

## COS30015 IT Security

### Lab 10 week 10 Answer

You will need:  
Lab Computer  
Assignment 2 file: Part  
B Incident Situational  
Report.docx  
Lab 10 SITREP Template.docx

This lab is essential preparation for your second technical assignment. It relates to part B, writing up your forensic findings in a situational report.

A situational report (sitrep) is a report provided to decision makers to give them a quick understanding of situation. Often, they are pre-defined templates an organisation has and specific information is entered into the required section. They form essential communications to keep key stakeholders informed of developments.

### Task 1 Compare Situational Reports

View the sitrep template provided by the Australian Cyber Security Centre (ACSC) on page 37 from this link:

[https://www.cyber.gov.au/sites/default/files/2023-03/ACSC%20Cyber%20Incident%20Response%20Plan%20Guidance\\_A4.pdf](https://www.cyber.gov.au/sites/default/files/2023-03/ACSC%20Cyber%20Incident%20Response%20Plan%20Guidance_A4.pdf)

Consider each field from *Date and Time incident detected* to *Date and Time of next update*. Compare the ACSC template with Assignment 2 file titled *Part B Incident Situational Report.docx*, and answer the following question:

#### 1. What are the main differences between these two sitreps?

- ACSC provides a general update across key information areas
- Part B has focus on understanding technical elements identified
- Likely Part B is for a technical audience

### Task 2 Identify incident information

Threat advisories are provided by many different stakeholders, often these are released by government agencies and cyber security vendors. They document an incident or campaign attributed to a given threat actor. While not all the same, they often document what occurred, provide information regarding indicators of compromise and tactics, techniques and procedures demonstrated by the threat actor.

A good sources for advisories can be found at the following link:

ACSC: <https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories>  
Scroll down to All alerts and advisories

## All alerts and advisories



Type 

Chose the type of advisory

## All alerts and advisories



Advisory 

A range of threat advisories are provided outlining threat actor campaigns.

Other advisories can be found at:

CISA: <https://www.cisa.gov/news-events/cybersecurity-advisories>

Filter the advisory type as follows:

### Advisory Type

- ☐ Alert
- ☐ Analysis Report
- ☒ Cybersecurity Advisory
- ☐ ICS Advisory
- ☐ ICS Medical Advisory
- ☐ ICS Alert

Browse these advisories and choose one which interests you and contains a decent amount of information (avoid a page or two advisories). This advisory will be used to fill out a sitrep, so select well.

### 1. Which advisory did you select?

- Student to enter their chosen link

This advisory forms part of the picture. Consider investigating other sources across the Internet. Often security vendors provide advisories also. The following is an example link to Mandiant's blog: <https://www.mandiant.com/resources/blog>

You may also find information on news websites and across the Internet in general.

**2. What other resources can you find about the threat you have been investigating**

- Student to enter their chosen links

**Task 3 Write up your SITREP**

With your collected information, it is time to take all the different knowledge and populate your SITREP template for Lab 10. You should be factual, concise but also informative with your writing.

Your sitrep will also be for a manager or executive, so make sure you are not technical where you don't need to be (*Hint*, IoC and TTPs are technical areas).

- 1. Take your resources and write up your sitrep**
- 2. Be concise, clear, informative with your information**
- 3. Don't be overly technical where you don't need to be**