**Redback Operations = Cyber Security Incident Document**

|  |  |
| --- | --- |
| **Incident ID** | eg :- ATF123 |
| **Incident Title** | eg :- Suspicious activity detected on GCP machine |
| **Date and Time of Incident** | dd/mm/yyyy hh:mm |
| **Date and Time of Escalation** | dd/mm/yyyy hh:mm |
| **Timezone** | AEST (GMT+11) |
| **Incident Severity** | eg :- Severe, High, Medium, Low |
| **Incident Priority** | eg :- Cat 1, Cat 2, Cat 3, Cat 4 |
| **Incident Category** | eg :- Phishing, Malware Infection, Network Attack |
| **Affected Project** | Project Num – Name |
| **Affected Assets** | Usernames, Devices etc…. |
| **Incident Manager** | Name of Cyber Sec member and corresponding project member |
| **Date and Time of Expected Resolution** | dd/mm/yyyy hh:mm |
| **Date and Time of Incident Resolution** | dd/mm/yyyy hh:mm |

**Incident Tags**

Phishing, Google Cloud Platform, Single Asset etc….

**Incident Summary**

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nulla cursus, ligula eget malesuada gravida, magna lorem pretium mauris, eu pretium magna mauris eu erat. Aenean consectetur felis nec diam viverra vehicula. Donec nec tincidunt magna. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Nulla a cursus tortor, nec pretium nisl. Aenean eleifend tortor eget nunc mollis, sit amet placerat eros efficitur. Quisque ut nibh malesuada orci condimentum iaculis.

**Incident Timeline**

**dd/mm/yyyy hh:mm =** Lorem ipsum dolor sit amet, consectetur adipiscing elit.

**dd/mm/yyyy hh:mm =** Lorem ipsum dolor sit amet, consectetur adipiscing elit.

**dd/mm/yyyy hh:mm =** Lorem ipsum dolor sit amet, consectetur adipiscing elit.

**dd/mm/yyyy hh:mm =** Lorem ipsum dolor sit amet, consectetur adipiscing elit.

**dd/mm/yyyy hh:mm =** Lorem ipsum dolor sit amet, consectetur adipiscing elit.

**dd/mm/yyyy hh:mm =** Lorem ipsum dolor sit amet, consectetur adipiscing elit.

**Actions taken in Incident**

1. Lorem ipsum dolor sit amet, consectetur adipiscing elit.
2. Lorem ipsum dolor sit amet, consectetur adipiscing elit.
3. Lorem ipsum dolor sit amet, consectetur adipiscing elit.
4. Lorem ipsum dolor sit amet, consectetur adipiscing elit.

**Status of actions required to be taken per playbook/incident response plan**

1. Lorem ipsum dolor sit amet, consectetur adipiscing elit.
2. Lorem ipsum dolor sit amet, consectetur adipiscing elit.
3. Lorem ipsum dolor sit amet, consectetur adipiscing elit.
4. Lorem ipsum dolor sit amet, consectetur adipiscing elit.

**Incident Findings**

* Lorem ipsum dolor sit amet, consectetur adipiscing elit.
* Lorem ipsum dolor sit amet, consectetur adipiscing elit.
* Lorem ipsum dolor sit amet, consectetur adipiscing elit.
* Lorem ipsum dolor sit amet, consectetur adipiscing elit.

**Threat Actors and Vectors**

* Lorem ipsum dolor sit amet, consectetur adipiscing elit.
* Lorem ipsum dolor sit amet, consectetur adipiscing elit.
* Lorem ipsum dolor sit amet, consectetur adipiscing elit.
* Lorem ipsum dolor sit amet, consectetur adipiscing elit.

**Additional Details**

* Lorem ipsum dolor sit amet, consectetur adipiscing elit.
* Lorem ipsum dolor sit amet, consectetur adipiscing elit.
* Lorem ipsum dolor sit amet, consectetur adipiscing elit.
* Lorem ipsum dolor sit amet, consectetur adipiscing elit.

**Incident Resolution**

**Steps taken =**

* Lorem ipsum dolor sit amet, consectetur adipiscing elit.
* Lorem ipsum dolor sit amet, consectetur adipiscing elit.
* Lorem ipsum dolor sit amet, consectetur adipiscing elit.
* Lorem ipsum dolor sit amet, consectetur adipiscing elit.

**Incident Impact and Outcome =**

* Lorem ipsum dolor sit amet, consectetur adipiscing elit.
* Lorem ipsum dolor sit amet, consectetur adipiscing elit.
* Lorem ipsum dolor sit amet, consectetur adipiscing elit.
* Lorem ipsum dolor sit amet, consectetur adipiscing elit.

**Legal, Governing and Other Entities**

|  |  |
| --- | --- |
| **Escalated to Company Board?** | **Yes/No** |
| **Escalated to Australia CERT?** | **Yes/No** |
| **Escalated to Australia Cyber Security Center?** | **Yes/No** |
| **Escalated to Australian Police?** | **Yes/No** |
| **Escalated to Office of Australian Information Commissioner** | **Yes/No** |
| **Informed Redback’s Customers (impacted)?** | **Yes/No** |
| **Informed Redback’s Partners (impacted)?** | **Yes/No** |
| **Legal Action Required?** | **Yes/No** |
| **Media Action taken?** | **Yes/No** |