SIEM App Database Schema Documentation

Table of Contents

User Model

- Link to code

The `User` model extends Django's `AbstractBaseUser` and `PermissionsMixin`, providing a custom user implementation for the SIEM app.

Fields:

- `user_id` (UUIDField): Primary key, automatically generated UUID.
- `email` (EmailField): Unique email address, max length 80 characters.
- `role` (ForeignKey): References the `Role` model, can be null.
- `is_active` (BooleanField): Indicates if the user account is active.
- `is_staff` (BooleanField): Determines if the user can access the admin site.

Methods:

- `create_user()`: Creates a regular user.
- `create_superuser()`: Creates a superuser with additional permissions.
- `has_permission(permission_name)`: Checks if the user has a specific permission.

Notes:

- Uses email as the unique identifier for authentication.
- Inherits from `BaseModel` and `BaseViewThrottleSet`.

Role Model

- Link to code The `Role` model defines user roles within the system.

Fields:

- `role_id` (UUIDField): Primary key, automatically generated UUID.
- `name` (CharField): Role name, max length 20 characters.
- `permissions` (ManyToManyField): Relates to the `Permission` model through `RolePermission`.

Choices:

- `ADMIN`: Administrator role
- `ANALYST`: Analyst role

Methods:

- `has_permission(permission_name)`: Checks if the role has a specific permission.

Notes:

- Inherits from `BaseModel` and `BaseViewThrottleSet`.

Employee Model

- Link to code The `Employee` model extends the `User` model with additional employment-related information.

Fields:

- `user` (OneToOneField): Primary key, references the `User` model.
- `employee_id` (CharField): Unique, auto-generated 6-digit employee ID.
- `first_name` (CharField): Employee's first name, max length 20 characters.
- `last_name` (CharField): Employee's last name, max length 20 characters.
- `department` (CharField): Optional, max length 50 characters.
- `job_title` (CharField): Optional, max length 50 characters.

Notes:

- Inherits from `BaseModel`.
- Automatically generates a unique employee ID when saving.

Permission Model

- Link to code The `Permission` model defines individual permissions in the system.

Fields:

- `permission_id` (UUIDField): Primary key, automatically generated UUID.
- `permission_name` (CharField): Unique permission name, max length 50 characters.

Notes:

- Inherits from `BaseModel` and `BaseViewThrottleSet`.

RolePermission Model

- Link to code The `RolePermission` model serves as an intermediary between `Role` and `Permission` models.

Fields:

- `role` (ForeignKey): References the `Role` model.
- `permission` (ForeignKey): References the `Permission` model.

Meta:

- Enforces unique combinations of role and permission.

Notes:

- Inherits from `BaseModel` and `BaseViewThrottleSet`.

Alert Model

- Link to code

The `Alert` model represents security alerts generated in the SIEM system.

Fields:

- `id` (AutoField): Primary key, auto-incrementing integer.
- `rule` (ForeignKey): References the `Rule` model.
- `event` (ForeignKey): References the `BronzeEventData` model.
- `severity` (CharField): Alert severity level, choices from `AlertSeverity`.

- `comments` (TextField): Optional comments on the alert.

Choices (AlertSeverity):

- `INFO`
- `LOW`
- `MEDIUM`
- `HIGH`
- `CRITICAL`

Meta:

- Ordered by creation date in descending order.

Notes:

- Inherits from `BaseModel` and `BaseViewThrottleSet`.

InvestigateAlert Model

- Link to code The `InvestigateAlert` model represents the investigation process for an alert.

Fields:

- `id` (AutoField): Primary key, auto-incrementing integer.
- `alert` (OneToOneField): References the `Alert` model.
- `assigned_to` (ForeignKey): References the `User` model.
- `status` (CharField): Investigation status, choices from `InvestigationStatus`.
- `notes` (TextField): Optional investigation notes.

Choices (InvestigationStatus):

- `OPEN`
- `IN PROGRESS`
- `CLOSED`

Notes:

- Inherits from `BaseModel` and `BaseViewThrottleSet`.
- Also referred to as `AssignedAlert` in comments.

Rule Model

- Link to code The `Rule` model defines detection rules for generating alerts.

