NORTH ATLANTIC TREATY ORGANISATION
NATO MARITIME INTERDICTION OPERATIONAL TRAINING CENTRE
NMIOTC
SOUDA BAY
73200 CHANIA
GREECE

5000 NSC-74/Ser.: NU 87

TO: See Distribution List

SUBJECT: **INVITATION LETTER FOR CYBER DEFENCE TRAINING FOR PURPLE TEAMS "3rd and 4th ITERATION - GUARDIAN PURPLE 2024 (GP24) - EMPOWERING THE DEFENDERS OF CYBERSPACE".**

DATE: 22 Jul 2024

REFERENCE: A. OCIO (2001) 0021 – NATO Cyber Adaptation, 9 December 2021
B. PO (2022) 0252 – Political-Military Advice for a Framework on the Implementation of Defensive Cyberspace on NATO Networks, 10 June 2022
C. OCIO (2022) 0133 – Cyber Adaptation Roadmap Annex 7 – Defensive Cyberspace Operations (DCO), 25 December 2022
D. NMIOTC Program of Work 2024 (NPOW 2024)
E. MC 0458/4, NATO Education, Training, Exercise and Evaluation (ETEE) Policy (Final), dated 3 January 2023
F. Bi-SC 075-007, Education and Individual Training Directive

1. NMIOTC in coordination with SHAPE Cyberspace Directorate and in support of NATO Cyber Adaptation Roadmap as Ref C, has decided to organize cyber defence **training** for Purple Teams (PTs) "Guardian Purple 2024 (GP24)".

2. GP24 is a cyber defence **training** for NATO PTs that is trying to equip participants with a thorough understanding of contemporary cyber-attack methods and the practical skills necessary to proactively prevent, detect, and respond to these threats. The course curriculum will center around the utilization of the MITRE ATT&CK framework (MITRE Corporation, developed the "ATT&CK": Adversarial Tactics, Techniques, and Common Knowledge) and the Cyber Kill Chain methodology to enhance participants' ability to secure their systems and networks effectively. GP24 will take place virtually in two periods from **7th to 14th October 24** and **25th November to 02nd December 24** in a six (6) days iteration.

3. The cybersecurity community has long recognized the importance of timely threat detection and response. In the rapidly evolving landscape of cyber threats, real-time monitoring, detection, and response have emerged as critical components of effective cybersecurity strategies. Significant advancements and focused training in these areas are required within the Cyber Security Operations Centres (CSOCs) for effective Cyber Defence."Guardian Purple" sessions are designed to provide to participants with unbeatable value, the cutting-edge techniques necessary to enhance on one hand your real-time monitoring, detection, and response capabilities and on the other hand to practice the "Purple" construct (Red & Blue).

3. The Purple Team (PT) training concept is that Blue Teams (BTs) and Red teams (RTs) (hence the title "Purple Team Training") are trained simultaneously from the same entity or organization. If possible, BTs and RTs should be trained at the same location. They are in contact with each other and can exchange observations and experience. The RTs are trained on how to mount cyber-attacks; the BTs are trained on how to respond. The outcome will be that together they learn to seek out the weak spots in their own network's defense and address them even before actual attacks are mounted, therefor being one step ahead of the attackers. Thus, this training could be defined as a pre-emptive defensive strike making it harder for an attacker to penetrate and inflict damage. To this end, **"Attackers" (Red Team) –** performs latest cyber-attacks to compromise or degrade the performance of the systems and **"Defenders" (Blue Team) –** are required to defend the network consisting of virtual machines (cyber range) resembling an HQ network against the "red team" (simulated hackers).

4. Training participants will be able to apply their newly acquired skills immediately after the training at the tactical, operational, and/or strategic levels. Training participants will be trained, in a highly interactive manner, on how verify their organization cyber-attack surface and vulnerabilities, verify the ability of adversaries to take advantage of those vulnerabilities, to recognize and respond to a cyber-attack. They will receive recommendations on responses and advice on how to evaluate strategies, tools, procedures, and how to effectively collaborate with other PT members.

