



NACIONALNI LABORATORIJ ZA  
ZDRAVJE, OKOLJE IN HRANO

## Specifikacija operativnih storitev kibernetске varnosti

### Kazalo vsebine

Obseg operativnih storitev kibernetске varnosti.....	2
Storitve varnostno operativnega centra.....	2
Operativne storitve kibernetске varnosti za NDR .....	3
Zahteve za XDR .....	3
Zahteve na osebnih računalnikih.....	4
Preprečevanje in zaznavanje .....	4
Preiskovanje in ublažitev .....	4
Spremljanje in nadzor.....	5
Zahteve na infrastrukturi – strežnikih .....	5
Splošne zahteve za XDR .....	6
Licenciranje XDR.....	6
Status in usposobljenost ponudnika .....	7

## Obseg zahtevanih storitev

Predmet tega sklopa naročila je izvajanje storitev varnostno operativnega centra s sistemoma XDR in NDR.

Naročnik uporablja sistema XDR Cynet in NDR Vectra Cognito. Ponudnik ponudi storitve, vezane na oba sistema ali ponudi nadomestni XDR, vključno z implementacijo. Nadomestni XDR mora ustrezati specifikaciji v nadaljevanju. Sistem NDR ostane Vectra Cognito, ker je vezan na nabavljeno strojno opremo in licence.

Ponudnik zagotovi:

- izvajanje storitev varnostno operativnega centra s sistemoma XDR in NDR,
- predpisano raven izvajanja sistemov XDR in NDR (operativno vzdrževanje),
- licenciranje sistema XDR.

## Storitve varnostno operativnega centra

Ponudnik mora nuditi sodelovanje svojega varnostno operativnega centra pri zaznavanju, interpretaciji in reševanju zaznanih varnostnih dogodkov (incidentov) za neomejeno število varnostnih dogodkov, zaznanih s sistemoma XDR in NDR.

Odziva se štiriindvajset ur na dan vse dni v letu po elektronski pošti, video klicu ali telefonu v predpisanih odzivnih časih. Začetek sodelovanja pri interpretaciji in reševanju zaznanih varnostnih dogodkov (incidentov) od prijave je:

- 1 ura pri kritični,
- 6 ur pri visoki,
- 12 ur pri srednji,
- 24 ur pri nizki resnosti incidenta.

Ekipo za sodelovanje mora biti locirana v EU in biti v celoti slovensko govoreča. Ponudnikov varnostno operativni center mora imeti certifikacijo za neprekinjeno poslovanje.

## Operativne storitve kibernetске varnosti za NDR

Za sklop operativnega delovanja sistema NDR ponudnik zagotavlja naslednje storitve:

- vzdrževanje in posodabljanje sistema z vidika programske opreme;
- nudenje pomoči pri upravljanju ponujenega sistema;
- storitev analize zaznav;
- storitev odziva na incident;
- forenziko v primeru incidenta.

Ponudnik nudi naslednje storitve rednega sodelovanja certificiranih in ustrezno usposobljenih strokovnjakov (storitve pomoči pri upravljanju ponujenega sistema in analizi zaznav):

1. redni tedenski pregled delovanja sistema, mesečna priprava poročil oziroma priporočil za morebitne izboljšave, posodobitve nastavitev oziroma optimizacijo delovanja sistema v naročnikovem okolju;
2. sprotno prilagajanje in optimiziranje triažnih filtrov, ter izločanje lažno pozitivnih zaznav;
3. kvartalni sestanek z naročnikom, ki vključuje pregled priporočil;
4. sodelovanje pri interpretaciji in reševanju zaznanih varnostnih dogodkov (incidentov) po potrebi in na zahtevo naročnika;
5. drugo svetovanje, integracije z ostalimi sistemi, ki so povezane z delovanjem in upravljanjem sistema v naročnikovem okolju;
6. zagotavljanje ekipe za odzivanje na incidente za izvajanje forenzike v primeru incidenta.

Za redne storitve pomoči pri upravljanju ponujenega sistema in analizi zaznav, kot so definirane v prvem odstavku, bo naročnik plačeval mesečni pavšal po predračunski postavki za mesečni pavšal. V to ceno so zajete 12 ur mesečno za storitve iz zgornjih točk.

V primeru, da bo število ur, potrebnih za izvedbo z naročnikom predhodno dogovorjenih storitev po zgornjih točkah v enem mesecu presegalo štiri 12 ur mesečnega pavšala, se te storitve štejejo kot dodatne storitve pomoči pri upravljanju sistema in analizi zaznav, in bo izvajalec le-te obračunal po predračunski postavki za uro dodatnih storitev.

