Program kurzov CCD CoE na rok 2016

Seminár „Spolupráca s CCD COE“

8. marca 2016

kpt. Ing. Michal PETRÁŠ

PREZENTÁCIA JE NEUTAJOVANÁ

Obsah

- Cieľ
- Kurzy poskytované v CCD CoE
- Mobilné kurzy
- On-line kurzy
- Administratívne pokyny
- Záver

Cieľ

Cieľom mojej prezentácie je Vás informovať o možnosti zapojenia sa do tréningového plánu Centra výnimočnosti pre kybernetickú obranu v Estónskom Talline.

Dozviete sa aké kurzy centrum poskytuje, pre koho sú určené, ako sa na dané kurzy prihlásiť a v neposlednom rade aj administratívne pokyny k daným kurzom.

Kurzy poskytované v CCD CoE

Kurzy poskytované v Talline (In – House):

- Cyber Defence Monitoring Course Suite Module 1
- Cyber Defence Monitoring Course Suite Module 2
- Botnet Mitigation Course
- Malware and Exploits Essentials
- Cyber Defence Monitoring Course Suite Module 3
- Introductory Digital Forensics
- IT Systems Attacks and Defence
- International Law of Cyber Operations

Kurzy poskytované v CCD CoE

CD Monitoring Course Suite Module 1 - Rule-based Threat Detection Course

JAN | FEB | MAR | APR | MAJ | JUN | JUL | AUG | SEP | OKT | NOV | DEC

18.1. **29.2.-4.3.**

Obsah:

- Praktický kurz zameraný iba na jednu z mnohých monitorovacích techník detekcie hrozieb a to rule-based, tiež známu ako Intrusion Detection – detekcia prienikov,
- bude sa využívať open-source program Suricata,
- Kurz ukazuje, ako sa Suricata hodí na monitorovanie zabezpečenia siete. Účastníci získajú praktické skúsenosti o tom, ako vybudovať škálovateľný systém a aký náročný proces je bezpečnostné inžinierstvo. Pri praktických cvičeniach sa začína inštaláciou základnej inštancie až po vybudovanie distribuovaného systému s centralizovaným riadením, analýzami a vizualizačnými riešeniami.

Kurzy poskytované v CCD CoE

CD Monitoring Course Suite Module 1 - Rule-based Threat Detection Course

JAN | FEB | MAR | APR | MAJ | JUN | JUL | AUG | SEP | OKT | NOV | DEC

18.1. 29.2.-4.3.

Predpoklady:

- Dobrá znalosť TCP IP sietí a správa siete / systému /,
- každodenná správa siete/systému, prax aspoň 2 roky v prostredí UNIX,
- podrobné vedomosti o týchto témach:
  - pracovné princípy operačných systémov UNIX a súborového systému UNIX,
  - UNIX Shell (napr. sh, bash),
  - bežné používateľské nástroje UNIX (napr. ls, ps, kill),
  - Bežné administračné nástroje UNIX.
- predchádzajúce skúsenosti s programovaním nie je nutné, ale je užitočné,
- znalosť anglického jazyka porovnateľná so STANAG 6001, 3,2,3,2.

Kurzy poskytované v CCD CoE

CD Monitoring Course Suite Module 2 - Semantic Network Security Monitoring Course

JAN | FEB | MAR | APR | MAJ | JUN | JUL | AUG | SEP | OKT | NOV | DEC

1.2. **14.3.-18.3.**

Obsah:

- Praktický kurz zameraný iba na jednu z mnohých monitorovacích techník detekcie hrozieb, a to semantic security monitoring – sémantické monitorovanie bezpečnosti,
- prirovnáva sa ku klasickému Intrusion Detection, ale má úplne iný prístup – poskytuje flexibilný Framework, ktorý sa ľahko personalizuje, a hĺbková kontrola ďaleko presahuje možnosti klasických systémov,
- bude sa využívať open-source program Bro,
- Ako pri predošlom module, na kurze sa bude ukazovať, ako využívať program Bro a čo všetko je s ním možné zabezpečiť.

