|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Student Name |  | Student Number | |  |
| Unit Code/s & Name/s | VU23220 Develop and carry out a cyber security industry project  VU23221 Evaluate and test an incident response plan for an enterprise | | | |
| Cluster Name  *If applicable* | Incident Response Project | | | |
| Assessment Name | Incident Response Project Implementation Portfolio | Assessment Task No. | | 2 of 2 |
| Assessment Due Date | Week 15 | Date submitted | | / / |
| Assessor Name |  | | | |
| **Student Declaration:** I declare that this assessment is my own work. Any ideas and comments made by other people have been acknowledged as references. I understand that if this statement is false, it will be regarded as misconduct and subject to disciplinary action as outlined in the TAFE Queensland Student Rules. I understand that by emailing or submitting this assessment electronically, I agree to this Declaration in lieu of a written signature. | | | | |
| Student Signature |  | | Date | / / |
| **PRIVACY STATEMENT:** TAFE Queensland is collecting your personal information on this form for the purpose of assessment. In accordance with the Information Privacy Act 2009 (Qld), your personal information will only be accessed by staff employed by TAFE Queensland for the purposes of conducting assessment. Your information will not be provided to any other person or agency unless you have provided TAFE Queensland with permission, if authorised under our Privacy Policy (available at <https://tafeqld.edu.au/global/privacy-policy.html>) or disclosure is otherwise permitted or required by law. Your information will be stored securely. If you wish to access or correct any of your information, discuss how it has been managed or have a concern or complaint about the way the information has been collected, used, stored, or disclosed, please contact the TAFE Queensland Privacy Officer at [privacy@tafeqld.edu.au](mailto:privacy@tafeqld.edu.au) | | | | |

|  |  |
| --- | --- |
| **Instructions to Student** | **General Instructions:**  MidTown IT has assigned you to plan and oversee the implementation of an Incident Response Project for RightPoint. The task involves preparing an Incident Response Plan, establishing red, blue and purple teams, assigning tasks and responsibilities to team members, and assigning resources to the project. Risk assessment and evaluation are also part of the project. Your teacher/assessor will take on the role of the Project Sponsor assigned to this project by MidTown IT.  Read the project documentation provided and familiarise yourself with the Project Scenario or Case Study before proceeding with portfolio tasks. Confirm anything you need clarification about the project with your manager (teacher/assessor). You must clearly understand the scenario and tasks you need to complete.  This assessment instrument requires the student to complete a project portfolio that is divided into five parts:   * PART 1 Implement IRTx * PART 2 Evaluate IRTX * PART 3 Project Closure * PART 4 Prepare Presentation * PART 5 Present   **Storage Devices:**   * Students are required to provide their own storage devices.   **Materials Required:**   * Access to the Internet * Access to Connect (LMS) * Access to a virtual networking environment * Access to a virtual testing environment * Access to cyber testing tools * Access to Word processing software, such as Microsoft Word * Access to special-purpose tools, equipment and materials to complete the assessment.   **Online Delivery:**   * You are to supply their own PC or laptop and peripherals and internet access * You will require permission to install the required software * You will require access to Microsoft Office or a similar application   **Documentation:**   * RightPoint Scenario or Case Study * RightPoint Project Charter Template * RightPoint IRP * RightPoint Communications Plan Template   **Assessment Criteria:**  To achieve a satisfactory result, your assessor will look for your ability to demonstrate the following key skills/tasks/knowledge to an acceptable industry standard. Demonstrated ability to:   * Understand the components of a Cyber Security Operation Centre (CSOC) * Implement an incident response project * Execute red, blue and purple team activities as per the project plan * Test and verify the functionality of the project activities * Document the outcomes of an incident response exercise according to organisational requirements * Analyse and communicate the outcomes of the incident response exercise * Implement security improvements from experience gained in the incident response exercise * Evaluate the performance of red, blue and purple teams * Document experiences gained from the project implementation * Contribute to continuous improvement * Obtain project final signoff   Refer to the marking criteria for specific details:  VU23220\_VU23221\_AT1\_MC\_TQM\_V1  **Details of location:**  TAFE will provide a simulated work environment in the classroom. Research activities may be conducted in the classroom or at home.  If you are unable to attend a scheduled assessment activity, you must notify your teacher before the assessment is due and supply a doctor's certificate and approval from the team manager for an extension.  **Time restrictions:**  This assignment is designed to take place over 8 weeks or approximately 32 hours. The student is expected to attend classes as per timetable details and should be able to commit up to 3 hours per week of their own time to study or study related activities.  **Interactions:**  Teamwork skills are essential in the IT industry therefore you should work in teams to consult and collaborate on practical activities. However, each student must complete the assessment tasks individually (unless indicated).  **Level of assistance permitted:**  Staff cannot directly show students answers or solutions but support and guide them to complete tasks individually. Teachers and tutors should be available in class, and accessible by email for students working from home.  **Reasonable Adjustments:**  Reasonable adjustments are available to students for a variety of reasons, including: disability, language, literacy and numeracy (LLN) problems or extenuating circumstances. Talk to your teacher, counsellor or disability officer if you require extra support or an extension based on the conditions identified.  **Number of Attempts:**  You will receive up to two (2) attempts at this assessment task. Should your 1st attempt be unsatisfactory (U), your teacher will provide feedback and discuss the relevant sections / questions with you and will arrange a due date for the submission of your 2nd attempt. If your 2nd submission is unsatisfactory (U), or you fail to submit a 2nd attempt, you will receive an overall unsatisfactory result for this assessment task. Only one re-assessment attempt may be granted for each assessment task.  ***For more information, refer to the Student Rules.***  **Work, Health and Safety:**  The work environment should be assessed for safety prior to class. Special consideration should be taken regarding potential ICT related hazards such as tripping hazards, electromagnetic radiation, ergonomics, and posture. TAFE Queensland health and safety policies and procedures should be followed at all times. |
| **Submission details** | **Evidence Required to be Submitted:**  Insert your details on the cover page and sign the Student Declaration. Include this template with your submission.  **Submission via Connect:**  Upload a single file into Assessment 1 (AT1) Assignment Folder in Connect.  Multiple files can be compressed into a single file.  Name the file:  VU23220\_VU23221\_AT1\_Surname\_Student Number  TAFE Queensland Learning Management System (Connect)  **Accessing Connect:**  Connect URL: https://connect.tafeqld.edu.au/d2l/login  Username: 9 digit student number  Password: <your password>  For password reset go to: <https://passwordreset.tafeqld.edu.au/default.aspx> |
| **Instructions to Assessor** | **Specifications of assessment:**  To be judged competent in this assessment item the student is required to demonstrate competence in all indicators shown in the marking guide.  Gather evidence to demonstrate consistent performance in conditions that are safe and replicate the workplace. Noise levels, production flow, interruptions and time variances must be typical of those experienced in the cyber security field of work and include access to:   * project requirements   Ensure that students read and familiarise themselves with the Project Scenario provided and relevant files and/or resources before attempting the assessment.  **Level of Assistance Permitted:**  Teachers and tutors should be available in class, and accessible by email for students working from home. Staff cannot directly show students answers but support and guide them to complete tasks individually. Students with disability will receive reasonable adjustments.  **Interactions:**  Teamwork skills are essential in the IT industry therefore you should work in teams to consult and collaborate on practical activities. However, each student must complete the assessment tasks individually (unless indicated).  **Contingencies:**  Reasonable adjustment is available to students for a variety of reasons, including: disability, language, literacy and numeracy (LLN) problems or extenuating circumstances.  **Work, Health and Safety:**  The work environment should be assessed for safety prior to class. Special consideration should be taken regarding potential ICT related hazards such as tripping hazards, electromagnetic radiation, ergonomics, and posture. TAFE Queensland health and safety policies and procedures should be followed at all times. |
| **Note to Student** | An overview of all Assessment Tasks relevant to this unit is located in the Unit Study Guide.  If you have any question or need help regarding this assessment item please contact your teacher/tutor through email or during face-to-face sessions. |

