**Swinburne University of Technology Hawthorn Campus   
Department of Computing Technologies**

**COS30015 IT Security**

Assignment 2 - *Semester 2, 2024*

# Part B Incident Situational Report

**Due Date**: AEST 23:59 on 31/10/2024.

Having investigated all the artefacts provided by STARFLEET, they have requested a situation report update to understand the incident.

Compute the following template with your findings from your investigation.

|  |  |  |
| --- | --- | --- |
| **STARFLEET SITREP** | | |
| **Impacted STARFLEET Accounts** | **Student & Student ID** |  |
| <list all user accounts impacted in the incident> | **Class** |  |
| **Tutor** |  |
| **Incident Timeline** | **Impacted STARFLEET Hosts** | |
| <provide an incident timeline> | <provide a list of hosts/assets impacted and the perceived severity of this host being compromised> | |
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
| **IoCs Observed** | **TTPs Observed** | |
| <list all IoCs observed>  e.g. - Malware Payload hash - SHA256: AAABB…. | <list all TTPs observed> | |
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
| **Remediation Advice** | | |
| <provide remediation advice for how STARFLEET should secure their systems given the TTPs observed> | | |
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|