# Solent University Unit Descriptor

## **Unit Code: COM522 Unit title: Threat Intelligence Analysis**

### **Why is this unit important?**

A growing number of cyber-attacks requires specialists to detect, analyse and defend against the cyber threats. In practice, timely dealing with such a large number of attacks is not possible without deeply perusing the attack features and taking corresponding intelligent defensive actions – this in essence defines cyber threat intelligence notion. Threat intelligence is aided by artificial intelligence, machine learning and advanced data mining techniques to collect, analyse, interpret and visualise cyber-attack evidences. This unit discusses the notion of cyber threat intelligence and its main challenges and opportunities, and then presents solutions and tools to provide threat intelligence.

### **What you will learn on the unit**

Prepare and use threat intelligence tools that allows evidence-based knowledge and provides actionable advice about known and unknown threats.

How organizations can develop predictive capabilities rather than just proactive measures beyond active defence mechanism.

You will be empowered with the skills to develop a professional, systematic, and repeatable real-life threat intelligence program.

You will be provided with an invaluable ability of structured threat intelligence which will enhance your skills and boost your employability.

### **How you will learn**

You will be introduced to the content of this unit and the practical and conceptual challenges it presents in introductory lectures supplemented by a follow-up experimental and practical study, which aim to either develop your understanding of a topic or will require your engagement in a research or problem-based activity. Regular formative testing will allow your progress to be monitored and feedback to be provided on key areas of learning. Practical case study based sessions, will provide you with the opportunity to apply the knowledge, concepts and skills encountered in the unit to theoretical contexts and in situations drawn from real life scenarios. In doing so you will be required to draw on independent study, supported on the Virtual Learning Environment, you will encounter opportunities in timetabled sessions to compare and discuss your work with your tutors and peers.

### How much time the unit requires: you are expected to study for 200 hours (which equates to 10 hours per credit.  This total learning time is made up of contact time, directed learning tasks, independent learning and assessment activity. Your tutor will offer you guidance on how you should best manage your study time on this unit.

### **How you will be assessed**

#### **Tasks which help you to learn and prepares you for summative tasks (Formative):**

You should maintain Portfolio each session and show it to the tutor at regular intervals during the timetabled sessions for feedback in order to maximise your summative assessment. Regular formative assessment will allow your progress to be monitored and feedback to be provided on key areas of learning.

#### **Tasks which count towards your degree (Summative):**

The summative assessment will be based on a portfolio. The portfolio will contain a practical sessions’ detailed summary on the topic in question and evidence of how they have applied the relevant technology and tools to the needs of the case study in theory, based on independent research and preparation, and in practice, based on experimental in class study.

#### 

#### **When assessment does not go to plan**

#### If the portfolio is not completed to a standard satisfactorily enough to pass the unit you will be expected to conduct preparation and independent practical study based on the original assessment and to submit a portfolio completed to at least a satisfactory standard according to the assessment criteria.

#### **What you will be able to do after the unit**

### On successful completion of the unit, you should be able to:

### Evaluate applications vulnerability and identify flaws in a targeted system and any holes in the application and system security.

### Analyse applications websites and online services vulnerability against different security threats that exploit holes in application’s code.

### Use tools for threats analysis and evaluation.

### Autonomously evaluate and critically assess various applications websites and online services vulnerability identifying improvements.

### Communicate effectively in the subject area.

### How this relates to the dimensions of Solent’s Real-world curriculum framework

|  |  |  |
| --- | --- | --- |
| Dimensions | How students learn | How students are assessed |
| Students are challenged to think in critical, creative and applied ways | Students will evaluate multiple perspectives; students will apply theory to practice. | In class lab activities on tools for threat analysis applied to particular cases will be summarised in Portfolio which will evidence knowledge and skill. |
| Students are inspired to do research through inquiry, curiosity and problem-solving | Students will conduct independent research on theories, technologies and tools which they will apply in practice based on experimental in class study. | Students will summarise their research for each activity supported with references, will evaluate their results against publications supported with visual representation of numerical data |
| Students experience an intellectually stimulating curriculum which inspires them to learn for life | Students will evaluate world leading challenges and problems and will propose their assessments and solutions. | Students compare and asses their results or achievements towards published solutions in the subject area. |

### Summative assessment details

|  |  |  |
| --- | --- | --- |
| AE1 | Weighting: | 100% |
|  | Assessment type: | Portfolio |
|  | Aggregation: | N/A |
|  | Length/duration: | 4000 words |
|  | Online submission: | Yes |
|  | Grade marking: | Yes |
|  | Anonymous marking: | No |

### Unit Author:

|  |  |  |  |
| --- | --- | --- | --- |
| Unit Title: Threat Intelligence Analysis | | | |
| Credit Points: | 20 | Unit Code: | COM522 |
| FHEQ Level: | 5 | School/Service | SMAT |
| Unit Delivery Model: | CD | Max/Min student numbers |  |
| Unit Leader: | Dr. Kalin Penev | | |
| HECOS code | 100376,100365 | | |

### Unit change history:

|  |  |  |  |
| --- | --- | --- | --- |
| Unit Approved/Year Implemented/Code |  |  |  |
| Unit modified/Year Implemented/Code |  |  |  |
| Add extra rows as required |  |  |  |