## Zahteve za XDR

Sistem za zaznavanje in preprečevanje naprednih kibernetских varnostnih groženj na končnih napravah in strežnikih je sestavljen iz strežniške programske opreme ter agentov, nameščenih na končnih napravah: osebnih računalnikih, strežnikih in uporabniških mobilnih napravah.

Sistem mora biti dostopen kot ena ali več spletnih aplikacij v naročnikovem intranetu, brez dodatnih zahtev za programsko opremo uporabnika, razen brskalnika. Podpirati mora brskalnike Chrome, Firefox in Edge.

Zahtevan je uporabniško prijazen vmesnik, grafičen prikaz za spremljanje aktivnosti v naročnikovem okolju, razreševanje groženj ter prikaz topologije povezanih naprav z možnostjo prilagajanja pogleda.

Omogočati mora vizualno podprto pregledovanje, raziskovanje, analiziranje in razreševanje varnostnih dogodkov in groženj s prikazom relevantnih povezanih podatkov v realnem času.

Omogočati mora stalen nadzor aktivnosti v omrežju, prepoznavanje znanih in neznanih potencialnih varnostnih groženj, razvrščanje groženj v skupine in posredovanje opozoril v realnem času, takoj ob zaznavi groženj ali anomalij.

Raven zaznave groženj mora biti prilagodljiva.

## Zahteve na osebnih računalnikih

### Preprečevanje in zaznavanje

Sistem prepozna zlonamerne datoteke in preprečuje njihovo izvajanje, vključno z virusi, trojanci, izsiljevalskimi virusi, vohunsko programsko opremo, virusi za rudarjenje kriptovalut in ostalimi tipi zlonamerne programske opreme.

Sistem ima zaščito »zeroday«.

Sistem prepozna zlonamerno obnašanje zagnanih datotek/izvajajočih se procesov/sprememb registrov/dostopov do pomnilnika in ga zaustavi ob zagonu ali posredovati opozorilo (izkoriščanje ranljivosti, brezdatotečni, makroji, Powershell, WMI idr.).

Sistem podpira ustvarjanje pravil za izločitev določenih naslovnih/IP segmentov.

Sistem prepozna in zaustavi napade za povečanje pravic.

Sistem prepozna in zaustavi izvidniške napade (skeniranje).

Sistem prepozna in zaustavi poskuse kraje poverilnic iz pomnilnika (izpust poverilnic, surova sila) in mrežnega prometa (zastrupljanje ARP, DNS).

Sistem prepozna in zaustavi stransko gibanje ter posreduje opozorilo.

Sistem prepozna zlonamerno vedenje uporabniškega računa, ki je posledica predhodne zlorabe.

Sistem prepozna zlonamerno interakcijo s podatkovnimi datotekami.

Sistem prepozna odtekanje podatkov prek legitimnih protokolov (tuneliranje prek DNS, tuneliranje prek ICMP).

Sistem prepozna in zaustavi uporabo običajnih orodij za izvajanje napadov (Metasploit, Empire, Cobalt itd.).

Sistem ima notranji zaščitni mehanizem pred dostopi in manipulacijami nepooblaščenih uporabnikov.

### Preiskovanje in ublažitev

Sistem stalno zbira podatke o vseh objektih in njihovih aktivnostih v okolju, najmanj o dogajanju z datotekami (kreiranje, odpiranje, preimenovanje, brisanje, izvajanje), zagonu procesov (vključno s prikazom drevesa procesa), prijavi uporabnikov, omrežnem prometu, spremembi registrov in nameščenimi programski opremi.

Sistem podpira prikaz podatkov o objektih in njihovih aktivnostih.

Sistem podpira dinamično analizo (peskovnik).

Sistem podpira poizvedbe čez organizacijske enote naročnika z iskanjem pojava aktivnosti procesa / datoteke / omrežja / uporabnika na vseh končnih točkah / strežnikih.

Sistem podpira možnost izvedbe forenzične preiskave.

Sistem podpira izolacijo in ublažitev zlonamerne prisotnosti in aktivnosti lokalno na končni točki / strežniku, vključno: zmožnost izvajanja ukaza (npr. prek vmesnika CMD), zagon skripta ali datotek iz omrežne lokacije ali preslikanega pogona, zaustavitev končne točke / strežnika, izolacija končne točke / strežnika iz omrežja, brisanje datoteke (tudi že zagnane datoteke), premaknitev datoteke v karanteno (tudi že zagnane datoteke), zaustavitev procesa, odstranitev ali brisanje. storitve/načrtovanega opravila, zaklepanje lokalnega uporabniškega računa ali domenskega uporabnika, onemogočanje komunikacij na podlagi domenskega naslova ali naslova IP, odklop omrežnih kartic, sprememba naslova IP, restart končne točke / strežnika.