Kurzy poskytované v CCD CoE

CD Monitoring Course Suite Module 2 - Semantic Network Security Monitoring Course

JAN	FEB	MAR	APR	MAJ	JUN	JUL	AUG	SEP	OKT	NOV	DEC
	1.2.	14.3.-18.3.									

Predpoklady:

- Dobrá znalosť TCP IP sietí a správa siete / systému /,
- každodenná správa siete/systému, prax aspoň 2 roky v prostredí UNIX,
- podrobné vedomosti o týchto témach:
  - pracovné princípy operačných systémov UNIX a súborového systému UNIX,
  - UNIX Shell (napr. sh, bash),
  - bežné používateľské nástroje UNIX (napr. ls, ps, kill),
  - Bežné administračné utility UNIX.
- Je nutná skúsenosť so skriptovaním,
- predchádzajúce skúsenosti s programovaním nie je nutné, ale je užitočné,
- znalosť anglického jazyka porovnateľná so STANAG 6001, 3,2,3,2.

Kurzy poskytované v CCD CoE

Botnet Mitigation Course

JAN | FEB | MAR | APR | MAJ | JUN | JUL | AUG | SEP | OKT | NOV | DEC

8.2. 4.4.-8.4.

Obsah:

- Tento kurz je zameraný na reverzné inžinierstvo malvéru a na iné metódy aplikovateľné na botnet infiltrácie.
- Praktický kurz pre mierne pokročilých, ktorý Vás uvedie do problematiky „state-of-the-art“ konceptu botnetov a naučí Vás ako sa brániť hrozbe botnetu.
- Väčšina botnetov navrhnutá ako spyware, kurz sa hlavne zameria na detekciu dátových priesakov (data-exfiltration) a na moderné techniky únikov IDS

Kurzy poskytované v CCD CoE

Botnet Mitigation Course

JAN | FEB | MAR | APR | MAJ | JUN | JUL | AUG | SEP | OKT | NOV | DEC

8.2. **4.4.-8.4.**

Obsah:

- Úvodné predstavenie histórie botnet
- Jednoduché botnety demonštrované v praxi
- Ukážka moderných malvérov ktoré využívajú na skrývanie svojej prevádzky techniky typu „blending and encryption“
- Predstavenie konceptov „crypto breaking and polymorphic blending“ – ukážka na nedávno odhalených botnetoch ako sú Operation Red October, Zeus and Zero Access Botnet

Kurzy poskytované v CCD CoE

Botnet Mitigation Course

JAN | FEB | MAR | APR | MAJ | JUN | JUL | AUG | SEP | OKT | NOV | DEC

8.2. 4.4.-8.4.

Predpoklady:

- Dobrá znalosť Linux a Windows
- Základná znalosť malware a sieťovej prevádzky
- Schopnosť používať virtualizačné nástroje ako je napr. VirtualBox
- Skúsenosti s firewallmi a analýzou sieťovej prevádzky (nástroj Wireshark)
- Základná znalosť assembléra a vyšších programovacích jazykov
- Skúsenosti s programovaním v assembléri, C (++) alebo Python
- znalosť anglického jazyka porovnateľná so STANAG 6001, 2,2,2,2.

Kurzy poskytované v CCD CoE

Malware and Exploits Essentials

JAN | FEB | MAR | APR | MAJ | JUN | JUL | AUG | SEP | OKT | NOV | DEC

7.3. 2.5 - 6.5.

Obsah :

- Kurz poskytuje hlboké technické náhľady do techník použitia moderných malvérov na zneužitie zraniteľností a na vniknutie do systémov,
- budú prednesené a vyskúšané najmodernejšie detekcie zraniteľnosti ako „fuzzing and code coverage“,
- po nájdení chýb zabezpečenia, existujú rôzne postupy ako ich využiť pre zneužitie systému. Kurz začne predstavením základných metód zneužitia ako „buffer and heap overflow techniques“, ale aj pokročilejšie techniky pre oba systémy Windows a Linux (ASLR, SEH/SEHOP, ROP, DEP atď.)

