  
Student Assignment Brief

**This document is intended for Coventry University Group students for their own use in completing their assessed work for this module. It must not be passed to third parties or posted on any website. If you require this document in an alternative format, please contact your Module Leader.**

# Contents:

* [Assignment Information](#_Assignment_Information_1)
* [Assignment Task](#_Assignment_Task_1)
* [Marking and Feedback](#_Marking_and_Feedback_1)
* [Assessed Module Learning Outcomes](#_Module_Learning_Outcomes)
* [Assignment Support and Academic Integrity](#_Assignment_Support_and_1)
* [Assessment Marking Criteria](#_Assessment_Marking_Criteria)

The work you submit for this assignment must be your own independent work, or in the case of a group assignment your own groups’ work. More information is available in the ‘[Assignment Task](#_Assignment_Task)’ section of this assignment brief.

# Assignment Information

**Module Name:** Incident Response

**Module Code:** 7025CEM

**Assignment Title: Coursework**

**Assignment Due: 04/08/2025 18:00** UK Time

**Assignment Credit:** 15 credits

**Word Count (or equivalent):** 3300 words +/- 10%

**Assignment Type:** Coursework

**Percentage Grade** (Applied Core Assessment). You will be provided with an overall grade between 0% and 100%. You have one opportunity to pass the assignment at or above 40%.

# Assignment Task

**Coursework Motivation**

This coursework is designed to assess your research and analytical abilities. Often, in the course of your career, you will find that you are faced with new technologies and concepts. Such situations will require you to conduct research and investigation to evaluate new tools and techniques. This requires a degree of independence of thought and building confidence in new approaches based on technical design. Your analytical abilities will be called into question almost daily and you will often be faced with challenges under economic, social, legal and ethical constraints.

**Writing Guidance**

This coursework requires you to answer ALL questions. The questions should be answered in the given order in a single report. You do not need to provide an abstract.

Be clear and precise with the use of terminology. So, for example, terms such as data, traffic, packets, messages and information are often used interchangeably. Note that these are different terms and convey different meaning in different contexts.

It is highly recommended that you read the questions carefully before answering. Illustrations are encouraged but should be clearly labelled and relevant to use. Otherwise, it may not help clarity and cause confusion.

**Client Network**

The network, shown in Figure 1, represents a client network that you are called to handle. Your role, as a network security evaluation specialist, is to help the client design and build an effective evaluation and monitoring solution. Your client has specific requirements that need to be met and expects you to address some of the technical and legal challenges involved. The client owns all the data created, processed, stored and communicated on the networked systems, some of which is sensitive.

The network is designed such that various services are spread out on server farms. The three server farms host server nodes via respective gateway nodes numbered 3,4 and 5. Gateway nodes 8-13 connect to client nodes (several hundred) distributed across subnets.

The nature of service traffic is a combination of web services (for external customer enquiries and ecommerce), and various application services for use within the organisation. Some of the services need to be accessible from the outside world.

The nodes are diverse in their configuration and with different levels of access to services and the outside world (internet) which is accessible by gateway node 0. Nodes 1, 2, 6 and 7 serve for the purpose of intermediary routing within the network. Nodes 14 and 15 are a series of APs providing WiFi networking to the offices.

A diagram of a network

Description automatically generated

Figure 1. Network diagram

The client is involved in innovation and product development within the defence and security sector serving clients ranging from government departments, multinational firms and foreign agencies. The nature of activity lends itself to sabotage and intellectual property theft. The collaborative nature of the organisation also means that it hosts development teams from other partners from a variety of countries.

Your role has specific deliverables and you are asked to prioritise the activities (set out in the questions) detailed below. You have a few weeks to present a report to the technical leadership of the client on these matters.

For the sake of consistency, in your answers, specific locations should be referred to by the labels used above. It would be wise to label and help clarify particular locations that you refer to including particular interfaces on the firewall, routers (as there are multiple), links between routers and switches and so on.

If you need to make any assumptions in addition to the brief given above, (e.g. any particular security software or hardware already deployed on the network, or what services are running on a particular subnet), you should clearly specify these in a section called ‘Assumptions’ at the beginning of your report. The assumptions section does not count toward the word limit.

