Proiect cofinantat din Programul Operational Capital Uman 2014-2020

Fondul Social European
Programul Operațional Capital Uman 2014-2020
Axa prioritara 3: Locuri de muncă pentru toți

Obiectivul tematic 10:	Investițiile în educație, calificare și formare profesională pentru dobândirea de competențe și învățare pe tot parcursul vieții
Prioritatea de investitii 10iii	Îmbunătățirea accesului egal la învățarea pe tot parcursul vieții pentru toate grupurile de vârstă într-un cadru formal, non-formal sau informal, actualizarea cunoștințelor, a aptitudinilor și a competențelor forței de muncă și promovarea unor căi de învățare flexibile, inclusiv prin orientare profesională și prin validarea competențelor dobândite
Obiectivul specific 3.12	Îmbunătățirea nivelului de cunoștințe/competențe/aptitudini aferente sectoarelor economice/domeniilor identificate conform SNC şi SNCDI ale angajaților
Titlu proiect:	IDEA – Innovate, Discover, Evolve, Apply /IDEA - Inoveaza, Descopera, Evolueaza, Aplica
CodMySMIS2014:	**142366**
Nr contract finanțare	**POCU/ /861/3/12/142366**
Nr. înregistrare OIRPOSDRU V	8937/18.06.2021

Documentatie PROCEDURA COMPETITIVA pentru atribuirea Contractului de servicii ”Programe de formare” — Lot [2] – Cursuri de specializare in domeniul CYBERSECURITY pentru dezvoltarea competentelor digitale destinate specialistilor din IT specifice in cadrul proiectului „IDEA - Inoveaza, Descopera, Evolueaza, Aplica"

Diana Stanese
Semnat digital de Diana Stanese
Data: 2022.11.09 15:52:56 +02'00'

Aprobat
NTT DATA Romania S.A.
Prin
Head of Coaching School&Acad Initiatives
Diana Stanese

Cuprins:

Sectiunea I. Cerinte minime pentru ofertanti

Nota: Ordinul 1284 nu reglementeaza notiunea "fisa de date". Beneficiarul privat nu are obligatia de a structura informatiile din procedura competitiva prin utilizarea "fisei de date".

Capitol 1. Informatii generale

Beneficiarul: NTT DATA ROMANIA S.A. Adresa: Cluj-Napoca, str. Constanta nr. 19-21 cod postal 400158, judetul Cluj Nr. Ordine ORC: J12/615/2000 Cod fiscal: RO13091574 Persoana de contact: Oana Suru Telefon: 0766.600.096 Posta electronica: idea@nttdata.com
Graficul de desfasurare a procedurii de atribuire: 1. Lansare procedura: Anunt publicat pe site https://beneficiar.fonduri-ue.ro:8080/anunturi **01.11.2022** 2. Termen limita de primire clarificari de la potentiali ofertanti: **09.11.2022, ora 16:00** Solicitarile de clarificari pot fi depuse astfel: ○ personal /posta /curier la adresa de contact. SAU ○ prin e-mail, la adresa de e-mail de contact. Solicitarile de clarificari telefonice nu vor fi luate in considerare. 3. Termen limita de raspuns la solicitarea de clarificari: **14.11.2022** 4. Termenul limita de depunere oferte: **18.11.2022, ora 14:00** 5. Publicarea anuntului de semnare a contractului: In maximum 5 zile calendaristice de la semnarea contractului de achizitie. Anuntul va fi publicat pe site-ul https://beneficiar.fonduri-ue.ro:8080/anunturi , rubrica - Anunturi-proceduri. Termenele de mai sus se pot decala in situatia in care achizitorul primeste solicitari de clarificari al caror raspuns necesita modificari /ajustari ale specificatiilor tehnice, sau ale altor cerinte minime obligatorii, astfel incat sa se asigure timpul necesar pentru elaborarea acestora, cu respectarea conditiilor de publicitate.

Capitol 2. Detalii contract

1. Obiectul contractului: Achizitie Programe de formare - **Lot [2] – Cursuri specializare in domeniul CYBERSECURITY** pentru dezvoltarea competentelor digitale specifice in cadrul proiectului „IDEA - Inoveaza, Descopera, Evolueaza, Aplica"
2. Descrierea achizitiei: Achizitia de servicii de livrare a cursurilor de formare destinate grupului tinta in vederea realizarii Activitatii: A.1.Furnizarea de programe de formare profesionala, Subactivitatii: A.1.1.Furnizarea de programe de formare profesionala. Conform cererii de finantare, cursul urmeaza sa se realizeze astfel:

• Curs in domeniul Cybersecurity, pentru SOC (Security Operations Center), specializarea Raspuns la Incidente si Amenintari, pentru un volum de 48h/ curs/cursant, pentru un numar de maxim 2 persoane • Curs in domeniul Cybersecurity, pentru Cloud Security (specializarea Arhitectura si Inginerie de securitate Defensiva), pentru un volum de 48h/ curs/cursant, pentru un numar de maxim 1 persoana • Curs in domeniul Cybersecurity, pentru Informatii (secrete) la Amenintari din domeniul Virtual, pentru un volum de 48h/ curs/cursant, pentru un numar de maxim 1 persoana • Curs in domeniul Cybersecurity, pentru SOC (Security Operations Center), raspunsuri avansate la atacuri cibernetice, pentru un volum de 48h/ curs/cursant, pentru un numar de maxim 1 persoana
3. Tipul contractului: servicii
4. Tipul procedurii: Procedura competitiva conform ORDIN nr. 1.284 din 8 august 2016 privind aprobarea Procedurii competitive aplicabile solicitantilor/beneficiarilor privati pentru atribuirea contractelor de furnizare, servicii sau lucrari finantate din fonduri europene
5. Locatia de prestare a serviciului: online
6. Cod CPV: 80530000-8 - Servicii de formare profesionala
7. Sursa de finantare: Fondul Social European Programul Operațional Capital Uman 2014-2020 Axa prioritara 3: Locuri de muncă pentru toți Obiectivul tematic 10: Investițiile în educație, calificare și formare profesională pentru dobândirea de competențe și învățare pe tot parcursul vieții Prioritatea de investitii 10iii Îmbunătățirea accesului egal la învățarea pe tot parcursul vieții pentru toate grupurile de vârstă într-un cadru formal, non-formal sau informal, actualizarea cunoștințelor, a aptitudinilor și a competențelor forței de muncă și promovarea unor căi de învățare flexibile, inclusiv prin orientare profesională și prin validarea competențelor dobândite Obiectivul specific 3.12 Îmbunătățirea nivelului de cunoștințe/competențe/aptitudini aferente sectoarelor economice/domeniilor identificate conform SNC şi SNCDI ale angajaților Titlu proiect: IDEA – Innovate, Discover, Evolve, Apply /IDEA - Inoveaza, Descopera, Evolueaza, Aplica CodMySMIS2014: 142366 Nr contract finanțare POCU/ /861/3/12/142366 Nr. înregistrare OIRPOSDRU NV 8937/18.06.2021

Capitol 3. Valoare estimata

Valoare estimata totala a contractului este de: 193,500.00 lei fara TVA cu urmatoarea defalcare: • Servicii livrare "Curs in domeniul Cybersecurity, pentru SOC (Security Operations Center), specializarea Raspuns la Incidente si Amenintari" – 77,400.00 lei fara TVA • Servicii livrare "Curs in domeniul Cybersecurity, pentru Cloud Security (specializarea Arhitectura si Inginerie de securitate Defensiva)" – 38,700.00 lei fara TVA • Servicii livrare "Curs in domeniul Cybersecurity, pentru Informatii (secrete) la Amenintari din domeniul Virtual" – 38,700.00 lei fara TVA

• Servicii livrare "Curs in domeniul Cybersecurity, pentru SOC (Security Operations Center), raspunsuri avansate la atacuri cibernetice" – 38,700.00 lei fara TVA
**Nota: Vor fi respinse ofertele care depasesc valorea estimata*

Capitol 4. Durata contractului

Durata contractului: maximum 3 luni, nu mai tarziu de data de 27.01.2023, cu posibilitate de prelungire. Prelungirea contractului se poate face in contextul implementarii proiectului prin act aditional semnat de ambele parti.

Capitol 5. Documente de calificare

Pentru participarea la procedura se solicita urmatoarele documente considerate cerinte minime:
1. Operatorii economici, care depun oferte in cadrul prezentei proceduri, trebuie sa nu se afle in situatiile de conflict de interese reglementate la art. 13-15 din OUG nr. 66/2011. Persoanele fata de care se verifica incidenta conflictului de interese sunt: Dl. Metz Daniel – Administrator, presedinte consiliu de administratie Dl. Murota Masaki – Administrator, membru în consiliu de administratie Dna. Metz Maria – Administrator, membru în consiliu de administratie si Director General Dl. Ruffinoni Walter - Administrator, membru în consiliu de administratie Dl. Miyuki Ide - Administrator, membru în consiliu de administratie Dna. Elena Musca - Manager proiect Dna. Daniela Bara - Responsabil financiar Dna. Diana Stanese – Presedinte comisie de evaluare Dna. Elena Musca - Membru comisie de evaluare Dna. Oana Suru - Membru comisie de evaluare Dl. Cristian Zdroba - Membru comisie de evaluare Dl. Dan Candea - Membru comisie de evaluare Se va prezenta **Formular 1 — Declaratie privind neincadrarea in situatiile prevazute la art. 13 si 14 din Ordonanta de urgenta a Guvernului nr. 66/2011.** ****Nota: se va prezenta acest formular pentru ofertant/ ofertant asociat/subcontractant***
2. Certificatul constatator emis de Oficiul Registrului Comertului 1. Certificat constatator emis de O.N.R.C. din care sa rezulte cel putin urmatoarele informatii: obiectul de activitate care sa includa activitatile ce fac obiectul licitatiei, autorizat, actionarii si administratorii firmei. Certificatul constatator trebuie sa fie eliberat cu cel mult 30 zile inainte de data de depunere a ofertelor. 2. In cazul in care ofertantul se incadreaza in categoria „Asociatie” sau „Fundatie” se va transmite un Extras din Registrul de evidenta al Asociatiilor si Fundatiilor in copie certificata pentru conformitate cu originalul impreuna cu cea mai noua versiune a documentelor constitutive: Act constitutiv si/sau Statut insotite de Hotararea /Incheierea judecatoreasca a cererii de inregistrare a modificarilor (privind Actul constitutiv /Statutul) in copie certificata pentru conformitate cu originalul, din care sa rezulte mentiunile anterior precizate si solicitate.

