pravilnega zajema podatkov (nadzor, zbiranje, normalizacija),
  - omogočanje/onemogočanje privzetih primerov uporabe (pravila - use cases),
  - izdelava namenskih primerov uporabe (use cases),
  - izdelava, prilagajanje in korelacija med pravili (rules) in gradniki (building blocks),

- izdelava namenskih iskalnih poizvedb,
- prilagoditev/kreiranje scenarijev (odzivov),
- izdelava in posodabljanje poročil,
- izdelava in posodobitev dokumentacije,
- vzdrževanje integracije tokov incidentov med orodji vključenimi v sistem.

Upravljanje s programsko opremo

V okviru te aktivnosti bo ponudnik izvajal naloge s področja upravljanje in vzdrževanja opreme vključene v sistem VOC. Vse storitve se izvajajo po dogovoru in naročilu. To vključuje izvajanje naslednjih nalog:

- Zagotavljanje razpoložljivosti virov, kakovost storitev in dogovorjenih ravni podpore.
- Odpravljanje napak na programski in strojni opremi.
- Odpiranje zahtevkov pri produktni podpori proizvajalca programske opreme in njihovo spremljanje (odgovarjanje na vprašanja, dostava zahtevanih materialov ipd.).
- Nameščanje varnostnih in ostalih popravkov in/ali verzij, ki zagotavljajo nemoteno delovanje in skladnost sistema.
- Posodabljanje tehnične dokumentacije programske opreme.
- Dobava novih tehničnih nadgradenj programske opreme.
- Izvajanje rednih operativnih nalog.
- Izvajanje rednega operativnega spremljanja delovanja rešitve za zaznavanje in obravnavo kibernetskih dogodkov.
- Sistemska administracija in natančnejše nastavljanje/prilagajanje celotnega sistema.
- Nadzor nad sistemskimi viri (helathcheck).
- Pomoč pri reševanju problemov z drugim/tretjim nivojem podpore za sistemsko opremo.
- Reševanje napak pri integraciji z drugimi sistemi.

Ostale storitve, kot so:

- Nadgradnje dvosmerne integracije s Help Desk orodji naročnika in njegovih naročnikov
- Forenzična analiza varnostnega incidenta
- Honeypot postavitev in upravljanje
- DDoS zaščita
- DNS zaščita
- Razširjena storitev VOC »lovca na incidente« (»incident hunter«),
- Naprednejši odziv na incidente kibernetske varnosti Security Analytics
- Odkrivanje ranljivosti v informacijskih sistemih
- Izvajanje testov vdorov
- Definiranje varnostnih izhodišč za informacijske sisteme
- Preverjanje izvorne kode
- IT modeliranje groženj
- Zaznava incidentov v industrijskem/procesnem okolju (SCADA, OT)
- Nadzor privilegiranih uporabnikov
- Centralno upravljanje mobilnih naprav z zaznavo in preprečevanjem kibernetskih napadov
- Centralno upravljanje identitet in dostopov (Identity and Access Management)
- OT varnostni pregled
- OT modeliranje groženj
- Upravljanje platforme za izobraževanje