Fields:

- `id` (AutoField): Primary key, auto-incrementing integer.
- `name` (CharField): Rule name, max length 255 characters.
- `description` (CharField): Rule description, max length 255 characters.
- `conditions` (TextField): Rule conditions.
- `severity` (CharField): Rule severity level, choices provided.

Choices (Severity):

- `INFO`
- `LOW`
- `MEDIUM` (default)
- `HIGH`
- `CRITICAL`

Notes:

- Inherits from `BaseModel` and `BaseViewThrottleSet`.

BronzeEventData Model

- Link to code

The `BronzeEventData` model stores raw event data from various sources.

Fields:

- `created_at` (DateTimeField): Auto-generated timestamp.
- `priority` (IntegerField): Optional event priority.
- `h_version` (IntegerField): Optional version number.
- `iso_timestamp` (DateTimeField): Optional ISO format timestamp.
- `hostname` (CharField): Optional hostname, max length 255 characters.
- `app_name` (CharField): Optional application name, max length 255 characters.
- `process_id` (CharField): Optional process ID, max length 50 characters.
- `Keywords` (CharField): Optional keywords, max length 50 characters.
- `EventType` (CharField): Optional event type, max length 50 characters.
- `EventID` (CharField): Optional event ID, max length 50 characters.
- `ProviderGuid` (CharField): Optional provider GUID, max length 255 characters.
- `Version` (CharField): Optional version, max length 10 characters.
- `Task` (CharField): Optional task, max length 10 characters.
- `OpcodeValue` (CharField): Optional opcode value, max length 10 characters.

- `RecordNumber` (CharField): Optional record number, max length 50 characters.
- `ActivityID` (CharField): Optional activity ID, max length 255 characters.
- `ThreadID` (CharField): Optional thread ID, max length 50 characters.
- `Channel` (CharField): Optional channel, max length 255 characters.
- `Domain` (CharField): Optional domain, max length 255 characters.
- `AccountName` (CharField): Optional account name, max length 255 characters.
- `UserID` (CharField): Optional user ID, max length 50 characters.
- `AccountType` (CharField): Optional account type, max length 50 characters.
- `Opcode` (CharField): Optional opcode, max length 100 characters.
- `PackageName` (CharField): Optional package name, max length 255 characters.
- `ContainerId` (CharField): Optional container ID, max length 255 characters.
- `EventReceivedTime` (DateTimeField): Optional event received time.
- `SourceModuleName` (CharField): Optional source module name, max length 50 characters.
- `SourceModuleType` (CharField): Optional source module type, max length 50 characters.
- `message` (TextField): Optional message content.
- `extra_fields` (TextField): Optional additional fields.
- `processed` (IntegerField): Processing status, default 0.

Notes:

- Inherits from `BaseModel` and `BaseViewThrottleSet`.
- Designed to accommodate various event data structures.

RouterData Model

- Link to code The `RouterData` model stores network router-specific event data.

Fields:

- `created_at` (DateTimeField): Auto-generated timestamp.
- `severity` (IntegerField): Optional severity level.
- `date_time` (CharField): Optional date and time, max length 100 characters.
- `hostname` (CharField): Optional hostname, max length 100 characters.
- `process` (CharField): Optional process name, max length 100 characters.
- `message` (TextField): Optional message content.

Notes:

- Inherits from `BaseModel` and `BaseViewThrottleSet`.

IncidentReport Model

- Link to code The `IncidentReport` model represents security incident reports generated in the SIEM system.

Fields:

- `title` (CharField): Report title, max length 255 characters.
- `type` (CharField): Report type, choices from `ReportType`.
- `status` (CharField): Report status, choices from `ReportStatus`.
- `rules` (ManyToManyField): Related `Rule` objects.
- `user` (ForeignKey): References the `User` model.
- `description` (TextField): Incident description.
- `pdf_file` (FileField): Optional PDF file upload.

Choices:

ReportType:

- `SECURITY_INCIDENT`
- `NETWORK_TRAFFIC`
- `USER_ACTIVITY`
- `SYSTEM_PERFORMANCE`
- `COMPLIANCE_AUDIT`

ReportStatus:

- `DRAFT`
- `OPEN` (default)
- `PENDING`
- `APPROVED`
- `REJECTED`
- `ARCHIVED`

Meta:

- Ordered by creation date in descending order.

Notes:

- Inherits from `BaseModel` and `BaseViewThrottleSet`.