Cyber Security Analyst

Course Outline

WITH
YOU
WITH
ME

WITH
YOU
WITH
ME

Cyber Security Analyst Course Outline

METADATA HISTORY

RELEASE	DATE	COMMENTS	APPROVER
v1.0	11 Jan 2019	first approved version	Michelle Mosey Head of WYWM Academy
v2.0	20 Mar 2019	additional information required from ANSI application submission	Kemal Pinjo Head of WYWM Academy
v2.2	25 Jun 2019	Updated completion dates for Squad cohorts.	Karl Jensen Cyber Manager
v2.3	10 Jul 2019	additional information required from onsite audit	Anindo Basu Head of WYWM Academy
v3.0	23 Sep 2019	updated for Semester 3_2019 Course	Anindo Basu Head of WYWM Academy
v4.0	31 Jan 2020	updated for Cyber Defender Program 1/2020	Anindo Basu, WYWM Chief Operating Officer

ACCEPTANCE OF POLICY DOCUMENT

1 **Approved**

Anindo Basu

WITH YOU WITH ME

Cyber Security Analyst Course Outline

ACADEMY PHILOSOPHY

We are proud of our methodology and standards which provide a holistic approach to training. Our content is aligned with in demand skills required in industry with rapid constant continual development to become highly sought-after members of industry. Our focus is on workforce “development”, long term career growth and challenging traditional placement systems and services.

COURSE DESCRIPTION

Throughout the WYWM Cyber Security Analyst Course you’ll be introduced to fundamental cyber security concepts and the technical skills in preparation for a role as a Tier 1 Cyber Security Analyst.

TARGET AUDIENCE

This course is for individuals interested in attaining a job as a Cyber Security Analyst who are enrolled on the WYWM Cyber Defender Pathway. Prior knowledge of hacking techniques, fundamental IT skills and Linux operating systems are assumed.

COURSE REQUIREMENTS

The information below is provided as a guide to assist students in meeting the requirements for enrolment on the course, participation in the course and certification for course completion.

Enrolment Prerequisites

The minimum requirement to enrol in the Cyber Security Analyst Course is successful completion of the following WithYouWithMe courses as part of the WYWM Cyber Defender Pathway:

- Linux Fundamentals
- Network Fundamentals
- IT Fundamentals

Completion Requirements

- Study all course materials provided
- Achieve a passing score for all assessment tasks

Course Pass score

The passing score for this course is 70%, while individual assessment tasks will have varying passing scores as outlined below.

CERTIFICATE REQUIREMENTS

Certificate Requirements

Academic: To fulfil the academic requirements of the curriculum, students must complete the curriculum and satisfactorily complete all assignments, as well as the knowledge checks in the curriculum. Knowledge checks and the assignments are created to test student achievement of established learning outcomes.

Certificate issuance: To be issued a certificate of completion, a student must complete all the academic requirements of the curriculum. Upon successful completion of the assignments, the student will receive a certificate of completion for the exam.

Certificate maintenance and use: Each certificate has a unique serial number which is tracked by a WYWM Administrator. Certificate is not transferable to another person or company. The certificate can only be used while it is valid. When certificate is invalidated for any reason, the person can no longer use the certificate.

Certificate term of validity is two years pursuant to industry updates.

Certificate Issue

Student will receive a Certificate of Completion upon completing the academic requirements of the course requirements.

Validation for an employer

Employers may validate authenticity and term of validity of WYWM certificate by contacting WYWM contact@withyouwithme.com and providing student name and course name. WYWM will provide a YES or NO. No further information will be provided to employers.

Validation for a student/graduate

Graduates may validate the term of validity of WYWM certificate by contacting WYWM contact@withyouwithme.com and providing their name and course name. WYWM will provide the term of validity of the certificate.

Information Regarding Changes to the Certificate Program

WYWM will strive to deliver its curriculums in accordance with the descriptions provided on the website at the time of enrolment. However, in some situations it might be beneficial or necessary for WYWM to implement changes to curriculum. The changes will not be very substantial so as to have an impact on students who have already started their curriculum. In some circumstances where it is necessary for WYWM to implement such changes after enrolment due to developments in the relevant subject, advances in teaching or evaluation practice, or requirements of accreditation processes, students will be notified of the changes made to curriculum immediately. Primary stakeholders will be notified of changes to program purpose, scope, intended learning outcomes via the WYWM website.

