



Proiect cofinanțat din Programul Operational Capital Uman 2014-2020

Fondul Social European

Programul Operational Capital Uman 2014-2020

Axa prioritara 3: Locuri de munca pentru toti

Obiectivul tematic 10: Investițiile în educație, calificare și formare profesională pentru dobândirea de competențe și învățare pe tot parcursul vieții

Prioritatea de investiții 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 cai 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 și SNCDI ale angajaților

Titlu proiect: IDEA – Innovate, Discover, Evolve, Apply /IDEA - Inoveaza, Descopera, Evolueaza, Aplica

CodMySMIS2014: 142366

Nr contract finantare POCU/ /861/3/12/142366

Nr. inregistrare 8937/18.06.2021

OIRPOSDRU V

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

Aprobat

**NTT DATA
Romania S.A.**

Prin

**Head of HR
Diana Stanese**

Proiect cofinanțat din Programul Operational Capital Uman 2014-2020

Cuprins:

Sectiunea I. Cerinte minime pentru ofertanti.....	4
Capitol 1. Informatii generale	4
Capitol 2. Detalii contract	4
Capitol 3. Valoare estimata.....	6
Capitol 4. Durata contractului	6
Capitol 5. Documente de calificare.....	6
Capitol 6. Modul de prezentare a propunerii tehnice.....	8
Capitol 7. Modul de prezentare a propunerii financiare	9
Capitol 8. Modalitate de evaluare	9
Capitol 9. Modul de prezentare si depunere a ofertei	11
Capitol 10. Informatii privind contractul de servicii.....	12
Capitol 11. Cai de atac	13
Capitol 12. Informatii despre modul de derulare a procedurii	13
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”	15
Capitolul 1. Generalitati	15
Capitolul 2. Obiectul prezentului caiet de sarcini	15
Capitolul 3. Cerinte minime obligatorii	16
3.1. Ofertantul	16
3.2. Continutul cursului.....	16
3.2.1. Curs in domeniul Cybersecurity, pentru Cloud Security (specializarea CCSP)	17
3.2.2 Curs in domeniul Cybersecurity, pentru Cloud Security (specializarea Arhitectura si Inginerie de securitate Defensiva)	18
3.2.3 Curs in domeniul Cybersecurity, pentru SOC (Security Operations Center), specializarea Raspuns la Incidente si Amenintari	21
3.2.4. Curs in domeniul Cybersecurity, pentru Informatii (secrete) la Amenintari din domeniul Virtual.....	24

Proiect cofinanțat din Programul Operational Capital Uman 2014-2020

3.2.5. Curs in domeniul Cybersecurity, pentru SOC (Security Operations Center), raspunsuri avansate la atacuri cibernetice.....	26
3.3. Metoda de livrare si de evaluare	27
3.4. Durata cursului.....	28
Capitolul 4. Aspecte organizatorice	28
4.1. Cursantii.....	28
4.2 Materiale necesare	29
4.3 Durata.....	29
4.4 Locatia	29
4.5 Certificare.....	29
4.6 Mentiuni referitoare la plata	30
4.7 Clauze contractuale.....	30

Proiect cofinanțat din Programul Operational Capital Uman 2014-2020

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: Alina Musat

Telefon: 0372294784

Posta electronica: idea@nttdata.ro

Graficul de desfasurare a procedurii de atribuire:

1. Lansare procedura: Anunt publicat pe site <https://beneficiar.fonduri-ue.ro:8080/anunturi>
15 noiembrie 2021

2. Termen limita de primire clarificari de la potentiali ofertanti: **22 noiembrie 2021, 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: **24 noiembrie 2021**

4. Termenul limita de depunere oferte: **06 decembrie 2021, 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”

Proiect cofinanțat din Programul Operational Capital Uman 2014-2020

<p>2. Descrierea achizitiei: Achiziția de servicii de livrare a cursurilor de formare destinate grupului tinta in vederea realizării Activității: A.1.Furnizarea de programe de formare profesionala, Subactivități: A.1.1.Furnizarea de programe de formare profesionala.</p> <p>Conform cererii de finanțare, cursul urmează să se realizeze astfel:</p> <ul style="list-style-type: none"> • Curs in domeniul Cybersecurity, pentru Cloud Security (specializarea CCSP) pentru un volum de 40h/ curs/cursant, pentru un număr de maxim 1 persoana • Curs in domeniul Cybersecurity, pentru Cloud Security (specializarea Arhitectura si Inginerie de securitate Defensiva), pentru un volum de 40h/ curs/cursant, pentru un număr de maxim 1 persoana • Curs in domeniul Cybersecurity, pentru SOC (Security Operations Center), specializarea Raspuns la Incidente si Amenintari, pentru un volum de 48h/ curs/cursant, pentru un număr de maxim 1 persoana • Curs in domeniul Cybersecurity, pentru Informatii (secrete) la Amenintari din domeniul Virtual, pentru un volum de 40h/ curs/cursant, pentru un număr 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 număr de maxim 2 persoane
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
<p>7. Sursa de finanțare:</p> <p>Fondul Social European</p> <p>Programul Operational Capital Uman 2014-2020</p> <p>Axa prioritara 3: Locuri de munca pentru toti</p> <p>Obiectivul tematic 10: Investitiile in educatie, calificare si formare profesionala pentru dobandirea de competente si invatare pe tot parcursul vietii</p> <p>Prioritatea de investitii 10iii Imbunatatirea accesului egal la invatarea pe tot parcursul vietii pentru toate grupurile de varsta intr-un cadru formal, non-formal sau informal, actualizarea cunostintelor, a aptitudinilor si a competentelor fortei de munca si promovarea unor cai de invatare flexibile, inclusiv prin orientare profesionala si prin validarea competentelor dobandite</p> <p>Obiectivul specific 3.12 Imbunatatirea nivelului de cunostinte/competente/aptitudini aferente sectoarelor economice/domeniilor identificate conform SNC și SNCDI ale angajatilor</p> <p>Titlu proiect: IDEA – Innovate, Discover, Evolve, Apply /IDEA - Inoveaza, Descopera, Evolueaza, Aplica</p> <p>CodMySMIS2014: 142366</p> <p>Nr contract finantare POCU/ /861/3/12/142366</p>