**Assignment**

**Question 1: Detecting reconnaissance (*25 Marks, 1000 words)***

The client is particularly vulnerable to insider attacks including sabotage (disruption and destruction) and espionage (stealing sensitive information). To detect any such attacks, it is important that the client has effective measures in place.

You are asked to evaluate the level of exposure for servers from insiders. Of particular interest here is network reconnaissance (scanning and enumeration) activity that originates internally.

* Briefly explain *how potential intruders (insider of the network) can collect and use reconnaissance data for malicious purposes*?
* Describe *what data would you prefer to collect and at what points on the network?* You are expected to adopt a systematic approach where you justify why are you collecting the various types of data and where?
* To support the above activity, *what tools would you use and what type of activity would you configure to detect?* Your answer is expected to prescribe tools that the client may wish to use and adopt in the future. Your client would appreciate suggestions for configuration of such tools to assist in efficient collection, logging and analysis of data collected.
* This is a high volume network and parts of it get very busy at peak times. Any activity of collecting traffic from the network would be a challenge. In the context of above activity, *discuss relevant strategies to help overcome the problem of scale.*

**Question 2: Session Data collection (*15 Mark, 500 words)***

Alert data and session data are two types of NSM data of standard form that is collected over networks. Discuss both forms of data briefly and present a justification for the collection of each. How could each type help you understand whether potential intrusion is taking place?

In Figure 1 identify three locations of strategic interest for collecting session data. Justify your choice. Describe what tools and configuration you will use for collection.

**Question 3: Splunk or Elastic stack? (*15 Marks, 500 words)***

A senior security analyst on the client site is considering deploying a separate solution for insider threat detection and automated response. She has asked you for advice on the choice between Splunk and Elastic stack solutions. They are both widely known products available for deployment as SIEM as well as XDR/SOAR and more.

Use your research skills to help the colleague make an informed decision. *Find out more about both solutions. What detection and automated response capabilities do they offer? Both come with high recommendations from the security community. What makes them a popular choice?* Your answer should facilitate a clear decision.

**Question 4: Incident Response (20 Marks, 600 words)**

The SOC team has detected and confirmed an incident with the following events been initially correlated: a suspicious out-of-office-hours activity (incl. external flash drive attached) on a workstation connected to gateway 10; opening of a large number of files on a file server connected to gateway 9; and a large volume of traffic between the workstation and a DB server connected to gateway 5. Based on the advice you provided in Question 1 which of the data that has been collected will be relevant to this case, and what evidence do you expect to derive from there?

This is an ongoing incident and as part of the Incident Response you have been asked to provide advice on whether they need to start collecting any additional data, if so what type and from where (both network-based as well as from end-points) – this is in addition to the advice you provided in Question 1. The approach you advise should be forensically sound so that any evidence collected can be used in court.

**Question 5: Advanced persistent threats (APTs), (15 Marks, 400 words)**

After devising your monitoring solution, you are asked to demonstrate how effective it is. Consider the following three issues:

* What kind of testing would you recommend in order to determine if the system is working accordingly to specifications and goal? *Explain types of tests to be performed, who should conduct them, where, and when.*
* Are there any concerns that the company should think of with respect to the qualifications of the testers? *Review through the kind of certification, knowledge base and toolset experience you would look for to ensure that the testers are up to the job.*
* APT attacks are an increasing threat. What mechanisms of your proposed monitoring system would address these particular threats? *Give some description of the kind of APT behaviour you may observe and how your monitoring deployment could detect or prevent it.*

**Question 6: Cost effectiveness (10 marks, 300 words)**

Security, be it in terms of equipment, human effort or inconvenience, has a cost. Fact! Security, therefore, involves trade-offs. Another fact!

Your recommendations, in your answers for questions 1, 2, 3 and 5, entail significant costs in terms of:

1. a)  *equipment*, including hardware, software and training resources,
2. b)  *human*, including manual configuration and steering of monitoring operations, and training, and
3. c)  *Inconvenience*, in terms of disruption to normal operations.

Present a *brief justification of these costs*. For each category, *describe the benefit your client receives for the investment made*.

### Submission Instructions:

Submit the coursework by the due date using the link on Aula.

Your assignment should be submitted as a single document (i.e., Word, PDF or Markdown).

If you make use of additional materials (such as GitHub, or supporting videos) you should include a clear link to the supporting material in your report.