Kurzy poskytované v CCD CoE

Malware and Exploits Essentials

JAN | FEB | MAR | APR | MAJ | JUN | JUL | AUG | SEP | OKT | NOV | DEC

7.3. 2.5 - 6.5.

Obsah :

- Odkedy je zabezpečenie systémov založené hlavne na šifrovacích technológiách, budú vysvetlené aj moderné šifrovacie systémy – nevynechá sa ani aspekt kryptografického zabezpečenia a ako sa ho votrelci snažia prelomiť.
- Ďalšou dôležitou témou je softvérová odolnosť: vykonanie malvéru je vždy založené na presmerovaní toku nechceného programu.
- Bude tiež ukázané ako možno chrániť kód jeho zmenou, technikami ako „code morphing and obfuscation“.

Kurzy poskytované v CCD CoE

Malware and Exploits Essentials

JAN | FEB | MAR | APR | MAJ | JUN | JUL | AUG | SEP | OKT | NOV | DEC

7.3. 2.5 - 6.5.

Predpoklady :

- Jedná sa o silne technicky zameraný kurz. Je nutná vynikajúca úroveň znalostí programovania, rovnako ako podrobné znalosti operačných systémov (Windows / Linux) na úrovni procesov / knižníc.
- Cieľová skupina je výhradne technický personál CSIRT / CERT alebo iných vládnych / vojenských subjektov, ktoré sú na technickej úrovni zapojené do IT bezpečnosti alebo do kybernetickej obrany.
- znalosť anglického jazyka porovnateľná so STANAG 6001, 2,2,2,2

Kurzy poskytované v CCD CoE

CD Monitoring Course Suite Module 3 - Large-Scale Packet Capture Analysis Course

JAN | FEB | MAR | APR | MAJ | JUN | JUL | AUG | SEP | OKT | NOV | DEC

14.3. 9.5.-13.5.

Obsah:

- V tomto kurze sa budú využívať najnovšie poznatky zachytené v sieťovej prevádzke počas posledného cvičenia Locked Shields
- Praktický kurz zameraný iba na jednu z mnohých monitorovacích techník detekcie hrozieb a to zachytávanie a analýzu paketov,
- Neznamená to nahradiť IDS systémy, ale spolupracovať s nimi pre ukladanie a indexáciu celej prevádzky v sieti a pre poskytnutie rýchleho prístupu k zozbieraným dátam.
- bude sa využívať open-source program Moloch na vybudovanie monitorovania bezpečnosti siete rôznych veľkostí – od SOHO/SME až po enterprise úroveň.

-

Kurzy poskytované v CCD CoE

CD Monitoring Course Suite Module 3 - Large-Scale Packet Capture Analysis Course

JAN | FEB | MAR | APR | MAJ | JUN | JUL | AUG | SEP | OKT | NOV | DEC

14.3. 9.5.-13.5.

Predpoklady:

- Členovia modrých tímov Locked Shields alebo národní zástupcovia
- Dobrá znalosť TCP IP sieti a správa siete
- každodenná správa siete/systému, prax aspoň 2 roky v prostredí UNIX,
- podrobné vedomosti o týchto témach:
  - pracovné princípy operačných systémov UNIX a súborového systému UNIX,
  - UNIX Shell (napr. sh, bash),
  - bežné používateľské nástroje UNIX (napr. ls, ps, kill),
  - Bežné administračné nástroje UNIX.
- Je nutná skúsenosť so skriptovaním,
- predchádzajúce skúsenosti s programovaním nie je nutné, ale je užitočné,
- znalosť anglického jazyka porovnateľná so STANAG 6001, 3,2,3,2.