Proiect cofințat din Programul Operational Capital Uman 2014-2020

Nr. inregistrare OIRPOSDRU NV 8937/18.06.2021

Capitol 3. Valoare estimata

Valoare estimata totala a contractului este de: 150,900.00 lei fara TVA cu urmatoarea defalcare:

- Servicii livrare „Curs in domeniul Cybersecurity, pentru Cloud Security (specializarea CCSP)” - 7,900.00 lei fara TVA
- Servicii livrare „Curs in domeniul Cybersecurity, pentru Cloud Security (specializarea Arhitectura si Inginerie de securitate Defensiva)” - 28,000.00 lei fara TVA
- Servicii livrare „Curs in domeniul Cybersecurity, pentru SOC (Security Operations Center), specializarea Raspuns la Incidente si Amenintari” - 29,200.00 lei fara TVA
- Servicii livrare „Curs in domeniul Cybersecurity, pentru Informatii (secrete) la Amenintari din domeniul Virtual” - 24,300.00 lei fara TVA
- Servicii livrare „Curs in domeniul Cybersecurity, pentru SOC (Security Operations Center), raspunsuri avansate la atacuri cibernetice” - 61,500.00 lei fara TVA

**Nota: Vor fi respinse ofertele care depasesc valoarea estimata*

Capitol 4. Durata contractului

Durata contractului: maximum 11 luni, nu mai tarziu de data de 21.11.2022, cu posibilitate de prelungire. Prolungirea 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:

DI. METZ DANIEL – Administrator, presedinte consiliu de administratie

DI. CERUTTI GIOVANNI – Administrator, membru in consiliu de administratie

DI. MUROTA MASAKI – Administrator, membru in consiliu de administratie

Dna. METZ MARIA – Administrator, membru in consiliu de administratie si director general

Proiect cofinanțat din Programul Operational Capital Uman 2014-2020

DI. RUFFINONI WALTER - Administrator, membru in consiliu de administratie

DI. Dan OLOVINARU - Manager proiect

Dna. Daniela Bara - Responsabil financiar

Dna. Diana Stanese – Presedinte comisie de evaluare

Dna. Elena Musca - Membru comisie de evaluare

Dna. Alina Musat - Membru comisie de evaluare

Dna. Oana Suru - Membru comisie de evaluare

DI. Cristian Zdroba - 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.

Proiect cofinanțat din Programul Operational Capital Uman 2014-2020

În cazul unei asocieri de operatori economici, toți operatorii economici asociați vor transmite toate documentele solicitate, cu excepția Propunerii financiare și a Propunerii tehnice care se vor transmite doar de către liderul asocierii, în numele asocierii.
În cazul unei asocieri este necesar să se transmită suplimentar și un acord de asociere.

Capitol 6. Modul de prezentare a propunerii tehnice

1. Informații generale

Propunerea tehnică va fi întocmită în așa fel încât să se asigure posibilitatea verificării conformității acesteia cu cerințele din caietul de sarcini.

Obligațiile pe care operatorul economic și le va asuma prin propunerea tehnică vor fi valabile pe toată durata contractului.

Cerințe tehnice din caietul de sarcini sunt minime și obligatorii.

Documentele oficiale emise de un organism tert în altă limbă decât română vor fi însoțite de traducerea autorizată în limba română.

În cazul în care, pe parcursul îndeplinirii contractului se constată faptul că anumite elemente ale propunerii tehnice sunt inferioare sau nu corespund cerințelor prevăzute în caietul de sarcini, prevalează prevederile caietului de sarcini.

2. Propunerea tehnică va cuprinde următoarele:

2.1. Informații generale despre ofertant.

2.2. Informații cu privire la experiența organizației în domeniul formării profesionale.

2.3. O descriere amănunțită a serviciilor oferite și a modului de acordare a acestora, în conformitate cu toate cerințele din cadrul secțiunii **Specificatii tehnice (Caiet de sarcini)**.

Atenție:

Aceste elemente vor constitui baza pentru evaluarea ofertelor.

Propunerile Tehnice incomplete (care nu vor conține cel puțin informațiile/datele indicate în caietul de sarcini) vor fi declarate neconforme și vor atrage excluderea ofertantului din procedura.

Nerespectarea cerințelor tehnice și a modului de prezentare a propunerii tehnice, cu toate celelalte cerințe menționate anterior, ofertele tehnice incomplete, precum și completarea/modificarea ofertei prin răspunsurile la eventualele solicitări de clarificări, constituie motiv de respingere a ofertantului.

Posibilitatea retragerii sau modificării ofertei

Ofertantul are dreptul de a-și retrage oferta, prin solicitare scrisă adresată achizitorului privat până la data și ora limită pentru depunerea ofertelor.

Ofertantul poate modifica conținutul ofertei, până la data și ora stabilite pentru depunerea ofertelor, adresând pentru aceasta achizitorului privat o cerere de retragere a ofertei în vederea

Proiect cofinanțat din Programul Operational Capital Uman 2014-2020

modificării. Achizitorul privat nu este răspunzător în legătură cu posibilitatea ofertantului de a depune noua ofertă, modificată, până la data și ora limită, stabilită în documentația de atribuire. Riscurile transmiterii ofertei, inclusiv forta majoră, cad în sarcina ofertantului.