**Important:** In the case of GitHub repositories, they should be set to **private, with** the relevant **teaching staff added as collaborators.** Having a publicly available repository could lead to an academic misconduct case being raised against you, as people have been known to steal work from other student's repos.

Late submissions will be awarded 0 marks. If you have a genuine reason for needing to submit late, you can request an extension from faculty registry.

# Marking and Feedback

**How will my assignment be marked?**

Your assignment will be marked by the course team.

**How will I receive my grades and feedback?**

Provisional marks will be released via Aula

Feedback will be provided by the module team alongside grades release

You will access the feedback via Aula on the Turnitin platform.

Your provisional marks and feedback should be available within 2 Weeks

**What will I be marked against?**

Details of the marking criteria for this task can be found at the [bottom of this assignment brief](#Marking_Rubric).

# Assessed Module Learning Outcomes

The Learning Outcomes for this module align to the [marking criteria](#Marking_Rubric) which can be found at the end of this brief. Ensure you understand the marking criteria to ensure successful achievement of the assessment task. The following module learning outcomes are assessed in this task:

1. Critical awareness of the legal, ethical and professional issues involved in incident response investigation.
2. Evaluate and apply appropriate technological solutions and processes in the detection, management and investigation of information and system security incidents.
3. Critically evaluate and apply digital forensic methodology to cyber security incidents and commercial investigation; establish an audit trail, documenting a digital investigation from a legal and professional perspective.
4. Ensure all actions undertaken are Association of Chief Police Officers (ACPO) Principles of Digital Evidence compliant.

# Assignment Support and Academic Integrity

If you have any questions about this assignment, please see the [Student Guidance on Coursework](https://share.coventry.ac.uk/students/Registry/Pages/Coursework.aspx) for more information.

### Spelling, Punctuation, and Grammar:

You are expected to use effective, accurate, and appropriate language within this assessment task.

### Academic Integrity:

The work you submit must be your own, or in the case of groupwork, that of your group. All sources of information need to be acknowledged and attributed; therefore, you must provide references for all sources of information and acknowledge any tools used in the production of your work, including Artificial Intelligence (AI). We use detection software and make routine checks for evidence of academic misconduct.

Definitions of academic misconduct, including plagiarism, self-plagiarism, and collusion can be found [on the Student Portal](https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fshare.coventry.ac.uk%2Fstudents%2FRegistry%2FPages%2FEssential-definitions.aspx&data=05%7C01%7Cab5576%40coventry.ac.uk%7C96dc42ffe3484dd999e808db0e964c5d%7C4b18ab9a37654abeac7c0e0d398afd4f%7C0%7C0%7C638119810903032146%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=%2FggkmIN9ZackqogiKZxEXKYD3QaXAk0jCME%2F1ne82YU%3D&reserved=0). All cases of suspected academic misconduct are referred for investigation, the outcomes of which can have profound consequences to your studies. For more information on academic integrity please visit the [Academic and Research Integrity](https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fshare.coventry.ac.uk%2Fstudents%2FRegistry%2FPages%2FAcademic-and-Research-Integrity.aspx&data=05%7C01%7Cab5576%40coventry.ac.uk%7C96dc42ffe3484dd999e808db0e964c5d%7C4b18ab9a37654abeac7c0e0d398afd4f%7C0%7C0%7C638119810903032146%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=%2BPYuaO%2FDqY2x3ajLRlKjxHoEvTPzEqm%2B8wuQ%2FMvxlZk%3D&reserved=0) section of the Student Portal.

### Support for Students with Disabilities or Additional Needs:

If you have a disability, long-term health condition, specific learning difference, mental health diagnosis or symptoms and have discussed your support needs with health and wellbeing you may be able to access support that will help with your studies.

If you feel you may benefit from additional support, but have not disclosed a disability to the University, or have disclosed but are yet to discuss your support needs it is important to let us know so we can provide the right support for your circumstances. Visit [the Student Portal](https://livecoventryac.sharepoint.com/sites/students-healthandwellbeing/SitePages/Disabilities.aspx) to find out more.