Kurzy poskytované v CCD CoE

Introductory Digital Forensics

JAN | FEB | MAR | APR | MAJ | JUN | JUL | AUG | SEP | OKT | NOV | DEC

11.4. 6.6.-10.6.

Obsah:

- Tento kurz poskytuje úvod do digitálnej forenzie, vrátane metodológie, hlásení a právnych úvah. Podstatná časť kurzu je vyšetrovanie počítačov so systémom Windows pomocou bezplatných open source nástrojov.
- Kurz je zameraný na IT zamestnancov, ktorí sú zvyknutí pracovať s informačnými technológiami v roliach ako správca, auditor, manažér a pod., a ktorých bežné úlohy nezahŕňajú forenznú analýzu. Skúsený personál, ktorý robí pravidelne forenznú analýzu nie je cieľovou skupinou.

Kurzy poskytované v CCD CoE

Introductory Digital Forensics

JAN FEB MAR APR MAJ JUN JUL AUG SEP OKT NOV DEC

11.4. 6.6.-10.6.

Predpoklady:

- Základná znalosť práce na počítači
- Dobré skúsenosti s prácou a administráciou v prostredí Linux a Windows, najmä príkazový riadok
- Používanie virtuálnych strojov ako VirtualBox
- znalosť anglického jazyka porovnateľná so STANAG 6001, 3,2,3,2.

Kurzy poskytované v CCD CoE

IT Systems Attacks and Defence

JAN | FEB | MAR | APR | MAJ | JUN | JUL | AUG | SEP | OKT | NOV | DEC

18.7. 12.9.-16.9.

Obsah:

- Praktický kurz zameraný na metódy a nástroje používané útočníkmi na získanie prístupu do IT systémov a na možné protiopatrenia k týmto útokom,
- kurz je postavený na praktických cvičeniach, ktoré sú zamerané viac na stranu útočníka,
- možnosť vyskúšania niekoľko najbežnejších typov útokov (v laboratóriu),
- počas praktických testov môžu účastníci súťažiť metódou Capture the flag – víťaz je ten, kto prvý zachytí špecifický token zo zraniteľného systému,
- Väčšina nástrojov sú open-source alebo aspoň nekomerčné,
- Zraniteľné webové aplikácie sú väčšinou postavené na PHP a MySQL

Kurzy poskytované v CCD CoE

IT Systems Attacks and Defence

JAN | FEB | MAR | APR | MAJ | JUN | JUL | AUG | SEP | OKT | NOV | DEC

18.7. 12.9.-16.9.

Obsah - teória:

- Úvod do prostredia laboratória, základy Kali Linux a Metasploit,
- zdroje a nástroje na zhromažďovanie informácií o cieľových sieťach,
- Sieťové skenovanie: TCP and UDP port scanning, operating system detection, vulnerability scanning, scanning in IPv6 networks, honeypots and tarpits
- Password attacks: password guessing and cracking, how passwords are stored in Linux and Windows, hashing functions and identified vulnerabilities in them, Rainbow Tables, Pass-the Hash.
- Network infrastructure attacks and defence: MAC flooding, ARP spoofing, ICMP redirection, IP spoofing and fragmentation, VLAN hopping, leaking data over CDP, BGP hijacking;

Kurzy poskytované v CCD CoE

IT Systems Attacks and Defence

JAN | FEB | MAR | APR | MAJ | JUN | JUL | AUG | SEP | OKT | NOV | DEC

18.7. 12.9.-16.9.

Obsah - prax:

- Použitie inžinierskych nástrojov, ako je The Harvester or Maltego pre zhromažďovanie informácií,
- skenovanie malých sieti s cieľom nájsť zariadenie s konkrétnymi zraniteľnosťami,
- použitie DNS záznamov s cieľom nájsť zaujímavého hostiteľa využívajúceho nechránenú službu SNMP,
- Guessing and cracking passwords.
- Kradnutie prihlasovacích údajov zo systémov Windows a použiť ich na vykonanie útokov Pass-the-Hash.
- Použitie Metasploit Framework a existujúci kód exploit proti rôznym cieľom. Toto zahŕňa útoky na strane klienta .

