FIELD mapping FROM Resilient to icd

This Booklet Gives you an Understanding of how to map Resilient fields to ICD

By AppOps-Security(INDIA)

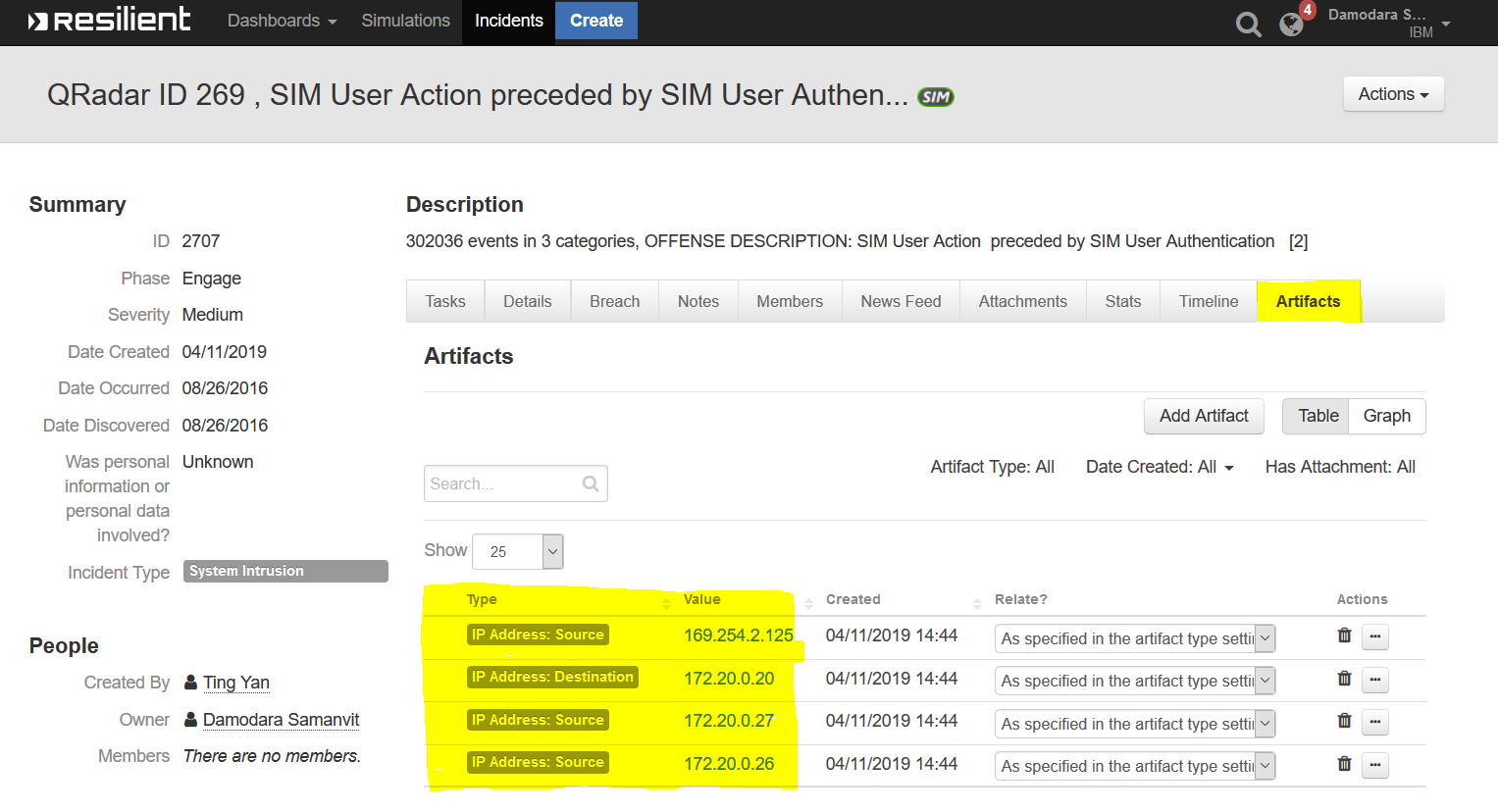
**Below are the fields of ICD and Resilient and how the communication must be between the two Applications**

