**END POINT::** http://54.242.228.131:5002

**1. Incidents**

**Create Incident (POST /api/incidents)**

{

"type": "Network Intrusion",

"severity": 5,

"status": "Open",

"detected\_at": "2024-11-20T10:00:00Z",

"resolved\_at": null,

"asset\_affected": "Server01",

"playbook\_id": 1,

"recovery\_status": "Pending",

"description": "Unauthorized access detected."

}

**Update Incident (PUT /api/incidents/:id)**

{

"type": "Network Intrusion - Updated",

"severity": 4,

"status": "In Progress",

"detected\_at": "2024-11-20T10:00:00Z",

"resolved\_at": null,

"asset\_affected": "Server02",

"playbook\_id": 2,

"recovery\_status": "In Progress",

"description": "Investigating unauthorized access."

}

**2. Playbooks**

**Create Playbook (POST /api/playbooks)**

{

"incident\_id": 107,

"created\_at": "2024-11-20T10:30:00Z",

"response\_steps": "Identify unauthorized access, contain impact.",

"recovery\_steps": "Restore data from backup, ensure data integrity.",

"continuity\_plan": "Engage cybersecurity team, communicate with stakeholders.",

"status": "In Progress"

}

**Update Playbook (PUT /api/playbooks/:id)**

{

"incident\_id": 107,

"created\_at": "2024-11-20T10:30:00Z",

"response\_steps": "Updated response steps.",

"recovery\_steps": "Updated recovery steps.",

"continuity\_plan": "Updated continuity plan.",

"status": "Completed"

}

**3. Recovery Actions**

**Create Recovery Action (POST /api/recovery\_actions)**

{

"incident\_id": 108,

"action\_taken": "Restart impacted servers and apply patches.",

"started\_at": "2024-11-20T11:00:00Z",

"completed\_at": null,

"status": "In Progress"

}

**Update Recovery Action (PUT /api/recovery\_actions/:id)**

{

"incident\_id": 108,

"action\_taken": "Recovery completed successfully.",

"started\_at": "2024-11-20T11:00:00Z",

"completed\_at": "2024-11-20T13:00:00Z",

"status": "Completed"

}

**4. Crisis Communications**

**Create Crisis Communication (POST /api/crisis\_communications)**

{

"incident\_id": 109,

"message": "High-severity incident detected. Immediate action required.",

"sent\_at": "2024-11-20T12:00:00Z",

"recipients": "security\_team@example.com, admin@example.com",

"status": "Sent"

}

**Update Crisis Communication (PUT /api/crisis\_communications/:id)**

{

"incident\_id": 109,

"message": "Updated crisis communication message.",

"sent\_at": "2024-11-20T12:00:00Z",

"recipients": "updated\_team@example.com",

"status": "Sent"

}

**5. Incident Logs**

**Create Incident Log (POST /api/incident\_logs)**

{

"incident\_id": 110,

"timestamp": "2024-11-20T12:30:00Z",

"event\_type": "Investigation",

"details": "Initial investigation started by the security team."

}

**Update Incident Log (PUT /api/incident\_logs/:id)**

{

"incident\_id": 110,

"timestamp": "2024-11-20T13:30:00Z",

"event\_type": "Resolution",

"details": "Incident resolved and recovery steps completed."

}

**6. Incident Recovery**

**Trigger Incident Recovery (POST /api/incidents/:id/recover)**

* **Endpoint**: /api/incidents/8/recover (Replace 8 with the desired incident ID)
* **Payload**: None
* **Expected Result**: Incident status changes to Resolved.

**Example Functional Test:**

1. Start with POST /api/incidents to create a new incident.
2. Use POST /api/incidents/:id/recover to recover the incident.
3. Update the incident with PUT /api/incidents/:id.