3. Pentru persoanele fizice/juridice straine: Documente edificatoare, traduse autorizat emise de organisme similare care sa dovedeasca o forma de inregistrare, in conformitate cu prevederile din tarile unde ofertantii isi au sediul si care sa contina cel putin: obiectul de activitate /dreptul de a presta activitatile ce fac obiectul licitatiei, actionarii si administratorii firmei, faptul ca organizatia nu se afla in stare de dizolvare, lichidare, insolventa sau faliment.

Acesta se va prezenta in oricare din formele: original/copie legalizata/copie lizibila "conform cu originalul" semnata si stampilata de reprezentantul legal. Este valabil si Certificatul eliberat in format electronic.

Nota : se va prezenta acest formular pentru ofertant, ofertant asociat si subcontractant

Atentie:

Aceste documente insotesc propunerea tehnica si financiara iar neprezentarea acestora, precum si neindeplinirea acestor cerinte conduce la respingerea ofertelor de la procedura.
Indeplinirea tuturor cerintelor minime conduce la calificarea ofertantilor in etapa de evaluare a propunerilor tehnice si cea de selectie a ofertelor pe baza modalitatii de evaluare.

In cazul unei asocieri de operatori economici, toti operatorii economici asociati vor transmite toate documentele solicitate, cu exceptia Propunerii financiare si a Propunerii tehnice care se vor transimte doar de catre liderul asocierii, in numele asocierii.
In cazul unei asocieri este necesar sa se transmita suplimentar si un acord de asociere.

Capitol 6. Modul de prezentare a propunerii tehnice

1. Informatii generale

Propunerea tehnica va fi intocmita in asa fel incat sa se asigure posibilitatea verificarii conformitatii acesteia cu cerintele din caietul de sarcini.
Obligatiile pe care operatorul economic si le va asuma prin propunerea tehnica vor fi valabile pe toata durata contractului.
Cerintete tehnice din caietul de sarcini sunt minime si obligatorii.
Documentele oficiale emise de un organism tert in alta limba decat romana vor fi insotite de traducerea autorizata in limba romana.
In cazul in care, pe parcursul indeplinirii contractului se constata faptul ca anumite elemente ale propunerii tehnice sunt inferioare sau nu corespund cerintelor prevazute in caietul de sarcini, prevaleaza prevederile caietului de sarcini.

2. Propunerea tehnica va cuprinde urmatoarele:

2.1. Informatii generale despre ofertant.
2.2. Informatii cu privire la experienta organizatiei in domeniul formarii profesionale.
2.3. O descriere amanuntita a serviciilor oferite si a modului de acordare a acestora, in conformitate cu toate cerintele din cadrul sectiunii ***Specificatii tehnice (Caiet de sarcini).***

Atentie:

Aceste elemente vor constitui baza pentru evaluarea ofertelor.
Propunerile Tehnice incomplete (care nu vor contine cel putin informatiile/datele indicate in caietul de sarcini) vor fi declarate neconforme si vor atrage excluderea ofertantului din procedura.

Nerespectarea cerintelor tehnice si a modului de prezentare a propunerii tehnice, cu toate cele cerintele mentionate anterior, ofertele tehnice incomplete, precum si completarea/modificare ofertei prin raspunsurile la evetualele solicitari de clarificari, constitui motiv de respingere a ofertantei.

Posibilitatea retragerii sau modificarii ofertei
Ofertantul are dreptul de a-si retrage oferta, prin solicitare scrisa adresata achizitorului privat pana la data si ora limita pentru depunerea ofertelor.
Ofertantul poate modifica continutul ofertei, pana la data si ora stabilite pentru depunerea ofertelor, adresand pentru aceasta achizitorului privat o cerere de retragere a ofertei in vederea modificarii. Achizitorul privat nu este raspunzator in legatura cu posibilitatea ofertantului de a depune noua oferta, modificata, pana la data si ora limita, stabilita in documentatia de atribuire.
Riscurile transmiterii ofertei, inclusiv forta majora, cad in sarcina ofertantului.

Capitol 7. Modul de prezentare a propunerii financiare

1. Propunerea financiara va fi prezentata conform **Formularului de oferta — Formular 2**, in lei (fara TVA). Ofertele in euro sau alta valuta se calculeaza la cursul BNR din ziua transmiterii ofertei.
2. Lipsa formularului de oferta reprezinta lipsa ofertei, respectiv lipsa actului juridic de angajare in contract.
3. Nu se accepta ajustarea pretului.
4. Propunerea financiara are caracter ferm si obligatoriu, din punctul de vedere al continutului pe toata perioada de valabilitate a ofertei, respectiv **minim 90 de zile**, si pe durata de derulare a contractului.
5. Toate documentele justificative vor fi certificate de ofertant prin semnare.

Atentie:
Aceste elemente vor constitui baza pentru evaluarea ofertelor.
Nerespectarea modului de prezentare a propunerii financiare cu toate punctele mentionate anterior, ofertele financiare incomplete, precum si completarea/modificare ofertei prin raspunsurile la evetualele solicitari de clarificari, constitui motiv de respingere a ofertantei.

Capitol 8. Modalitate de evaluare

In vederea respectarii principiilor asa cum sunt definite in Ordinul Ministrului Fondurilor Europene nr. 1284/2016 si pentru respectarea principiilor economicitatii, eficientei si eficacitatii, beneficiarul va alege **oferta cu cele mai multe avantaje pentru realizarea scopului proiectului.**
Pe parcursul intregului proces de achizitie prin procedura competitiva, la adoptarea oricarei decizii, se va tine cont de urmatoarele principii:

a) principiul transparentei;
b) principiul economicitatii;
c) principiul eficientei;
d) principiul eficacitatii.

Prin transparenta se intelege aducerea la cunostinta publicului a informatiilor referitoare la aplicarea procedurii de atribuire, astfel incat operatorii economici care opereaza pe piata, sa poata participa la competitie, asigurandu-se prin aceasta promovarea concurentei. Respectarea acestui principiu asigura premisele pentru respectarea celorlalte 3 principii.
Principiul economicitatii prevede minimizarea costului resurselor alocate pentru atingerea rezultatelor estimate ale unei activitati, cu mentionarea calitatii corespunzatoare acestor rezultate.
Principiul eficientei presupune asigurarea unui raport optim intre resursele utilizate si rezultatele obtinute.
Principiul eficacitatii vizeaza gradul de indeplinire a obiectivelor specifice stabilite pentru fiecare activitate planificata, in sensul obtinerii rezultatelor scontate.

1. Raspundere
Beneficiarul va evalua modul in care fiecare oferta indeplineste cerintele de participare la procedura, se incadreaza in valoarea estimata si specificatiile tehnice prezentate din prezenta documentatie.
Analizarea documentelor prezentate de ofertanti nu angajeaza din partea Beneficiarului nici o raspundere sau obligatie fata de acceptarea acestora ca autentice sau legale si nu inlatura raspunderea exclusiva a ofertantilor sub acest aspect.

2. Elemente de departajare a ofertelor
Desemnarea ofertei castigatoare si atribuirea contractului de achizitie se va realiza in conformitate cu prevederile OMFE nr. 1284/2016, Sectiunea 4 - Derularea procedurii competitive, punctul 4.2. Analiza ofertelor și elaborarea notei justificative de atribuire.
Se vor compara ofertele prin raportarea lor la toate cerintele publicate si se va alege oferta care indeplineste cerintele tehnice si prezinta avantaje fata de acestea, la un raport calitate/pret competitiv.
Prin urmare se vor analiza si compara, in vederea realizarii scopului proiectului, urmatoarele elemente:

1. **Componenta financiara - pretul**

Pentru dovedirea ofertei financiare, ofertantul va depune:

- **Formular de oferta** — Formular nr. 2

Nota: In cazul in care o oferta prezinta un pret aparent neobisnuit de scazut in raport cu ceea ce urmeaza prestat atunci cand pretul ofertat, fara TVA, reprezinta mai putin de 85% din valoarea estimata publicata, beneficiarul are dreptul de a efectua verificari detaliate in sensul ca va solicita ofertantului inclusiv documente, dupa caz, privind modul de intocmire a costului. In cazul in care ofertantul nu prezinta informatiile solicitate in termen de 3 zile sau aceste informatii nu pot justifica pretul aparent neobisnuit de scazut, oferta va fi respinsa.

