FAQs - SureView Virtual Operator

YOUR SOC ASSISTANT: EFFICIENT, COST-EFFECTIVE, ALWAYS ON GUARD

General Overview

What AI capabilities does SureView offer?
SureView has developed a Virtual Operator that uses the latest AI models to automate many functions of a modern Security Operations Center (SOC). This functionality is offered as an optional platform feature and is currently in Beta testing with select customers.

How does the Virtual Operator work?
The Virtual Operator uses a combination of Large Language Models (LLM) and object detection models to:

- Take over some of the routine response functions of the operator
- Pickup and determine the nature of an event quicker
- Deliver cost savings for command centers as they grow and scale

Technical Implementation

What specific AI technologies are being used?
The SureView Virtual Operator uses a plugin framework, providing the flexibility to connect to different AI models. The standard deployment uses the following technologies:

- Large Language Models: OpenAI API (GPT-4)
- Object Detection: AWS Rekognition

Data Security and Privacy

How is client data protected?

- All systems are governed by ISO 27001 certification
- All data in transit is encrypted using TLS 1.2 / SSL encryption standards
- Access is controlled through a strict least-privilege policy
- API keys are stored in a secure data vault and rotated annually

How is data isolation maintained?
The SureView API enforces client data isolation when using AI functionality. Each client's data is segregated and protected from other clients' data through the API architecture.

Is client data used for AI training?
No. SureView does not train models on client data. When using the OpenAI API, no information is used to train models. As per OpenAI's privacy statement: "Data submitted through the OpenAI API is not used to train OpenAI models or improve OpenAI's service offering."

What client data is processed by the AI?
The AI processes SureView event response details, including:

- Alarm details
- Audited steps of operator actions
- Time/date entries of actions taken

How is PII and confidential data handled?
By default, the system does not process PII or confidential company data. This type of sensitive data will only be processed if a client specifically configures their SureView workflows to include such information in operator prompts or event handling procedures.

The type of PII that is typically added by clients into SureView is for User and Contact Setup, it may contain:

- Full Name
- Email Address
- Physical Address
- Phone Number(s)
- Role/Job Title
- Location Data (if using a mobile app for real-time location tracking)

Access to this information is strictly controlled through role-based access controls and the principle of least privilege.

Quality Control and Safety

How do you ensure AI output quality?

Several measures are in place:

- Use of multiple models to provide greater context
- Tools for users to provide additional context in prompts
- Ability for teams to edit output
- User controls over Virtual Operator behavior
- Standardization of messages through the SureView API

How do you ensure AI output quality?

We employ several key measures to ensure reliable and accurate AI outputs:

Multiple AI Models Working Together

- Combines Language Models (OpenAI API) with Object Detection (AWS Rekognition)
- Each model provides different perspectives on events
- Multiple models help validate information and reduce errors

User Context Tools

- Pre-built templates for common security events
- Tools for adding site-specific security protocols
- Ability to include additional context when needed
- Integration with existing security procedures

Human Oversight

- Security teams can review all AI outputs
- Full editing capabilities for any AI-generated content
- Customizable Virtual Operator Settings
- Adjustable confidence levels for automated actions
- Custom rules for different types of security events
- Flexible operating parameters based on security needs
- Time-based settings for different security conditions

Standardized Information Processing

- Consistent handling of all security events
- Uniform data structure across different security systems
- Validated formats to ensure accurate interpretation

How do you protect against AI security risks?

- Combination of Language Model and Object detection models to reduce vulnerability to prompt injections
- Regular penetration testing by accredited third parties

Audit and Compliance

How is AI activity tracked?

All AI outputs are recorded in an audit trail with user-configurable retention periods.

What certifications and standards are followed?

- ISO 27001 certification
- OWASP security standards
- Industry-accepted security best practices for coding

Integration and Access

What systems does the AI integrate with?

The AI solutions are exclusively connected to SureView systems and do not integrate with external platforms.

How is access to the AI system controlled?

Access is governed by our ISO 27001-certified Access Control Policy and covers the following :

- Principle of least privilege
- Secure authentication methods
- Role-based access controls

ABOUT SUREVIEW SYSTEMS

SureView Systems is a global provider of software that improves the ability of security operation centers to manage and respond to security events. SureView is deployed successfully in a wide variety of environments including law enforcement, transportation, criticalnfrastructure and commercial organizations. SureView supports the largest integration library in the industry, enabling ease of deployment and system administration for a wide variety of organizations across the globe SureView Systems is an ISO27001 certified company and software is compliant with the most demanding corporate standards for IT and Networking security.

More Information

For more information please contact SureView at 1-888-387-2860 or visit us www.SureViewSystems.com