Capitol 7. Modul de prezentare a propunerii financiare

1. Propunerea financiară va fi prezentată conform **Formularului de ofertă — Formular 2**, în lei (fără TVA). Ofertele în euro sau altă valută se calculează la cursul BNR din ziua transmiterii ofertei.
2. Lipsa formularului de ofertă reprezintă lipsa ofertei, respectiv lipsa actului juridic de angajare în contract.
3. Nu se acceptă ajustarea pretului.
4. Propunerea financiară are caracter ferm și obligatoriu, din punctul de vedere al conținutului pe toată perioada de valabilitate a ofertei, respectiv **minim 90 de zile**, și pe durata de derulare a contractului.
5. Toate documentele justificative vor fi certificate de ofertant prin semnare.

Atenție:

Aceste elemente vor constitui baza pentru evaluarea ofertelor.

Nerespectarea modului de prezentare a propunerii financiare cu toate punctele menționate anterior, ofertele financiare incomplete, precum și completarea/modificarea ofertei prin răspunsurile la eventualele solicitări de clarificări, constitui motiv de respingere a ofertanței.

Capitol 8. Modalitate de evaluare

În vederea respectării principiilor așa cum sunt definite în Ordinul Ministrului Fondurilor Europene nr. 1284/2016 și pentru respectarea principiilor economicității, eficienței și eficacității, beneficiarul va alege **oferta cu cele mai multe avantaje pentru realizarea scopului proiectului**.

Pe parcursul întregului proces de achiziție prin procedura competitivă, la adoptarea oricărei decizii, se va ține cont de următoarele principii:

- a) principiul transparenței;
- b) principiul economicității;
- c) principiul eficienței;
- d) principiul eficacității.

Prin transparență se înțelege aducerea la cunoștința publicului a informațiilor referitoare la aplicarea procedurii de atribuire, astfel încât operatorii economici care operează pe piață, să poată participa la competiție, asigurându-se prin aceasta promovarea concurenței. Respectarea acestui principiu asigură premisele pentru respectarea celorlalte 3 principii.

Proiect cofinanțat din Programul Operational Capital Uman 2014-2020

Principiul economicității prevede minimizarea costului resurselor alocate pentru atingerea rezultatelor estimate ale unei activități, cu menționarea calității corespunzătoare acestor rezultate.

Principiul eficienței presupune asigurarea unui raport optim între resursele utilizate și rezultatele obținute.

Principiul eficacității vizează gradul de îndeplinire a obiectivelor specifice stabilite pentru fiecare activitate planificată, în sensul obținerii rezultatelor scontate.

1. Raspundere

Beneficiarul va evalua modul în care fiecare ofertă îndeplinește cerințele de participare la procedură, se încadrează în valoarea estimată și specificatiile tehnice prezentate din prezenta documentație.

Analizarea documentelor prezentate de ofertanți nu angajează din partea Beneficiarului nici o răspundere sau obligație față de acceptarea acestora ca autentice sau legale și nu înlătură răspunderea exclusivă a ofertanților sub acest aspect.

2. Elemente de departajare a ofertelor

Desemnarea ofertei castigatoare și atribuirea contractului de achiziție se va realiza în conformitate cu prevederile OMFE nr. 1284/2016, Secțiunea 4 - Derularea procedurii competitive, punctul 4.2. Analiza ofertelor și elaborarea notei justificative de atribuire.

Se vor compara ofertele prin raportarea lor la toate cerințele publicate și se va alege oferta care îndeplinește cerințele tehnice și prezintă avantaje față de acestea, la un raport calitate/preț competitiv.

Prin urmare se vor analiza și compara, în vederea realizării scopului proiectului, următoarele elemente:

1. Componenta financiară - prețul

Pentru dovedirea ofertei financiare, ofertantul va depune:

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

Nota: În cazul în care o ofertă prezintă un preț aparent neobisnuit de scăzut în raport cu ceea ce urmează prestat atunci când prețul oferit, fără TVA, reprezintă mai puțin de 85% din valoarea estimată publicată, beneficiarul are dreptul de a efectua verificări detaliate în sensul că va solicita ofertantului inclusiv documente, după caz, privind modul de întocmire a costului. În cazul în care ofertantul nu prezintă informațiile solicitate în termen de 3 zile sau aceste informații nu pot justifica prețul aparent neobisnuit de scăzut, oferta va fi respinsă.

2. Componenta tehnică, respectiv experiența ofertantului în livrarea de cursuri de specializare în domeniul CYBERSECURITY

Proiect cofinanțat din Programul Operational Capital Uman 2014-2020

În dovedirea experienței în furnizarea de cursuri de formare profesională ofertantul va depune:

- **Declarația privind experiența ofertantului în livrarea de cursuri — Formular nr. 3**

3. **Componenta tehnică, respectiv prezentarea de scrisori de recomandare/rapoarte de acceptanță/etc din partea clienților finali ce atestă faptul că cursurile de specializare în domeniul CYBERSECURITY au fost prestate la un standard ridicat de calitate.**

Nota: Dacă în urma aplicării avantajelor mai multe oferte se clasează pe primul loc, se va solicita o nouă ofertă financiară, urmând a fi declarată câștigătoare oferta cu prețul cel mai mic.

Nota: Beneficiarul în analiza documentelor depuse își rezervă dreptul de a solicita prin clarificări dovezi în sprijinul susținerii criteriilor de evaluare.