2. **Componenta tehnica, respectiv experienta solicitata ofertantului/formatorului in conformitate cu cerintele mentionate in cadrul capitolului 3 Cerinte minime**

obligatorii - 3.1. Ofertantul si trainerul/ii din Sectiunea II. Specificatii tehnice (Caiet de sarcini)

In dovedirea experientei in furnizarea de cursuri de formare profesionala ofertantul va depune:

- **Declaratia privind experienta ofertantului in livrarea de cursuri — Formular nr. 3**

  In dovedirea experientei in furnizarea de cursuri de formare profesionala a formatorului, ofertantul va depune:
- **Declaratia privind experienta formatorului — Formular nr. 4**

3. **Componenta tehnica, respectiv prezentarea de scrisori de recomandare/rapoarte de acceptanta/etc din partea clientilor finali ce atesta faptul ca cursurile de specializare in domeniul CYBERSECURITY au fost prestate la un standard ridicat de calitate.**

Nota: Daca in urma aplicarii avantajelor mai multe oferte se claseaza pe primul loc, se va solicita o noua ofertare financiara, urmand a fi declarata castigatoare oferta cu pretul cel mai mic.
Nota: Beneficiarul in analiza documentelor depuse isi rezerva dreptul de a solicita prin clarificari dovezi in sprijinul sustinerii criteriilor de evaluare.

Capitol 9. Modul de prezentare si depunere a ofertei

Formalitati ce trebuie indeplinite in legatura cu participarea la procedura:
Adresa la care se depun ofertele: Cluj-Napoca, str. Constanta nr. 19-21 cod postal 400158, judetul Cluj
Data limita de depunere a ofertelor: **18.11.2022 orele 14.00**

Modalitatea de solicitare a clarificarilor:
Clarificarile pot fi trimise prin email: idea@nttdata.com
Data limita de solicitare clarificari: **09.11.2022, ora 16.00**
Data limita de raspuns la clarificari: **14.11.2022**
Raspunsurile la clarificari vor fi postate pe pagina web www.fonduri-ue.ro , sectiunea „Achizitii privati" https://beneficiar.fonduri-ue.ro:8080/ .
Ofertantii au obligatia de a verifica pe site-ul www.fonduri-ue.ro publicarea eventualelor clarificari cu referire la aceasta procedura de achizitie.

Modul de prezentare a ofertei:
1. Oferta se prezinta intr-un exemplar original, pe suport hârtie, și un exemplar în format electronic (.pdf), pe suport fizic (CD/DVD/USB), in plic sigilat, netransparent.
Din motive de operativitate în evaluarea ofertelor, propunerea tehnică și cea financiară din cadrul exemplarului în format electronic, vor fi în mod obligatoriu prezentate și în format editabil (de tip .doc/.docx sau .xls/.xlsx).

2. Plicul trebuie sa fie marcat cu:
   2.1. Adresa beneficiarului
   2.2. Adresa ofertantului si datele de contact
   2.3. Mentiunea "A NU SE DESCHIDE INAINTE DE DATA de: 18.11.2022 orele 14.00"
   2.4. Mentiunea "Oferta in vederea participarii la PROCEDURA COMPETITIVA pentru atribuirea Contractului de servicii ”Programe de formare” - **Lot [2] – Cursuri specializare in domeniul CYBERSECURITY** pentru dezvoltarea competentelor digitale specifice in cadrul proiectului „IDEA - Inoveaza, Descopera, Evolueaza, Aplica".

3. Plicul va contine:
   3.1. Documente de calificare, conform Capitolului 5.
      - Formular 1 — Declaratie privind neincadrarea in situatiile prevazute la art. 13 si 14 din Ordonanta de urgenta a Guvernului nr. 66/2011.
      - Certificatul constatator emis de Oficiul Registrului Comertului sau documentul echivalent;
   3.2. Propunerea tehnica, *conform Capitolului 6.*
   3.3. Declaratia privind experienta ofertantului in livrarea de cursuri — *Formular nr. 3*
   3.4. Propunerea financiara, *conform Capitolului 7*.
   3.5. Declaratia privind experienta formatorului — Formular nr. 4
   3.6. Declaratie de disponibilitate — Formular nr. 5

4. Plicul va fi insotit de o **Scrisoare de inaintare — Formular 6**, care se va depune in acelasi timp cu plicul, dar separat, in afara plicului, **Imputernicire — Formular 7 (pentru situatile in care oferta este asumata de alta persoana decat reprezentantul legal)** si **Copie dupa CI /BI pentru persoana imputernicita (daca este cazul).**

Limba de redactare a ofertei: limba romana.
Documentele oficiale emise de un organism tert in alta limba decat romana vor fi insotite de traducerea autorizata in limba romana.
Documentele justificative pot fi prezentate în oricare din formele: copie legalizată, copie lizibilă cu mențiunea ”conform cu originalul”.
Nu se accepta oferte alternative.

Capitol 10. Informatii privind contractul de servicii

Contractul va mentiona datele de identificare a celor doua parti semnatare, obiectul, valoarea, modalitatea de plata, documentele contractului, durata si obligatiile contractuale. Contractul va fi semnat de ambele parti si datat.
Daca ofertantul castigator nu semneaza contractul in termenii stabiliti, beneficiarul privat poate relua procedura de achizitie.
Operatorul economic care va semna contractul de servicii datoreaza Beneficiarului contravaloarea daunelor directe si indirecte referitoare la proiectul “IDEA – Innovate, Discover, Evolve, Apply /IDEA - Inoveaza, Descopera, Evolueaza, Aplica”, SMIS 142366, cauzate de neindeplinirea sau indeplinirea necorespunzatoare a obligatiilor asumate prin oferta si prin

contractul de servicii, inclusiv, dar fara a se limita la eventualele reduceri/corectii financiare sau alte retineri, penalitati si obligatii de plata imputate de Autoritatea de Management/Organismul Intermediar sau de alte structuri de control.
Operatorul economic care va semna contractul de servicii are obligatia de a asigura disponibilitatea informatiilor si documentelor referitoare la Proiect/Contract, cu ocazia misiunilor de control desfasurate de Autoritatea de Management/Organismul Intermediar pentru Program sau de alte structuri cu competente in controlul si recuperarea debitelor aferente fondurilor europene si/sau fondurilor publice nationale aferente acestora, dupa caz.

Capitol 11. Cai de atac

Rezultatul evaluarii ofertelor va fi publicat pe site-ul https://beneficiar.fonduri-ue.ro:8080/anunturi rubrica - Anunturi-proceduri
In conformitate cu prevederile art. 4.3, Sectiunea a 4-a, Capitolul 5 din Ordinul 1284/ 08.08.2016 privind aprobarea Procedurii competitive aplicabile solicitantilor/beneficiarilor privati pentru atribuirea contractelor de furnizare, servicii sau lucrari, din fonduri europene, contestarea rezultatului procedurii se realizeaza la instanta de judecata competenta pentru solutionarea cauzei. Concomitent, operatorut economic va instiinta Beneficiarul NTT DATA Romania S.A..
Consiliul National de Solutionare a Contestatiilor nu are competente privind solutionarea contestatiilor in contextul derularii procedurii competitive, conform precizarilor Ordinului nr. 1284/2016.

Capitol 12. Informatii despre modul de derulare a procedurii

In conformitate cu OMFE 1284/2016 NU se organizeaza sedinta de deschidere a ofertelor.
Ofertantii poarta intreaga raspundere pentru depunerea ofertelor la adresa indicata in prezentul capitol si inainte de data si ora limita de depunere a ofertelor. Ofertele depuse la o alta adresa decat cea indicata la prezentul capitol sau dupa data si ora limita vor fi respinse.

Beneficiarul privat nu evalueaza ofertele care sunt transmise dupa data de expirare (data si ora din anunt) sau sunt transmise la alta adresa decat cea precizata in prezenta documentatie. Acestea se vor returna nedeschise.
In analiza ofertelor se tine cont de toate cerintele pe care le-a mentionat beneficiarul privat în documentele achizitiei. In analiza ofertelor nu se pot adauga alte cerinte si nu se poate renunta la specificatiile deja enuntate în anunt/specificatii/clarificari/modificari.
Daca beneficiarul privat identifica erori de fond în documentele achizitiei care nu au fost clarificate înainte de data de expirare a anuntului, procedura nu se va încheia cu atribuirea contractului. În acest caz procedura se va anula, se vor corecta erorile identificate si se va relua procedura.
In procesul de analiza a ofertelor, beneficiarul poate solicita clarificari cu privire la ofertele depuse prin email/fax, ofertantii fiind obligati sa raspunda in termenul acordat de beneficiar. Raspunsul la clarificari poate fi transmis pe email sau poate fi trimis prin posta/curier la adresa la care se depun ofertele.

In situatia in care ofertantul nu raspunde la clarificari in termenul indicat de beneficiar sau raspunsurile nu sunt concludente, oferta este respinsa.
Nerespectarea cerintelor din prezenta documentatiei, neprezentarea informatiilor solicitate completate in mod corespunzator, propunerea tehnica incompleta, lipsa propunerii financiare, o propunere financiara cu un cost mai mare sau un cost nobisnuit de scazut si/sau transmiterea documentelor intr-o forma improprie care face imposibila vizualizarea continutului acestora sunt activitati realizate pe riscul ofertantului, iar esecul de a depune o oferta care sa nu indeplineasca cerintele minime si obligatorii de calificare, cu o propunere tehnica incompleta, necorespunzatoare, neconforma, neadecvata obiectului contractului si instructiunile de prezentare/completare a documentelor indicate prin prezenta documentatie, precum si lipsa propunerii financiare, o propunere financiara cu un cost mai mare sau un cost nobisnuit de scazut si/sau transmiterea documentelor intr-o forma improprie care face imposibila vizualizarea continutului acestora poate conduce la respingerea ofertei ca fiind inacceptabila/neconforma/neadecvata.
Ofertantii trebuie sa transmita o oferta completa conform solicitarilor din prezenta documentatie.
Ofertantii poarta exclusiv raspunderea pentru examinarea cu atentia cuvenita a documentatiei de atribuire, inclusiv a oricarei clarificari aduse documentatiei de atribuire in timpul perioadei de pregatire a ofertei prin raspunsurile beneficiarului la solicitarile de clarificari, precum si pentru obtinerea tuturor informatiilor necesare cu privire la orice fel de cerinte/conditii si obligatii care pot afecta in vreun fel valoarea, conditiile stabilite, natura/continutul ofertei si/sau executia contractului. Riscurile transmiterii ofertei, conform cerintelor din prezenta documentatie, inclusiv forta majora, cad in sarcina ofertantului.

