|  |  |  |
| --- | --- | --- |
| **SITREP** | | |
| **Incident Reference** | **Student ID** |  |
| <link your chosen threat advisory> | **Class** |  |
| **Tutor** |  |
| **Incident Summary** | | |
| Provide a summary of the incident as best you can from open source resources  Consider the following talking points:   * Timeline of events * Extent of the compromise * Dwell time * What is understood of the adversary   You are not limited to these points only, consider what else you might like to convey to a manager or executive. | | |
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
| **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 to mitigate against the TTPs observed> | | |
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|