Capitol 9. Modul de prezentare și depunere a ofertei

Formalități ce trebuie îndeplinite în legătură cu participarea la procedură:

Adresa la care se depun ofertele: Cluj-Napoca, str. Constanta nr. 19-21 cod postal 400158, județul Cluj

Data limită de depunere a ofertelor: **06.12.2021 orele 14.00**

Modalitatea de solicitare a clarificărilor:

Clarificările pot fi trimise prin email: idea@nttdata.ro

Data limită de solicitare clarificări: **22.11.2021, ora 16.00**

Data limită de răspuns la clarificări: **24.11.2021**

Răspunsurile la clarificări vor fi postate pe pagina web www.fonduri-ue.ro, secțiunea „Achiziții private” <https://beneficiar.fonduri-ue.ro:8080/>.

Ofertanții au obligația de a verifica pe site-ul www.fonduri-ue.ro publicarea eventualelor clarificări cu referire la această procedură de achiziție.

Modul de prezentare a ofertei:

1. Oferta se prezintă într-un exemplar original, pe suport hârtie, și un exemplar în format electronic (.pdf), pe suport fizic (CD/DVD/USB), în 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 să fie marcat cu:

2.1. Adresa beneficiarului

2.2. Adresa ofertantului și datele de contact

2.3. Mențiunea "A NU SE DESCHIDE ÎNAINTE DE DATA de: 06.12.2021 orele 14.00"

Proiect cofinanțat din Programul Operational Capital Uman 2014-2020

2.4. Mențiunea "Oferta în vederea participării la PROCEDURA COMPETITIVĂ pentru atribuirea Contractului de servicii "Programe de formare" - **Lot [2] – Cursuri specializare în domeniul CYBERSECURITY** pentru dezvoltarea competențelor digitale specifice în cadrul proiectului „IDEA - Inoveaza, Descopera, Evolueaza, Aplica”.

3. Plicul va conține:

3.1. Documente de calificare, *conform Capitolului 5*.

- Formular 1 — Declarație privind neîncadrarea în situațiile prevăzute la art. 13 și 14 din Ordonanța de urgență a Guvernului nr. 66/2011.
- Certificatul constatator emis de Oficiul Registrului Comerțului sau documentul echivalent;

3.2. Propunerea tehnică, *conform Capitolului 6*.

3.3. Declarația privind experiența ofertantului în livrarea de cursuri — *Formular nr. 3*

3.4. Propunerea financiară, *conform Capitolului 7*.

4. Plicul va fi însoțit de o **Scrisoare de înaintare — Formular 4**, care se va depune în același timp cu plicul, dar separat, în afara plicului, **Imputernicire — Formular 5 (pentru situațiile în care oferta este asumată de altă persoană decât reprezentantul legal)** și **Copie după CI /BI pentru persoana imputernicită (dacă este cazul)**.

Limba de redactare a ofertei: limba română.

Documentele oficiale emise de un organism terț în altă limbă decât română vor fi însoțite de traducerea autorizată în limba română.

Documentele justificative pot fi prezentate în oricare din formele: copie legalizată, copie lizibilă cu mențiunea "conform cu originalul".

Nu se acceptă oferte alternative.

Capitol 10. Informații privind contractul de servicii

Contractul va menționa datele de identificare a celor două părți semnatare, obiectul, valoarea, modalitatea de plată, documentele contractului, durata și obligațiile contractuale. Contractul va fi semnat de ambele părți și datat.

Dacă ofertantul câștigător nu semnează contractul în termenii stabiliți, beneficiarul privat poate relua procedura de achiziție.

Operatorul economic care va semna contractul de servicii datorează Beneficiarului contravaloarea daunelor directe și indirecte referitoare la proiectul "IDEA – Innovate, Discover, Evolve, Apply /IDEA - Inoveaza, Descopera, Evolueaza, Aplica", SMIS 142366, cauzate de neîndeplinirea sau îndeplinirea necorespunzătoare a obligațiilor asumate prin oferta și prin contractul de servicii, inclusiv, dar fără a se limita la eventualele reduceri/corecții financiare sau

Proiect cofinantat din Programul Operational Capital Uman 2014-2020

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, operatorul 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 in documentele achizitiei. In analiza ofertelor nu se pot adauga alte cerinte si nu se poate renunta la specificatiile deja enuntate in anunt/specificatii/clarificari/modificari.

Daca beneficiarul privat identifica erori de fond in documentele achizitiei care nu au fost clarificate inainte de data de expirare a anuntului, procedura nu se va incheia cu atribuirea contractului. In acest caz procedura se va anula, se vor corecta erorile identificate si se va relua procedura.

Proiect cofinanțat din Programul Operational Capital Uman 2014-2020

În procesul de analiză a ofertelor, beneficiarul poate solicita clarificări cu privire la ofertele depuse prin email/fax, ofertanții fiind obligați să răspundă în termenul acordat de beneficiar. Răspunsul la clarificări poate fi transmis pe email sau poate fi trimis prin poșta/curier la adresa la care se depun ofertele.

În situația în care ofertantul nu răspunde la clarificări în termenul indicat de beneficiar sau răspunsurile nu sunt concludente, oferta este respinsă.

Nerespectarea cerințelor din prezenta documentație, neprezentarea informațiilor solicitate completate în mod corespunzător, propunerea tehnică incompletă, lipsa propunerii financiare, o propunere financiară cu un cost mai mare sau un cost nobisnuit de scăzut și/sau transmiterea documentelor într-o formă improprie care face imposibilă vizualizarea conținutului acestora sunt activități realizate pe riscul ofertantului, iar eșecul de a depune o ofertă care să nu îndeplinească cerințele minime și obligatorii de calificare, cu o propunere tehnică incompletă, necorespunzătoare, neconformă, neadecvată obiectului contractului și instrucțiunile de prezentare/completare a documentelor indicate prin prezenta documentație, precum și lipsa propunerii financiare, o propunere financiară cu un cost mai mare sau un cost nobisnuit de scăzut și/sau transmiterea documentelor într-o formă improprie care face imposibilă vizualizarea conținutului acestora poate conduce la respingerea ofertei ca fiind inacceptabilă/neconformă/neadecvată.