COURSE CONTENT AND SCHEDULE

Course Content

INTRODUCTION

The course is arranged into modules with various learning topics, exercises and assessment tasks forming those modules as follows:

INTRODUCTION

- Overview of course

INTRODUCTION TO CYBER SECURITY

- CIA Triad
- Defence in Depth
- Security, Controls and Limitations
- Introduction to Types of Data
- Introduction to Malware
- Introduction to Cryptography
- Introduction to Social Engineering
- Introduction to Threat Actors
- Security Analyst Overview
- Module Quiz

INTRODUCTION TO THE SOC AND THE TIER 1 ANALYST ROLE

- Understanding the Role
- Overview of the Capabilities of a SOC
- SOC Job Roles
- Tasks, Duties and Responsibilities
- Monitoring, Detection and Alerts
- Isolation and Containment
- Reporting
- Online Services and Tools

OPERATING SYSTEM SECURITY

- Technical Foundations
- OS Lockdown Exercises
- OS Lockdown Quiz

ANALYSING ADVANCED THREATS

- The Cyber Kill Chain™
- The Diamond Model of Intrusion Analysis
- Scenario-based assessment task

INCIDENT RESPONSE

- Introduction to Incident Response
- Introduction to Playbooks
- Tech Stack Introduction
- Tech Stack Details
- Firewalls
- IDPS
- Incident Response Quiz
- Incident Response Playbook Assessment Task
- Scenario-based Assessment Task

SIEMS and NETWORK TRAFFIC ANALYSIS

- Security Information and Event Management
- Event Logs
- Interpreting Logs
- Wazuh Overview and Operations
- Wazuh Installation and Exercise
- Wireshark Installation and Operation
- Network Traffic Analysis Exercises
- SIEMS and Network Traffic Analysis Quiz

CYBER SECURITY ANALYST CERTIFICATION QUIZ

- Final knowledge quiz

COURSE SCHEDULE

The course is intended to be completed in 100 hours over a period of 12 weeks. Course modules and their elements should be undertaken in the order presented in the course – in some instances this will be enforced. All course activity must be satisfactorily completed by the published course-end date. Some assessment tasks must be completed by a specified due date. The table below outlines when each module should be commenced to allow for the course to be completed part-time over 12 weeks.

MODULE NAME	EXPECTED COMMENCEMENT/ DUE DATES
Introduction	Week 1
Introduction to Cyber Security	Week 2
Introduction to the SOC and the Tier 1 Analyst Role	Week 3
Operating System Security	Week 4
Analysing Advanced Threats	Week 5
Incident Response Create an Incident Response Playbook	Week 6 DUE 1st day of Week 8
SIEMs and Network Traffic Analysis	Week 9
Cyber Security Analyst Certification Quiz	Week 12

TECHNICAL REQUIREMENTS

Hardware and Software required

- Access to a computer (desktop, laptop, notebook, etc)
- High-speed Internet connection
- CPU: 64-bit Processor (Intel or AMD chipsets; example i5 to i9)
- RAM: 8GB or Better (16GB Recommended)
- Free Hard Drive Space: 60 GB
- Operating Systems: Windows 7 to Windows 10, Linux 3.x (and up) Distros, Mac OS X
- Office Productivity for Reports e.g. Microsoft Office or LibreOffice
- Reader for PDF Files e.g. Adobe Acrobat Reader or MS Word 2016
- Web Browser: **Recommended** - Google Chrome or Firefox (some versions of Microsoft and MAC OS Operating Systems Browsers experience difficulty showing interactive video)

CAREERS

Employment can be found in most state capitals and large commercial hubs.
You can gain employment at the following:

- Boutique Cyber Security firms
- Large consulting companies - PwC, Accenture, Deloitte, KPMG, EY etc.
- Form part of an internal security team for larger organisations, such as banks and telecommunication companies.
- Government departments

INSTRUCTOR PROFILE

Required Qualifications for Cyber Instructor

- Evidence of practical experience as a member of a cyber protection team or a technical operations role or course related experience
- Certificate IV in Training and Assessment or evidence of prior instructional experience
- Completion of WYWM Cyber Defender Program

Required Qualifications for Senior Cyber Instructor

- Relevant Bachelor Degree or 3 years of practical experience
- Certificate IV in Training and Assessment or evidence of prior instructional experience
- Evidence of practical experience as a member of a cyber protection team or a technical operations role
- Completion of WYWM Cyber Defender Program

ENQUIRIES FOR SUBJECT MATTER EXPERTISE CONTACT

Eric McIntyre
Cyber Security
Instructor

Eric has a Bachelor of Arts, majoring in History and Philosophy

Since graduating in July 2019, Eric has honed his degree to suit a Cyber Security context, completing the WYWM Defender Program and continuously developing his skills in the industry.
After moving into a teaching role at WYWM, Eric has gained experience in learning development and managing student experience throughout the WYWM pathway.