Sistem podpira izolacijo in ublažitev zlonamerne prisotnosti in aktivnosti naenkrat v celotnem okolju prek Active Directory (onemogočitev uporabnika, ponastavitev gesla) in/ali požarne pregrade/proxy (blokiranje naslovov IP, blokiranje domen, blokiranje vrat).

Sistem omogoča izvajanje samodejnega odzivanja z ustrezno akcijo za preprečitev grožnje po prednastavljenih potekih odzivanja s strani proizvajalca in po potekih odzivanja, ki jih lahko opredeli skrbnik sistema.

Sistem ima možnost postavljanja pasti za napadalce (datotečne, uporabniške, mrežne).

## Spremljanje in nadzor

Sistem podpira spremljanje integritete datotek (ang. File Integrity Monitoring - FIM) z obveznim opozarjanjem ob vsaki spremembi datotek.

Sistem ima vgrajeno ocenjevanje ranljivosti z odkrivanjem manjkajočih varnostnih posodobitev v sistemih in aplikacijah.

Sistem omogoča vodenje seznama objektov s preslikavo in povezavo vseh objektov v okolju kot so končne točke, strežniki, nameščene aplikacije in uporabniški računi z možnostjo priprave poročil.

Sistem zagotavlja zbiranje in hrambo dnevnika prijav in aktivnosti s hrambo za različna časovna obdobja.

Sistem vključuje lov na grožnje.

Sistem podpira odkrivanje površin za napad, ki niso pod nadzorom.

Sistem podpira nadzor USB naprav priključenih na kočno točko / strežnik (angl. Device Control)

## Zahteve na infrastrukturi – strežnikih

Sistem podpira hitro in nemotečo namestitve agenta na končne točke / strežnike v okolju.

Sistem podpira samodejno odkrivanje naknadno dodanih končnih točk / strežnikov z avtomatizirano namestitvijo agenta na njih.

Sistem (agent) ima minimalen vpliv na delovanje končne točke / strežnika s porabo:

- do okoli 30 MB sistemskega pomnilnika (RAM) na končno točko / strežnik.
- do okoli 10% procesorske zmogljivosti na končno točko / strežnik.

Sistem ima možnost nastavitve različnih stopenj obremenitve procesorske enote končne točke / strežnika s strani agenta.

Sistem zagotavlja šifrirano komunikacijo med strežnikom za upravljanje in agenti na končnih točkah / strežnikih.

Sistem (agent) podpira operacijske sisteme:

- Windows XP \ Vista, Server 2003, Windows 7,8,10 in 11
- Windows strežnik 2008 R2 in novejši
- Glavne distribucije Linuxa: Fedora, Ubuntu, Debian, Centos, Red Hat, Suse
- OS X Mavericks in novejši

Sistem podpira povezavo z Active Directory z namestitvijo na končne točke / strežnike v organizacijskih skupinah (OU) z AD.

Sistem deluje skupaj z obstoječo programsko opremo na končnih točkah \ strežnikih in omogoča brezhibno delovanje zaščitene končne točke / strežnika brez modrega zaslona ali zaustavljanja procesov.

Sistem zagotavlja zaščito končnih točk / strežnikov, ki niso povezani z omrežjem organizacije. Mehanizem za zaščito pred grožnjami ni odvisen od povezljivosti s strežnikom za upravljanje.

Sistem zna samostojno zbirati aktivnost končnih točk / strežnikov, datotek, procesov in uporabnikov ter omrežni promet.

## Splošne zahteve za XDR

Sistem ima možnost določiti seznam pravil za izključitev opozoril za izbrane objekte.

Sistem podpira namestitve strežnika na več ločenih lokacijah s poročanjem na centralno lokacijo in z upravljanjem sistema skozi enotno upravljavsko aplikacijo.

Sistem ima možnost izvoza trenutne konfiguracije programa za poznejši uvoz v isti ali drug računalnik.

Sistem omogoča 2-faktorsko prijavo.

Sistem omogoča ustvarjanje različnih vlog uporabnikov (z različnimi pravicami).

Sistem ima možnost, da omogoči / onemogoči določene vrste obvestil ter lokalna opozorila na končni točki / strežniku.