Sectiunea II. Specificatii tehnice (Caiet de sarcini) - achizitie „Programe de formare” - Lot [2] – Cursuri specializare in domeniul CYBERSECURITY pentru dezvoltarea competentelor digitale specifice in cadrul proiectului „IDEA - Inoveaza, Descopera, Evolueaza, Aplica"

Capitolul 1. Generalitati

Caietul de sarcini face parte integranta din documentatia pentru elaborarea ofertei si constituie ansamblul cerintelor pe baza carora se elaboreaza de catre ofertant propunerea tehnica.
Caietul de sarcini cuprinde specificatii tehnice minime pentru achizitia de servicii de formare profesionata.

Nota:
Caracteristicile tehnice din prezenta documentatie reprezinta conditii minimale pe care trebuie sa le îndeplineasca oferta castigatoare. Specificatiile tehnice care par a indica o anumita origine, sursa, productie, un procedeu special, o marca de fabrica sau de comert, un brevet de inventie, o licenta de fabricatie sau altele asemenea sunt mentionate doar pentru identificarea cu usurinta a tipului de serviciu/produs si nu au ca efect favorizarea sau eliminarea anumitor operatori economici sau a anumitor servicii/produse. Aceste specificatii vor fi luate în considerare cu mentiunea „sau echivalent".

Capitolul 2. Obiectul prezentului caiet de sarcini

Prezenta procedura vizeaza achizitia de servicii de formare si certificare dupa cum urmeaza:

- Servicii livrare „Curs in domeniul Cybersecurity, pentru SOC (Security Operations Center), specializarea Raspuns la Incidente si Amenintari”, sesiuni de formare la care participa 2 persoane angajate ale solicitantului;
- Servicii livrare „Curs in domeniul Cybersecurity, pentru Cloud Security (specializarea Arhitectura si Inginerie de securitate Defensiva)”, sesiuni de formare la care participa 1 persoana, angajata a solicitantului;
- Servicii livrare „Curs in domeniul Cybersecurity, pentru Informatii (secrete) la Amenintari din domeniul Virtual”, sesiuni de formare la care participa 1 persoana, angajata a solicitantului;
- Servicii livrare „Curs in domeniul Cybersecurity, pentru SOC (Security Operations Center), raspunsuri avansate la atacuri cibernetice”, sesiuni de formare la care participa 1 persoana, angajata a solicitantului.

Pentru fiecare din cursurile specializare in domeniul CYBERSECURITY s-au estimat urmatoarele volume de ore distribuite astfel:

- Curs in domeniul Cybersecurity, pentru SOC (Security Operations Center), specializarea Raspuns la Incidente si Amenintari pentru un volum de 48h/ curs/cursant
- Curs in domeniul Cybersecurity, pentru Cloud Security (specializarea Arhitectura si Inginerie de securitate Defensiva), pentru un volum de 48h/ curs/cursant

- Curs in domeniul Cybersecurity, pentru Informatii (secrete) la Amenintari din domeniul Virtual, pentru un volum de 48h/ curs/cursant
- Curs in domeniul Cybersecurity, pentru SOC (Security Operations Center), raspunsuri avansate la atacuri cibernetice, pentru un volum de 48h/ curs/cursant

Întregul program de formare va fi centrat pe cursantul la curs, metodele de predare fiind interactive, cu aplicatii practice si adaptate la situatiile intalnite de acestia.
Programul de formare va contribui la dezvoltarea competentelor digitale specifice sectorului economic competitiv si adaptate nevoilor individuale ale locului de munca si respectiv personale ale participatilor, imbunatatind competentele tehnice ale angajatilor NTT DATA Romania si contribuind la cresterea productivitatii si performantelor acestora si a competitivitatii intreprinderii.

Capitolul 3. Cerinte minime obligatorii

3.1. Ofertantul

Ofertantul trebuie sa faca dovada experientei similare in livrarea de cursuri de specializare in domeniul CYBERSECURITY, din ultimii 3 ani, in cadrul a minim 3 contracte similare finalizate.

In dovedirea experientei in furnizarea de cursuri de formare profesionala ofertantul va depune:

- Declaratia privind experienta ofertantului in livrarea de cursuri — Formular nr. 3
- Scrisori de recomandare/rapoarte de acceptanta/etc din partea clientilor finali ce atesta faptul ca cursurile de specializare in domeniul CYBERSECURITY au fost prestate la un standard ridicat de calitate.

Totodata, ofertantul trebuie sa puna la dispozitia beneficiarului trainer/i cu:

- experienta specifica in minim 3 contracte ce au presupus livrarea de cursuri similare (prin similare intelegem "cursuri de specializare in domeniul CYBERSECURITY");
- experiență profesională relevantă (minim 5 ani) în domeniul care face obiectul cursului pentru care este propus, dovedită prin intermediul CV-ului (acesta va include referiri precise la activitățile profesionale relevante, defalcate pe perioade de timp)

Pentru demonstrarea cerintei, pentru fiecare dintre traineri, se vor depune in cadrul ofertei urmatoarele documente:

- CV-ul expertilor propusi, in limba romana, care sa contina informatii actualizate referitoare la experienta specifica si certificarile/diplomele detinute, necesare pentru indeplinirea cerintelor minime de calificare
- Declaratia privind experienta formatorului — Formular nr. 4.
- Pentru fiecare dintre trainerii propusi se va depune Declaratia de disponibilitate — Formular nr. 5.

3.2. Continutul cursului

In propunerea tehnica a ofertei se va include programa cursului (structurata pe capitole, continut tematic detaliat si orar aferent aproximativ), detaliind si serviciile de certificare aferente.

Ofertantul va propune câte un curs mapat întocmai pe temele/programa solicitată prin Caietul de sarcini. Se vor include referințe cu privire la fiecare dintre cursurile propuse: Programa de curs, link la site-ul ofertantului cu descrierea cursului, recomandări de la minim 1 beneficiar al fiecărui curs, detalierea tipului de certificare pusă la dispoziție pentru fiecare curs.
Fiecare curs include o secțiune teoretică, respectiv una practică. Pentru secțiunea practică Ofertantul va pune la dispoziție o platformă online, disponibilă cursanților pentru exersarea și evaluarea abilităților/competențelor tehnice acumulate pe parcursul cursului.
Fiecare curs va avea o certificare corespondentă, emisă de un organism recunoscut la nivel național/international. Pentru fiecare curs se va indica / include în oferta tehnică certificarea aferentă.

3.2.1. Curs in domeniul Cybersecurity, pentru SOC (Security Operations Center), specializarea Raspuns la Incidente si Amenintari

Obiectivele asteptate ale cursului sunt:

a. Cresterea competentelor prin aplicatii practice ce privesc elementele mentionate in continut
b. Detectarea momentului si metodei prin care a avut loc un incident de securitate
c. Identificarea sistemelor compromise și afectate
d. Evaluarea daunelor și determinarea elementelor afectate si modul in care acestea au fost afectate
e. Izolarea si remedierea incidentelor de securitate
f. Dezvoltarea unor surse cheie de “Threat Intelligence”
g. Identificarea breselor de Securitate aditionale folosind cunoasterea adversarului

Printre subiectele care sunt obligatorii a fi atinse se regasesc:

Modul 1
Arhitectură de rețea

- Standarde de securitate și audit
- Authentication, Authorization and Accounting
- Apărarea infrastructurii de rețea
- Sisteme de prevenire a intruziunilor și firewall-uri
- Name Resolution Attacks and Defense
- Securizarea infrastructurii cloud private și publice

Modul 2
Penetration testing

- Scop și reguli ale jocului
- Online Reconnaissance
- Inginerie sociala
- Tehnici de Network Mapping and Scanning
- Scanarea Enterprise Vulnerability
- Instrumente și tehnici de exploatare a rețelei
- Post-exploatare și pivotare
- Instrumente și tehnici de exploatare a aplicațiilor web

- Raportare și debriefing

Modul 3
Fundamentele Security Operations

- Monitorizarea securității rețelei
- Analiză Advanced package
- Detectarea/Prevenirea intruziunilor în rețea
- Scrierea de cod pentru detectare
- Network Forensics și altele
- Intoducere in Event Management
- Monitorizare continuă
- Analiză, logare și Event Collection
- SIEM și Analytics

Modulul 4
Digital forensics și răspuns la incidente

- Apărare activă
- Concepte de bază DFIR: Digital Forensics
- Concepte de bază DFIR: Incident Response
- DFIR
- Lărgirea rețelei: Scaling and Scoping

Modul 5
Malware Analysis

- Introducere în Malware Analysis
- Etapele analizei programelor malitoase: Fully Automated and Static Properties Analysis
- Etapele analizei programelor malitiose: Interactive Behavior Analysis
- Etapele analizei programelor malitioase: Manual Code Reversing

Modul 6
Simulări de situații reale care le permit participanților să pună în aplicare informațiile asimilate în celelalte module rezolvând exerciții de la simplu la complex.

Temele de discutie ale acestui curs trebuie ajustate pe nevoile beneficiarului, astfel încat vor fi selectate în programul ce va fi livrat de prestator cele mai potrivite teme pentru domeniul „IT" în care activeaza beneficiarului.

