# COIT11241 *Cyber Security Technologies*
## Term 1 - 2023

Profile information current as at 02/05/2024 04:06 pm



## General Information

### Overview

Cyber security professionals need to create, analyse and test computer systems and networks to assure they will operate in the presence of attacks. In this unit, you will learn the types of attacks that may be encountered and the tools and techniques to prevent, detect and respond to those attacks. You will build your skills in virtualisation, cloud services and scripting to solve cyber security challenges. You will also learn special cyber security tools for detecting vulnerabilities, monitoring network traffic and responding to attacks.

### Details

Career Level: *Undergraduate*
Unit Level: *Level 1*
Credit Points: *6*
Student Contribution Band: *8*
Fraction of Full-Time Student Load: *0.125*

### Pre-requisites or Co-requisites

Pre-Requisites: COIT11238 Networked Infrastructure Foundations AND COIT11222 Programming Fundamentals.
Important note: Students enrolled in a subsequent unit who failed their pre-requisite unit, should drop the subsequent unit before the census date or within 10 working days of Fail grade notification. Students who do not drop the unit in this timeframe cannot later drop the unit without academic and financial liability. See details in the Assessment Policy and Procedure (Higher Education Coursework).

### Offerings For Term 1 - 2023

- Brisbane
- Cairns
- Melbourne
- Online
- Rockhampton
- Sydney
- Townsville

### Attendance Requirements

All on-campus students are expected to attend scheduled classes – in some units, these classes are identified as a mandatory (pass/fail) component and attendance is compulsory. International students, on a student visa, must maintain a full time study load and meet both attendance and academic progress requirements in each study period (satisfactory attendance for International students is defined as maintaining at least an 80% attendance record).

### Website

This unit has a website, within the Moodle system, which is available two weeks before the start of term. It is important that you visit your Moodle site throughout the term. Please visit Moodle for more information.

## Class and Assessment Overview

### Recommended Student Time Commitment

Each 6-credit Undergraduate unit at CQUniversity requires an overall time commitment of an average of 12.5 hours of study per week, making a total of 150 hours for the unit.

### Class Timetable

**Regional Campuses**
Bundaberg, Cairns, Emerald, Gladstone, Mackay, Rockhampton, Townsville

**Metropolitan Campuses**
Adelaide, Brisbane, Melbourne, Perth, Sydney

### Assessment Overview

1. **Online Quiz(zes)**
Weighting: 30%
2. **Portfolio**
Weighting: 50%
3. **Presentation**
Weighting: 20%

### Assessment Grading

This is a graded unit: your overall grade will be calculated from the marks or grades for each assessment task, based on the relative weightings shown in the table above. You must obtain an overall mark for the unit of at least 50%, or an overall grade of 'pass' in order to pass the unit. If any 'pass/fail' tasks are shown in the table above they must also be completed successfully ('pass' grade). You must also meet any minimum mark requirements specified for a particular assessment task, as detailed in the 'assessment task' section (note that in some instances, the minimum mark for a task may be greater than 50%). Consult the University's Grades and Results Policy for more details of interim results and final grades.

## CQUniversity Policies

**All University policies are available on the CQUniversity Policy site.**
You may wish to view these policies:

- Grades and Results Policy
- Assessment Policy and Procedure (Higher Education Coursework)
- Review of Grade Procedure
- Student Academic Integrity Policy and Procedure
- Monitoring Academic Progress (MAP) Policy and Procedure – Domestic Students
- Monitoring Academic Progress (MAP) Policy and Procedure – International Students
- Student Refund and Credit Balance Policy and Procedure
- Student Feedback – Compliments and Complaints Policy and Procedure
- Information and Communications Technology Acceptable Use Policy and Procedure

This list is not an exhaustive list of all University policies. The full list of University policies are available on the CQUniversity Policy site.

## Previous Student Feedback

### Feedback, Recommendations and Responses

Every unit is reviewed for enhancement each year. At the most recent review, the following staff and student feedback items were identified and recommendations were made.

#### Feedback from Student Reflections

**Feedback**
Students found there was too much assessment.

**Recommendation**
The assessments will be redeveloped.

#### Feedback from Teaching Team Reflections

**Feedback**
More real world exercises are required.

**Recommendation**
Materials will be developed to cover more advanced and more recent attacks.

## Unit Learning Outcomes

**On successful completion of this unit, you will be able to:**

1. Explain cyber security challenges and the technologies available to address those challenges
2. Apply cyber security tools to identify vulnerabilities and protect computer systems
3. Apply cloud services tools to automate common IT processes and task.