5. The training should ensure that participants will achieve the following objectives:

a. **Understanding Attacks:** Participants must comprehend the execution of high-profile attacks and possess strategies to thwart them effectively.

b. **MITRE ATT&CK Utilization:** Participants should be capable to conduct penetration testing to their organization and implement the right security controls across all phases of the Cyber Kill Chain using the MITRE ATT&CK framework to prevent future attacks.

c. **Adversary Behavior:** Participants should be adept at recognizing diverse attack types and understanding adversary motivation, behaviors and mindset.

d. **Strengthen** coordination and communication between Red and Blue Teams by sharing information and insights in order to address acute weaknesses and improve the organization's overall security posture.

6. The training audience is **Cyber Defence PTs (PTs) consisting of BTs/RTs'** personnel from NATO member countries and other NATO entities**.** Due to the limit in the number of BTs/RTs per iteration [eight (8)], the selection of the PTs attending these iterations will be under the responsibility of SHAPE's Cyberspace Directorate based on the PTs' timely registration order. The minimum number of teams should be three with 10 members each in order the training to be executed.

7. The Value of "Purple Team" Training outlined to :

- Collaboration for Continuous Improvement: Discover how to bridge the gap between Red and Blue Teams, fostering a collaborative environment that drives continuous enhancement of your security posture.

- Comprehensive Threat Response: Develop the skills to integrate offensive insights into defensive strategies, ensuring a holistic approach to threat management leading to business continuity and mission assurance.

7. **Training Schedule:** The duration of training iteration will be six (6) days:

a. Four (4) days of hands-on, virtually guided technical BTs'/RTs' training (**07-10 Oct and 25-28 Nov 24**), from 09:00 - 18:00 CET (GMT+2) every day, including time for a lunch/coffee breaks.

b. One (1) day of simulated live-fire type cyber-attack scenarios and BTs'/RTs' evaluation and assessments (**11 Oct and 29 Nov 24**), from 09:00 - 18:00 CET (GMT+2) including time for a lunch/coffee breaks.

c. One (1) day of Game Based Training (**14 Oct and 02 Dec 24**) with individual for each PT, instructor mentored sessions, splited in two (2) periods, 09:00 – 13:30 CET (GMT+2) and 14:00 – 18:30 CET (GMT+2) including time for coffee breaks.

d. A detailed daily Schedule of Events (SoE), administrative details, training specifications, guidelines for the training environment, and further directions will be promulgated promptly before training dates, for better preparation and familiarization of the participant BTs'/RTs' members.

8. **Training Description:** For the preparation and conduct of the aforementioned training the following team structure will be followed:

a. **Purple Teams (PTs)** are the members of the Blue Teams (BT) and Red Teams as described below. The maximum number of participant Teams per training iteration is eight (8), consisting preferably of 6-10 members per PT. **The participation capacity extends from a minimum of three (3) to a maximum of eight (8) teams per iteration. Please note that the training will only proceed if a minimum of three teams are registered. If fewer than three teams enroll, the course will be canceled.**

b. **Blue Teams (BTs)**

BTs are the main training audience. Trainees (BT members) – are required to learn how to defend a pre-built network consisting of virtual machines (cyber range) resembling an HQ network against the Red Team (RT - simulated hackers/adversaries). The BTs' role is to preserve the integrity, confidentiality, and availability of their organization's IT services, CIS infrastructure, and cyberspace in general. BTs are expected to participate in the training **from their own facilities. No traveling will be required**.

c. **Red Teams (RTs)**

RTs also are the main training audience The RT's mission is to compromise or degrade the performance of the systems that are protected. Members of the RT are basically performs latest cyber-attacks to compromise or degrade the performance of the systems. RTs are expected to participate in the training **from their own facilities. No traveling will be required**.

d. **White Team (WT)**

The WT has a key role in designing and preparing the training and controlling the scenarios during 4th day's training execution. The WT defines the training objectives, and the scenario develops the attack campaign together with the RT and defines the rules of 4th day challenges' scenarios. During the execution phase, the WT acts as the training controllers' cell. They decide when to start different phases, control the execution of the RT's attack campaigns, and make scoring/assessment decisions.

e. **Green Team (GT)**

The GT is responsible for preparing and configuring the cyber range technical infrastructure which will be used in the training. The main tasks for the GT include:

(1) Designing and setting up the core training infrastructure/ environment: computing nodes, virtualization platform, storage, and networking.