# PART 1 Implementing IRTx

**Team Briefings**

This task is to be carried out at the first session at least 1 week before running the IRTx.

The purpose of this task is to:

* Create team match-ups (see grid below for suggestions)
* Exchange Blue Team Playbooks and Rules of Engagement
* Q & A

Teams must respond professionally to questions and suggestions during the team briefing.

### **IRTx Sessions Table**

|  |  |  |
| --- | --- | --- |
| **IRTx**  **Session (Seq 7)** | **Team 1** | **Team 2** |
| **1** | Red Team | Blue Team |
| **2** | Blue Team | Red Team |

**IRTx Week**

1.1 This task is about setting up and running the IRTx:

1. Set up and configure the virtual network according to the IRTx plan
2. The Red Team starts the attacks according to the Red Team runbook (This should start at least 1 hour before the Blue Team arrives. If possible, the Red Team could start the attack sequence up to a week before the exercise if all requirements re: VMs etc., are met.)
3. Blue Team begins analysing logs/data to determine if the incident has occurred. The Observer (Purple) Team can begin to inject manual incidents.
4. The Blue Team follows the process as outlined in the Blue Team Playbook from the IRP.
5. The Observer (Purple) Team monitors the Blue Team’s response handling and performance according to the Observer’s Checklist.

1.2 When completing the task you must ensure that:

1. The end to end functionality of the virtual network has been verified. Screenshot of ping results to be included in final submission.
2. The Red Team uses attacks/intrusions as specified in Red Team runbook. Attacks need not to be successful.
3. Blue Team determines that reconnaissance and scanning has taken place, using the Blue Team playbook.