The Australian Computer Society (ACS) recognises the Skills Framework for the Information Age (SFIA). SFIA is adopted by organisations, governments and individuals in many countries and provides a widely used and consistent definition of ICT skills. SFIA is increasingly being used when developing job descriptions and role profiles. ACS members can use the tool MySFIA to build a skills profile.
This unit contributes to the following workplace skills as defined by SFIA 7 (the SFIA code is included)

- Information security (SCTY)
- Programming/software development (PROG)
- Security administration (SCAD)
- Penetration testing (PENT)

## Alignment of Learning Outcomes, Assessment and Graduate Attributes

— N/A Level  • Introductory Level  • Intermediate Level  • Graduate Level  ◦ Professional Level  ◦ Advanced Level

### Alignment of Assessment Tasks to Learning Outcomes

| Assessment Tasks | Learning Outcomes | | |
|---|---|---|---|
| | 1 | 2 | 3 |
| 1 - Online Quiz(zes) - 30% | | • | • |
| 2 - Portfolio - 50% | | • | • |
| 3 - Presentation - 20% | • | | |

## Alignment of Graduate Attributes to Learning Outcomes

| Graduate Attributes | Learning Outcomes | | |
|---|---|---|---|
| | 1 | 2 | 3 |
| 1 - Communication | • | | |
| 2 - Problem Solving | | • | • |
| 3 - Critical Thinking | • | • | • |
| 4 - Information Literacy | • | • | • |
| 5 - Team Work | • | | |
| 6 - Information Technology Competence | • | • | • |
| 7 - Cross Cultural Competence | | | |
| 8 - Ethical practice | | • | • |
| 9 - Social Innovation | | | |
| 10 - Aboriginal and Torres Strait Islander Cultures | | | |

## Alignment of Assessment Tasks to Graduate Attributes

| Assessment Tasks | Graduate Attributes | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 1 - Online Quiz(zes) - 30% | | • | • | • | | • | | • | | |
| 2 - Portfolio - 50% | | • | • | • | | • | | • | | |
| 3 - Presentation - 20% | • | | • | • | • | • | | | | |

# Textbooks and Resources

## Textbooks

**There are no required textbooks.**

## IT Resources

**You will need access to the following IT resources:**

- CQUniversity Student Email
- Internet
- Unit Website (Moodle)
- VirtualBox
- Suitable storage media, such as a removable USB 3.0 stick (≥128GB) for oncampus students without a laptop or as a fallback if you do not have enough harddrive space free
- A computer with hardware resources suitable to run multiple virtual machines simultaneously, e.g. 12GB RAM, 128GB HDD free, Intel core i5 or above, Windows 7 or later

## Referencing Style

All submissions for this unit must use the referencing style: Harvard (author-date)
For further information, see the Assessment Tasks.

## Teaching Contacts

**Jamie Shield** Unit Coordinator
j.shield@cqu.edu.au

## Schedule

**Week 1 - 06 Mar 2023**

| Module/Topic | Chapter | Events and Submissions/Topic |
|---|---|---|
| 1 Cybersecurity involves people, processes & ICTs | | |

**Week 2 - 13 Mar 2023**

| Module/Topic | Chapter | Events and Submissions/Topic |
|---|---|---|
| 2 Controls | | |

**Week 3 - 20 Mar 2023**

| Module/Topic | Chapter | Events and Submissions/Topic |
|---|---|---|
| 3 Threat intelligence | | A1 Quiz: PowerShell (8%) |

**Week 4 - 27 Mar 2023**

| Module/Topic | Chapter | Events and Submissions/Topic |
|---|---|---|
| 4 Vulnerabilities | | |

**Week 5 - 03 Apr 2023**

| Module/Topic | Chapter | Events and Submissions/Topic |
|---|---|---|
| 5 Monitoring | | A2 Portfolio: Controls (20%) |

**Vacation Week - 10 Apr 2023**

| Module/Topic | Chapter | Events and Submissions/Topic |
|---|---|---|

**Week 6 - 17 Apr 2023**

| Module/Topic | Chapter | Events and Submissions/Topic |
|---|---|---|
| 6 Risk | | |

**Week 7 - 24 Apr 2023**

| Module/Topic | Chapter | Events and Submissions/Topic |
|---|---|---|
| 7 Linux | | |

**Week 8 - 01 May 2023**

| Module/Topic | Chapter | Events and Submissions/Topic |
|---|---|---|
| 8 Attacks | | A1 Quiz: Bash (8%) |

