TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

Kyberuhkatietojen hyödyntäminen

kurssikuvaus

Euroopan unionin rahoittama
NextGenerationEU

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus

Koulutus on rahoitettu Euroopan unionin elpymis- ja palautumistukivälineellä (RRF), joka on EU:n elpymisvälineen (Next Generation EU) suurin ohjelma. Rahoituksen on myöntänyt Jatkuvan oppimisen ja työllisyyden palvelukeskus. Palvelukeskuksen tehtävänä on edistää työikäisten osaamisen kehittämistä ja osaavan työvoiman saatavuutta sekä vastata nopealla toiminnalla työmarkkinoiden äkillisiin rakennemuutoksiin. Palvelukeskuksen toimintaa ohjaavat opetus- ja kulttuuriministeriö sekä työ- ja elinkeinoministeriö.

Cyber Threat Intelligence

OBJECTIVES

Students are expected to broaden their knowledge of different ways to utilise cyber threat intelligence information (CTI), especially from the defenders' viewpoint. Students conduct and perform data analysis on various cyber threat intel datasets gathered from different sources. Students will also design and implement customised dataset and information models for more efficient cyber threat contextualisation in various sectors.

The course is intended to stimulate the students' creativity, critical thinking and threat assessment by engaging in the analysis of short-term and long-term, real-life cyber threats.

This course focuses on the correlation of information regarding threat-related data and metadata to assist in decision making. The emphasis will be on proactive preparedness for and anticipation of potential threats for organisations

COMPETENCES

- Utilise cyber threat intelligence platform for threat information management and dissemination
- Conduct and perform threat analysis and conclude its relevance to key stakeholders and industries
- Plan and document concept of operations for cyber protection teams
- Use enrichments and customised taxonomies to enhance threat contextualisation and to improve the CTI quality
- Utilise threat intelligence information in conventional detection systems

KNOWLEDGE

- Cyber threat intelligence sharing standards, methodologies, frameworks
- Cyber threat intelligence context development
- Cyber threats & threat actors
- Threat actors' tactics, techniques and procedures (TTPs)
- Cyberattack procedures
- Advanced and persistent cyber threats
- Ethical & responsible information sharing procedures

SKILLS

- Assess and enhance an organisation's cybersecurity posture
- Collect, analyse, correlate and enrich cyber threat information originating from multiple sources
- Communicate, coordinate and cooperate with internal and external stakeholders
- Model & identify threat actors' TTPs and campaigns
- Conduct technical analysis and reporting
- Extend CTI platform's functionalities through integrations

Schedule, breakdown and grading

Onsite labwork 16h
Group and individual work 119 h

The course consists of a total of ten group assignments, each of which is assessed separately. The grades of the course are determined on the basis of the total score (maximum 100 p). Tasks are divided into theoretical tasks and practical laboratory tasks as follows:

Cyber threat intelligence – theory (30 p)
Cyber threat analysis – technical assignments: analysis, enrichment and exploitation in practice (70 p)

Grading limits:

0-39 points = Rejected

40..49 points = 1

50..59 points = 2

60..74 points = 3

75..89 points = 4

90..100 points = 5

The rhythm and content of the course and the assessment criteria

1. Technical platforms used in the course
    a. MISP
        i. https://www.misp-project.org/documentation/
        ii. https://github.com/MISP/misp-training
        iii. https://www.misp-project.org/misp-training/cheatsheet.pdf
        iv. https://github.com/MISP/misp-modules
    b. TheHive
    c. Mattermost
    d. Other systems, e.g. sandbox platforms

2. Forming teams
    a. Ideal size for 4-6 people with different skill profiles

3. Group Task Topic Selections

4. CTI concepts - Cyberthreat and intelligence; Main themes: data collection, analysis, aggregation and contextualization; identification of technical methods and threat actor; mapping of cyberthreats by sector and sharing of analysed data

5. CTI theory group assignments (30 points)
    a. 1 – Threat Modelling (assignment introduced in-class)
    b. 2 – Kill Chains (assignment introduced in-class)
    c. 3 – SOC Tactical Playbooks (assignment introduced in-class)

6. CTI technical lab-assignments
    NB. These assignments involve the analysis of real and dangerous software samples. Some of the software packages are handed out to in-class participants only, and only in exchange to a written risk management plan delivered by the student.
    a. #1
    b. #2
    c. #3
    d. #4
    e. #5
    f. #6
    g. #7