1. SIEM API Overview Documentation

1. Overview

The SIEM application exposes a RESTful API for interacting with various components of the system. The API is versioned (v1) and follows standard HTTP methods.

Base URL: `/api/v1/`

Authentication

The API uses JWT (JSON Web Token) for authentication. To access protected endpoints, include the JWT token in the Authorization header:

`Authorization: Bearer <your_jwt_token>`

To obtain a JWT token:

- **Endpoint:** `POST /api/v1/accounts/token/`
- **Request Body:**

```
{
  "email": "user@example.com",
  "password": "password123"
}
```

- **Response:**

```
{
  "refresh": "jwt-refresh-token",
  "access": "jwt-access-token"
}
```

To refresh a JWT token:

- **Endpoint:** `POST /api/v1/accounts/token/refresh/`
- **Request Body:**

```
{
  "refresh": "jwt-refresh-token"
}
```

- **Response:**

```
{
  "access": "new-jwt-access-token"
}
```

API Endpoints

Accounts

1. **User Management**
   - List Users: `GET /api/v1/accounts/users/`
   - Create User: `POST /api/v1/accounts/users/`
   - Retrieve User: `GET /api/v1/accounts/users/{user_id}/`
   - Update User: `PUT /api/v1/accounts/users/{user_id}/`
   - Delete User: `DELETE /api/v1/accounts/users/{user_id}/`
2. **Role Management**
   - List Roles: `GET /api/v1/accounts/roles/`
   - Create Role: `POST /api/v1/accounts/roles/`
   - Retrieve Role: `GET /api/v1/accounts/roles/{role_id}/`
   - Update Role: `PUT /api/v1/accounts/roles/{role_id}/`
   - Delete Role: `DELETE /api/v1/accounts/roles/{role_id}/`
3. **Permission Management**
   - List Permissions: `GET /api/v1/accounts/permissions/`
   - Create Permission: `POST /api/v1/accounts/permissions/`
4. **Role-Permission Management**
   - List Role-Permissions: `GET /api/v1/accounts/role-permissions/`
   - Assign Permissions to Role: `POST /api/v1/accounts/role-permissions/`

Alerts

1. **Alert Management**
   - List Alerts: `GET /api/v1/alerts/`
   - Create Alert: `POST /api/v1/alerts/`
   - Retrieve Alert: `GET /api/v1/alerts/{id}/`
   - Update Alert: `PATCH /api/v1/alerts/{id}/`
   - Delete Alert: `DELETE /api/v1/alerts/{id}/`
   - Assign Alert: `POST /api/v1/alerts/{id}/assign/`
   - Latest Alerts: `GET /api/v1/alerts/latest_alerts/`
2. **Investigate Alerts**
   - List Investigate Alerts: `GET /api/v1/investigate/`
   - Create Investigate Alert: `POST /api/v1/investigate/`
   - Retrieve Investigate Alert: `GET /api/v1/investigate/{id}/`
   - Update Investigation Alert: `PATCH /api/v1/investigate/{id}/`
   - Delete Investigation Alert: `DELETE /api/v1/investigate/{id}/`

Logs

1. **Bronze Event Data**
   - List Bronze Events: `GET /api/v1/logs/bronze-events/`
   - Export Bronze Events as PDF: `GET /api/v1/logs/bronze-events/export_pdf/`
   - Count Bronze Events: `GET /api/v1/logs/bronze-events/count/`
2. **Router Data**

- List Router Data: `GET /api/v1/logs/router-data/`
- Export Router Data as PDF: `GET /api/v1/logs/router-data/export_pdf/`
- Count Router Data Logs: `GET /api/v1/logs/router-data/router_log_count/`

3. **Log Analysis**
   - Get Log Percentages: `GET /api/v1/logs/log-percentage/log_percentages/`
   - Logs Per Hour: `GET /api/v1/logs/logs-aggregation/logs_per_hour/`
   - Count Events Today: `GET /api/v1/logs/events-today/events_today/`

Reports

1. **Incident Reports**
   - List Incident Reports: `GET /api/v1/reports/incident-reports/`
   - Create Incident Report: `POST /api/v1/reports/incident-reports/`
   - Retrieve Incident Report: `GET /api/v1/reports/incident-reports/{id}/`
   - Update Incident Report: `PUT /api/v1/reports/incident-reports/{id}/`
   - Delete Incident Report: `DELETE /api/v1/reports/incident-reports/{id}/`
   - Generate PDF Report: `GET /api/v1/reports/incident-reports/{id}/generate_pdf/`