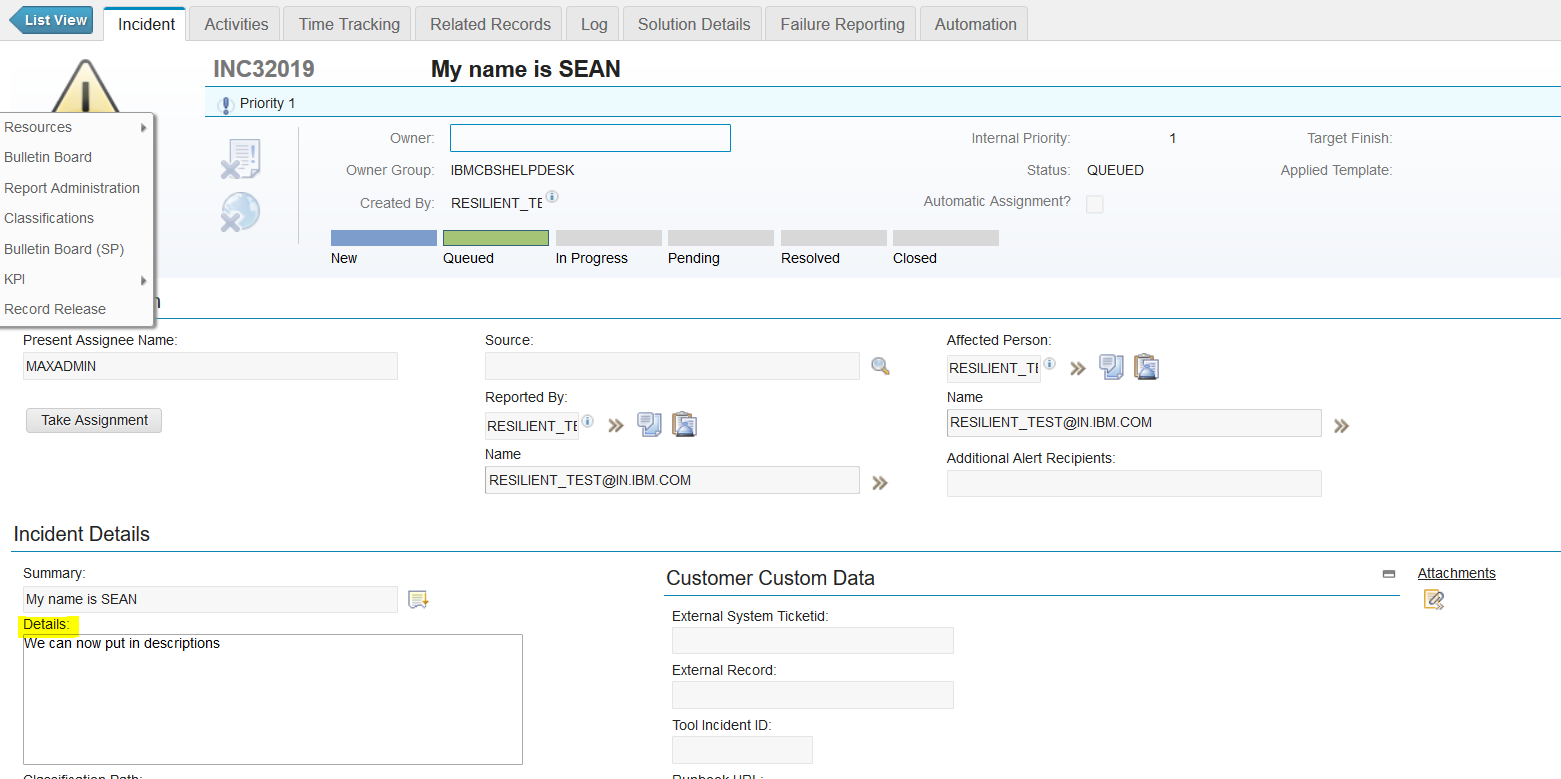
1.**Artifacts** in Resilient must be communicated to the **Details** field of the ICD.