Contact: eric@withyouwithme.com

GENERAL ENQUIRIES

Pathfinder Team (during Australian – AEST and US – EST office hours 9 to 5, Mon to Fri)

pathfinders@withyouwithme.com

EXPECTATIONS OF STUDENTS IN THIS COURSE

Student attendance/participation

The online courses are designed to be highly interactive and collaborative, as authentic learning takes place within a sociHal context refer to instructor outline for further guidance on interaction. To help ensure an effective learning experience, all students in online courses are expected to participate on a regular basis. Participation is defined as "submitting required work as assigned; being an active contributor and responder to fellow students and the instructor in a timely basis, as set forth by online discussion guidelines in each course." Failure to participate may be counted as an absence.

If technical circumstances prevent a student from entering the course site for a period, it is the student's responsibility to contact the instructor in a timely manner if the student wishes to receive credit for any missed online activities.

There is a student Administration file located in the course that will provide useful information such as student code of conduct, assessment requirements, and course outline.

Instructors participation

Staff and Affiliates of WYWM are expected to perform all work, duties and functions associated with their positions this includes and not limited to engagement process refer to instructor outline for further guidance on interaction.

CONTINUAL COURSE IMPROVEMENT

Periodically student responses are gathered, using online evaluation forms. Student responses are taken seriously, and continual improvements are made to the course based in part on such feedback. Significant changes to the course will be communicated to subsequent cohorts of students taking the course. It is important that students and teachings complete the surveys for this course. This is completely anonymous and provides important student observations and suggestions to ensure that the course is continually improved.

ASSESSMENT

The assessment shall be administered with a level of identity verification and security congruent with the certificate program's purpose, scope and intended learning outcomes. Academic integrity is an ethical standard of WYWM courses. It ensures that students graduate because of proving they are competent in their discipline. Each industry has expectations and standards of the skills and knowledge within that discipline and these are reflected in assessment. Academic integrity means that you do not engage in any activity that is academic fraud; including plagiarism, collusion or outsourcing any part of any assessment item to any other person. You are expected to be honest and ethical by completing all work yourself and indicating in your work which ideas and information were developed by you and which were taken from others. You cannot provide your assessment work to others.

You are also expected to provide evidence of wide and critical reading, usually by using appropriate academic references. To minimise incidents of academic fraud, this course may require that some of its assessment tasks, when submitted to a software that will check for text comparison.

Late Submission Penalties

Late submission of assessment tasks will be penalised at the following maximum rate:

- Five percent (of the assessment task's identified value) per day for the first two days from the date identified as the due date for the assessment task

- 10 percent (of the assessment task's identified value) for the third day

- 20 percent (of the assessment task's identified value) for the fourth day and subsequent days up to and including seven days from the date identified as the due date for the assessment task

- A result of zero is awarded for an assessment task submitted seven days from the date identified as the due date for the assessment task.

- Weekdays and weekends are included in the calculation of days late.

Assessment marks

The assessment scoring is designed and conducted by qualified personnel following industry accepted practices, uses methods appropriate to purpose, scope and intended Learning Outcomes, and is based on a passing score established through a criterion-referenced method in advance of the assessment being administered. The results of the assessment are communicated to learners in a consistent, timely and appropriate manner and documented as part of the learner's record.

Assessment Task

As an WYWM student, you can expect to undertake various types of assessment. These may be either formative or summative. Formative assessment help students identify weaknesses in their understanding and/or performance in this course. In this course a formative assessment is delivered by short answers and multiple-choice questions which are not graded to your overall pass mark for this course. However, a summative assessment passes judgement on the quality of a student's learning and in this course the summative assessment is detailed below:

Assessment Task 1. End of Module Quiz

Assessment Task	Intro to Cyber Security - Module Quiz
Pass Mark	70%
Weighting	5%
Task description	End of topic quizzes are used to assess comprehension of knowledge and skills gained throughout the topic.

Assessment Task 2. End of Module Quiz

Assessment Task	Operating System Lockdown Quiz
Pass Mark	100%
Weighting	5%
Task description	End of module quizzes are used to assess acquisition of knowledge and skills gained throughout the topic. This quiz checks the satisfactory completion of the Operating System Lockdown exercises.

