# Incident management - Post incident review template

The following template aims to help entities complete their post incident review.

The review should provide a comprehensive summary of all actions and decisions made during the incident response.

The post incident review should include specific and actionable changes to existing processes, procedures, ICT, systems, and policies to increase efficiency in future incident response incidents.

|  |  |  |
| --- | --- | --- |
| **Post incident review owner** | | <First name, Last name> |
| **Detection time** | | <DD/MM/YYYY><HH:MM> UTC |
| **Detection method** | | <Agency report, alert, etc> |
| **Service restoration time** | | <Time> |
| **BIL Impact** | | <Low, Med, High> |
| **Attack vector** | ***Threat action*** |  |
| ***Enumeration*** |  |
| **Executive summary** | | |
|  | | |

#### Impact Assessment

|  |  |  |  |
| --- | --- | --- | --- |
| **Systems impacted?** | Yes/No | ***If yes, list*** | <System type(s), number> |
| **Data impacted?** | Yes/No | ***If yes, list*** | <Data type(s), sensitivity, amount> |
| **Network impacted?** | Yes/No | ***If yes, describe*** | <Downtime, etc> |
| **Other impacts?** | <i.e., financial, reputation, etc> | | |

#### Cause analysis

|  |  |
| --- | --- |
| **Incident leadup** |  |
| **Root cause** |  |
| **Contributing factors** |  |
| **Incident recurrence** |  |

#### Incident response evaluation

|  |  |  |  |
| --- | --- | --- | --- |
| **Was the playbook effective?** | Yes/No | *If no, detail* |  |
| **Was internal or external communication effective?** | Yes/No | *If no, detail* |  |
| **What created a positive impact to the incident?** | <Detail i.e., actions, technical, or organisational factors> | | |
| **What challenges were noted?** | <Detail i.e., actions, technical, or organisational factors> | | |
| **Lessons learned** | | | |
|  | | | |

#### Action items

|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **Action item(s)** | **Owner** | **Ticket number (if applicable)** |
| *1* |  |  |  |
| *2* |  |  |  |
| *3* |  |  |  |
| *4* |  |  |  |
| *5* |  |  |  |
| *6* |  |  |  |
| *7* |  |  |  |
| *8* |  |  |  |
| *9* |  |  |  |
| *10* |  |  |  |
| *11* |  |  |  |
| *12* |  |  |  |
| *13* |  |  |  |
| *14* |  |  |  |
| *15* |  |  |  |
| *16* |  |  |  |
| *17* |  |  |  |
| *18* |  |  |  |
| *19* |  |  |  |
| *20* |  |  |  |
| *21* |  |  |  |
| *22* |  |  |  |
| *23* |  |  |  |
| *24* |  |  |  |
| *25* |  |  |  |
| *26* |  |  |  |

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Attack vector | Note the threat action and enumeration per the VERIS framework classifications.  I.e., Threat action: social, enumeration: phishing |
| Contributing factors | Examine and record the elements that either directly led to the incident or exacerbated its effects, such as procedural mistakes which may leave a system uncontained, allowing the incident to spread. |
| Executive summary | Craft a succinct overview of the incident, including the nature of the Write a summary of the incident in a few sentences. Include the nature and reasons of the incident, along with level of severity and duration of impact. |
| Incident recurrence | Assess whether past incidents share a similar root cause. If it is noted, document the mitigation that was attempted in the previous incidents and determine why this incident occurred again. |
| Leadup | Describe the sequence of events that led to the incident. For example, previous changes to a system that introduced vulnerabilities or a system remaining unpatched for a vulnerability. |
| Lessons learned | Reflect on the incident response process, noting the strengths and weaknesses experiences. Identify areas of improvement. Such as:   * Create detections the attack IOCs and TTPs. * Heighten staff technical capabilities in Splunk. * Increase forensic tooling capabilities. |
| Root cause | Note the fundamental cause of the incident. Addressing the identified cause is essential to mitigate the risk of similar incidents occurring in the future. |