Ofertanții trebuie să transmită o ofertă completă conform solicitărilor din prezenta documentație.

Ofertanții poartă exclusiv răspunderea pentru examinarea cu atenție convenită a documentației de atribuire, inclusiv a oricărei clarificări aduse documentației de atribuire în timpul perioadei de pregătire a ofertei prin răspunsurile beneficiarului la solicitările de clarificări, precum și pentru obținerea tuturor informațiilor necesare cu privire la orice fel de cerințe/condiții și obligații care pot afecta în vreun fel valoarea, condițiile stabilite, natura/conținutul ofertei și/sau executia contractului. Riscurile transmiterii ofertei, conform cerințelor din prezenta documentație, inclusiv forța majoră, cad în sarcina ofertantului.

Proiect cofinanțat din Programul Operational Capital Uman 2014-2020

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 profesionala.

Nota:

Caracteristicile tehnice din prezenta documentatie reprezinta conditii minimale pe care trebuie sa le indeplineasca 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 in 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 Cloud Security (specializarea CCSP)” sesiuni de formare la care participa 1 persoana, angajata a 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 SOC (Security Operations Center), specializarea Raspuns la Incidente si Amenintari” 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 2 persoane, angajate ale solicitantului;

Proiect cofinanțat din Programul Operational Capital Uman 2014-2020

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

- Curs in domeniul Cybersecurity, pentru Cloud Security (specializarea CCSP) pentru un volum de 40h/ curs/cursant
- Curs in domeniul Cybersecurity, pentru Cloud Security (specializarea Arhitectura si Inginerie de securitate Defensiva), pentru un volum de 40h/ 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 40h/ curs/cursant
- Curs in domeniul Cybersecurity, pentru SOC (Security Operations Center), raspunsuri avansate la atacuri cibernetice, pentru un volum de 48h/ curs/cursant

Intregul 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 participantilor, 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 de minim 5 ani.

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.**

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.

Proiect cofinanțat din Programul Operational Capital Uman 2014-2020

3.2.1. Curs in domeniul Cybersecurity, pentru Cloud Security (specializarea CCSP)

Obiectivele asteptate ale cursului si certificarii

Ne dorim ca angajatii nostri sa dobandeasca urmatoarele competente ca urmare a cursului si sa parcurga subiecte care sa atinga:

- a. Descrierea componentelor fizice si virtuale si identificarea principalelor tehnologii bazate pe cloud.
- b. Definirea rolurilor si responsabilitatilor jucatorilor care folosesc mediile de cloud computing
- c. Identificarea si explicarea caracteristicilor necesare pentru a satisface definitia NIST a cloud computingului
- d. Diferentierea intre diversele modele si cadre de livrare ca servicii care sunt incorporate in arhitectura de referinta cloud computing
- e. Discutarea strategiilor pentru protejarea datelor, clasificarea datelor, asigurarea confidentialitatii, asigurarea conformitatii cu agentile de reglementare si colaborarea cu autoritatile in timpul investigatiilor legale
- f. Diferentele dintre analiza criminalistica din centrele de date traditionale si mediile de cloud computing
- g. Evaluarea si implementarea controalelor de securitate necesare pentru a asigura confidentialitatea, integritatea si disponibilitatea in cloud computing
- h. Identificarea si explicarea celor sase faze ale ciclului de viata al datelor
- i. Explicarea strategiilor pentru protejarea datelor fixe si a datelor dinamice
- j. Descrierea rolului criptarii in protejarea datelor si strategii specifice pentru managementul cheilor de encryptie
- k. Compararea strategiilor de continuitate a afacerii/recuperare in caz de dezastru bazate pe cloud si selectiunei solutii adecvate pentru cerintele specifice ale afacerii
- l. Securitatea de-a lungul ciclului de viata al dezvoltarii software (SDLC) in mediile traditionale de stocare versus cloud computing
- m. Descrierea modului in care solutiile de gestionare a identitatii si a accesului atenueaza riscurile in sistemele de cloud computing
- n. Analiza decalajelor dintre cele mai bune practici de baza si cele standard din industrie
- o. Dezvoltarea acordurilor de nivel de servicii (SLA) pentru mediile de cloud computing
- p. Efectuarea evaluarii de risc ale mediilor bazate pe cloud existente si propuse
- q. Discutarea standardelor profesionale si etice ale (ISC)² si Certified Cloud Security Professional

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

Proiect cofinatat din Programul Operational Capital Uman 2014-2020

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

- Invitatie la sesiunile de curs;
- Curs de specializare in domeniul Cybersecurity, pentru Cloud Security (specializarea CCSP) (40 de ore/ curs/cursant, 1 cursant)
- 1 Suport de curs pentru fiecare cursant, care respecta regulile de identitate vizuala, in 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 de specializare in domeniul Cybersecurity, pentru Cloud Security (specializarea CCSP);
- Accesul cursantilor la examenul de certificare
- Formularele de feedback completat de cursanti - arhivate si centralizate tabelar;

Nume	Feedback cursant	Feedback trainer	Feedback metode de livrare

- Alte documente justificative relevante conform POCU.

Orice rezultate sau drepturi legate de acestea, inclusiv drepturi de autor si/sau orice alte drepturi de proprietate intelectuala si/sau industriala, obtinute ca urmare a executarii serviciilor ce fac obiectul prezentului anunt privind procedura competitiva va fi proprietatea Beneficiarului, care o va utiliza, publica sau transfera dupa cum considera necesar.

