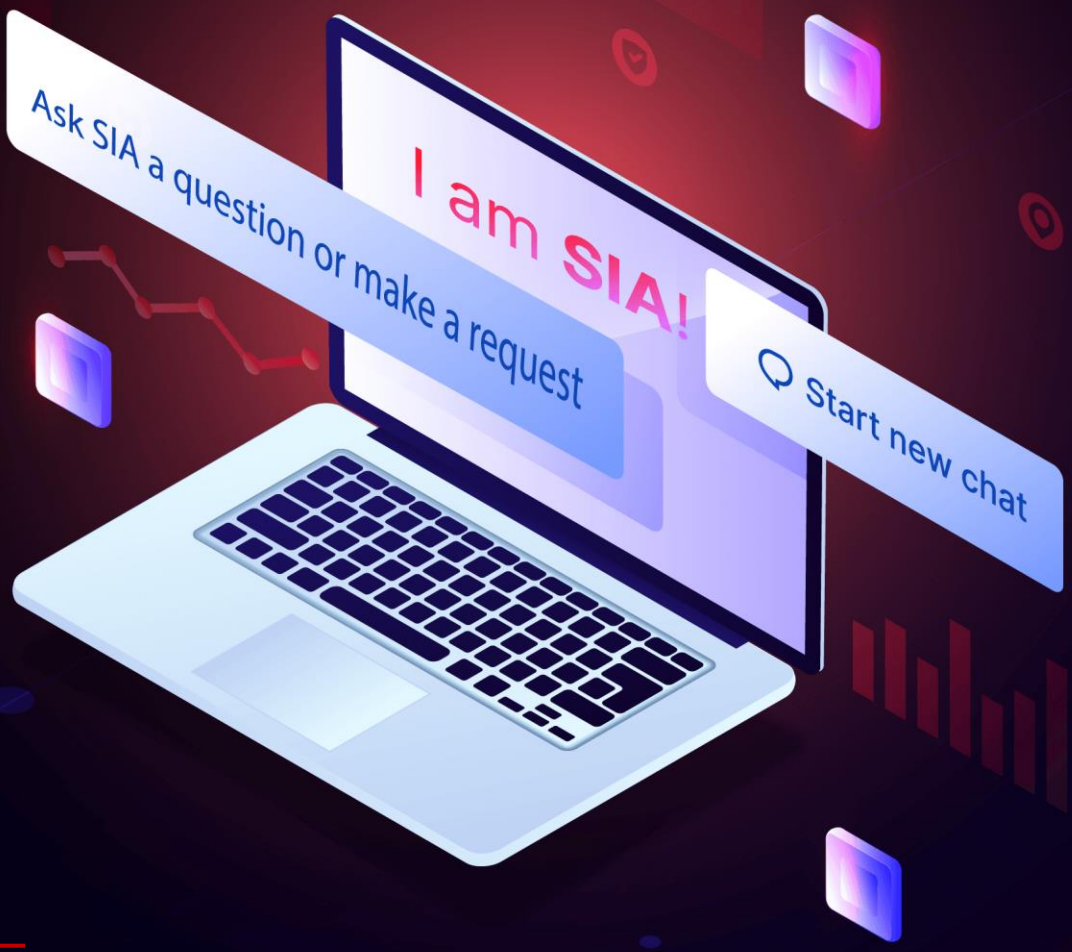
Seqrite
Intelligent Assistant

Seqrite Intelligent Assistant



Release Notes

V1.0.0.0 | 15 Apr 2025

www.seqrite.com

Contents

SIA: Comprehensive User Prompting Guide

Seqrite Intelligent Assistant for XDR

Welcome to the comprehensive guide on how to effectively interact with SIA, the Seqrite Intelligent Assistant for XDR. This document will help you formulate effective prompts to get the most out of SIA's capabilities while understanding its scope.

Introduction to SIA

SIA is an LLM-powered chatbot designed to help you navigate and utilize cybersecurity capabilities. SIA with Seqrite XDR can help with:

- Investigating security incidents
- Querying and analyzing alerts
- Providing product documentation and guidance
- Answering cybersecurity questions
- Summarizing incident data for remediation

SIA processes your questions based on their content, delivering accurate and relevant responses.

Best Practices for Prompting

To get the best results from SIA, follow these guidelines:

DO:

- **Be specific**: For Example, "Show me critical alerts from the last 24 hours" works better than "show me some alerts"
- **Include timeframes**: Specify time periods such as "last 7 days" or "since yesterday"
- **Use clear verbs and objects**: "List incidents with high severity" or "Count alerts by rule type"
- Specify **data sources** when relevant
- **Use entity-focused language**: "List incident IDs with critical severity" rather than vague requests

AVOID:

- **Ambiguous requests**: "Show me everything" or "What's happening?"
- **Multiple unrelated questions**: Ask one clear question at a time
- **Excessive technical jargon**: Use standard cybersecurity terminology
- **Very long, complex queries**: Break them down into multiple questions

Investigating Incidents

For incident investigation, SIA with Seqrite XDR can provide overview of incidents or in-depth analysis of specific incident IDs.