Sistem ima možnost zagona v načinu samo spremljanja ter v načinu spremljanja in preprečevanja/ukrepanja.

Sistem ima možnost vklopa/izklopa lastne protivirusne zaščite.

Sistem ima možnost ocenjevanja resnosti varnostnih opozoril

Sistem zagotavlja centralno zbiranje in obdelavo opozoril v realnem času.

Sistem ima možnost blokiranja dostopa do nastavitev programa za končne uporabnike.

Sistem zagotavlja centralno distribucijo posodobitev brez posredovanja uporabnika in ponovnega zagona končne točke / strežnika.

Sistem ima možnost določanja razporeda za prenos posodobitev, vključno z možnostjo onemogočanja samodejnih posodobitev.

Sistem mora vsem objektom v zaščitenem okolju dodeliti oceno tveganja.

Rešitev podpira beleženje dogodkov, opozoril in posodobitev.

Sistem podpira integracijo z e-pošno infrastrukturo naročnika za obveščanje skrbnikov sistema v primeru opozoril.

Sistem podpira integracijo z rešitvijo SIEM.

Sistem podpira pripravo standardiziranih in prilagojenih varnostnih in forenzičnih poročil.

Sistem podpira vmesnik REST API.

Sistem podpira možnost ustvarjanja podskupin za nadzor znotraj varovanega okolja.

Sistem podpira posredovanje zahteve za sodelovanje pri interpretaciji in reševanju zaznanih varnostnih dogodkov (incidentov) iz nadzorne plošče.

## Licenciranje XDR

Ponudnik je dolžan zagotavljati pravico do sprotnega posodabljanja in nadgrajevanja programske opreme za zaznavanje in preprečevanje naprednih kibernetičnih varnostnih groženj v celotnem obdobju naročila.

Storitve pomoči pri upravljanju sistema in prijava napak je možna pri ponudniku storitev sistema štiriindvajset ur na dan, vse dni v tednu in vse dni v letu preko telefona ali elektronske pošte.

Rok za odpravo napake pri storitvah podpore in vzdrževanja sistema je 24 ur od prijave napake.

## Status in usposobljenost ponudnika

Ponudnik je pooblaščen partner proizvajalca ponujenega sistema v Sloveniji in usposobljen za namestitve in zagotavljanje vzdrževanja ponujenega sistema.

Ponudnikov VOC (Varnostno operativni center) mora zaradi pomembnosti naročnikove infrastrukture zagotavljati ISO 22301.

Ponudnik mora imeti vsaj 5 referenčnih družb iz EU, kjer so integrirali 500 ali več ponujenih XDR klientov in za iste izvajajo VOC operacijo.

Ponudnik ima najmanj pet (5) slovensko govorečih usposobljenih strokovnjakov za upravljanje ponujenega sistema za zaznavanje in preprečevanje naprednih kibernetских varnostnih groženj.

Ponudnik ima v Sloveniji najmanj deset (10) usposobljenih strokovnjakov s pooblastili za dostop do tajnih podatkov (vsaj stopnje interno) za sodelovanje pri interpretaciji in reševanju zaznanih varnostnih dogodkov (incidentov), za neomejeno število varnostnih dogodkov, z odzivom po elektronski pošti, video klicu ali telefonu, s pripravljenostjo štiriindvajset ur na dan, vse dni v tednu in vse dni v letu.

Ponudnik mora imeti visoko kvalificiran in certificiran podporni kader in sicer vsaj:

- 1 × GCIH (GIAC Certified Incident Handler);
- 1 × OSCP (Offensive Security Certified Professional);
- 3 × CEH (Certified Ethical Hacker);
- 2 × certifikati za izvajanje forenzike npr: SANS - GNFA, GSEC;
- 4 × inženirski certifikat višje stopnje za upravljanje z rešitvijo proizvajalca Vectra Cognito – VCIE;
- 2 × strokovnjak s poznavanjem varnosti na področju okolja operativne tehnologije, IoT in medicinsko laboratorijskih naprav, npr.: SANS – GICSP, GRID, GCIP;
- 10 × strokovnjak za izvajanje prvega nivoja triaže;
- 8 × strokovnjak za izvajanje drugega nivoja triaže in odziva na incident.

### Dokazila:

**Ponudnik (partnerji pri skupni ponudbi) mora v informacijskem sistemu e-JN v razdelek druge priloge naložiti potrdila, certifikate in drugo dokumentacijo s katero dokazuje ustreznost ponudbe.**