TEHNILINE KIRJELDUS

1. NÕUDED TOOTELE

1.1. Tootele on väljastatud litsents kasutusaja kehtivusega vähemalt kolm aastat alates tarnekuupäevast;
1.2. Litsentsis peab sisalduma vähemalt 5 pettevõrgu operatsiooni süsteemiga hosti ja üks keskne haldusplatvorm, mille kaudu on võimalike pakutud hoste hallata;
1.3. Lepingu perioodi jooksul on hankijal õigus sarnastel tingimustel litsentse ja tootetuge juurde soetada;
1.4. Teenus peab olema litsentseeritud Kaitseväe nimele;
1.5. Kõik litsentsid peavad olema kaetud lepingu perioodi jooksul võimalike uuendustega;
1.6. Kõik litsentsid peavad olema kaetud tootja poolse tootetoega nende kehtivusaja jooksul;
1.7. Konsultatsiooniteenuse juurutamiseks 40 tunni ulatuses;
1.8. Kasutaja ja teenuseadministraatori koolitusi teenuse kasutamiseks vähemalt viiele inimesele 40 akadeemilise tunni jagu;
1.9. Toode peab sisaldama vähemalt järgmisi funktsionaalsusi:

1.9.1. Võltsteenuste loomine ning nende sidumine võltsdokumentide ja -piltide kaudu (leivapuru - *breadcrumb*);
1.9.2. Võltsteenused peavad sisaldama terviklikku operatsioonisüsteemi;
1.9.3. Skriptitav (tegevused automatiseeritavad);
1.9.4. Skriptitav sisuloome võimalus – nt Postkastid, dokumendid, AD kasutajad jne;
1.9.5. Toodete Microsoft „*Active Directory*“ ja „*Exchange*“ pette teenuse loomise võimekus;
1.9.6. Pettevõrgu monitooring lubab sissetungijat detailselt jälgida. Näiteks kuvada postkastis avatud ja otsituid kirju/märksõnu;
1.9.7. Kuvama kokkuvõtvaid raporteid ja visuaalsed vaateid toimunud tegevustest;
1.9.8. Ühilduvus vähemalt alljärgnevate SIEM toodetega:

1.9.8.1. Elastic Search;
1.9.8.2. SPLUNK;
1.9.8.3. ArcSight.

1.9.9. Liivakasti ja ohuteadmusplatvormi ühilduvus vähemalt toodetega

1.9.9.1. Cuckoo versioon alates 2.0.0;
1.9.9.2. MISP versioon alates 2.4.165 (*Malware Information Sharing Platform*).

1.9.10. Teenuse liidestamine vähemalt alljärgnevate kiirsuhtlus platvormidega:

1.9.10.1. Mattermost;
1.9.10.2. Telegram;
1.9.10.3. Microsoft Teams;
1.9.10.4. Slack.

1.9.11. Töövoo halduskeskkondade Jira ja TheHive API liidestus võimekust;
1.9.12. Pettevõrgu teenuse ja keskhalduse logi peab olema eristatav ja keskselt kogutav vastavalt punktis 1.9.8 välja toodud toodetega;
1.9.13. Halduskeskkonnast ligipääs pettevõrgu virtuaalmasina käsuviibale;
1.9.14. Ühilduvus MITRE CALDERA simulatsiooniga;
1.9.15. Kaardistama pettevõrkude sündmusi luues neist TTP-d (tactics, techniques, and procedures) vastavalt MITRE ATT&CK raamistikule.

1.10. Funktsionaalsed nõuded

1.10.1. Pettevõrgu teenus peab toetama vähemalt alljärgnevaid:

1.10.1.1. Teenuseid:

1.10.1.1.1. Windows SMB 3.0;
1.10.1.1.2. Windows RDP;
1.10.1.1.3. Microsoft Exchange OWA koos veebi rakendusega;
1.10.1.1.4. OpenVPN;
1.10.1.1.5. Git;
1.10.1.1.6. Veebiserver, nt. Apache;
1.10.1.1.7. Cisco ASA VPN;
1.10.1.1.8. Fortigate VPN.
1.10.1.1.9. SMTP;
1.10.1.1.10. SNMP;
1.10.1.1.11. POP3/IMAP;
1.10.1.1.12. Syslog;
1.10.1.1.13. Apatche;
1.10.1.1.14. HTTPS.

1.10.1.2. Operatsioonisüsteeme:

1.10.1.2.1. Windows Server viimane stabiilne versioon;
1.10.1.2.2. Windows 11 viimane stabiilne versioon;
1.10.1.2.3. Ubuntu 18.04, 20.04 ja 22.04 LTS.

1.10.2. Halduskeskkond peab toetama vähemalt:

1.10.2.1. Kogu pettevõrgu haldus ja analüüs peab olema ühes keskselt usaldatud SSL sertifikaadiga lahenduvas veebirakenduses;
1.10.2.2. Meili teel alertide saatmine;

1.10.2.2.1. Alertide saatmise funktsionaalust peab saama hankija ise seadistada;

1.10.2.3. Muudatuste keskkonnas tehtavate haldustoimingute logimine;
1.10.2.4. 3 eri tasemel kasutajate profiile ja funktsionaalsusi. Näiteks:

1.10.2.4.1. Administraator:
1.10.2.4.1.1. kasutaja kontode loomine;
1.10.2.4.1.2. liidestuste loomine teiste süsteemidega;
1.10.2.4.1.3. uuenduste teostamine;

1.10.2.4.2. Arhitekt:

1.10.2.4.2.1. pettevõrgu teenuste looja.

