



NACIONALNI LABORATORIJ ZA
ZDRAVJE, OKOLJE IN HRANO

Specifikacija storitev platforme kibernetkega zavajanja

Kazalo vsebine

Opis obstoječega sistema	2
Zahtevane storitve	2
Arhitektura	2
Upravljanje.....	2
Funkcijske zahteve	3
Zahteve za integracijo	5
Zahteve za licenco.....	5
Splošni pogoji	5
Status in usposobljenost ponudnika	6

Opis obstoječega sistema

Računalniško omrežje naročnika je razvejano po vseh naročnikovih lokacijah v Sloveniji (Maribor, (sedež), Ljubljana, Brežice, Celje, Hrastnik, Koper, Kranj, Murska Sobota, Nova Gorica, Novo mesto, Slovenska Bistrica). Vsi strežniki so virtualizirani.

Zahtevane storitve

Predmet tega sklopa naročila je izvajanje storitev licenciranja, postavitve, vzdrževanja in upravljanja sistema za preprečevanje vdorov naslednje generacije, platforme kibernetkega zavajanja, ki ustvari omrežne pasti in zaznava zlonamerno obnašanje.

Arhitektura

1. Rešitev se v okolje namesti brez reorganizacije obstoječe topologije omrežja.
2. Rešitev mora vsebovati vsaj naslednje komponente:
 - a. osrednje vozlišče za upravljanje,
 - b. vozlišče za izvajanje pasti,
 - c. agenta za delovne postaje in strežnike (za puščanje sledi do pasti).
3. Rešitev mora podpirati implementacijo v virtualna okolja in podpirati vsaj naslednje hipervizorje:
 - a. Vozlišče za upravljanje: VMware vSphere 6.0/6.5/7.0,
 - b. Vozlišče za pasti: VMware vSphere 6.0/6.5/7.0.
4. Rešitev mora omogočati kreiranje lažnih podatkov na produkcijskih napravah (puščanje sledi do pasti) na sistemih Linux in Windows.
5. Rešitev mora omogočati razširitev platforme v dodatna omrežja brez ponovne namestitve sistema.
6. Rešitev mora vsebovati vgrajeno podporo za ločevanje instanc pasti, ki se upravljajo z ene točke.
7. Rešitev mora omogočati namestitev simulacijskih pasti v več omrežnih segmentih.
8. Rešitev mora delovati brez dodatnih informacij s strani IP prometa (npr. pridobivanja kopije prometa IP, kot so NetFlow, sFlow, jFlow, itd.).

Upravljanje

1. Rešitev mora omogočati intuitiven vmesnik za upravljanje brez dodatnih stroškov za upravljanje in podporo.
2. Rešitev mora omogočati upravljanje preko spletne konzole za najbolj razširjene spletne brskalnike: Mozilla Firefox, Google Chrome, Apple Safari, v njihovih zadnjih različicah.
3. Rešitev mora omogočati podporo za ločevanje instanc pasti, ki so upravljane z ene točke upravljanja.
4. Rešitev mora omogočati upravljanje posamezne ločene instance za ločen nabor administratorjev, ki imajo dostop samo do svojih omrežnih segmentov.

5. Rešitev mora vzdrževati podrobne zapise vseh aktivnosti znotraj konzole za upravljanje. Kadar se nastavitve spremenijo, mora revizijska sled jasno označiti začetne in končne vrednosti spremenjenih nastavitev.
6. Rešitev mora podpirati možnost nastavitve vlog administratorjev za granularen nadzor dostopov do konzole za upravljanje.