In 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 nostri dupa participarea la training sa poata:

Proiect cofinanțat din Programul Operational Capital Uman 2014-2020

- a. Analiza o Arhitectura de Securitate, sa identifice punctele vulnerabile si sa reuseasca sa creeze o arhitectura cu calitati defensive.
- b. Implementa tehnologii pentru capabilitati de prevenire, detectare si raspuns la atacurile ciberneticesi sa le utilizeze
- c. Determine nevoile adecvate de monitorizare a securitatii pentru organizatiile de toate dimensiunile
- d. Maximizeze investitiile existente in arhitectura de securitate prin reconfigurarea infrastructurii existente
- e. Determine capabilitatile necesare pentru a sprijini monitorizarea continua a Controalelor Critice de Securitate principale.
- f. Configura inregistrarea si monitorizarea adecvate pentru a sprijini un Centru de operatiuni de securitate si un program de monitorizare continua;
- g. Sa fi aplicat practic elementele teoretice invatate in cadrul trainingului.

Continut:

Modul 1 - Arhitectura si inginerie 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 – abordari si practice (“Network closets, penetrare Dropbox-uri, Rubber Ducky)
5. Layer 2 - abordari si practice (VLAN-uri, private LANs, atacuri si solutii pentru acestea)
6. NetFlow (NetFlow, Sflow, Jflow, VPC Flow, Suricata si Endpoint Flow)

Modul 2 - Arhitectura si inginerie de securitate a retelei

1. Layer 3
 - a. Routere – abordari si practici
 - b. Atacuri si modalitati de mitigare (rutare sursa IP, ICMP, actualizare neautorizate, atacuri de tip wormhole, securizare protocoale)
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: Blackwholes, Bogon, Darknet
6. Despre IPv6 si securizarea IPv6
7. VPN
8. Layer 3 si 4 - Firewall-uri
9. Proxy (WEB & SMTP)

Proiect cofinanțat din Programul Operational Capital Uman 2014-2020

Modul 3 - Securitate centrata pe retea

1. NGFW
2. NIDS/NIPS (cum sa scrii regulile)
3. Monitorizarea securitatii retelei
4. Sandboxing
5. Criptare – principii, SSL/ TLS, SSL/SSH
6. Acces securizat Remote
7. Distributia Denial-of-Service (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 pierderii datelor (DLP)
7. Ownership datelor
8. Managementul dispozitivelor mobile (MDM) si Managementul aplicatiilor mobile (MAM)
9. Private Cloud Security
10. Public Cloud Security
11. Container Security

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 End Points ca senzori de securitate consolidati
8. Scalarea grupului de Endpoint Logs /Stocare/Analiza

Modul 6: Aplicatii practice pentru Modulele 1-5

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

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

- Invitatie la sesiunile de curs;

Proiect cofințat din Programul Operational Capital Uman 2014-2020

- 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, in 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.

Orice rezultate sau drepturi legate de acestea, inclusiv drepturi de autor si/sau orice alte drepturi de proprietate intelectuala si/sau industrială, obtinute ca urmare a executării serviciilor ce fac obiectul prezentului anunt privind procedura competitiva va fi proprietatea Beneficiarului, care o va utiliza, publica sau transfera dupa cum considera necesar.

In vederea pastrării confidentialității, 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 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 si afectate

Proiect cofinanțat din Programul Operational Capital Uman 2014-2020

- d. Evaluarea daunelor si 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

- 1. Tactici reale de raspuns la incidente (Pregatire, identificare/scoping/dezvoltarea informatiilor, eradicare/remediere, recuperare, evitarea raspunsului la incident „Whack-A-Mole”
- 2. Proactivitatea in tratarea amenintarilor – threat hunting versus react
- 3. Threat Hunting la nivel de organizatii
- 4. Raspunsuri la Incidente si actiunea de “Hunting” la nivelul EndPoint-urilor
- 5. Identificarea, evitarea si prevenirea Malware-urilor
- 6. Identificarea persistentei unui Malware
- 7. Prevenirea, detectarea si minimizarea riscurilor ce privesc furtul de credentiale.

Modul 2 – Analiza elementelor de intruziune

- 1. Furtul si utilizarea credentialelor legitime (Pass The hash, SSO, cache, LSA, atacuri Kerberos, NTDS.DIT)
- 2. Dovezi avansate de detectare a atacului (TTP, „Prefetch analysis”, ShimCache, registru Amcache, scalare SlimCache)
- 3. TTP - Tactici, Tehnici si Proceduri (ale adversarilor)
- 4. Analiza log-urilor pentru respondentii la incidente si hunting
- 5. Investigarea atacurilor bazate pe WMI si PowerShell

Modul 3- Memory Forensics in raspunsul la incidente si in actiunea de Threat Hunting

- 1. Analiza memoriei din sistemele infectate (Stuxnet, TDL3/ TDSS, CozyDuke APT29 RAT, Rundll32 and Living Off the Land Executions, Zeus/Zbot, Storm Worm Rootkit, Black Energy Rootkit, WMI and PowerShell, Cobalt Strike Beacons and Powerpick, Cobalt Strike Sacrificial Processes, Metasploit, Custom APT command and control malware)
- 2. Interventie la incidente la distanta in organizatii - Velociraptor, F-Response, and KAPE
- 3. Triajul prin intermediul sistemelor de detectie si interventie la nivel de endpoint
- 4. Achizitie de memorie
- 5. Procesul de analiza criminalistica a memoriei pentru actiune de Raspuns si Threat Hunting
- 6. Examinarea memoriei dpv al criminalitatii digitale
- 7. Instrumente folosite in examinarea memoriei – Volatility, F-Response, Velociraptor

Proiect cofinanțat din Programul Operational Capital Uman 2014-2020

Modulul 4 – Analiza cronologiei

1. Detectarea si eradicarea Malware-urilor
2. Procesul general de analiza a Timeline-ului
3. Creare si analiza de Filesystem Timeline
4. Creare si analiza de „Super Timeline-uri”

Modul 5 - Raspuns la incidente si actiunea de Hunting in organizatie | Detectare avansata a „inamicului” si anti- criminalistica digitala

Aplicatii practice ce cuprind:

- Analiza de „Volume shadow snapshot”
- Timeline care incorporeaza date de tip volume shadow snapshot
- Analiza anticriminatiate digitala folosind componente ale sistemului de documente NTFS
- Identificare Timestomp si detectari de fisiere suspecte
- Recuperare avansata a datelor – configuratii NTFS, string searching, procese de tip File carving, Volume Shadow Carving etc.

