Common Module

Social Engineering Protection

Module Description

Implementation Group	
Doc.:	ESDC/2021/247
Date:	5 Nov 2021
Origin:	Portuguese Military Academy

Country	Institution	Non-Common Module	ECTS
PT	**Portuguese Military Academy**	**Social Engineering Protection**	**2.0**

Service **ALL**	**Minimum Qualification of Instructors** • **Officers and Civilian Lecturers**: ○ English: Common European Framework of Reference for Languages (CEFR) Level B2 or NATO STANAG Level 3-. ○ Relevant experience in social engineering (SE) risks and human firewall construction. ○ Relevant experience in training on the different aspects of SE.
Language **English**	
SQF MILOF	**Competence area** - Military technician **Learning area** - C4ISR systems & cyber defence **Organisation level** – Single Arm/Branch / Single Service

Prerequisites for international participants:

- English: Common European Framework of Reference for Languages (CEFR) Level B1 or NATO STANAG Level 2.
- At least 2 years of national (military) higher education.

Goals of the Module

- Explain the characteristics of cyber security specifics to the branch/service
- Learn about cyber-attacks: fundamentals of SE and its attacking methods.
- Theoretical aspects of cybersecurity policies and awareness programmes within the cyber protection systems and future development and trends in SE protection.

Learning outcomes		
	Know-ledge	• Describe how a SE attack develops based on SE risks and the associated risk for the organisation. • Explain how the human firewall is created and his/her role in this line of defence.
	Skills	• Act as an active element in the human firewall (detect an attack, stop it, and report it to the lines of defence). • Creation/change of security policies according to the risks of SE attacks.
	Responsi bility and autonomy	• Make decisions in line with the cyber security human firewall policy. • Takes responsibility for reporting new vulnerabilities in improving security policies and awareness programs.

Verification of learning outcomes

- **Observation:**
  - Through the use of quizzes, online pools, and case studies, students can demonstrate the acquisition of knowledge.
  - Group activities requiring presentations of teamwork results.
  - During some practical tasks students are evaluated to verify their performance, namely in case studies' solutions.
- **Evaluation:** Group presentations of the case study deliverables that will run through the entire module, in a chain of systematic construction on the previous work.
- **Test**: Written exam at the end of the module.

Draft: Carlos Alexandre ..... 02nd June 2021
Revised by Col Assoc. Prof. Harald Gell, PhD / Chairman Implementation Group ..... 07th June 2021
Revised Lt. Col. Enrico Spinello / Chairman LoD 8 ..... 13th June 2021
Revised: Carlos Alexandre ..... 16th June 2021
Approved as "Common" by the Implementation Group ..... 08th September 2021
Revised according to SQF MILOF by CAPT (N) N. Dimitrov and Assoc. Prof. N. Karadimas / Chairpersons LoD 2/8 ..... 20th November 2024

Module Details		
Main Topic	**Recom-mended WH**	**Details**
SE: introduction and concepts	1	• SE: main concepts and definitions • SE in information warfare • SE attacks
Information collection and intelligence production	2	• SE process • Information collection • Case Study (Chief Executive Officer (CEO) fraud attack – phase 1 and 2)
Attack planning	3	• Psychological vulnerabilities (reciprocity, scarcity, authority, consistency, liking, and consensus) • Pretexting • Phishing, vishing, and smishing case studies • Attack matrix • Case study (CEO fraud attack – phase 3)
Security policies	3	• The construction of the human firewall • Risk analysis • Policy setting • Incident reporting channels (information systems security, physical security, and fraud) • Case study (CEO fraud attack – phase 4)
Awareness programmes	3	• Awareness tools • Resistance training • Organisation pain • Case study (CEO fraud attack – Phase 5)
Final group assignment presentation & wrap-up	2	• Group presentations • Wrap up
Final test	1	
Total	**15**	
Additional hours (WH) to increase the learning outcomes		
Self-studies	20	• Reflection of the topics issued. • Preparation for the upcoming lessons and for exam(s).
Group assignment preparation	15	• Work group discussions • Preparation of deliverables for each phase of the case study • Development of presentation/final report
Total WH	**50**	The detailed amount of hours for the respective main topic is up to the course director according to national law or the home institution's rules. During which topic(s) the syndicate elaborations and presentations will take place is up to the course director. See in the appendix hereinafter a proposal for the estimated hours and activities for each main topic.

Draft: Carlos Alexandre ..... 02nd June 2021
Revised by Col Assoc. Prof. Harald Gell, PhD / Chairman Implementation Group ..... 07th June 2021
Revised Lt. Col. Enrico Spinello / Chairman LoD 8 ..... 13th June 2021
Revised: Carlos Alexandre ..... 16th June 2021
Approved as "Common" by the Implementation Group ..... 08th September 2021
Revised according to SQF MILOF by CAPT (N) N. Dimitrov and Assoc. Prof. N. Karadimas / Chairpersons LoD 2/8 ..... 20th November 2024

APPENDIX

Main Topic	Recommended WH	Syndicate Work	
		Activity	Estimated WH
SE: introduction and concepts	1	Initial quiz	15 min
Information collection and intelligence production	2	Online pool Case study	15 min 30 min
Attack planning	3	Online pool Case study	15 min 30 min
Security policies	3	Online pool Case study	15 min 30 min
Awareness programmes	3	Online pool Case study	15 min 30 min
Final group assignment presentation & wrap up	2	Online pool	n/a
Final test	1	n/a	n/a
Total	**15**		

List of Abbreviations:

B1, B2 ..... CEFR Levels
CEFR ..... Common European Framework of Reference for Languages
CEO ..... Chief Executive Officer
ECTS ..... European Credit Transfer and Accumulation System
NATO ..... North Atlantic Treaty Organisation
PRT ..... Portugal
SE ..... Social Engineering
STANAG ..... Standardization Agreement
WH ..... Working hour

Draft: Carlos Alexandre ..... 02nd June 2021
Revised by Col Assoc. Prof. Harald Gell, PhD / Chairman Implementation Group ..... 07th June 2021
Revised Lt. Col. Enrico Spinello / Chairman LoD 8 ..... 13th June 2021
Revised: Carlos Alexandre ..... 16th June 2021
Approved as "Common" by the Implementation Group ..... 08th September 2021
Revised according to SQF MILOF by CAPT (N) N. Dimitrov and Assoc. Prof. N. Karadimas / Chairpersons LoD 2/8 ..... 20th November 2024