Funkcijske zahteve

1. Vsaka od pasti mora biti unikatna, vsaka s svojim naborom lastnosti (naslov MAC, naslov IP, ime naprave, simulirane storitve in ostale nastavitve).
2. Pasti ne smejo uporabljati opcije »IP-alias-based scaling«, ki omogoča, da imajo pasti več naslovov IP, kar omogoča napadalcu hitrejšo zaznavo podobnih pasti v okolju.
3. Rešitev mora omogočati možnost ustvarjanja pasti, ki se bo periodično:
 - a. povezala na zunanje spletne vire,
 - b. izvajala zahteve preko protokolov DNS, mDNS, LLMNR, NetBIOS,
 - c. zahtevala seznam datotek preko protokola SMB (Windows File Share).
4. Rešitev mora omogočati možnost ustvarjanja in distribuiranja lažnih podatkov (sledi do pasti) na prave, produkcijske naprave v omrežju.
5. Sledi do pasti morajo vsebovati vsaj:
 - a. shranjene podatke za prijavo,
 - b. povezave do simuliranih pasti,
 - c. povezave do omrežnih virov,
 - d. shranjene RDP in SSH seje,
 - e. konfiguracijske datoteke z računi za dostop do simuliranih baz podatkov.
6. Rešitev mora znati zaznavati omrežne tehnike vdorov (brute-force napad, poskuse povezav na storitve, itd.), jih kategorizirati glede na kritičnost, ne glede na tip in princip napada. Zaznavanje in kategorizacija se mora izvajati za kriptiran in nekriptiran promet.
7. Rešitev mora izpisati zgodovino povezav na pasti ter zgodovino vseh aktivnosti na pasti, kot npr.:
 - a. naslov IP naprave, s katere je bil izveden napad,
 - b. uporabljene poverilnice,
 - c. uporabljeni protokoli in omrežni porti.
8. Rešitev mora omogočati grafičen izpis statistike napadov, delovanja sistema, ipd.
9. Rešitev mora omogočati zaznavanje tehnike napada »Man-in-the-Middle«, ki vključuje tudi:
 - a. ARP spoofing,
 - b. NBT/LLMNR/mDNS resolve poisoning,
 - c. preusmerjanje zahtevkov HTTPS.
10. Rešitev mora omogočati zmožnost samodejnega ustvarjanja pasti.
11. Rešitev mora omogočati ustvarjanje vsaj naslednje tipe pasti:
 - a. Microsoft RDP strežnik,

- b. Microsoft SMB strežnik,
 - c. Microsoft MS RPC past za zaznavanje RPC povezav,
 - d. strežniki z Linux OS,
 - e. grafični vmesnik za IBM QRadar,
 - f. grafični vmesnik za VMware ESX,
 - g. grafični vmesnik za Fortinet,
 - h. grafični vmesnik za Microsoft Outlook Web Access,
 - i. SCADA/HMI/PLC,
 - j. DNS strežnik,
 - k. MySQL strežnik,
 - l. PostgreSQL strežnik,
 - m. FTP strežnik,
 - n. Samba file share strežnik,
 - o. Modbus TCP strežnik,
 - p. MQTT vmesnik.
12. Rešitev mora omogočati ustvarjanje pasti, ki temeljijo na kateri koli spletni aplikaciji v okolju. Te pasti morajo vključevati znane ranljivosti spletnih protokolov (OWASP TOP 10).
13. Spletne pasti morajo vključevati sledeče parametre:
- a. spremenljiv »header« za simulacijo različnih strežnikov,
 - b. omejevanje pristopov za preprečevanje DoS napadov (rate-limiting),
 - c. dovoljene metode HTTP,
 - d. dodatne poti in datoteke, ki so dosegljive samo na pasti, vključno z odzivi,
 - e. dodajanje lastnih parametrov v »header«,
 - f. možnost spreminjanja TLS certifikata.
14. Pasti za procesna omrežja morajo omogočati grafične vmesnike za vsaj dva uveljavljena proizvajalca sistemov PLC.
15. Pasti za procesna omrežja morajo podpirati vsaj dva uveljavljena protokola, na primer S7comm in Modbus TCP.
16. Rešitev mora natančno kategorizirati in kombinirati dogodke povezane z napadi v eno detekcijo, s čimer zniža čas odzivanja na napad.
17. Rešitev mora omogočati ustvarjanje lastnih tipov pasti, ki temeljijo na sistemih, ki so že prisotni v okolju. Po ustvarjanju novih tipov pasti mora rešitev omogočati večkratno uporabo tega tipa pasti. Konfiguracija novih tipov pasti mora biti enostavna in v standardiziranem formatu (YAML ali JSON).
18. Rešitev mora omogočati sledenje odzivanju na grožnje, ki nakazuje status vsake zaznave.
19. Vsaka past mora biti unikatna, z lastnim naslovom IP, brez uporabe polnega operacijskega sistema.