Rezultate imediate ce vor fi asigurate de prestator sau **livrabilele asteptate**:

- Invitatia la sesiunile de curs;
- Curs in domeniul Cybersecurity, pentru SOC (Security Operations Center), specializarea Raspuns la Incidente si Amenintari (48 de ore/ curs/cursant, 2 cursanti)
- 1 Suport de curs pentru fiecare cursant, care respecta regulile de identitate vizuala, în conformitate cu Manualul de Identitate Vizuala POCU 2014-2020, pus la dispozitie de catre beneficiar;

- Materiale curs/ instrumente/ fise de lucru/ teme de discutie elaborate pentru curs dupa caz;
- Liste de prezenta la curs sau dovada prezentei cursantilor la sesiunile integrale (export din platforma de prezentare - de ex: Teams;
- 1 raport cu toate documentele aferente sesiunilor de formare elaborate;
- 2 cursanti la in domeniul Cybersecurity, pentru SOC (Security Operations Center), specializarea Raspuns la Incidente si Amenintar ;
- Accesul cursantilor la examenul de certificare;
- Formularele de feedback completat de cursanti - arhivate si centralizate tabelar;

Nume	Feedback continut curs	Feedback trainer	Feedback metode de livrare

- Alte documente justificative relevante conform POCU.

În vederea pastrarii confidentialitatii, beneficiarul va semna cu operatorul economic declarat castigator o Declaratie de confidentialitate care va deveni parte integranta a contractului de prestari servicii.

3.2.2. Curs in domeniul Cybersecurity, pentru Cloud Security (specializarea Arhitectura si Inginerie de securitate Defensiva)

Obiectivele asteptate ale cursului si certificarii

Ne dorim ca angajatii nostrii dupa participarea la training sa poata:

a. Analiza o Arhitectură de Securitate, sa identifice punctele vulnerabile si sa reuseasca sa creeze o arhitectura cu calitati defensive.
b. Implementa tehnologii pentru capabilitati de prevenire, detectare și răspuns la atacurile cibernetice si sa le utilizeze
c. Determine nevoile adecvate de monitorizare a securității pentru organizațiile de toate dimensiunile
d. Maximizeze investițiile existente în arhitectura de securitate prin reconfigurarea infrastructurii existente
e. Determine capabilitățile necesare pentru a sprijini monitorizarea continuă a Controalelor Critice de Securitate principale.
f. Configura, înregistrarea și monitorizarea adecvata pentru a sprijini un Centru de operațiuni de securitate și un program de monitorizare continua;
g. Aplica practic elementele teoretice invatate in cadrul trainingului.

Continut:

Modul 1 - Arhitectura si ingineria de securitate defensibila

1. Punctele slabe ale arhitecturii traditionale de securitate

2. Abordari, modele (Zero-Trust, Kill Chain, diamant etc.) , microsegmentarea si software-ul necesar pentru o arhitectura de securitate defensiva
3. Analiza amenintarilor, vulnerabilitatilor si fluxului de date
4. Layer 1 – cele mai bune practici in securitatea fizica (Network closets, penetrare Dropbox-uri, Rubber Ducky)
5. Layer 2 - cele mai bune practici in securitatea retelelor (VLAN-uri, private LANs, atacuri si solutii pentru acestea)
6. NetFlow (NetFlow, Sflow, Jflow, VPC Flow, Suricata si Endpoint Flow)

Modul 2 - Arhitectura si ingineria de securitate a retelei

1. Layer 3
    a. Routere – cele mai bune practici
    b. Atacuri si modalitati de mitigare (rutare sursa iP, ICMP, actualizare rutare neautorizata, atacuri de tip wormwhole, securizare protocoale de rutare)
2. Layer 2 si 3 Benchmark si instrumente de audit
    a. Referinte – Cisco, CISecurity, DISA STIG-uri, Nipper-ng
3. Securizare SNMP
4. Securizare NTP
5. Filtrari: Blackholes, Bogon, Darknet
6. Despre IPv6 si securizarea IPv6
7. VPN
8. Layer 3 si 4 - Firewall-uri
9. Segmentare
10. Proxy (WEB & SMTP)

Modul 3 - Securitate centrata pe retea

1. NGFW
2. NIDS/NIPS (cum sa scrii reguliele
3. Monitorizarea securitatii retelei
4. Sandboxing
5. Criptare – principii, SSL/ TLS, SSL/SSH
6. Acces securizat Remote
7. Atac de tip Denial-of-Service Distribuit (tehnici de minimizare riscuri, IOT, tipuri de atacuri).

Modul 4: Securitate centrata pe date

1. Proxy (reverse) de aplicatie
2. Full Stack Security Design
3. Firewall-uri pentru aplicatii web
4. Firewall-uri pentru baze de date/Monitorizarea activitatii bazei de date
5. Clasificarea fisierelor
6. Prevenirea pierderilor de datelor (DLP)
7. Ownership-ul datelor
8. Managementul dispozitivelor mobile (MDM) si Managementul aplicatiilor mobile (MAM)
9. Securitatea in Cloud privat
10. Securitatea in cloud public
11. Securitate de tip Container

Modul 5 – Arhitectura de tip "Zero-Trust"

1. Ce inseamna arhitectura Zero - Trust si de ce securitatea perimetrului este insuficienta
2. Rotatia/Schimbarea credentialelor
3. Identificarea activelor interne deja compromise
4. Securizarea retelei
5. Aparari de tip "Tripwire" si "Red Herring"
6. Patching – adaptari ale sistemului pentru cresterea securitatii in fata vulnerabilitatilor.
7. Utilizarea Endpoint-urilor ca senzori de securitate consolidati
8. Scalarea colectarii/stocarii/analizei logurilor de pe Endpoint-uri

Modul 6: Aplicatii practice pentru Modulele 1-5

Temele de discutie ale acestui curs trebuie ajustate pe nevoile beneficiarului, astfel încat vor fi selectate în programul ce va fi livrat de prestator cele mai potrivite teme pentru domeniul „IT" în care activeaza beneficiarului.

Rezultate imediate ce vor fi asigurate de prestator sau **livrabilele asteptate**:

- Invitatia la sesiunile de curs;
- Curs de specializare avansat in domeniul Cybersecurity, pentru Cloud Security (specializarea Arhitectura si Inginerie de securitate Defensiva) (40 de ore/ curs/cursant, 1 cursant)
- 1 Suport de curs pentru fiecare cursant, care respecta regulile de identitate vizuala, în conformitate cu Manualul de Identitate Vizuala POCU 2014-2020, pus la dispozitie de catre beneficiar;
- Materiale curs/ instrumente/ fise de lucru/ teme de discutie elaborate pentru curs dupa caz;
- Liste de prezenta la curs sau dovada prezentei cursantilor la sesiunile integrale (export din platforma de prezentare - de ex: Teams;
- 1 raport cu toate documentele aferente sesiunilor de formare elaborate;
- 1 cursant la Cursul in domeniul Cybersecurity, pentru Cloud Security (specializarea Arhitectura si Inginerie de securitate Defensiva)
- Accesul cursantilor la examenul de certificare
- Formularele de feedback completat de cursanti - arhivate si centralizate tabelar;

Nume	Feedback continut curs	Feedback trainer	Feedback metode de livrare

- Alte documente justificative relevante conform POCU.

În vederea pastrarii confidentialitatii, beneficiarul va semna cu operatorul economic declarat castigator o Declaratie de confidentialitate care va deveni parte integranta a contractului de prestari servicii.

3.2.3. Curs in domeniul Cybersecurity, pentru Informatii (secrete) la Amenintari din domeniul Virtual

Obiectivele asteptate ale cursului sunt:

- Dezvoltarea de competete de analiză pentru a înțelege mai bine, a sintetiza și a valorifica scenarii complexe
- Dezvoltarea de competete de identificare și creare de cerințe de intelligence prin practici precum modelarea amenințărilor
- Dezvoltarea de competete de înțelegere și dezvoltare de abilități de a obtine informatii legate amenințări tactice, operaționale și strategice
- Dezvoltarea de competete de generare de intelligence pentru a detecta, a răspunde și a învinge amenințările specifice și cele targetate
- Dezvoltarea de competete de obtine informatii din diferite surse, de a colecta date și cum să exploatați aceste date
- Dezvoltarea de competete de valida informațiile primite extern pentru a minimiza costurile unor informatii gresite
- Dezvoltarea de competete de creare indicatori de compromis (IOC) în formate precum YARA și STIX/TAXII
- Dezvoltarea de competete de înțelegere și exploatare tactici, tehnici și procedure ale adversarului și folosirea de framework-uri precum Kill Chain, Diamond Model și MITRE ATT&CK
- Dezvoltarea de competete de analitiza structurata pentru a avea succes în orice rol de securitate

Continut:

Modul 1
Intelligence și cerințe privind amenințările cibernetice

- Înțelegerea conceptului de informatii secrete despre amenintari cibernetice(CTI)
  - Taxonomie pentru informatii secrete și definiții
  - Ciclul obișnuit al informatiilor secrete
  - Tehnici analitice structurate
- Înțelegerea informatiilor secrete în cazul amenințările cibernetice
  - Definirea ameninţărilor
  - Înțelegerea riscului
  - CTI si rolul sau in uz
  - Aşteptările organizaţiilor şi analiştilor
  - Modelul diamond și grupuri de activități
  - Patru tipuri de detectare a amenințărilor
- Consumul de informații despre amenințări
  - Sliding Scale of Cybersecurity
  - Folosirea informatiei secrete pentru diferite obiective

- Sprijinirea altor echipe folosind CTI
- Poziționarea echipei pentru a genera CTI
  - Construirea unei echipe de CTI
  - Poziţionarea echipei în organizaţie
  - Condiții preliminare pentru generarea de CTI
- Planificare și direcție (dezvoltarea cerințelor)
  - Cerințe de CTI
  - Cerințe prioritare de CTI
  - Începerea ciclului de viață al CTI
  - Modelarea ameninţărilor