Additionally we must capture the IP Source/Destination depending on the offense(Refer the Explanation), Search the details of that IP in MDR database. And get the DOU and PA(Primary Admin) name and communicate the same to ICD

Explanation:

There are Number of Incident Classifications, based on the incident type we can categorize them as “Source is Affected” or “ Destination is Affected”. Depending on the classification we have to perform STEP-1.

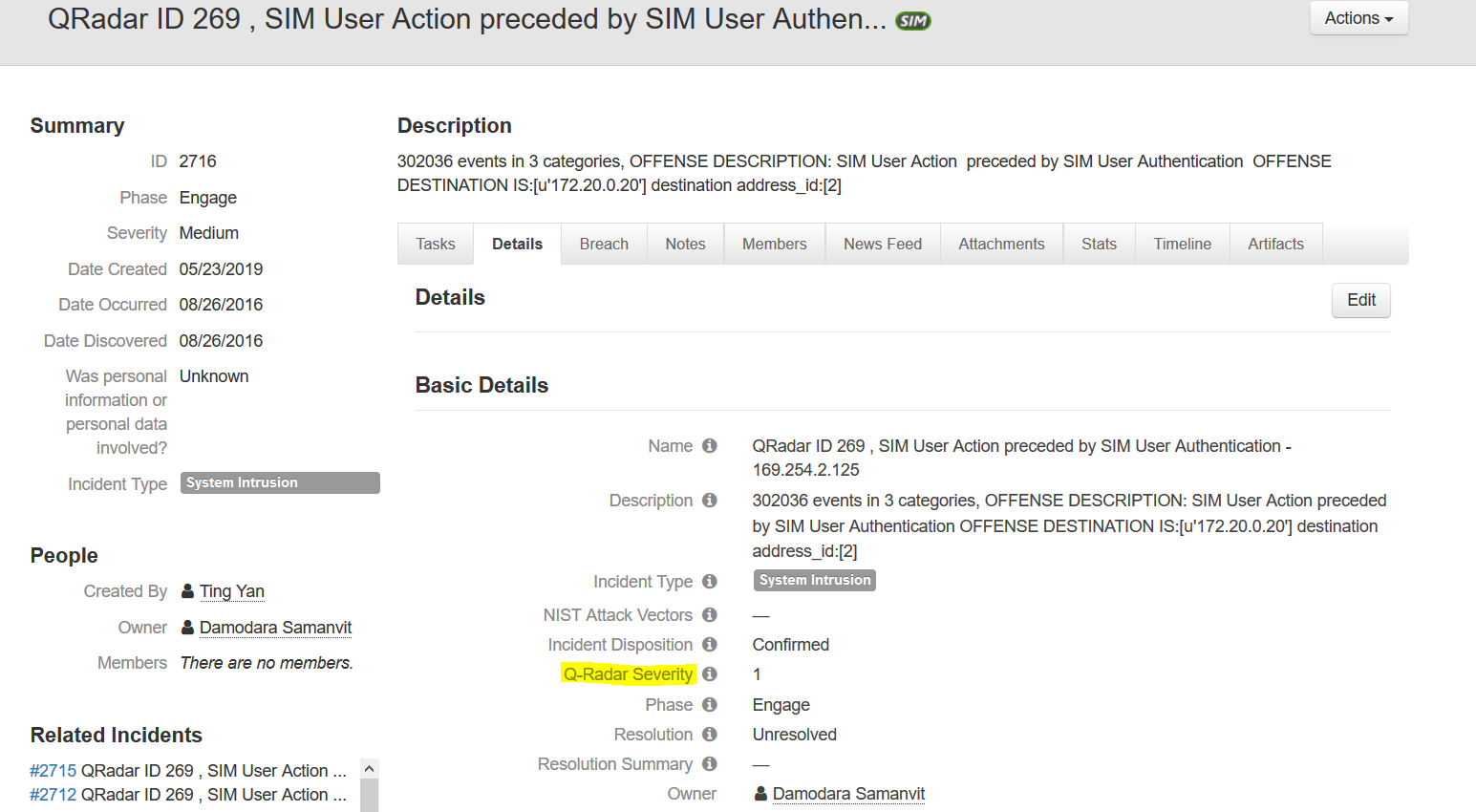




**2.Severity communication to ICD.**

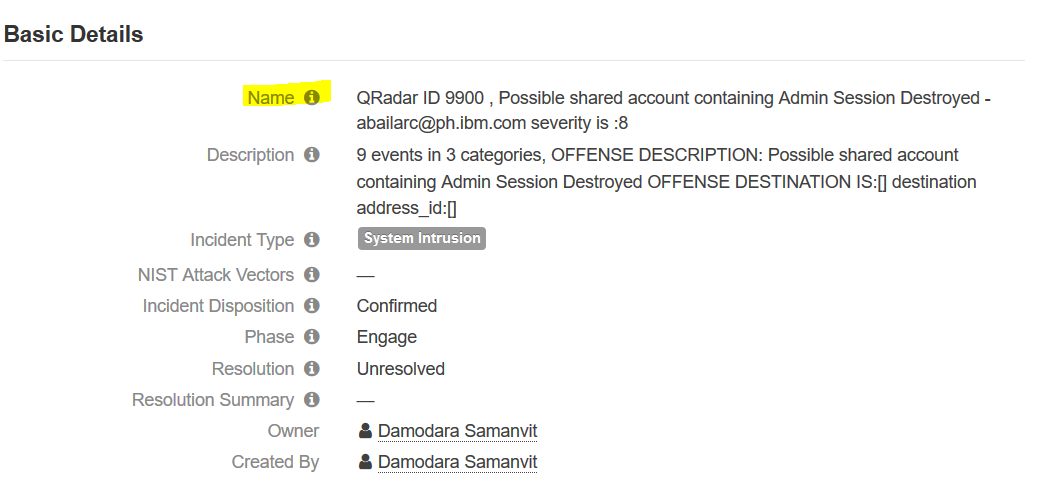
We can communicate the **Q-Radar Severity** field in Resilient to **INTERANAL PRIORITY** field in ICD. Below is the table that shows how severity in Resilient must be classified according to severity in ICD.

