SOLENT UNIVERSITY SOUTHAMPTON

Solent University Module Descriptor

Module Code: COM613 **Module title: Cyber Ops**

Why is this module important?

A Security Analyst working with a Security Operations Centre team or more specifically a product security incident response team needs a high level of technical knowledge of threat analysis and computer forensics, network intrusion detection, incidence response and handling and data and event analysis. They must be able to gather cybersecurity intelligence data, to document it, to manage and to analyse this data and to perform a risk assessment. They must also be able to plan for risk management and incidence response.

What you will learn on the module

You will complete a Cisco academy training course on cybersecurity operations to discover, identify and analyse threats, perform attack techniques, discover vulnerabilities and apply mitigations.

By completing practical computer-based lab tasks you will learn how to perform a threat analysis for an organisation by applying a methodology and collecting metrics to record the vectors, complexity, scope and required privileges of cyber-attacks.

Working in your security operations team you will use the case study to undertake risk modelling, analysis and planning, ethical system reconnaissance and intelligence analysis. You will collect cybersecurity operations metrics and analyse them to infer a threat level.

The tasks to perform this will include data and event analysis, security monitoring and analysis and intrusion detection. You should be able to recognise anomalies & behaviours and manage intrusion response including with 3rd parties.

How you will learn

Firstly, you will complete training for cybersecurity operations by reading online materials and completing a series of practical computer-based tasks. You will provide evidence of professional skills and training gained to apply for a position to work in a simulated Security Operations Centre team, you will work in this team to perform realistic cybersecurity operations intelligence gathering, analysis and incidence response planning for a real-world case study or brief.

How much time the module requires

You will need to attend and engage in 4 hours per week of timetabled practical workshops and tutorials for this module. You will also need to engage in an additional 12 hours each week of directed and independent learning outside of these sessions in order to work towards proficiency in this subject. This will include work on the training course and working in the group.

How you will be assessed

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

The training course includes online mini topic quizzes, skills based tests and cyberops planning exercises. Completion of the training course will prepare you for the tasks you will perform in the team.

Tasks which count towards your degree (Summative):
You will create a portfolio which includes your training course evidence and results, job application documentation for the security operations team and your contribution to the team case study including your vulnerability assessment and/or risk assessment and/or incidence or threat response or risk management plan for the brief.

When assessment does not go to plan
If the portfolio has missing training course evidence or below failure threshold results the training course must be completed, gathered and resubmitted.

If the portfolio shows that the whole teams' performance for gathering data from vulnerability and/or risk assessment meeting the brief of the case study is below the failure threshold in the required criteria the whole team will resubmit the case study and their contributions in their portfolios.

If the portfolio has insufficient evidence of your contribution to the case study or it is below failure threshold you must write a report which demonstrates one or some of the following: the analysis and planning with your vulnerability assessment, the risk assessment, the incident or threat response or risk management plan where example metrics will be supplied.

What you will be able to do after the module
1. Critically evaluate and apply cybersecurity operations data gathering techniques.
2. Analyse and apply structured methods to evaluate the risks and threats to an organisation
3. Review, evaluate and document threat levels for an organisation based on cyber security metrics.
4. Present solutions by designing and documenting a cyber security plan based on analysis of cyber security metrics.
5. Research and communicate effectively in a team and individually the cybersecurity operations of an organisation.

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	Working with the cyber ops team you will create methods for analysing security issues and vulnerabilities and plan how they will be mitigated	Your portfolio will include the results from your technical training evidencing the relevant skills you will need to contribute to the cyber ops team.
Students are inspired to do research through inquiry, curiosity and problem-solving	You will collect data using structured security evaluation methodology while performing tests	You will document and visualise the data gathered in the tests and compare with cyber security metrics
Students learn from authentic, engaging and programmatic assessment	The formative tasks are related to the cyber operations profession.	Your portfolio will evidence authentic and engaging artefacts related to the realistic

		case study this will include how you would be suitable for this profession

Summative assessment details

AE1	Weighting:	100%
	Assessment type:	Portfolio
	Aggregation:	N/A
	Length/duration:	3000 words
	Online submission:	Yes
	Grade marking:	Yes
	Anonymous marking:	Yes

Module Author: Warren Earle

Module Title: CyberOps			
Credit Points:	20	Module Code:	COM613
FHEQ Level:	6	School/Service	SMAT
Module Delivery Model:	CD	Max/Min student numbers	25 max
Module Leader:	Warren Earle		
HECOS code	100376		

Module change history:

Module Approved/Year Implemented/Code	May 2019	2020/21	COM613
Module modified/Year Implemented/Code			
Add extra rows as required			