Modul 2

Setul de abilități fundamentale: analiza intruziunilor

- Sursa de colectare primară: Analiza intruziunilor
  - Analiza intruziunilor ca un set de competențe de bază
  - Metode de realizare a analizei intruziunilor
  - Intrusion Kill Chain
  - MITRE ATT&CK
  - Modelul Diamond
- Mod de operare în Kill Chain
  - Descoperirea pasivă a activității în date istorice și jurnalele de evenimente
  - Detectarea acțiunilor și capacităților viitoare de amenințări
  - Blocarea amenințărilor cibernetice
  - Blocarea tacticilor adverse și a programelor de tip malware
- Kill Chain Deep Dive
  - Introducere
  - Notificarea activitatii malitioase
  - Pivotarea de pe un singur indicator- descoperirea activitatilor atacatorilor
  - Identificarea și clasificarea activitatii malitioase
  - Utilizarea retelei si a datelor de pe host-uri
  - Interacțiunea cu echipele de Incident Response
  - Interacțiunea cu echipa de inginerie inversa pe malware
  - Valorificarea eficientă a cererilor de informații
- Gestionarea mai multor Kill Chain-uri
  - Identificarea diferitelor intruziuni simultane
  - Gestionarea și construirea mai multor Kill Chain-uri
  - Corelarea intruziunilor
  - Extragerea de cunoștințe(indicatori) din intruziuni pentru monitorizarea pe termen lung

Modul 3

Surse de colectare

- Sursa colecție: Malware
  - Date din analiza malware

- Tipuri principale de date de analizat și pivotat
- VirusTotal și Analizatoare Malware
- Identificarea tiparelor de intruziune și a indicatorilor cheie

- Sursa colecție: Domenii
  - Deep Dive despre Domenii
  - Diferite tipuri de domenii adverse
  - Pivotarea de pe informațiile din domenii
- Sursa de colectare: Seturi de date externe
  - Construirea de depozite din seturi de date externe
  - Instrumente și cadre de colectare a informațiilor open-source
- Sursa de colectare: Certificate TLS
  - Certificate TLS/SSL
  - Urmărirea noilor mostre de malware și C2 cu TLS
  - Pivotarea de pe informațiile din certificatele TLS

Modul 4

Analiza și producerea de CTI

- Exploatarea: Stocarea și Structurarea Datelor
  - Stocarea datelor din amenințări
  - Partajarea informațiilor despre amenințări
  - MISP ca platformă de stocare
- Analiză: Erorile logice și prejudecăți cognitive
  - Erorile logice
  - Prejudecăți cognitive
  - Erori informale comune ale CTI
- Analiză: Explorarea ipotezelor
  - Analiza ipotezelor concurente
  - Generarea de ipoteze
  - Înțelegerea și identificarea lacunelor de cunoștințe
- Analiză: Diferite tipuri de analiză
  - Analiza vizuală
  - Analiza datelor
  - Analiza temporală
  - Studiu de caz: Panama Papers
  - Analiză: Clustering Intrusions
  - Ghid de stil
  - Nume și reguli de grupare
- ACH pentru intruziuni
- Grupuri de activități și model diamant pentru clustere
  - Ghid de stil
  - Nume și reguli de grupare
  - ACH pentru intruziuni
  - Grupuri de activitate și model diamant pentru clustere

Modul 5
Diseminare și atribuire

- Erori logice și părtiniri cognitive
  - Identificarea și înfrângerea părtinirii
  - Erorile logice și exemple
  - Erori comune in CTI
  - Prejudecăți cognitive și exemple
- Diseminare: Tactică
  - Înțelegerea publicului și a consumatorului
  - Fluxuri de date despre amenințări și limitările acestora
  - YARA
  - YARA: Concepte și exemple
- Diseminare: Operațională
  - Metode diferite de corelare a campaniei
  - Înțelegerea intențiilor adverse percepute
  - Utilizarea modelului diamant pentru analiza campaniei
  - STIX și TAXII
  - Colaborarea guvernului și a partenerilor
- Diseminare: Strategică
  - Capcanele la intocmirea rapoartelor
  - Cele mai bune practici de redactare a rapoartelor
  - Diferite tipuri de rezultate strategice
- O cerință specifică de inteligență: Atribuire
  - Identificarea și remedierea noilor cerințe de inteligență
  - Ajustarea cadrului de management al colecțiilor
  - Tipuri de atribuire
  - Construirea unui model de atribuire
  - Efectuarea evaluărilor de atribuire

Modul 6
Activitati de analiza, activitati practice si studii de caz care vor oferi posibilitatea cursantilor sa foloseasca in mod real informatiile teoretice asimilate in celelalte module.

Furnizorul va pune la dispozitie urmatoarele instrumente de lucru:

a. Suport de curs
b. Masina virtuala de curs (VM) cu toate exercitiile de laborator care pot fi refacute in afara sesiunilro de curs
c. Linii de Infrastructure-as-code pentru fiecare platforma cloud pe care sa le putem folosi in activitatea de zi cu zi.

Temele de discutie ale acestui curs trebuie ajustate pe nevoile beneficiarului, astfel încat vor fi selectate în programul ce va fi livrat de prestator cele mai potrivite teme pentru domeniul „IT" în care activeaza beneficiarului.

Rezultate imediate ce vor fi asigurate de prestator sau **livrabilele asteptate**:

- Invitatia la sesiunile de curs;
- Curs in domeniul Cybersecurity, pentru Informatii (secrete) la Amenintari din domeniul Virtual (40 de ore/ curs/cursant, 1 cursant)
- 1 Suport de curs pentru fiecare cursant, care respecta regulile de identitate vizuala, în conformitate cu Manualul de Identitate Vizuala POCU 2014-2020, pus la dispozitie de catre beneficiar;
- Materiale curs/ instrumente/ fise de lucru/ teme de discutie elaborate pentru curs dupa caz;
- Liste de prezenta la curs sau dovada prezentei cursantilor la sesiunile integrale (export din platforma de prezentare - de ex: Teams;
- 1 raport cu toate documentele aferente sesiunilor de formare elaborate;
- 1 cursant la Cursul in domeniul Cybersecurity, pentru Informatii (secrete) la Amenintari din domeniul Virtual;
- Accesul cursantilor la examenul de certificare
- Formularele de feedback completat de cursanti - arhivate si centralizate tabelar;

Nume	Feedback continut curs	Feedback trainer	Feedback metode de livrare

- Alte documente justificative relevante conform POCU.

În vederea pastrarii confidentialitatii, beneficiarul va semna cu operatorul economic declarat castigator o Declaratie de confidentialitate care va deveni parte integranta a contractului de prestari servicii.

3.2.4. Curs in domeniul Cybersecurity, pentru SOC (Security Operations Center), raspunsuri avansate la atacuri cibernetice

Obiectivele cursului sunt:

- Dezvoltarea abilitatilor de a intelege modul de operare a atacatorilor pentru a evalua gradul de compromitere a sistemelor
- Dezvoltarea abilitatilor de a detecta cum și când a avut loc o scurgere de informatii/incident de securitate
- Dezvoltarea capacitatii de a identifica rapid sistemele compromise și infectate
- Dezvoltarea abilitatilor de a efectua evaluări ale daunelor și determinarea a ceea ce a fost citit, furat sau schimbat
- Dezvoltarea abilitatilor de a limita si remedia efectele unor incidente de securitate informatica de toate tipurile
- Dezvoltarea abilitatilor de a identifica si dezvolta solutii de monitorizare a retelei
- Dezvoltarea de abilitati de identificare a incidentelor de securitate folosind infomatii despre modul de lucru al atacatorului

- Dezvoltarea competentelor de a folosi instrumentele, tehnicile și procedurile necesare pentru a investiga, detecta și limita efectele incidentelor de securitate în mod eficient.
- Dezvoltarea competentelor de a detecta și investiga programe malitioase necunoscute in timp real , latente și personalizate în memorie pe mai multe sisteme Windows.
- Dezvoltarea abilitatilor de răspuns la incidente simultan în sute de sisteme unice , folosind PowerShell sau F-Response Enterprise și stația de lucru SIFT.
- Dezvoltarea competentelor de a identifica și urmări semnalizarea programelor malitioase care reies din canalul de comanda si control (C2) prin analiza criminalistică a memoriei, analiza registrului și istoricul de conexiune la rețea.
- Dezvoltarea abilitatilor necesare determinarii tacticilor folosite pentru incidentele de securitate prin identificarea cauzei fundamentale, a sistemelor „ beachhead”/legaturilor și a mecanismelor inițiale de atac.
- Dezvoltarea abilitatilor necesare identificarii unor tehnici tip „living off the land”, inclusiv utilizarea rău intenționată a PowerShell și WMI.
- Dezvoltarea abilitatilor necesare folosirii de tehnici de tip „hidden and time-stomped malware”.
- Dezvoltarea abilitatilor necesare de urmarire continua a activitatii utilizatorilor și a atacatorului, printr-o cronologie aprofundată
- Dezvoltarea abilitatilor necesare de recuperare a datelor șterse utilizând tehnici anti-criminalistică via „Volume Shadow Copy” si analiza de tip „Restore Point”.
- Dezvoltarea abilitatilor necesare identificarii modului de patrundere al atacatorilor in sisteme fără a fi detectați.
- Dezvoltarea abilitatilor necesare înțelegerii modului in care atacatorii pot obține drepturi de administrator de domeniu - chiar și într-un mediu de tip ”locked down”.
- Dezvoltarea abilitatilor necesare identificarii circuitului datelor in cazul unor incidente de securitate.