Kurzy poskytované v CCD CoE

IT Systems Attacks and Defence

JAN | FEB | MAR | APR | MAJ | JUN | JUL | AUG | SEP | OKT | NOV | DEC

18.7. 12.9.-16.9.

Predpoklady:

- Administrácia systémov založených na Windows a Linux,
- porozumenie sieťových protokolov (napr. ARP, IP, ICMP, TCP, UDP, DNS, HTTP, SNMP, SMTP),
- skúsenosti s webovými technológiami (ako je HTML, PHP, JavaScript),
- pracovné stanice budú Kali Linux – základné znalosti s prácou s týmto systémom,
- znalosť anglického jazyka porovnateľná so STANAG 6001, 2,2,2,2.

Kurzy poskytované v CCD CoE

International Law of Cyber Operations

JAN	FEB	MAR	APR	MAJ	JUN	JUL	AUG	SEP	OKT	NOV	DEC
		28.3.		23.5.-27.5.					3.10.	28.11.-2.12.	

Obsah:

- 5 dňový kurz začína voliteľným dňom (tech-day), v ktorom budú predstavené technológie zahrnuté v kybernetických operáciách, vrátane štruktúry internetu, obranných a útočných nástrojov a techník. Navyše, úvodná fáza skúma miesto kybernetických operácií v súčasnom geopolitickom prostredí,
- hlavné 4 dni sú rozdelené do dvoch blokov štúdie:
  - Medzinárodné právo upravujúce kybernetické operácie v čase mieru
  - Medzinárodné humanitárne právo, ktoré sa použije počas ozbrojeného konfliktu zahrňujúceho kybernetické operácie
- každý blok (1,5 dňa), končí komplexným cvičením, ktoré účastníkom umožní aplikovať právo, ktoré bolo preberané počas prednášok a diskusií,

Kurzy poskytované v CCD CoE

International Law of Cyber Operations

JAN	FEB	MAR	APR	MAJ	JUN	JUL	AUG	SEP	OKT	NOV	DEC
		28.3.		23.5.-27.5.					3.10.	28.11.-2.12.	

Obsah:

- Blok 1 sa zoberá otázkami ako suverenita, jurisdikcia, náležitá starostlivosť, právnymi predpismi daného štátu, zákaz intervencie, a nakoniec sebaobrana v kontexte kybernetických operácií,
- budú zodpovedné otázky ako napr. ktoré kybernetické operácie okrem ozbrojeného konfliktu porušujú medzinárodné právo, kedy štáty môžu vykonať protiútok (hack back), a v prípade ak došlo ku ozbrojenému kybernetický útoku, kedy sa môžu štáty zapojiť do sebaobrany
- Blok 2 pokrýva témy tradičného medzinárodného humanitárneho práva, ako je napr. klasifikácia kybernetického konfliktu, princíp rozlišovania počas kybernetických operácií, a zacielenie a ochrana osôb a objektov v kontexte „cyber“.
- Tento blok sa vyučuje z operačného hľadiska právneho poradcu, skúmajúc všetky potrebné kroky zacielené na „cyber“ právnu analýzu.

Kurzy poskytované v CCD CoE

International Law of Cyber Operations

JAN	FEB	MAR	APR	MAJ	JUN	JUL	AUG	SEP	OKT	NOV	DEC
		28.3.		23.5.-27.5.					3.10.	28.11.-2.12.	

Obsah:

- Prednášky budú vedené významnými učencami a praktikantmi podieľajúcimi sa „Tallinn Manual and Tallinn 2.0 projects“, vrátane riaditeľa oboch projektov, profesora Michaela Schmitta (United States Naval War College and University of Exeter). Účastníci majú jedinečnú príležitosť diskutovať o „cyber“ právnych záležitostiach s niektorými z najznámejších vedcov v oblasti. Účastníci dostanú aj bezplatnú kópiu manuálu „Tallinn Manual on the International Law Applicable to Cyber Warfare“.