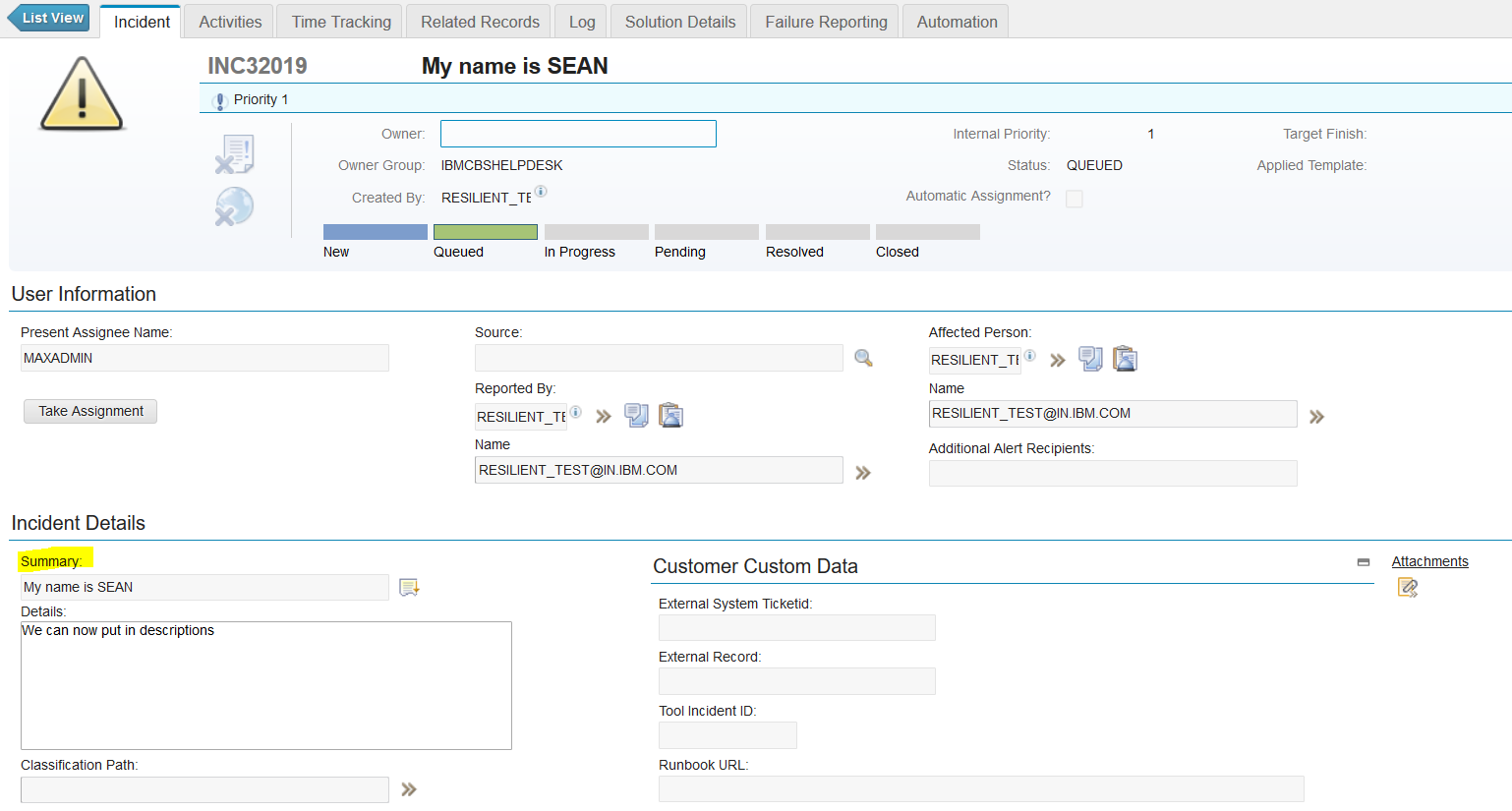
|  |  |
| --- | --- |
| Q-RADAR SEVERITY | ICD SEVERITY/INTERNAL PRIORITY |
| 7-10 | **1** |
| 5-6 | **2** |
| 4 | **3** |
| 1-3 | **4** |