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

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

- Invitatie la sesiunile de curs;
- Curs in domeniul Cybersecurity, pentru SOC (Security Operations Center), specializarea Raspuns la Incidente si Amenintari (48 de ore/ curs/cursant, 1 cursant)
- 1 Suport de curs pentru fiecare cursant, care respecta regulile de identitate vizuala, in 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 in domeniul Cybersecurity, pentru SOC (Security Operations Center), specializarea Raspuns la Incidente si Amenintari ;
- Accesul cursantilor la examenul de certificareFormularele de feedback completat de cursanti - arhivate si centralizate tabelar;

Proiect cofinantat din Programul Operational Capital Uman 2014-2020

Nume	Feedback curs	Feedback continut	Feedback trainer	Feedback metode de livrare

- Alte documente justificative relevante conform POCU.

Orice rezultate sau drepturi legate de acestea, inclusiv drepturi de autor si/sau orice alte drepturi de proprietate intelectuala si/sau industriala, obtinute ca urmare a executarii serviciilor ce fac obiectul prezentului anunt privind procedura competitiva va fi proprietatea Beneficiarului, care o va utiliza, publica sau transfera dupa cum considera necesar.

In 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 Informatii (secrete) la Amenintari din domeniul Virtual

Obiectivele asteptate ale cursului sunt:

- Training practic cu exercitii din viata reala care sa cuprinda subiecte precum:
 - Credentialele VM
 - Feature-uri avansate IAM
 - Intarirea politicilor AWS IAM
 - Intarirea politicilor Azure and GCP Policies
 - Provocari DevOps - Public Cloud Security – CloudWars
 - Blocarea retelei
 - Analiza traficului de retea
 - Private Endpoint Security
 - Cloud VPN si gestionarea SSH
 - Auditarea evenimentelor de decriptare
 - Blocarea serviciului de stocare
 - Partajare neautorizata de fisiere
 - Serverless Prey si consolidarea functiilor serverless
 - Application Service Security
 - Broken Firebase DB Access Control
 - Integrare multicloud
 - Conectarea cu Azure AD
 - Benchmarking automatizat
 - CloudWars
 - Lab Tear Down

Proiect cofinanțat din Programul Operational Capital Uman 2014-2020

Furnizorul va pune la dispoziție următoarele instrumente de lucru:

- Support de curs
- Masina virtuala de curs (VM) cu toate exercitiile de laborator care pot fi refacute in afara sesiunilor de curs
- 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 incat vor fi selectate in programul ce va fi livrat de prestator cele mai potrivite teme pentru domeniul „IT” in care activeaza beneficiarului.

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

- Invitatie la sesiunile de curs;
- Curs in domeniul Cybersecurity, pentru Informatii (secrete) la Amenintari din domeniul Virtual (40 de ore/ curs/cursant, 1 cursant)
- 1 Support de curs pentru fiecare cursant, care respecta regulile de identitate vizuala, in 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 cursant	Feedback trainer	Feedback metode de livrare

- Alte documente justificative relevante conform POCU.

Orice rezultate sau drepturi legate de acestea, inclusiv drepturi de autor si/sau orice alte drepturi de proprietate intelectuala si/sau industriala, obtinute ca urmare a executarii serviciilor ce fac obiectul prezentului anunt privind procedura competitiva va fi proprietatea Beneficiarului, care o va utiliza, publica sau transfera dupa cum considera necesar.

Proiect cofinanțat din Programul Operational Capital Uman 2014-2020

În vederea păstrării confidențialității, beneficiarul va semna cu operatorul economic declarat castigator o Declarație de confidențialitate care va deveni parte integrantă a contractului de prestări servicii.

3.2.5. Curs în domeniul Cybersecurity, pentru SOC (Security Operations Center), răspunsuri avansate la atacuri cibernetice

Obiectivele așteptate ale cursului sunt:

- a. Învățarea componentelor de bază ale construirii unei infrastructuri de rețea protejate și modalități de securizare corectă a routerelor, switch-urilor și a altor infrastructuri de rețea
- b. Asimilarea metodelor formale necesare efectuării evaluării vulnerabilităților și testarea penetrării pentru a găsi punctele slabe în rețeaua companiei
- c. Învățarea metodelor de detectare a atacurilor avansate împotriva rețelei unei organizații și indicatorii de compromis asupra sistemelor implementate, inclusiv colecția de artefacte din punct de vedere criminalistic și ceea ce se poate învăța din acestea
- d. Cum să răspundă la un incident utilizând procesul în șase pași de răspuns la incident: pregătire, identificare, izolare, eradicare, recuperare și "lessons learned".
- e. Discutarea abordărilor ale analizei programelor malware, variind de la tehnici complet automatizate la analiza manuală a proprietăților statice, comportamentul interactiv și inversarea codului

Conținut, competențe și abilități dobândite ca urmare a acestui curs practic:

