UZAICINĀJUMS

dalībai cenu aptaujā

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

Valsts policijas koledžas Izmeklētāju mācību centrs tirgus izpētes nolūkos vēlās noskaidrot mācību programmas “Live Online Network Forensics Training "PCAP in the Morning Europe"”iegādes izmaksas balstoties uz sekojošiem nosacījumiem:

1. Nepieciešamais apmācāmo skaits - ne mazāk kā 3 (trīs).
2. Apmācību procesa ietvaros jānodrošina kursa tēmas:
3. Ļaunprogrammatūras pielikumu izmeklēšana mērķētos e-pasta uzbrukumos;
4. Izfiltrēto datu atkārtota apkopošana;
5. C2 datu plūsmas identificēšana atšifrētā HTTPS datu plūsmā;
6. Atšifrētās HTTPS datu plūsmas analīze no caurredzama TLS pārbaudes starpniekservera;
7. Datu izplatīšanas izsekošana ar nozagtiem *Windows* piekļuves datiem;
8. Lietojumprogrammas slāņveida datu meklēšana, izmantojot *Wireshark*, *TShark*, *TCPflow* un *ngrep;*
9. Draudu meklēšana, izmantojot *Security Onion;*
10. Pasīva DNS piesaistīšana, lai izsekotu C2 domēnus;
11. Patentētas C2 datu plūsmas dekodēšana no RAT*;*
12. Ļaunprogrammatūru atvēršana un to uzvedības analizēšana izmēģināšanas (*sandbox*) vidē;
13. *Supply chain* uzbrukumi;
14. Datņu izvilkšana no SMB un SMB2 plūsmas;
15. APT stila uzbrucēja eksfiltrācijas analīze;
16. Mērķēto uzbrukumu izmeklēšana piekļuves datu zādzības gadījumos;
17. Teorija: HTTP sīkdatnes;
18. *Cobalt Strike Beacon* analīze;
19. Robottīkla izsekošana C2 datu plūsmā, izmantojot JA3;
20. X.509 sertifikātu izvilkšana no tīkla plūsmas un to apliecināšana;
21. *“Man-on-the-Side”* (MOTS) uzbrukumu specifikācijas apgūšana;
22. Brutālā spēka uzbrukumu izmeklēšana pret tīmekļa CMS;
23. Tīmekļa servera ļaunprātīgas izmantošanas analīze;
24. Uz tīmekļa čaulām nosūtīto komandu izsekošana;
25. Datu izplatīšanas izsekošana, izmantojot *Linux* serverus;
26. JA3 izmantošana, lai izsekotu TLS šifrētās ļaunprogrammatūras datu plūsmu.

* Sīkākā informācija pieejama: <https://www.netresec.com/?page=Training>

1. Pakalpojuma sniegšanas vieta un nosacījumi:
2. Katram izglītojamajam jānodrošina atsevišķa piekļuve mācību materiāliem;
3. Kursi jānodrošina tiešsaistē;
4. Katram izglītojamajam jānodrošina licence *NetworkMiner Professional* un *CapLoader* programmatūrām;
5. Piegādātājam jānodrošina pakalpojuma piegāde līdz 2024. gada 7. martam no iepirkuma līguma abpusējas parakstīšanas dienas.

Lai iesniegtu pieteikumu cenu aptaujā, pretendents aizpilda un iesūta atbildē uzaicinājuma dokumenta pielikumus “Tehniskā specifikācija” un “Finanšu piedāvājums”.

**Lūdzam pieteikumu iesniegt elektroniski līdz 2024. gada 12. janvāra plkst. 16:00 uz e-pastu** [**paula.ansonska@koledza.vp.gov**](mailto:paula.ansonska@koledza.vp.gov)**.**