Mobilné kurzy

V priebehu roka 2016 poskytne centrum svojich lektorov aj zariadenia do priestorov členov Centra pre poskytnutie týchto 4 kurzov:

- IT Systems Attacks and Defence Course.
- Malware and Exploits Essentials Course.
- Smartphone Security and Forensics Course.
- Introductory Digital Forensics Course.

- Témy, cieľové publikum, obsah kurzov a predpoklady, sú rovnaké ako tie, ktoré ponúkajú in-house kurzy uvedené v predchádzajúcej kapitole,
- sponzorské krajiny, prispievajúci účastníci a orgány NATO si môžu vyžiadať vykonať mobilné kurzy v ich priestoroch.
- výberové konanie bude vykonané v súlade s kritériami stanovenými riadiacim výborom NATO CCD COE
- Registrácia účastníkov bude riadená hostiteľskou krajinou, ktorá môže zdieľať voľné miesta s inými sponzorskými krajinami.

On-line kurzy

Cyber Defence Awareness e-Course:

- Cieľové publikum: kurz si kladie za cieľ zvýšiť všeobecné povedomie užívateľov o kybernetických bezpečnostných rizikách a opatreniach na zmiernenie týchto rizík. Kurz zahŕňa všetkých užívateľov siete NATO,
- Učebné ciele: Tento kurz poskytuje úvod do všeobecnej kybernetickej bezpečnosti, aby sa účastníci zoznámili s útokmi, terminológiou a obrannými technikami.
- Registrácia: Kurz je prístupný prostredníctvom portálu NATO eLearning Joint Advanced Distributed Learning Portal (https://jadl.act.nato.int/), a je prístupný pre všetkých užívateľov portálu. Po registrácii majú užívatelia prístup ku kurzu cez menu ‘NATO Courses’ -> ‘Centres of Excellence’ -> ‘COE Cyber Defence’ -> ‘Cyber Defence Awareness’ course listing.

Administratívne pokyny

Administrative pokyny pre in-house kurzy:

1. Registrácia:
   - Registrácia do kurzu prebieha prostredníctvom PoC pre SR za oblasť CD kurzov,
   - pred registráciou je potrebné si overiť informácie o kurze na stránke CCD CoE,
   - po zaslaní požiadavky o zaradenie do kurzu budete informovaní PoC o ďalšom postupe až po samotné zaradenie / nezaradenie do kurzu,
   - Kontaktné informácie na PoC SR
     - kpt. Ing. Michal Petráš
     - michal.petras @ mil.sk
     - 0960 311 443
     - 0903 824 977
2. Ako sa dostať z letiska na hotel:
   - Lennart Meri Tallinn International Airport je vzdialený od centra cca 4km
   - Náklady na prepravu z letiska na hotel nie je preplácané centrom výnimočnosti
   - Na hotel som môžete dostať taxíkom (cca 10€) alebo verejnú dopravu. Lístok si môžete zakúpiť u vodiča alebo na terminály v blízkosti autobusovej zástavky.
   - Z letiska sa dostanete do centra mesta alebo do hotela „Original Sokos Hotel Viru“ autobusom číslo 2 zo zastávky situovanej pri príletovom teminál a vystúpite na zastávke „A. Laikmaa“

