# AI Assistance & SIEM Setup Guide

This guide will help you add the new AI Assistance and SIEM tables to your existing database.

## 📋 Prerequisites

* Existing RAS Dashboard API database
* Node.js environment with database access
* Environment variables configured (DATABASE\_URL)

## 🚀 Step 1: Run Database Migration

Execute the migration script to create all new tables:

# Navigate to your API directory  
cd api  
  
# Run the migration script  
node scripts/migrate\_ai\_siem\_tables.js

The script will create:

### SIEM Tables (8 tables)

* siem\_log\_sources - Log source configurations
* siem\_rules - Detection rules and correlation logic
* siem\_events - Individual security events
* siem\_alerts - Correlated alerts from multiple events
* siem\_dashboards - Custom dashboard configurations
* siem\_incidents - High-level security incidents
* siem\_threat\_intelligence - Threat indicators and IOCs
* siem\_analytics - Pre-computed analytics and metrics

### AI Assistance Tables (6 tables)

* ai\_assistance\_requests - Core AI interaction tracking
* ai\_knowledge\_base - Curated AI-generated knowledge
* ai\_training\_data - Training examples and feedback
* ai\_analytics - Performance metrics and usage analytics
* ai\_model\_configurations - AI model settings and configurations
* ai\_automation\_rules - Rules for automated AI assistance

## 🔧 Step 2: Configure Environment Variables

Add these environment variables to your .env file:

# AI Provider Configuration (choose one or more)  
OPENAI\_API\_KEY=your\_openai\_api\_key\_here  
OPENAI\_ORG\_ID=your\_openai\_org\_id\_here  
  
ANTHROPIC\_API\_KEY=your\_anthropic\_api\_key\_here  
  
AZURE\_OPENAI\_API\_KEY=your\_azure\_openai\_key\_here  
AZURE\_OPENAI\_ENDPOINT=https://your-resource.openai.azure.com/  
  
# Elasticsearch Configuration (optional)  
ELASTICSEARCH\_URL=https://localhost:9200  
ELASTICSEARCH\_USERNAME=elastic  
ELASTICSEARCH\_PASSWORD=your\_password\_here  
  
# AI Configuration  
AI\_DEFAULT\_PROVIDER=openai  
AI\_DEFAULT\_MODEL=gpt-4  
AI\_MAX\_TOKENS=2000  
AI\_TEMPERATURE=0.7

## 📊 Step 3: Verify Installation

Check that the tables were created successfully:

-- Check SIEM tables  
SELECT table\_name FROM information\_schema.tables   
WHERE table\_name LIKE 'siem\_%'   
ORDER BY table\_name;  
  
-- Check AI Assistance tables  
SELECT table\_name FROM information\_schema.tables   
WHERE table\_name LIKE 'ai\_%'   
ORDER BY table\_name;

## 🧪 Step 4: Test AI Assistance

Create a test AI assistance request:

# Test the AI assistance endpoint  
curl -X POST http://localhost:3000/api/v1/ai-assistance/requests \  
 -H "Content-Type: application/json" \  
 -H "Authorization: Bearer YOUR\_JWT\_TOKEN" \  
 -d '{  
 "requestType": "threat\_analysis",  
 "title": "Test Threat Analysis",  
 "description": "Analyze suspicious IP address 192.168.1.100",  
 "context": {  
 "ip": "192.168.1.100",  
 "timeframe": "24h"  
 },  
 "priority": "medium"  
 }'

## 🔒 Step 5: Configure Permissions

Add AI assistance permissions to your RBAC system:

-- Insert AI assistance permissions  
INSERT INTO permissions (name, description, category, resource, action) VALUES  
('ai\_assistance', 'read', 'AI Assistance', 'ai\_assistance', 'read'),  
('ai\_assistance', 'write', 'AI Assistance', 'ai\_assistance', 'write'),  
('ai\_assistance', 'admin', 'AI Assistance', 'ai\_assistance', 'admin'),  
('siem', 'read', 'SIEM', 'siem', 'read'),  
('siem', 'write', 'SIEM', 'siem', 'write'),  
('siem', 'admin', 'SIEM', 'siem', 'admin');  
  
-- Assign permissions to admin role  
INSERT INTO role\_permissions (role\_id, permission\_id)  
SELECT r.id, p.id   
FROM roles r, permissions p   
WHERE r.name = 'admin'   
AND p.resource IN ('ai\_assistance', 'siem');

## 📈 Step 6: Initialize Default Data

Create default AI model configurations:

-- Insert default AI model configuration  
INSERT INTO ai\_model\_configurations (  
 name, provider, model, configuration, parameters,   
 system\_prompt, is\_active, created\_by  
) VALUES (  
 'Default GPT-4',  
 'openai',  
 'gpt-4',  
 '{"endpoint": "https://api.openai.com/v1/chat/completions"}',  
 '{"temperature": 0.7, "max\_tokens": 2000}',  
 'You are a helpful cybersecurity assistant specializing in government security requirements.',  
 true,  
 1  
);  
  
-- Insert default SIEM log source  
INSERT INTO siem\_log\_sources (  
 name, type, status, configuration, created\_by  
) VALUES (  
 'System Logs',  
 'syslog',  
 'active',  
 '{"port": 514, "protocol": "udp"}',  
 1  
);

## 🎯 Step 7: Start Using Features

### AI Assistance Features

* **Threat Analysis** - Analyze security threats and indicators
* **Incident Response** - Generate response playbooks
* **Compliance Guidance** - Get compliance framework guidance
* **Policy Generation** - Create security policies and procedures
* **Training Content** - Generate personalized security training

### SIEM Features

* **Event Management** - Collect and analyze security events
* **Alert Correlation** - Create alerts from multiple events
* **Threat Intelligence** - Manage threat indicators and IOCs
* **Incident Tracking** - Track security incidents end-to-end
* **Analytics** - Generate security metrics and reports

## 🔍 Troubleshooting

### Common Issues

1. **Migration fails with permission error**

* # Ensure your database user has CREATE privileges  
  GRANT CREATE ON DATABASE your\_database TO your\_user;

1. **AI requests fail with API key error**

* # Verify your API keys are correctly set  
  echo $OPENAI\_API\_KEY

1. **Tables not appearing in schema exports**

* # Restart your application after running migration  
  npm restart

### Verification Commands

# Check if migration completed successfully  
node -e "  
const { db } = require('./src/db');  
const { aiAssistanceRequests } = require('./src/db/schema');  
console.log('AI tables available:', !!aiAssistanceRequests);  
"  
  
# Test AI service initialization  
node -e "  
const aiService = require('./src/services/aiAssistanceService');  
console.log('AI service initialized successfully');  
"

## 📚 Next Steps

1. **Configure AI Providers** - Set up your preferred AI service providers
2. **Create Automation Rules** - Set up automated AI assistance for common tasks
3. **Train the System** - Provide feedback to improve AI response quality
4. **Integrate with SIEM** - Connect your existing security tools
5. **Customize Dashboards** - Create custom SIEM dashboards for your needs

## 🆘 Support

If you encounter issues:

1. Check the application logs for detailed error messages
2. Verify all environment variables are correctly set
3. Ensure database connectivity and permissions
4. Review the API documentation for endpoint usage
5. Test with simple requests before complex scenarios

The AI Assistance and SIEM platforms are now ready to enhance your cybersecurity operations!