Assessment Task 3. Lazarus 1 Assessment Task

Assessment Task	Lazarus 1 Questionnaire
Pass Mark	74%
Weighting	15%
Task description	The Lazarus report assessments are based on an incident scenario involving the Lazarus Group. The Lazarus Group are a North Korean linked hacking group associated to multiple attacks. This assessment consists of research into the group and its activities, applying your research to a given scenario and simulating the writing of a Cyber Threat Intelligence Report through the completion of a time-limited questionnaire.

Assessment Task 4. Draft an Incident Response Playbook

Assessment Task	Create an Incident Response Playbook (IRP)
Pass Mark	70%
Weighting	25%
Task description	Within a Security Operations Centre (SOC) playbooks provide clear instructions/procedures, roles and responsibilities to be followed in the event of an incident. Upon reviewing IRPs available within the WYWM Security Analyst course you are to select a subject, which hasn't been covered with the available IRPs, and using the supplied IRP template develop your own playbook. (further info is available within the course) **Outline** • Review example IRPs • Download the IRP Template Document • Draft a new IRP **Objectives** • Familiarisation with Incident Response processes • Ability to create and update Incident Response processes than passive voice) **Subject Ideas** • The subject can be anything related to tasks performed by an Analyst; Insider Threat, Social Engineering or the subject can be of a sub-category of a broad event, for example: an IRP for Worms or Ransomware is possible. The IRP for Malware is a generalisation of all forms of malware. However, treating a worm requires different set of steps than treating a ransomware infection. Note, that a worm may have used ransomware as a payload, thus two IRPs would be needed. **Report requirements** • The IRP will consist of a list of steps • The steps should list which tools or systems to use when appropriate. • Further information can be provided on each step where necessary • Submit the IRP via the appropriate submission field. • The yellow highlighted areas are required to be edited. • Write in the third person; avoid the use of "I", "we", "our" etc. • Graph or flow chart is required to be included

Reference requirements

- Academic referencing is not required for this assessment however, please note your sources and observe that plagiarism will not be accepted.

Formal and respectful language requirements

- This assessment task must be in professional and formal language. This means there should be no abbreviations or slang.
- Care must be taken to avoid spelling, grammar and punctuation errors.
- This report should predominantly be written in active voice (rather than passive voice)

Assessment Task 5. Lazarus 2 Assessment Task

Assessment Task	Lazarus 2 Questionnaire
Pass Mark	65%
Weighting	10%
Task description	You are provided with a further scenario building on the Lazarus I scenario and are asked a series of questions which assesses your ability to draw on all of the course content in a single analytical exercise.

Assessment Task 6. End of Module Quiz

Assessment Task	Wazuh and Network Traffic Analysis Quiz
Pass Mark	70%
Weighting	15%
Task description	End of module quizzes are used to assess acquisition of knowledge and skills gained throughout the topic. This quiz checks the satisfactory completion of the Wazuh and Network Traffic Analysis exercises.

Assessment Task 6. Tier 1 Analyst Certification Quiz

Assessment Task	Tier 1 Analyst Quiz
Pass Mark	70%
Weighting	25%
Task description	This quiz will be used to assess comprehension of knowledge and skills gained throughout the course.

Complaints Process

We have a separate complaints process that provides information and clear steps to assist you in lodging an appeal or making a complaint about decision or determination made by a member of the WYWM academic staff. Please notify WYWM at contact@withyouwithme.com or +61 2 83118755.

STUDENT CODE OF CONDUCT

The Student Code of Conduct ("the Code") sets out WYWM's expectations of students as members of the academic community. All students at enrolment must accept their shared responsibility for maintaining a safe, harmonious and tolerant environment in which to study and work. The Code details WYWM's responsibilities and what students can reasonably expect in terms of quality provision, a safe and fair learning environment, and the student experience.

Student Conduct

The Code provides a framework for the standard of conduct expected of students with respect to their academic integrity and behaviour. It outlines the primary obligations of students and directs staff and students to the code and related procedures. Where a student breaches the Code, WYWM may take disciplinary action.

Student Complaints

The Code also provides for a Student Complaint Procedure which contains guiding principles and processes for student complaint resolution. This framework can be accessed through the Complaints Process described earlier.