Administratívne pokyny

3. Ubytovanie
   - Najvhodnejšie ubytovanie, ktoré centrum odporúča pre študentov je „Original Sokos Hotel Viru “, ktorý sa nachádza v samom centre Tallinu, pár minút chôdze od starého mesta a asi 20 – 25 minút chôdze do CCD CoE
     - Štandardná izba pre jednu osobu s raňajkami – 66 € za noc
     - Štandardná izba pre dve osoby s raňajkami – 71 € za noc
     - Izba superior pre jednu osobu s raňajkami – 86 € za noc
     - Izba superior pre dve osoby s raňajkami – 91 € za noc
   - Pre rezerváciu kontaktujte:
     - E-mail: viru.reservation@sok.fi
     - +372 6809 300 (24 hodín)
4. Preprava hotel – centrum
   - Pokiaľ nie sú k dispozícii iné konkrétne inštrukcie, odchody autobusu sú nasledovné:
     - Z hotela: pondelok 8:50 , utorok – štvrtok 8:40
     - Z centra: pondelok – štvrtok 17:00, piatok 15:15

Administratívne pokyny

3. Stravovanie
   - V priebehu dňa sú poskytnuté dve „Coffee break“ hradené centrom,
   - je veľa možností stravovania v okolí, ale centrum odporúča obed v jedálni vo veliteľstve EDF, ktorá je v tesnej blízkosti CCD CoE. Jedlo si môžete objednať z denného menu a zaplatiť môžete kartou alebo v hotovosti,

4. Oblečenie
   - Smart casual (nič prísne, niečo v čom chodievate na večeru, do kina ....)
   - Uniforma

Administratívne pokyny

5. Všeobecný plán kurzu
   - Deň 1 – Deň 4 (pondelok až štvrtok)
     - 8:40 cNATO CCD COE (Pondelok 08:50)
     - 9:00 Prvé sedenie
     - 10:30 Coffee Break
     - 10:45 Druhé sedenie
     - 12:15 Obedná prestávka
     - 13:30 Tretie sedenie
     - 15:15 Coffee Break
     - 15:30 Štvrté sedenie
     - 17:00 Autobus na hotel
   - Deň 5 (piatok)
     - 8:40 Autobus z hotela do NATO CCD COE
     - 9:00 Prvé sedenie
     - 10:30 Coffee Break
     - 10:45 Druhé sedenie
     - 12:15 Obedná prestávka
     - 13:30 Tretie sedenie
     - 15:15 Autobus na hotel a na letisko

NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE)

Filtri tee 12, 10132 Tallinn, Estonia
E-Mail: events@ccdcoe.org
Tel: +372 717 6800
Fax: +372 717 6308

CCDCOE
NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia

STUDENT JOINING REPORT

(will be accepted only from the national training Point of Contact)

Course	
Name of the course:	
Date:	

Applicant data[1]			
First Name		ID/Passport Number	
Last Name		Date of birth (DD/MM/YYYY)	
Nationality		Place of birth	
Former Visitor	☐ Yes ☐ No ☐ Unknown	Service	☐ Army ☐ Navy ☐ Air Force ☐ Civilian ☐ Marines ☐ Gendarmerie ☐ Other:
Military Rank		NATO Grade	
Organisation		Military Organisation	

Applicant contact data			
Applicant Email			
Organisation Email			
Address			
City, Post Code		Country	
Phone		Fax	

Logistics	
Hotel[2]	☐ Sokos Hotel Viru ☐ Other (please specify): ☐Transportation is needed from Sokos Hotel Viru
Lunch[3]	☐ Pre-register for the whole course (5 EUR per day) ☐ Individually

[1] The attendee's personal information will be processed and stored in the NATO CCD COE data management system. Upon completion of the registration, a confirmation message containing detailed administrative information will be sent to the applicant.
[2] Transportation is provided ONLY from the Sokos Hotel Viru. Rate of a standard single room is 66 € per night (special price, subject to availability). More information can be found in the Training Catalogue. Students are responsible for booking their own accommodation.
[3] Pre-regisered students will be sent a PayPal/Credit card payment link. A soup, a main dish and a dessert is included in the indicated price.

Otázky

?

Kontaktné údaje

- **kapitán Ing. Michal PETRÁŠ**
- PoC pre SR pre oblasť kurzov CCD CoE
- Generálny štáb ozbrojených síl SR
- 0960 311 443, 0903 824 977
- michal.petras @ mil.sk