**Week 9 - 08 May 2023**

| Module/Topic | Chapter | Events and Submissions/Topic |
|---|---|---|
| 9 Cloud | | A2 Portfolio: Attack (30%) |

**Week 10 - 15 May 2023**

| Module/Topic | Chapter | Events and Submissions/Topic |
|---|---|---|
| 10 Python | | |

**Week 11 - 22 May 2023**

| Module/Topic | Chapter | Events and Submissions/Topic |
|---|---|---|
| 11 Presentations (tutorial only) | | A3 Presentation (20%). You must present live in class to be eligible for full marks for Assignment 3. |

**Week 12 - 29 May 2023**

| Module/Topic | Chapter | Events and Submissions/Topic |
|---|---|---|
| No classes | | A1 Quiz: Review (14%) |

## Term Specific Information

Unit Coordinator: Jamie Shield, Cairns,
j.shield@cqu.edu.au,
Office: 07 4037 4750
You must present live in class during your Week 11 tutorial to be eligible for full marks for Assignment 3.

## Assessment Tasks

### 1 Quizzes

**Assessment Type**
Online Quiz(zes)

**Task Description**
There are three quizzes to encourage your ongoing engagement with the unit materials. You will be assessed on background concepts in cybersecurity, networking, ICT and computer security technologies, offensive types of cybersecurity technologies, and applying defensive cybersecurity technologies. The quizzes will involve short answer questions and activities such as writing shell commands. You might be required to download software to complete the quizzes. You may attempt the quiz(zes) as many times as you like until the due date.

**Number of Quizzes**
3

**Frequency of Quizzes**
Other

**Assessment Due Date**

Weeks 3, 8 and 12.

**Return Date to Students**

Immediate feedback

**Weighting**
30%

**Assessment Criteria**
This assessment consists of short answer questions and small activities. Each question will be marked according to the correctness of the answer.

- Quiz 1: PowerShell
- Quiz 2: Bash
- Quiz 3: Review

**Referencing Style**

- Harvard (author-date)

**Submission**
Online

**Submission Instructions**
Complete the quizzes on the unit website.

**Learning Outcomes Assessed**

- Apply cyber security tools to identify vulnerabilities and protect computer systems
- Apply cloud services tools to automate common IT processes and task.

**Graduate Attributes**

- Problem Solving
- Critical Thinking
- Information Literacy
- Information Technology Competence

- Ethical practice

## 2 Portfolio

**Assessment Type**
Portfolio

**Task Description**
You will create a portfolio to demonstrate that you can apply malicious and defensive cybersecurity technologies such as file integrity monitors and network scanners. You will be provided with an information system such as a small business network. You need to prepare the system to survive an imminent attack from a particular adversary. You will complete the following tasks:

- Defend: Prioritise, implement and test defensive cybersecurity technologies. This will involve tasks such as writing scripts to install and configure software features or network devices, for example, a DNS filter. You will also develop pre- and post-tests. For a DNS filter, your pre-test could demonstrate that a malicious domain name is resolved. Your post-test could demonstrate that the malicious domain name cannot be resolved. As you will run these tests live in your Assignment 3 presentation, you will develop automated test scripts.
- Attack: Improve the resilience of the system against the adversary. You will analyse threat intelligence, develop and run attacks on the system similar to those used by the adversary. You will then improve the detection of and mitigations and protections against the adversary. For example, threat intelligence might identify that the adversary attacks a particular application. You could first develop a test that demonstrates a successful exploit of the application. Subsequently, you could implement a protection and rerun the first test to demonstrate that the protection stops the exploit. As you will run these tests live in your Assignment 3 presentation, you will develop automated tests.

You will use cybersecurity standards and frameworks to inform the development of your portfolio, for example, to help you prioritise the defensive cybersecurity technologies to implement.
Optional Groupwork
You may work alone or in groups of up to 3 people for this assignment. All group members must be identified in the groupwork artefacts. All group members must submit via the unit website. You must inform the unit coordinator immediately if your group disbands. The moderation process might allocate group members different marks. Sharing of materials, for example, code, between groups is not permitted.
Repository
Create a private code repository and invite your tutor and the unit coordinator. One code repository is to be used by all group members.

**Assessment Due Date**

Weeks 5 and 9.

**Return Date to Students**

Feedback will be provided within 2 weeks of the due date.

**Weighting**
50%

**Assessment Criteria**
You will be marked on aspects such as adherence to cybersecurity standards and frameworks, use of threat intelligence, quality of implementation, configuration and testing scripts and other artefacts including functionality, modularity, style, reuse and documentation, lack of deprecated features, level of automation and use of code repository tools.

