*Personāla apmācības “Live Online Network Forensics Training "PCAP in the Morning Europe"”*

1. *pielikums*

**TEHNISKĀ SPECIFIKĀCIJA/TEHNISKAIS PIEDĀVĀJUMS**

|  |  |  |
| --- | --- | --- |
| Personāla apmācības kurss **“Live Online Network Forensics Training "PCAP in the Morning Europe"”** | | |
| Pakalpojuma mērķis | ***Live Online Network Forensics Training "PCAP in the Morning Europe"*** digitālās kriminālistikas kurss ir praktiska un padziļināta PCAP datņu satura analīzes pieeja ar mērķi pilnveidot apmācāmos tīkla drošības uzraudzības un tīkla datu plūsmas izmeklēšanas jomās. | **Pretendenta piedāvātā pakalpojuma apraksts atbilstoši tehniskās specifikācijas prasībām**  *(aizpildīt veidlapas tukšās ailes)* |
| Sasniedzamais rezultāts | ***Live Online Network Forensics Training "PCAP in the Morning Europe"*** nodrošinās darbinieka kompetenci PCAP datņu pilnvērtīgas analīzes veikšanai un ļaunprātīgu digitālu uzbrukumu noteikšanai, izsekošanai un izmeklēšanai. |  |
| Apmācāmo skaits vienā grupā | Ne mazāk kā 3 cilvēkam |  |
| Plānotais mācību periods | 3 mēneši kopš iegādes brīža |  |
| Pakalpojuma programma | ***“Live Online Network Forensics Training "PCAP in the Morning Europe"”*** |  |
| Pakalpojuma sniedzējam jānodrošina | Apmācības procesa ietvaros jānodrošina kursa "*Live Online Network Forensics Training*" tēmas:   1. Ļaunprogrammatūras pielikumu izmeklēšana mērķētos e-pasta uzbrukumos; 2. Izfiltrēto datu atkārtota apkopošana; 3. C2 datu plūsmas identificēšana atšifrētā HTTPS datu plūsmā; 4. Atšifrētās HTTPS datu plūsmas analīze no caurredzama TLS pārbaudes starpniekservera; 5. Datu izplatīšanas izsekošana ar nozagtiem *Windows* piekļuves datiem; 6. Lietojumprogrammas slāņveida datu meklēšana, izmantojot *Wireshark*, *TShark*, *TCPflow* un *ngrep*; 7. Draudu meklēšana, izmantojot *Security Onion*; 8. Pasīva DNS piesaistīšana, lai izsekotu C2 domēnus; 9. Patentētas C2 datu plūsmas dekodēšana no RAT; 10. Ļaunprogrammatūru atvēršana un to uzvedības analizēšana izmēģināšanas (*sandbox*) vidē; 11. *Supply chain* uzbrukumi; 12. Datņu izvilkšana no SMB un SMB2 plūsmas; 13. APT stila uzbrucēja eksfiltrācijas analīze; 14. Mērķēto uzbrukumu izmeklēšana piekļuves datu zādzības gadījumos; 15. Teorija: HTTP sīkdatnes; 16. *Cobalt Strike Beacon* analīze; 17. Robottīkla izsekošana C2 datu plūsmā, izmantojot JA3; 18. X.509 sertifikātu izvilkšana no tīkla plūsmas un to apliecināšana; 19. “*Man-on-the-Side*” (*MOTS*) uzbrukumu specifikācijas apgūšana; 20. Brutālā spēka uzbrukumu izmeklēšana pret tīmekļa CMS; 21. Tīmekļa servera ļaunprātīgas izmantošanas analīze; 22. Uz tīmekļa čaulām nosūtīto komandu izsekošana; 23. Datu izplatīšanas izsekošana, izmantojot *Linux* serverus; 24. JA3 izmantošana, lai izsekotu TLS šifrētās ļaunprogrammatūras datu plūsmu. |  |
| Pakalpojuma sniegšanas vieta un nosacījumi | * 1. Katram izglītojamajam jānodrošina atsevišķa piekļuve mācību materiāliem;   2. Kursi jānodrošina tiešsaistē;   3. Katram izglītojamajam jānodrošina licence *NetworkMiner Professional* un *CapLoader* programmatūrām;   4. Piegādātājam jānodrošina pakalpojuma piegāde līdz 2024. gada 7. martam no iepirkuma līguma abpusējas parakstīšanas dienas. |  |
| Pakalpojuma sniedzēja kvalitātes prasības | Vēlama   * pieredze līdzīgu mācību pakalpojumu sniegšanā pēdējo divu gadu laikā;   un/vai   * apmācību speciālista ar speciālām zināšanām programmatūras izmantošanā praktiskā darbā piesaiste. |  |

2024.gada \_\_\_.\_\_\_\_\_\_\_

(paraksts) \* (paraksta atšifrējums)

**\*** *Ja Pretendents piedāvājuma dokumentus paraksta ar drošu elektronisko parakstu un laika zīmogu, Pretendents to norāda attiecīgā dokumenta paraksta vietā. Piemēram, “amats, Vārds, Uzvārds, DOKUMENTS PARAKSTĪTS AR ELEKTRONISKO IEPIRKUMU SISTĒMAS PIEDĀVĀTO ELEKTRONISKO PARAKSTU”.*