### Unable to Submit on Time?

The University wants you to do your best. However, we know that sometimes events happen which mean that you cannot submit your assessment by the deadline or sit a scheduled exam. If you think this might be the case, guidance on understanding what counts as an extenuating circumstance, and how to apply is [available on the Student Portal.](https://livecoventryac.sharepoint.com/sites/students-registry-extensions-deferrals/SitePages/CU-Extensions-and-Deferrals-Guidance.aspx)

# 

# Administration of Assessment

**Module Leader Name:** Antal Goldschmidt

**Module Leader Email:** [**ab2216@coventry.ac.uk**](mailto:ab2216@coventry.ac.uk)

**Assignment Category:** Coursework

**Attempt Type:** Main Sit

**Component Code:** CW

## Assessment Marking Criteria

**Mark allocation guidelines to students (to be edited by staff per assessment)**

**70%+ Excellent**

(A mark above 80% indicates an exceptional piece of work that excels in every respect of the following criteria)

The overall report is clearly written, with accessible language and demonstrably within the word limit. All questions are attempted, for which the answers are in the order listed and the logical arguments are coherent.

Excellent use of relevant evidence to support the technical design choices made and their comparative analysis. This is accompanied by evidence of independent research for every question. The legal and ethical aspects of using monitoring technology are clearly recognised and sensibly expressed. The need for human resource training is also recognised and appropriate sources for training are identified. Question 6, which requires well-judged commentary, is well attempted and opinions are carefully expressed with regards to each aspect identified in the coursework. Overall, there is comprehensive examination of the chosen monitoring, sensor placement and data collection methodologies, and the assumptions underlying them. All sources are correctly cited in a recognised format. Irrelevant material is excluded.

The report demonstrates the ability of the student to think independently, originally and critically.

**60-69% Very Good**

A clear attempt has been made to ensure that the overall report is written clearly, with generally good language and demonstrably within the word limit. All questions are attempted, for which the answers are in the order listed and the logical arguments are mostly coherent.

Good use of relevant evidence to support the technical design choices made and their comparative analysis. There is evidence of independent research for most questions. The legal and ethical aspects of using monitoring technology are identifiably recognised and expressed. The need for human resource training is also recognised and some sources for training are identified. Question 6, which requires well-judged commentary, is attempted with some clear opinions expressed with regards to each aspect identified in the coursework. Overall, there is good examination of the chosen monitoring, sensor placement and data collection methodologies, and the assumptions underlying them. All sources are correctly cited in a recognised format .

The report demonstrates some ability of the student to think independently, originally and critically.

**50-59% Satisfactory to Good**

An attempt has been made to ensure that the overall report is written clearly and demonstrably within the word limit. All questions are attempted, for which the answers are in the order listed and logical arguments are attempted.

General use of relevant evidence to support the technical design choices made and their comparative analysis. There is some evidence of independent research for questions. At least some legal and ethical aspects of using monitoring technology are recognised and expressed. The need for human resource training is recognised and at least a few sources for training are identified. Question 6, which requires well-judged commentary, is attempted with some opinion expressed with regards to some of the aspects identified in the coursework. Overall, there is some examination of the chosen monitoring, sensor placement and data collection methodologies, and the assumptions underlying them. At least some sources are cited and attempted so in a recognised format.

The report presents some evidence that the student has attempted independent and original thinking.

**40-49% Pass**

An attempt has been made to ensure that the most parts of the report are legibly written and with most answers within the word limit. Most questions are attempted, answers for which are in labelled order and arguments are present.

Some use of relevant evidence to support the technical design choices made and their comparative analysis. There is some evidence of research for questions. Some knowledge of legal or ethical aspects is present. The need for human resource training is recognised and some supporting argument made. Question 6 is addressed with some attempted commentary. Overall, there is acknowledgment of some of the chosen monitoring, sensor placement and data collection methodologies, and the assumptions underlying them. Some sources are cited and attempted so in a recognised format.

The report presents some evidence of effort put in by the student towards a thought process for the assessment.

**0-39% Fail**

No attempt has been made to ensure that at least some parts of the report are legibly written, with answers not attempted within the word limit. Three or less questions are attempted, answers for which are not in order.

There is no evidence of support for any technical design choices made. Legal or ethical aspects are entirely ignored. The need for human resource training is recognised and some supporting argument made. Question 6 is not addressed, or no coherent arguments are presented. Overall, there is no identifiable evidence of any monitoring, sensor placement or data collection methodologies. No references are presented.

The report presents very little or no evidence of logical effort or thought process towards any of the six questions.