Continut, competente si abilitati dobandite ca urmare a acestui curs practic:

Modul 1
Răspunsuri avansate la incidente și identificarea activă a amenințărilor cibernetice
Tactici reale de răspuns la incidente

- Pregătire: instrumente, tehnici și proceduri cheie necesare pentru a raspunde la incidente de securitate
- Identificare intentiei din spatele unui incident de securitate și detectarea tuturor sistemelor afectate
- Solutii de minimizare a efectelor unor incidente de securitate: restricționarea accesului, monitorizarea și studiul modului de operare al atacatorului in vederea dezvoltării de metode eficiente de răspuns
- Identificarea pașilor cheie care trebuie urmati pentru a ajuta la eliminarea efectelor incidentului curent și remediere în timp real
- Realizarea unui set de bune practici care urmează să fie urmate în cazul unui atac similar
- Evitarea situatiilor de tip „Whack-A-Mole” - o situație în care o problemă continuă să se repete după ce se presupune că este rezolvată

Identificarea proactivă de amenințări
- Identificarea proactivă versus răspuns reactiv
- Răspuns la incident bazat pe informatii
- Construirea unei modalitati continue de răspuns la incident/de monitorizare a amenințărilor
- Analiză criminalistică versus identificare proactivă la endpoints
- Rolurile echipei Threat Hunt
- ATT&CK - Tacticile, tehnicile și cunoștințele comune ale lui MITRE (ATT&CK(TM))

Identificarea proactivă în sistem Enterprise
- Identificarea sistemelor compromise
- Găsirea programelor malitioase active și latente
- Program malitios semnat digital
- Caracteristicile programelor malitioase
- Mecanisme obișnuite de ascundere și persistență
- Identificarea infracțiunii prin înțelegerea normalului

Răspuns la incidente și identificare proactivă la Endpoints
- WMIC și PowerShell
- Scalabilitate Remoting PowerShell
- Măsuri de protejare a credențialelor remote PowerShell
- Framework IR Remoting Kansa PowerShell

Evitare și identificarea programelor malitioase
- Deturnarea/Înlocuirea
- Compilare frecventă
- Binary Padding
- Packing/Armoring
- Malware latent
- Cod de semnare cu certificate valabile
- Anti-Forensics/Timestomping

Identificarea persistenței malware
- Locații de pornire automată, RunKeys
- Crearea/Înlocuirea serviciului
- Service Failure Recovery
- Task-uri programate
- DLL Hijacking Attacks
- Evenimente WMI

Prevenirea, detectarea și atenuarea furtului de credențiale
- Pass the Hash
- Atacuri folosind Mimikatz
- Furtul de dispozitive de logare (Token)
- Credențiale în cache

- Secretele LSA
- Atacurile folosind Kerberos
- Golden tickets
- Kerberoasting
- DCSync
- NTDS.DIT furt
- Bloodhound și Active Directory Graphing

Modul 2
Analiza intruziunilor
Furtul și utilizarea credențialelor legitime

- Pass the Hash
- SSO Dumping folosind Mimikatz
- Furtul de dispozitive de logare (Token)
- Credențiale în cache
- Secretele LSA
- Atacurile Kerberos
- NTDS.DIT

Dovezi avansate de detectare a execuției

- Tactici, tehnici și proceduri ale atacatorului (TTP)
- Analiză Prefetch
- Cache de compatibilitate cu aplicații (ShimCache)
- Examinarea Registrului Amcache
- Scalarea ShimCache și investigarea Amcache

Tactici, tehnici și proceduri adverse ale mișcării laterale (TTP)

- Tehnici de compromitere a credențialelor
- Utilizare greșită a serviciilor remote desktop
- Windows Admin Share Abuse
- Activitate PsExec și Cobalt Strike Beacon PsExec
- Tehnici Windows Remote Management Tool
- PowerShell Remoting/WMIC Hacking
- Cobalt Strike Lateral Movement și utilizarea credențialelor
- Exploatarea vulnerabilităților

Analiza jurnalului pentru respondenții la incident și investigatori

- Realizarea unui profil a utilizării conturilor și a logărilor
- Urmărirea și identificarea proactivă de Lateral Movement
- Identificarea Suspticious Services
- Detectarea Rogue Application Installation
- Găsirea Malware Execution și Process Tracking
- Identificarea liniilor de comandă și a scripturilor
- Ștergerea log-urilor și anti-forensics

Investigarea atacurilor bazate pe WMI și PowerShell

- Prezentare generală WMI
- Atacurile WMI
- Auditarea WMI Repository
- Sistem WMI și Registry Residue
- Analiză Command-Line și WMI Activity Logging
- PowerShell Transcript și ScriptBlock Logging
- Descoperirea PowerShell și Cobalt Strike Beacon
- Detectarea PowerShell Injection de la Cobalt Strike, Metasploit și Empire

Modul 3

Criminalistica memoriei digitale în timpul răspunsurilor în cadrul incidentelor și identificarea proactivă de amenințări

Răspunsuri la incidente remote și enterprise

- Acces Remote Endpoint în Enterprise
- Analiză bazată pe Remote Endpoint
- Analiză bazată pe Scalable Host
- Analiza remote a Momoriei Digitale
- Velociraptor, F-Response și KAPE

Triaj și EDR – Endpoint Detection and Response

- Endpoint Triage Collection
- EDR capacitate și provocări
- EDR și Memory Forensics

Achiziție de memorie digitală

- Achiziția de memorie de sistem
- Hibernation și Pagefile Memory Extraction and Conversion
- Achiziția memoriei digitale la Virtuale Machine
- Modificări ale memoriei digitale în Windows 10 și 11

Analiză criminalistică a memoriei digitale pentru răspuns la incidente și identificare proactivă

- Înțelegerea serviciilor și proceselor Windows
- Identificarea proceselor Rogue
- Procesul de analiză DLL-urile și opțiuni
- Examinarea Network Artifacts
- Identificarea de dovezi ale Code Injection
- Identificare Rootkit

Examinări criminalistice ale memorie digitale

- Criminalistica Live Memory
- Analiză Advanced Memory folosind Volatility
- Detectare Webshell prin Process Tree Analysis

- Code injection, Malware and Rootkit Hunting
- WMI și PowerShell
- Identificare linii de cod ale atacatorilor
- Investigarei serviciile Windows
- Identificare proactivă a programelor malware utilizând Comparison Baseline Systems
- Identificare și Stergere Cached Files din RAM

Instrumente de analiză a memoriei
- Volatility
- F-Response
- Velociraptor

Modul 4
Analiză cronologica
Detectarea apărării de evitare a programelor malware
- Indicatori de compromitere - YARA
- Entropie și Analiza Packing
- Detectarea fisierelor executabile neobișnuite
- Analiza Digital Signature

Prezentare generală a Timeline Analysis
- Timeline - Beneficii
- Cunoștințe predefinite
- Găsirea Pivot Point
- Indicii Timeline Context
- Procesul Timeline Analysis

Crearea și analiza cronologiei sistemului de fișiere
- Marcaje de tip MACB
- Reguli Windows (File copy vs. File Move)
- Filesystem Timeline folosind Sleuthkit, fls și MFTECmd
- Analiză și filtrare Bodyfile folosind mactime Tool

Crearea și Analiza Super Timeline
- Reguli de Super Timeline Artifact
- Program Execution, File Knowledge, File Opening, File Deletion
- Creare Timeline cu log2timeline/Plaso
- log2timeline/ Componente Plaso
- Filtrarea Super Timeline folosind psort
- Creare Targeted Super Timeline
- Tehnici de analiză Super Timeline Analysis
- Analiză Scaling Super Timeline Analysis folosind Elastic Search (ELK)

Modul 5
Răspuns la incidente de securitate și Identificare proactivă în Enterprise | Subiecte avansate
Analiza Volume Shadow Copy

- Serviciu Volume Shadow Copy
- Opțiuni pentru accesarea datelor istorice în Volume Snapshots
- Accesarea Shadow Copies cu vshadowmount
- Timeline Volum Shadow Copy

Tactici avansate ale NTFS Filesystem

- Analiza NTFS Filesystem
- Zonele critice ale Master File Table (MFT).
- Fișiere de sistem NTFS
- Atribute NTFS Metadata
- Regulile Windows Timestamps for $StdInfo and $Filename
- Detectarea Timestamp Manipulation
- Fișiere Resident vs Nonresident
- Fluxuri Data Streams
- Atribute NTFS Directory
- Prezentare generală B-Tree Index
- Găsirea fișierelor Wiped/Deleted Files folosind $I30 indexes
- Filesystem Flight Recorders: $Logfile și $UsnJrnl
- Tipare comune de activitate în Journals
- Filtre și căutări utile în Journals
- Ștergere fișiere NTFS Filesystem - efecte

Recuperare avansată a dovezilor

- Indicatori de Common Wipers and Privacy Cleaners
- Registry Keys - stergere
- Detectarea programelor malware în regiștrii
- File Carving
- Volume Shadow Carving
- Carving for NTFS artifacts și Event Log Records
- Căutări eficiente în String
- Modificări ale configurației NTFS pentru Combat Anti-Forensics

Modul 6
Exerciții de răspuns la incidente de securitate de tip APT
Subiecte

- Exerciții de simulare în echipă a unor atacuri de tip APT.
- Identificare și urmărire acțiuni atacatori în întreaga rețea
- Identificarea de dovezi ale atacurilor de tip Cobalt Strike, Metasploit, PowerShell și malware realizați de diverși actori statali.

IDENTIFICARE ȘI SCOPING:

1. Identificarea metodelor folosite și a momentului în care a apărut incidentul de securitate?
2. Identificarea sistemelor compromise după adresa IP și dovezile specifice ale acestor intruziuni.
3. Identificarea metodelor și momentelor acțiuniunilor de tip lateral movement în fiecare sistem?