**Referencing Style**

- Harvard (author-date)

**Submission**
Online

**Submission Instructions**
Submit artefacts to both a private code repository and to the unit website. Submit a link to your private repository to the unit website. All group members must submit.

**Learning Outcomes Assessed**

- Apply cyber security tools to identify vulnerabilities and protect computer systems
- Apply cloud services tools to automate common IT processes and task.

**Graduate Attributes**

- Problem Solving
- Critical Thinking
- Information Literacy
- Information Technology Competence
- Ethical practice

## 3 Presentation

**Assessment Type**
Presentation

**Task Description**
In this assignment you will demonstrate, live, the information system you prepared in Assignment 2:

- Defend: You will run live tests to demonstrate the defensive cybersecurity technologies have been successfully implemented on the system. For example, for a DNS filter, you could run a pre-test that disables the DNS filter and shows that a malicious domain name is resolved. You could then run a post-test that enables the DNS filter and show that the malicious domain name is now longer resolved.
- Attack: You will run live attacks on the system and demonstrate the detection, mitigation or protections in action. You will demonstrate that the system is now more resilient against the adversary. For example, for an application exploit, you could run two tests – a pre-test that shows a successful attack against the system; and a second, post-test that shows that the attack is no longer successful after protections have been applied.

Optional Groupwork
You may work alone or in the same groups as Assignment 2. All group members must be identified in the groupwork artefacts. All group members must submit via the unit website. You must inform the unit coordinator immediately if your group disbands. Group members are marked individually on presentation criteria.

**Assessment Due Date**

Presentations are due in your Week 11 tutorial. PowerPoint slideshow (and video if you do not present in class) are due the end of Week 11.

**Return Date to Students**

Certification of Grades day

**Weighting**
20%

**Assessment Criteria**
You will be marked on aspects such as whether you present live or record a video, your stage presence and slideshow content and framing and the quality of the demonstration including the use of tools and evidence of the effectiveness of the implemented technologies as typically shown by the test cases.

**Referencing Style**

- Harvard (author-date)

**Submission**
Online

**Submission Instructions**
Submit PowerPoint slideshow and any evidence to the unit website. If you do not present in class, you should also submit a video of your presentation. You will not receive full marks if you do not present live in class. Submissions need to be less than 100Mb.

**Learning Outcomes Assessed**

- Explain cyber security challenges and the technologies available to address those challenges

**Graduate Attributes**

- Communication
- Critical Thinking
- Information Literacy
- Team Work
- Information Technology Competence

## Academic Integrity Statement

As a CQUniversity student you are expected to act honestly in all aspects of your academic work.

Any assessable work undertaken or submitted for review or assessment must be your own work. Assessable work is any type of work you do to meet the assessment requirements in the unit, including draft work submitted for review and feedback and final work to be assessed.

When you use the ideas, words or data of others in your assessment, you must thoroughly and clearly acknowledge the source of this information by using the correct referencing style for your unit. Using others' work without proper acknowledgement may be considered a form of intellectual dishonesty.

Participating honestly, respectfully, responsibly, and fairly in your university study ensures the CQUniversity qualification you earn will be valued as a true indication of your individual academic achievement and will continue to receive the respect and recognition it deserves.

As a student, you are responsible for reading and following CQUniversity's policies, including the **Student Academic Integrity Policy and Procedure**. This policy sets out CQUniversity's expectations of you to act with integrity, examples of academic integrity breaches to avoid, the processes used to address alleged breaches of academic integrity, and potential penalties.

**What is a breach of academic integrity?**
A breach of academic integrity includes but is not limited to plagiarism, self-plagiarism, collusion, cheating, contract cheating, and academic misconduct. The Student Academic Integrity Policy and Procedure defines what these terms mean and gives examples.

**Why is academic integrity important?**
A breach of academic integrity may result in one or more penalties, including suspension or even expulsion from the University. It can also have negative implications for student visas and future enrolment at CQUniversity or elsewhere. Students who engage in contract cheating also risk being blackmailed by contract cheating services.

**Where can I get assistance?**
For academic advice and guidance, the Academic Learning Centre (ALC) can support you in becoming confident in completing assessments with integrity and of high standard.

**What can you do to act with integrity?**

**Be Honest**
If your assessment task is done by someone else, it would be dishonest of you to claim it as your own

**Seek Help**
If you are not sure about how to cite or reference in essays, reports etc, then seek help from your lecturer, the library or the Academic Learning Centre (ALC)

**Produce Original Work**
Originality comes from your ability to read widely, think critically, and apply your gained knowledge to address a question or problem