**Features of "Security Incident Response" (SIR) in ServiceNow**

ServiceNow's Security Incident Response (SIR) provides a comprehensive suite of features designed to help organizations effectively manage and respond to security incidents.

**Key features include:**

**1. Incident Management:**

* Creation, tracking, and resolution of security incidents.
* Automation of incident response workflows.
* Integration with various security information and event management (SIEM) tools.

**2. Orchestration and Automation:**

* Automated threat intelligence gathering and enrichment.
* Playbooks for standardized response procedures.
* Automated remediation actions based on predefined rules.

**3. Threat Intelligence:**

* Integration with threat intelligence feeds.
* Automated correlation of threat data with incidents.
* Centralized threat intelligence repository.

**4. Collaboration:**

* Communication tools for collaboration among incident response teams.
* Integration with IT service management (ITSM) for coordinated responses.

**5. Incident Analysis and Reporting:**

* Detailed incident analysis with root cause identification.
* Customizable dashboards and reports for tracking and reporting incidents.
* Metrics and KPIs for incident response performance.

**6. Integration:**

* Seamless integration with other ServiceNow modules and third-party security tools.
* APIs for extending and customizing SIR capabilities.

**7. Compliance and Audit:**

* Audit trails and compliance tracking.
* Integration with governance, risk, and compliance (GRC) tools.

**APIs Available to Access SIR Features and Data**

ServiceNow provides a range of REST APIs that allow you to interact with and manage the Security Incident Response (SIR) module. Below are some key APIs and their functionalities:

**1. Security Incident API**

* + Endpoint: `/api/now/table/sn\_si\_incident`
  + Description: This API allows you to create, retrieve, update, and delete security incidents.
  + Methods: `GET`, `POST`, `PUT`, `DELETE`

**2. Security Case API**

* + Endpoint: `/api/now/table/sn\_si\_case`
  + Description: This API is used to manage security cases.
  + Methods: `GET`, `POST`, `PUT`, `DELETE`

**3. Threat Intelligence API**

* + Endpoint: `/api/now/table/sn\_ti\_observable`
  + Description: This API allows you to manage threat intelligence observables.
  + Methods: `GET`, `POST`, `PUT`, `DELETE`

**4. Playbook API**

* + Endpoint: `/api/now/table/sn\_playbook`
  + Description: This API is used to manage playbooks for incident response.
  + Methods: `GET`, `POST`, `PUT`, `DELETE`

**Additional Resources**

ServiceNow Developer Portal: [ServiceNow Developer Portal] (<https://developer.servicenow.com/>)

ServiceNow REST API Documentation: [ServiceNow REST API]

(<https://docs.servicenow.com/bundle/paris-application-development/page/integrate/inbound-rest/reference/r_TableAPI-GET.html>)

<https://docs.servicenow.com/bundle/vancouver-api-reference/page/build/applications/concept/api-rest.html>

<https://docs.servicenow.com/bundle/vancouver-api-reference/page/integrate/inbound-rest/concept/ext-user-mapping-api.html>

<https://docs.servicenow.com/bundle/washingtondc-api-reference/page/integrate/inbound-rest/task/t_GetStartedRetrieveExisting.html>

<https://developer.servicenow.com/dev.do#!/learn/learning-plans/washingtondc/new_to_servicenow/app_store_learnv2_scripting_washingtondc_servicenow_apis>

**Design Your Plugin –** [**download sample plugin**](https://raw.githubusercontent.com/TripathiAshutosh/invoice-metadata-extraction/main/SIRPlugin.yaml)

Identify what data you need to access and what actions your plugin will perform. For example:

* Retrieve a list of current security incidents.
* Create a new security incident.
* Update the status of an existing security incident.
* Retrieve threat intelligence observables.

**Write the YAML Configuration for Copilot:** Create a YAML file that defines your plugin. This includes specifying the data sources, actions, and functions.