(2) Setting up routing and remote access to the training environment.

(3) Designing and building BT networks.

(4) Programming the automatic scoring/assessment bot and agents.

(5) Setting up solutions that are required for monitoring the general training infrastructure.

f. **Game Based Training**

Game based training's primary value lies in its ability to demystify the often complex world of cybersecurity. For cyber defence teams' leaders and managers, the challenge has always been twofold: understanding the technical jargon and grasping the strategic/operational implications of cyberspace operations. This game based training addresses both. By providing hands-on experience of technical terms and operations, PT leaders are better equipped to communicate with their teams, fostering an environment of mutual respect and understanding. Moreover, by delving into both offensive (Red Team) and defensive (Blue Team) scenarios, the **game offers a panoramic view of cyberspace operations, emphasizing strategy over technical details.** Using an intuitive and engaging gaming environment, PT members navigate through a series of rooms, each presenting its own set of challenges and decisions. The visual interface is streamlined: rooms are interconnected with four directional paths, and highlighted objects within these rooms serve as points of interaction. This design ensures that even those with minimal gaming experience can navigate the scenarios with ease.

g. **Training Practical Skills Development Objectives:**

(1) Attack Emulation: Facilitate hands-on experience with attack emulation to simulate real-world attack scenarios.

(2) Defensive Countermeasures: Provide techniques for implementing defensive countermeasures to proactively impede attacks.

(3) Malicious Payloads: Instruct participants on developing and detecting malicious payloads, emphasizing their role in attack prevention.

(4) Bypass Strategies: Detail various bypass strategies, such as Unmanaged PowerShell and AMSI bypasses, highlighting their importance in evading script controls.

(5) Malware Persistence: Guide participants through detecting and preventing malware persistence within systems.

(6) Lateral Movement: Instruct participants on identifying and preventing lateral movement within networks.

h. The training will be conducted in English. Translation to/from other languages will not be provided. The following proficiency standards in English (as described/ coded in STANAG 6001) are required to follow the training content: Listening – Professional (3), Speaking – Functional (2), Reading – Professional (3) and Writing – Functional (2) (STANAG 6001).

9. **Registration:**

Participant PTs are kindly requested to register by filling out the Registration Form below and sending it by email directly to the Training Director with Cc the SHAPE J6 POC and Registration POC in paragraph 11, **NLT 29 of Sep 2024 for October iteration and NLT 15 Nov for November iteration. The registration is FREE of charge.** A PT Leader must be identified for coordination and effective collaboration with the training organizers before and during the training conduct.

Registration Form	
Cyber Defence Purple Teams Training 2024 "Guardian Purple 2024" 7th to 14th October 24 / 25th November to 02nd December 24	
NATO Member Country/ NATO Entity	PT's Country
Organization	PT's Organization
	Rank/ Title, First-Last Name, email: Tel.:
Estimated number of PT members	The estimated number of PT members (RT and BT members included) will be engaged in training (**No more than 10 per PT**)
Preferred Game Based Training session (**14 Oct / 02 Dec 24**)	1. 09:00 - 13:30 CET (GMT+2) **or** 2. 14:00 - 18:30 CET (GMT+2)

10. **Training Classification:** The training content is marked as "NATO Unclassified''

11. **Point of Contacts (POCs)**:

a. **Training Director** :Commander (OF-4) Dimitrios Megas GRC (N)
Phone : +30 2821085711, NCN: 498-5711, Mobile : +30 6943482491
e-mail: megasd@nmiotc.nato.int (NU)
megasd@nmiotc.grc.nato.int (NS)

b. **SHAPE J6 POC** : Mr Emmanouil Christofis
Phone : +32 6544 3287 (Office) NCN: 254-3287 ,
e-mail: emmanouil.christofis@shape.nato.int (NS/NU)

c. **Registration POC**: Cdr (OF-4) Konstantinos Papanastasis GRC(N)
Phone : +30 28210 85710 (Office), NCN : 498-5710,
e-mail: papanastasisk@nmiotc.nato.int (NU)
studentadmin@nmiotc.nato.int (NU)

Efstathios Kyriakidis
Commodore GRC(N)
Commandant NMIOTC