1.10.2.4.3. Vaatleja:

1.10.2.4.3.1. pettevõrkudes toimuva jälgimine;
1.10.2.4.3.2. analüüs.

1.11. Mittefunktsionaalsed nõuded

1.11.1. Teenus võimaldab koguda nii pettevõrkude kui ka haldusliidese muudatuste logi.

Sobivad tooted:
- National Security & Defence Platform License including - Install, Deployment, Monitoring (Self Hosted);
- National Security & Defence 5 Host License including - Install, Deployment, Monitoring (Self Hosted).

2. NÕUDED PAKKUJALE

2.1. Pakkuja peab garanteerima, et tootetugi tagab rikete teavitamise ja registreerimise võimekuse 24/7/365 emaili või telefoni teel;
2.2. Teenuse tehniline tugi peab vastama vähemalt 1 tööpäeva jooksul.
2.3. Pakkuja peab garanteerima, et tootetugi tagab teenuse tehnilise toe tööpäeviti vähemalt 3 aasta jooksul alates teenuse tarnekuupäevast;
2.4. Tootetugi sisaldab minimaalselt alljärgnevaid komponente:

2.4.1. Teenuse vigade/anomaaliate parandused:

2.4.1.1. Väga kriitiline – 1 tööpäev (Kogu teenus on kasutuskõlbmatu ja või kriitilise haavatavusega, mis seab ohtu pettevõrgu enda halduskeskkonna terviklikkuse ja konfidentsiaalsuse)
2.4.1.2. Kriitiline viga (muudatus halvab pettevõrgu analüüsi või haldamise funktsionaalsust) – 3 tööpäeva
2.4.1.3. Viga – 20 tööpäeva jooksul (viga ei sega pettevõrkude monitoorimist ja haldust)

2.4.2. Teenuse liidestamiste tehniline nõustamine;
2.4.3. Teenuse kasutamisalane tehniline nõustamine;

Punktis 2.2.-2.4. kajastatud tootetoe teenuste maksumus peab sisalduma pakkumuse hinnas.

3. NORMATIIVID

3.1. MITRE ATT&CK - https://attack.mitre.org/;
3.2. MITRE CALDERA - https://github.com/mitre/caldera;
3.3. MISP versioon alates 2.4.165 (*Malware Information Sharing Platform*) - https://www.misp-project.org/;

4. MATERJALID
Tooted peavad olema kvaliteetsed ning vastama peatükis 1 toodud nõuetele.

5. TOOTE MARKEERIMINE
Kõik komplektis olevad tooted peavad olema markeeritud tootjapoolse infoga selliselt, et on võimalik toode tuvastada.
Toode on markeeritud tootjapoolse informatsiooniga, mis peab sisaldama endas minimaalselt alljärgnevat:

5.1. tootja;
5.2. toote nimetus;
5.3. versioon;
5.4. kogus ja ühik;
5.5. hoiatustähised;
5.6. tootja tootekood;
5.7. lepingu number;
5.8. tarnekoha aadress.

6. PAKENDAMINE

Tooted edastatakse meili teel.
Võtmed ja litsentsid edastatakse eraldi meili teel vastuvõtja nimele krüpteeritud *.cdoc ümbrikuga või mõnel sarnasel kürpteeritud viisil.

7. TARNETINGIMUSED

7.1. Füüsilisest tarnest tuleb kontaktisikut ette teavitada minimaalselt 3 tööpäeva, ning edastada alljärgnev info:

7.1.1. Tarneaeg;
7.1.2. Kulleri nimi ja isikukood;
7.1.3. Transpordi vahendi mark ja registreerimisnumber.

Asutus	**Aadress**
Küberväejuhatus	Filtri 12, Tallinn, 10132

7.2. Elektroonilise tarne puhul kontaktisikut ette teavitada minimaalselt 1 tööpäev, ning edastada alljärgnev info:

7.2.1. Tarneaeg;
7.2.2. Tarnija e-mail;
7.2.3. *.cdoc vastuvõtja nimele krüpteeritud ümbrik.

8. SAATEDOKUMENDID

Tarnega koos tuleb esitada üleandmise-vastuvõtmise akt.
Üleandmisaktil peab olema välja toodud:

8.1. tellija nimi;
8.2. tellija aadress;
8.3. tellimuse number;
8.4. saatja nimi;
8.5. saatja aadress;
8.6. tootenumbrid;
8.7. toote kirjeldus;
8.8. toote kogus;
8.9. toote ühik;
8.10. üleandmise kuupäev.

9. KVALITEEDIKONTROLL

Tellijal peab olema võimalus vahetult enne toote saabumist kontrollida toote vastavust esitatud nõuetele.