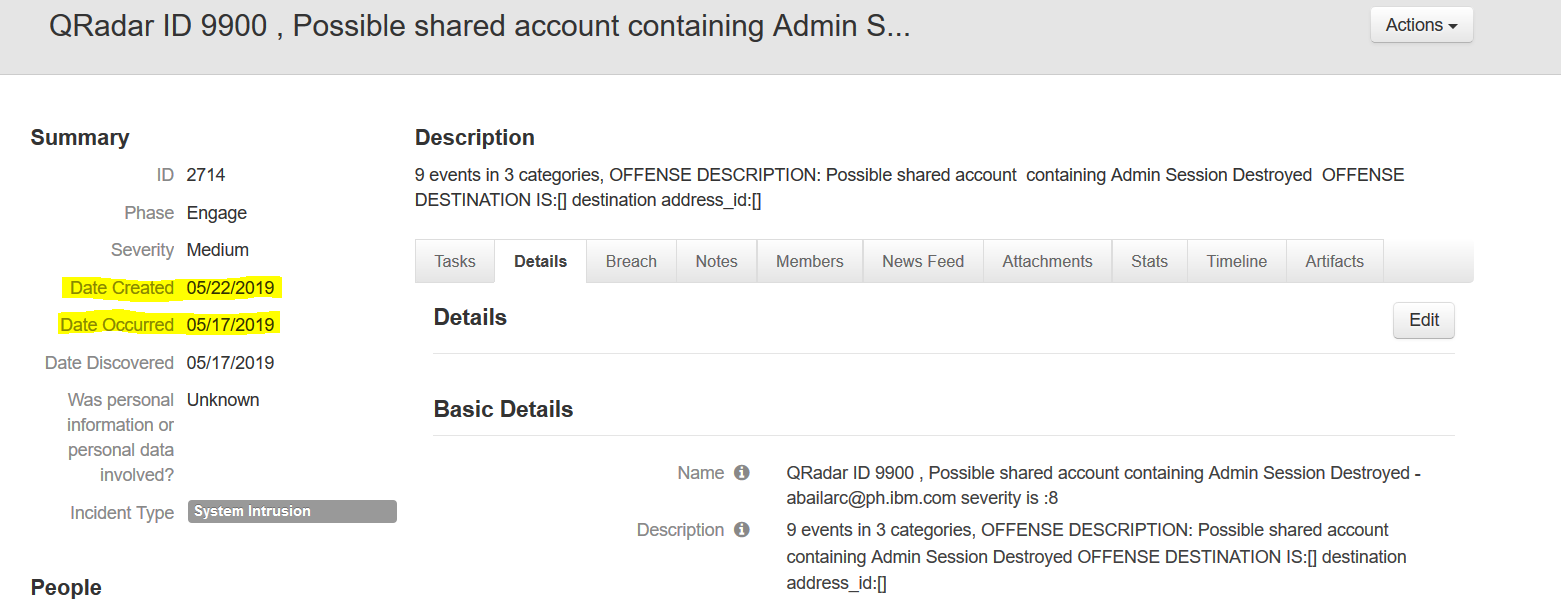
**3.Name Communication to ICD.**

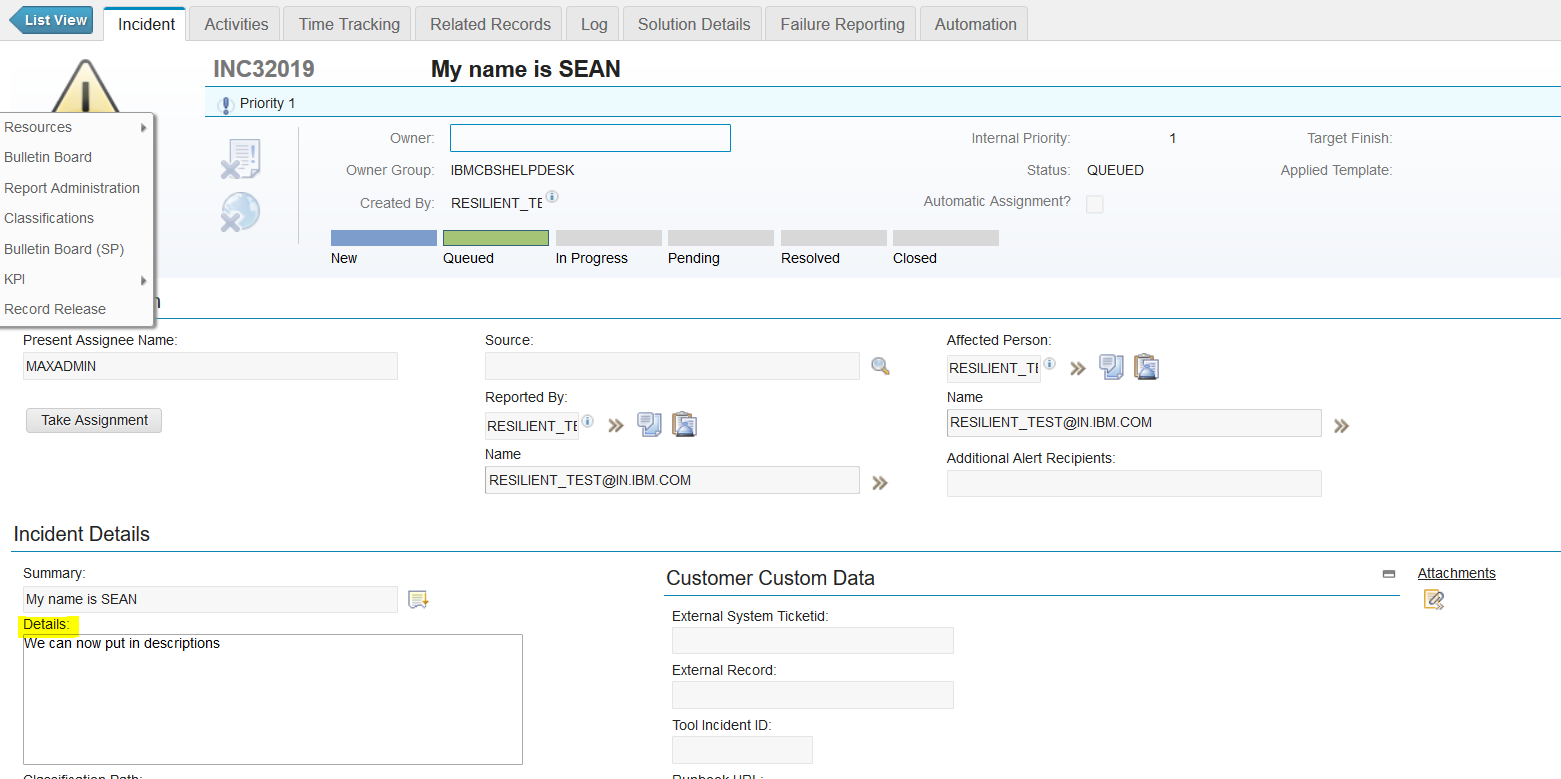
We have to communicate the **Name** field in Resilient to **Summary** field in ICD.