20. Rešitev ne sme temeljiti na uporabi podpisov za zaznavanje napadov.
21. Rešitev mora omogočati vizualizacijo interakcij s pastmi in naprav med sabo.
22. Rešitev mora omogočati dostop do zajema prometa za posamezno zaznavo za potrebe odzivanja na napad v formatu PCAP.
23. Rešitev mora omogočati dodajanje legitimnih storitev na seznam zaupanja vrednih lokacij (izjeme), s čimer znižujemo število lažnih zaznav. Rešitev mora omogočati tudi časovne okvirje, v katerih so izjeme veljavne.

Zahteve za integracijo

1. Rešitev mora omogočati integracijo z zunanjo platformo EDR/XDR, ki omogoča vsaj izolacijo zaznanega naslova IP, iz katerega poteka napad.
2. Rešitev mora omogočati dvosmerno integracijo s sistemi SIEM: podprta morata biti vsaj dva uveljavljena sistema.
3. Rešitev mora omogočati povezavo z zunanjo požarno pregrado, ki omogoča vsaj izolacijo zaznanega naslova IP, iz katerega poteka napad.
4. Rešitev mora omogočati možnost pošiljanja opozoril preko elektronske pošte.
5. Rešitev mora omogočati možnost pošiljanja opozoril v zunanje sisteme SIEM preko protokola syslog.
6. Rešitev mora omogočati dostop preko klicev API:
 - a. pridobivanje podatkov o sistemu, vključno z licenco, izoliranimi okolji, pastmi in alarmi,
 - b. upravljanje s statusi pasti in varnostnimi incidenti.

Zahteve za licenco

1. Rešitev ne sme zahtevati nakup dodatne programske opreme (razen za potrebe virtualizacije), kar vključuje programsko opremo za operacijske sisteme (npr. Microsoft Windows), sistemsko programsko opremo ali posebno programsko opremo za delovanje pasti.
2. Rešitev mora omogočati vsaj 20 aktivnih pasti (simulacija operacijskih sistemov, omrežne opreme, mrežnih storitev) v poljubnem številu omrežnih segmentih brez dodatne licence.
3. Rešitev mora vključevati možnost namestitve agentov na delovne postaje in strežnike za vsaj 20 naprav, v poljubnem številu omrežnih segmentov za potrebe puščanja sledi do pasti brez dodatne licence.
4. Rešitev mora zagotavljati tehnično podporo s strani proizvajalca, ki vključuje:
 - a. brezplačne nadgradnje komponent programske opreme, baz podatkov in ostale programske opreme, ki je potrebna za pravilno delovanje platforme;
 - b. nadgradnje in popravke obstoječih napak s strani proizvajalca po zaključeni implementaciji, brez potrebe ponovnega zagona sistema;
 - c. možnost kontaktiranja tehnične podpore v primeru težav v režimu 8×5.

Splošni pogoji

Storitve ponudnika se opravljajo v režimu 8×5: vsak delovni dan od 7:00 do 15:00.

Odzivni čas je največ 8 ur med delovnim časom.

Status in usposobljenost ponudnika

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

Ponudnik ima v Sloveniji najmanj 2 usposobljena strokovnjaka za upravljanje ponujenega sistema.

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.