REDUCERE PAGUBE ȘI INTELLIGENCE:

1. Identificarea metodelor și momentulului în care au obținut atacatorii credențialele de administrator de domeniu?
2. Identificarea obiectivelor atacatorilor pe fiecare sistem?
3. Găsirea de e-mailuri exfiltrate din conturile și evaluarea daunelor.
4. Identificarea datelor furate: recuperarea arhivele atacatorilor, identificare parole de criptare și extragere de conținul pentru a verifica datele exfiltrate.
5. Colectarea și enumerarea programelor malware utilizate în atac.
6. Dezvoltarea și prezentarea informații despre amenințările cibernetice pe baza indicatorilor de compromis la nivel de calculator host dar și la nivel de rețea.

REMEDIERE ȘI RECUPERARE:

1. Idenficarea nivel de compromitere. Este necesară o resetare completă a parolei în timpul remedierii?
2. Identificarea pașilor recomandați pentru remedierea și recuperarea datelor după un incident de securitate?
3. Identificarea sistemelor ce trebuie reconstruite?
4. Identificarea adreselor IP ce trebuie blocate?
5. Identificarea contramăsurilor ce ar trebui să fie implementate pentru a încetini sau opri acești atacatori dacă revin?
6. Identificarea de acțiuni pentru a detecta din nou acești intruși în propria rețea?

Temele de discutie ale acestui curs trebuie ajustate pe nevoile beneficiarului, astfel încat vor fi selectate în programul ce va fi livrat de prestator cele mai potrivite teme pentru domeniul „IT" în care activeaza beneficiarului.

Rezultate imediate ce vor fi asigurate de prestator sau **livrabilele asteptate**:

- Invitatia la sesiunile de curs;
- Curs in domeniul Cybersecurity, pentru SOC (Security Operations Center), raspunsuri avansate la atacuri cibernetice (48 de ore/ curs/cursant, 1 cursant)
- 1 Suport de curs pentru fiecare cursant, care respecta regulile de identitate vizuala, în conformitate cu Manualul de Identitate Vizuala POCU 2014-2020, pus la dispozitie de catre beneficiar;
- Materiale curs/ instrumente/ fise de lucru/ teme de discutie elaborate pentru curs dupa caz;
- Liste de prezenta la curs sau dovada prezentei cursantilor la sesiunile integrale (export din platforma de prezentare - de ex: Teams;
- 1 raport cu toate documentele aferente sesiunilor de formare elaborate;

- 1 cursant la Cursul in domeniul Cybersecurity pentru SOC (Security Operations Center), raspunsuri avansate la atacuri cibernetice;
- Accesul cursantilor la examenul de certificare
- Formularele de feedback completat de cursanti - arhivate si centralizate tabelar;

Nume	Feedback continut curs	Feedback trainer	Feedback metode de livrare

- Alte documente justificative relevante conform POCU.

În vederea pastrarii confidentialitatii, beneficiarul va semna cu operatorul economic declarat castigator o Declaratie de confidentialitate care va deveni parte integranta a contractului de prestari servicii.

3.3. Metoda de livrare si de evaluare

- Cursul va fi livrat in mediul online/ virtual, prin intermediul platformelor de comunicare online (de ex. Microsoft Teams etc.).
- Sesiunile de curs de specializare in domeniul CYBERSECURITY trebuie sa includa dezabateri, studii de caz, exercitii prin care cursantii sa poata asimila informatiile cat mai usor si sa le creasca sansa de a promova examenul de certificare.
- In propunerea tehnica a ofertei se va include metodologia de desfasurare a cursurilor în sistem online, mentionandu-se aplicatiile, instrumentele, platformele utilizate atat pentru partea teoretica, cat si pentru cea practica;
- Tot in propunerea tehnica se va mentiona si modalitatea de evaluare a cursului, respectiv formularul de evaluare care va fi oferit cursantilor (acesta va cuprinde categoriile – continut curs, trainer si metoda de livrare).
- Toate cheltuielile cu logistica necesara pregatirii sau sustinerii sesiunilor de formare în sistem online, vor fi asigurate de prestator.
- În derularea programelor de formare se va tine cont de respectarea de catre expertii prestatorului a unor principii fundamentale, precum transparenta, egalitatea de sanse, nediscriminarea, accesibilitatea, coerenta în comunicare.

3.4. Durata cursului

Durata cursurilor de specializare in domeniul CYBERSECURITY este urmatoarea:

- Curs in domeniul Cybersecurity, pentru Cloud Security (specializarea Arhitectura si Inginerie de securitate Defensiva), pentru un volum de 48h/ curs/cursant
- Curs in domeniul Cybersecurity, pentru SOC (Security Operations Center), specializarea Raspuns la Incidente si Amenintari, pentru un volum de 48h/ curs/cursant
- Curs in domeniul Cybersecurity, pentru Informatii (secrete) la Amenintari din domeniul Virtual, pentru un volum de 48h/ curs/cursant

- Curs in domeniul Cybersecurity, pentru SOC (Security Operations Center), raspuns, distribuite in sesiuni de curs distincte uri avansate la atacuri cibernetice, pentru un volum de 48h/ curs/cursant

Capitolul 4. Aspecte organizatorice

4.1. Cursantii

Cursurile de specializare in domeniul CYBERSECURITY se adreseaza angajatilor beneficiarului, specialisti Cybersecurity, care activeaza la sediile Solicitantului din NTT DATA Romania in Cluj, Timisoara, Iasi, Sibiu, Brasov.
Zilele si orele de curs vor fi organizate în functie de programul de lucru si disponibilitatea de a participa la formare.
O planificare mai temeinica va fi propusa de Beneficiar si negociata cu prestatorul în vederea asigurarii resurselor necesare pentru desfasurarea în conditii optime a cursurilor, ulterior incheierii contractului de servicii. Distributia angajatilor poate varia în functie de disponibilitatea angajatilor, nivelul de încarcare cu sarcini curente precum si în urma graficului de formare realizat împreuna cu prestatorul, pentru a grupa acei angajati cu profile similare si obiective aliniate.

4.2 Materiale necesare

Ofertantul va pune la dispozitia grupului tinta materialele didactice necesare desfasurarii cursului în conditii optime.
Ofertantul va pune la dispozitia cursantilor suportul de curs. Suportul de curs trebuie sa respecte regulile de identitate vizuala, în conformitate cu Manualul de Identitate Vizuala POCU 2014-2020, pus la dispozitie de catre beneficiar.
Pe langa programa si suportul de curs, ofertantii vor trebui sa defineasca si sa puna la dispozitia cursantilor fisele de lucru si orice alte documente suport pentru desfasurarea în conditii optime a cursurilor.

4.3 Durata

Dupa organizarea grupelor, stabilirea continutului de curs, a instrumentelor optime care vor fi utilizate în procesul de predare, pregatirea aplicatiei online, va începe livrarea propriu zisa a cursurilor, pe o durata estimativa de maxim 3 luni, nu mai tarziu de data de 27.01.2023.
În cazul prelungirii duratei proiectului prestatorul va fi notificat si se va prelungi si durata prestarii cursurilor, daca va fi cazul.
Graficul de desfasurare a tuturor sesiunilor de curs (ex. numarul de ore/zi, numarul de zile pe saptamana etc.) va fi propusa de beneficiar si agreata cu ofertantul, ofertantul asigurandu-se ca va acoperi insa cel putin durata programului de formare, numarul de zile pentru livrarea online putand sa varieze în functie de aceasta planificare.

4.4 Locatia

Cursurile vor fi organizate cu instructor în sistem online (ILO – instructor-led online).

4.5 Certificare

Prestatorul va asigura acces la serviciul de certificare, în vederea verificarii competentelor dobandite si certificarii cursantilor care au finalizat programul nu mai tarziu de data de 27.01.2023.
Accesul la serviciile de certificare este o cerinta obligatorie a Beneficiarului în cadrul programului de formare si specializare. Aceste cursuri trebuie sa pregateasca pe cursanti pentru certificari de tip GIAC - Global Information Assurance Certification

4.6 Mentiuni referitoare la plata

Pretul serviciilor de formare se va achita în termen de maxim 45 zile calendaristice de la semnarea proceselor verbale de receptie (intermediare sau finale) si primirii facturii/ facturilor de la prestator.
În vederea semnarii procesului verbal de receptie, ofertantul declarat castigator va trebui sa prezinte urmatoarele documente justificative:

- Invitatia la sesiunile de curs
- Metodologia de desfasurare a cursurilor în sistem online, mentionandu-se aplicatiile, instrumentele, platformele utilizate atat pentru partea teoretica, cat si pentru cea practica
- Graficul de desfasurare a cursurilor si examenelor de certificare
- Suport de curs si orice alte fise/instrumente utilizate in procesul de formare
- Liste de prezenta pentru toate zilele de desfasurare a sesiunilor de instruire (teorie si practica, dupa caz);sau dovada prezentei cursantilor la sesiunile integrale (export din platforma de prezentare - de ex: Teams;
- Fotografii/print-screen-uri relevante din timpul cursului
- Formularele de feedback completat de cursanti - arhivate si centralizate tabelar
- 1 raport cu toate documentele aferente sesiunilor de formare elaborate
- Accesul la certificarea competentelor dobandite in urma cursurilor de formare finalizate, pentru persoanele ce beneficiaza de cursurile de specializare

Toate documentele justificative mentionate vor fi folosite de beneficiar în vederea solicitarii sumelor avansate pentru plata cursurilor de formare, în cadrul cererilor de rambursare.
Prestarorul va emite factura fiscala, numai dupa semnarea de catre beneficiar a procesului verbal de receptie a serviciilor.
Contravaloarea serviciilor de formare se va achita prin transfer bancar, din contul de proiect al beneficiarului în contul indicat de prestator, în baza facturii, în conditiile receptionarii pe baza de proces verbal de receptie.
Nu se fac plati in avans.

4.7 Clauze contractuale

Contractul se va incheia doar cu operatorul economic desemnat prin Nota justificativa de atribuire.