- Identificarea amenințărilor de securitate de vizează infrastructura și modalități de construireți a rețelelor defensibile care să minimizeze impactul atacurilor
- Utilizarea instrumentelor pentru analiza rețelei cu scopul de a preveni atacurile și a detecta potențialele atacuri.
- Decodificarea și analiza pachetelor folosind diverse instrumente pentru a identifica anomaliile și pentru a îmbunătăți apărarea rețelei
- Înțelegerea cum adversarul compromite sistemele și cum să se răspundă atacurilor folosind procesul de tratare a incidentelor
- Efectuarea testelor de penetrare împotriva unei organizații pentru a determina vulnerabilitățile și punctele de compromis
- Utilizarea diverselor instrumente pentru a identifica și remedia programele malware în întreaga companie

Proiect cofinanțat din Programul Operational Capital Uman 2014-2020

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

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

- Invitatie la sesiunile de curs;
- Curs in domeniul Cybersecurity, pentru SOC (Security Operations Center), raspunsuri avansate la atacuri cibernetice (48 de ore/ curs/cursant, 2 cursanti)
- 1 Suport de curs pentru fiecare cursant, care respecta regulile de identitate vizuala, in 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 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 curs	continut	Feedback trainer	Feedback metode de livrare

- Alte documente justificative relevante conform POCU.

Orice rezultate sau drepturi legate de acestea, inclusiv drepturi de autor si/sau orice alte drepturi de proprietate intelectuala si/sau industriala, obtinute ca urmare a executarii serviciilor ce fac obiectul prezentului anunt privind procedura competitiva va fi proprietatea Beneficiarului, care o va utiliza, publica sau transfera dupa cum considera necesar.

In 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.).

Proiect cofinanțat din Programul Operational Capital Uman 2014-2020

- 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 in 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 in sistem online, vor fi asigurate de prestator.
- In 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 in comunicare.

3.4. Durata cursului

Durata cursurilor de specializare in domeniul CYBERSECURITY este urmatoarea:

- Curs in domeniul Cybersecurity, pentru Cloud Security (specializarea CCSP) pentru un volum de 40h/ curs/cursant
- Curs in domeniul Cybersecurity, pentru Cloud Security (specializarea Arhitectura si Inginerie de securitate Defensiva), pentru un volum de 40h/ 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 40h/ 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.

Proiect cofinanțat din Programul Operational Capital Uman 2014-2020

Zilele și orele de curs vor fi organizate în funcție de programul de lucru și disponibilitatea de a participa la formare.

O planificare mai temeinică va fi propusă de Beneficiar și negociată cu prestatorul în vederea asigurării resurselor necesare pentru desfășurarea în condiții optime a cursurilor, ulterior încheierii contractului de servicii. Distribuția angajaților poate varia în funcție de disponibilitatea angajaților, nivelul de încărcare cu sarcini curente precum și în urma graficului de formare realizat împreună cu prestatorul, pentru a grupa acei angajați cu profile similare și obiective aliniate.

4.2 Materiale necesare

Ofertantul va pune la dispoziția grupului țintă materialele didactice necesare desfășurării cursului în condiții optime.

Ofertantul va pune la dispoziția cursanților suportul de curs. Suportul de curs trebuie să respecte regulile de identitate vizuală, în conformitate cu Manualul de Identitate Vizuală POCU 2014-2020, pus la dispoziție de către beneficiar.

Pe lângă programa și suportul de curs, ofertanții vor trebui să definească și să pună la dispoziția cursanților fișele de lucru și orice alte documente suport pentru desfășurarea în condiții optime a cursurilor.

4.3 Durata

După organizarea grupelor, stabilirea conținutului de curs, a instrumentelor optime care vor fi utilizate în procesul de predare, pregătirea aplicației online, va începe livrarea propriu-zisă a cursurilor, pe o durată estimativă de maxim 11 luni, nu mai târziu de data de 21.11.2022.

În cazul prelungirii duratei proiectului prestatorul va fi notificat și se va prelungi și durata prestării cursurilor, dacă va fi cazul.

Graficul de desfășurare a tuturor sesiunilor de curs (ex. numărul de ore/zi, numărul de zile pe săptămână etc.) va fi propusă de beneficiar și agreată cu ofertantul, ofertantul asigurându-se că va acoperi însă cel puțin durata programului de formare, numărul de zile pentru livrarea online putând să varieze în funcție de această planificare.

4.4 Locația

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 verificării competențelor dobândite și certificării cursanților care au finalizat programul nu mai târziu de data de 22.11.2022.

Proiect cofinanțat din Programul Operational Capital Uman 2014-2020

Accesul la serviciile de certificare este o cerință obligatorie a Beneficiarului în cadrul programului de formare și specializare.

4.6 Mențiuni referitoare la plată

Pretul serviciilor de formare se va achita în termen de maxim 45 zile calendaristice de la semnarea proceselor verbale de recepție (intermediare sau finale) și primirii facturii/ facturilor de la prestator. În vederea semnării procesului verbal de recepție, ofertantul declarat câștigător va trebui să prezinte următoarele documente justificative:

- lista de prezență pentru toate zilele de desfășurare a sesiunilor de instruire (teorie și practică, după caz);
- fotografii/print-screen-uri relevante din timpul cursului;
- dovada accesului la serviciul de certificare pentru cursanți;
- suportul de curs și orice alte fișe/instrumente utilizate în procesul de formare;
- documentarea sesiunilor de formare în sistem online, conform reglementărilor în vigoare.

Toate documentele justificative menționate vor fi folosite de beneficiar în vederea solicitării sumelor avansate pentru plata cursurilor de formare, în cadrul cererilor de rambursare.

Prestatorul va emite factura fiscală, numai după semnarea de către beneficiar a procesului verbal de recepție 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 condițiile recepționării pe baza de proces verbal de recepție.

Nu se fac plăți în avans.

4.7 Clauze contractuale

Contractul se va încheia doar cu operatorul economic desemnat prin Nota justificativă de atribuire.