* Follows the IRP for handling this event
* Follows the IRP for events/incidents manually injected by the Observer (Purple) Team

1. The Observer (Purple) Team checklist is used to record items such as:

* How the event/incident was responded to in accordance with the IRP
* Time taken to report the event/incident

1. What was reported - effectiveness of communication(s)

# PART 2 Evaluate the IRTx

This task is about evaluating the effectiveness of the exercise. It requires each team member to meet and discuss the IRTx.

2.1 Each team is to host a round table discussion with the other teams involved in the IRTx. This discussion is to cover the following topics:

1. What improvements can be made to the incident response plan?

The Playbooks could be made easier to follow and not be as vague as they were.

1. How well did the Blue Team strategy work in identifying events/incidents?

All incidents were successfully detected using the created alerts and by following the runbook

1. How effective was the use of the IRTx as a method of evaluating and testing the IRP

It was an effective way of testing the IRP as both red and blue playbooks were tested completely

1. How effective was the communication between team members?

There was constant communication between all present team members throughout the exercise.

1. How effective was the communication between team members and stakeholders?

Communication with the stakeholders was also constant as the stakeholders were kept up to date on the status of both the blue and red team.

1. Any other feedback to improve the IRTx

Clearer runbooks.

2.2 From the round table discussion, each team will write an Exercise Closure Report using the feedback from the round table discussion on your team’s IRTx

You must follow the guidelines below:

* The report must not exceed five (5) pages
* The report must have the following headings:
  + Overview - Provide a brief overview of the purpose of the exercise and a summary of results
* Review of the effectiveness of the Incident/Event Identification Strategy
  + Blue Team strategy is outlined
  + Summarise results of Incident/event identification
  + Review effectiveness of strategy
  + Review to be consistent with observer team report
  + Review of effectiveness of communication between team roles
* The review of the communications between Blue Team members during the exercise is summarised
* Review for consistency with Observer Team report
  + Lessons Learned
* What went right
  + At least three (3) actions that the team got right during the exercise
* What went wrong
  + At least three (3) issues/problems or actions that did not go as planned.
* Recommended improvements
  + At least three (3) recommendations to improve the effectiveness of the IRTx are listed and described
* Appendix
* Observer Team Report

2.3 All team members have contributed to the report and each team member’s contribution must be referenced in the appendix

# PART 3 Project Closure

3.1 Performance of the Project Management Team

This is a short section that:

* Reviews the team’s performance against the objective of developing an Incident Response Team Exercise
* Validates the team objectives against the project targets
* Proposes changes/improvements to the project development process
* Recognises the achievements of individual team members

3.2 Project Management Closure

This section includes the following:

* Project timeframes, scope, and quality expectations are evaluated against actual performance
* Review project risk strategy and recommended improvements
* Reviews performance against a minimum of three (3) objectives
* Proposes a minimum of three (3) changes/improvements
* Discusses the need for end-user training and provide a brief plan to train the end users
* Shows the difference between when tasks were planned to be completed and when they were actually completed, using a graph or other visualisation
* A project sign-off checklist for the project sponsor (teacher) to sign.
* Final project sign-off (all tasks completed according to the Marking Criteria)

# Part 4 Preparing the presentation

4.1 The team is to prepare the presentation outlining the lessons learnt and the experience gained during the development and implementation of the project plan.

The presentation is to be a team presentation and include the following sections:

1. Welcome and explanation of goals/objective of the presentation (Why are we here?)
2. Overview of the project plan
3. Lessons learnt – each team member to present their own lessons learnt
4. Summary of what the team has learnt and what they feel they can improve on.
5. Wrap-up and thank you

4.2 The team shall prepare and submit a presentation plan that:

1. Identifies the audience and clarifies the purpose of the presentation
2. Outlines the structure and flow/sequence of the presentation
3. Identifies the media sources, such as images, graphs, videos, and presentation templates to be used.

* 4.3 When completing the presentation preparation, you must observe the following:

1. The presentation plan will not exceed two (2) pages
2. The presentation is to be no longer than 15 minutes
3. Each team member must present their Lessons Learned section plus at least 1 other section of the presentation
4. Each team member will use the same template, slide structure, and format
5. Provide a brief overview of the project
6. Each team member to present two (2) good experiences and two (2) non-favourable experiences
7. Each team member to present two (2) lessons learned from the project

# Part 5 Present

5.1 For this task, the team members must present the presentation as prepared and ensure that:

* 1. Each team member presented the lessons learnt, and one (1) other section
  2. Presenter used appropriate language
  3. Presentation material was appropriate for the purpose
  4. Team members responded to questions in an appropriate manner
  5. Length of presentation was 15 minutes (12 – 20 minutes is acceptable)
  6. Presentation was structured and organised

# Deliverables

1. IRTx closure report (max five pages)
2. Project Closure Report (max three pages)
3. Presentation slides (max ten slides)

# Documentation requirements are as follows:

* Written report format is appropriate
* Document is logically organised
* Written language is appropriate for to the communication purpose
* Each team member has signed the report
* Reports submitted on time

**End of Assessment**