4.**Date Occurred and Date Created** should be communicated to The Details field of ICD with the prefix as **Date Occurred and Date Created** respectively.





5.**Owner** communication to the ICD  
  
We have to search for the **PA details from the MDR** database and then communicate the name to the ICD.

6.**Reported** **By** field in the ICD must be set to **Resilient(Appops)**

7.**Created by** field in the ICD must be set to [**Resilient\_test@in.ibm.com**](mailto:Resilient_test@in.ibm.com)

8.**Status** field in the ICD must be set to **Queued**

9.**Source** field in the ICD must be set to **Resilient(Appops)**

10.**Name** field in the ICD must be set to **Resilient(Appops)**

11.**Site ID** Field in the ICD must be set to **APPOPINT**

12.**Classification path** Field in ICD must be **Security Issue**

13.**Affected Person** field in ICD must be **PA(Primary Admin)**

14. **Class Description** Field in ICD must be **Security Issue**.

15.**End User Classification** Field in ICD must be **Security Issue**.

**CONCLUSION**:

List of Resilient Fields that must be communicated to ICD

|  |  |  |
| --- | --- | --- |
| **S.NO** | **RESILIENT FIELD** | **ICD FIELD** |
| 1 | Artifacts | Details |
| 2 | Q-Radar Severity | INTERANAL PRIORITY |
| 3 | Name | Summary |
| 4 | Date Occurred and Date Created | Date Occurred and Date Created |
| 6 | Description | Details |

List of ICD Fields that must be set:

|  |  |  |
| --- | --- | --- |
| **S.NO** | **ICD FIELD** | **DEFAULT ICD VALUE** |
| 1 | Owner | Must be obtained from MDR Database |
| 2 | Reported By | Resilient(Appops) |
| 3 | Created by | [Resilient\_test@in.ibm.com](mailto:Resilient_test@in.ibm.com) |
| 4 | Status | Queued |
| 5 | Source | Resilient(Appops) |
| 6 | Name | Resilient(Appops) |
| 7 | Site ID | APPOPINT |
| 8 | Classification path | Security Issue |
| 9 | Affected Person | Must be obtained from MDR Database |
| 10 | Class Description | Security Issue |
| 11 | End User Classification | Security Issue |