Scope

The Student Code of Conduct is the basis for the relationship between WYWM and our students. WYWM is committed to providing a fulfilling and rewarding learning and research experience that enables students to achieve their full academic potential. This commitment is underpinned by an expectation that all members of the WYWM academic community will conduct themselves in a manner consistent with WYWM's values and guiding principles to maintain our strong tradition of excellence in learning, teaching and research, innovation and community engagement.

WYWM Responsibilities

This Code is underpinned by two primary objectives:

1. To provide a learning, teaching and research environment that enables students to achieve their full potential
2. To provide an academic experience for students consistent with the values and guiding principles.

Student’s expectations
Students are expected to:

● Participate in subjects in accordance with the requirements of students described in Subject Outlines and in this study guide.

● Read Subject Outlines and ensure that they are familiar with subject requirements.

● Participate fully in subjects and submit assignments by the due dates.

● Check Subject Outlines and other relevant sources to see whether their question has been answered, before contacting staff and asking individual questions.

● Use advertised consultation times to seek assistance from lecturers and tutors.

● Understand what plagiarism is, and how to avoid it.

● If any piece of work that is found to contain plagiarism, the student may be ineligible for marking and may earn the student a grade of ZERO for the subject. Should plagiarism be suspected, the student will be informed of appropriate investigative and possible disciplinary action.

Students have a right to expect:

● That course content will be up to date and based on research, study and academic discussion in the field.

● Feedback on their work and their performance will be provided in a timely manner.

● To have access throughout the session to lecturers, coordinators and general staff including access to teaching staff outside class times in accordance with consultation and contact information provided for each subject.

Integrity in academic work

Students are expected to:

- That course content will be up to date and based on research, study and academic discussion in the field.

- Not engage in plagiarism or other academic misconduct

- Conduct themselves in a manner conducive to the pursuit of academic excellence

- Actively participate in the learning process

- Submit assessment tasks by required dates and times, unless unforeseen or exceptional circumstances arise

- Behave ethically, avoiding any action or behaviour that would unfairly advantage or disadvantage either themselves or another student

- Ensure their academic activities are conducted safely and do not place others at risk of harm, including abiding by all ethics requirements in relation to that academic activity

- Be familiar with the programs and resources made available or recommended by WYWM to assist them in conducting their studies and research appropriately, including resources to help students avoid plagiarism and to comply with the ethics requirements of research

- Not behave in any way which impairs the reasonable freedom of other persons to pursue their studies, work or research or to participate in the life of the University.

Equity, respect and safety

Students are expected to:

- Treat all staff, other students, and visitors online with courtesy, tolerance and respect.
- Respect the rights of others to be treated equitably, free from all forms of unlawful discrimination, harassment and bullying
- Respect the rights of others to express political and religious views in a lawful manner
- Not engage in behaviour that is perceived to be threatening or intimidating or causes any person to fear for their personal safety or well-being
- Not engage in unlawful behaviour
- Not participate in any learning activity, such as, tutorials, laboratory classes, under the influence of alcohol or a prohibited substance.

Use of WYWM Course Forums

The WYWM Course Forums hosted on either the learning platform or externally established as a convenient means for WYWM students of the relevant course, course instructors and course mentors (invited by WYWM for that purpose) to share information to assist students successfully complete the Course.

All participants are required to conduct themselves on the Course Forums in accordance with their obligations set out in the in this document as well comply with any Terms and Conditions of usage for the platform used.

The Course Forums enable students to problem-solve technical issues, share understanding of course content, alert each other to interesting and relevant open source information relating to cyber security. Participants may also draw attention to industry-related events being held from time to time.

Collaboration and sharing information are important aspects of cyber security work and we encourage this. However, many people doing this course are doing so as part of a wider engagement with WYWM in order to start a new and fulfilling career. Often, they have not participated in academic training previously AND often, they have not been part of a jobs-network previously. This can sometimes lead to a misunderstanding of their academic obligations and sometimes the posting of well-meaning but misplaced career advice. Some problems include:

- **Plagiarism.** While helping one another with assignments such as the interpretation of questions, ideas for selecting topics and sharing useful information or links, is perfectly acceptable you must write and submit your own work.

- **Career Advice.** Often well-intentioned but rarely well-informed, such advice in a WYWM forum attracts credibility without any of the necessary professional underpinning and is therefore prohibited.

- **Jobs Board.** The Course Forums are not to be used as a de-facto jobs board. If you become aware of opportunities which might be suitable for course participants or graduates you are strongly encouraged to contact your instructors directly as WYWM has other processes better suited to such situations.