Incident Query Examples:

Basic Incident Queries:

- "Show me open incidents"
- "List high severity incidents from the last 7 days"
- "How many incidents are in remediation state?"
- "List incident IDs with critical severity"

Investigation Commands:

- "Investigate incident [incident IDs]
- "Analyze incident [incident IDs]
- "What steps should I take to mitigate incident [incident IDs]?

Incident Query Tips:

1. Use exact incident IDs: For detailed investigation, provide the specific incident ID
2. Be specific about status: Use terms like "NEW", "CLOSED", "REMEDIATION" for status filters as defined in Seqrite XDR
3. Combine filters: You can filter by severity, source, and time period simultaneously
4. For investigation: Use verbs like "investigate," "analyze," or "mitigate" with specific incident IDs

Querying Alerts

SIA excels at retrieving and analysing alert data. For best results, include these elements in your queries:

Alert Query Examples:

Basic Alert Queries:

- "How many alerts were triggered in the past week?"
- "Show me alerts from last 24 hours"
- "List all critical severity alerts from the last 24 hours"

Alert Aggregation Queries:

- "Group alerts by MITRE TTPs"
- "List Top 10 rules triggered in the last 7 days"
- "Count alerts by severity for the last month"

Alert Details Queries:

- "Summarize alert ID1234, ID5678"<<alert IDs>>
- "Show me the command lines for alert ID1234"

Alert Query Tips:

1. Alert Counting: Use "how many," "count," or "number of" when you want a total
2. Alert Filtering: Specify severity (critical, high, medium, low), time period
3. Alert Grouping: Use "group by," "aggregate," or "top N" for summarized views
4. Alert Details: Provide specific alert IDs when looking for detailed information

Product Documentation & Help

SIA can provide information about Seqrite XDR features, capabilities, and best practices.

Documentation Query Examples:

General Information:

- "What is Seqrite XDR?"
- "How does XDR differ from traditional EDR?"
- "Explain the incident lifecycle in Seqrite XDR"

How-To Guides:

- "How to isolate a compromised endpoint?"
- "Steps to investigate a suspicious network connection"
- "How to perform threat hunting in Seqrite XDR?"

Best Practices:

- "Best practices for reducing alert fatigue"
- "How to prioritize security incidents?"
- "Recommendations for effective incident response"

Documentation Query Tips:

1. Use "how to" format: Phrase questions as "How to X?" for procedural guidance
2. Ask about "any" vs specific: "How to analyze any incident" vs. "Analyze incident UUID"
3. Request templates/guides: Ask for report templates, checklists, or documentation

Follow-up Questions

SIA maintains context up to 3 messages. Use these patterns for effective follow-ups:

Follow-up Examples:

Clarification:

- "Can you explain that alert in more detail?"

- "Why is this incident marked critical?"
- "What do these command lines indicate?"

Progression:

- "Was there any lateral movement after this alert?"
- "Are these commands linked to any known attack techniques?"
- "What's the next step I should take?"

Filtering Previous Results:

- "From the above incidents, show only the critical ones"

Follow-up Tips:

1. Reference "above" or "previous": Use terms like "from above" or "in previous results"
2. Ask about relationships: Between alerts, incidents, or techniques
3. Request explanations: Ask "explain that [attribute]" for more insight

Currently Out of Scope

Out of Scope Questions:

Taking Actions:

- "Close incident [ID]"
- "Ignore alert [ID]"
- "Delete/modify incident or alert data"
- "Execute remediation actions"

Performance Metrics:

- "Average closure time of incidents"
- "SLA breach incidents"
- "Endpoint performance metrics"

Operational Management:

- "Offline endpoints status"
- "Playbook execution status"
- "Parent process queries"

Administration:

- "Creating custom rules"
- "Connector configuration"

- "User access management"
- "Licensing and pricing"

External Intelligence:

- "Reputation check for this MD5/IP"
- "Third-party intelligence integration"

Troubleshooting

Common Issues and Solutions:

Receiving "I don't understand" responses:

- Rephrase with clearer verb-object structure
- Avoid complex, run-on sentences
- Use standard cybersecurity terminology

Receiving too many or very few results:

- Add or remove filters (severity, timeframe)
- Be more specific about what you're looking for
- Break complex queries into simpler ones

Unsupported feature responses:

- Check the "Currently Out of Scope" section to see if your request is supported
- Focus on supported capabilities listed above in this guide

Not getting detailed incident analysis:

- Ensure you're using the exact incident ID
- Use investigation-specific verbs like "analyze" or "investigate"

Quick Reference: Common Query Templates

Incident Queries

- "List incidents with [STATUS] status and [SEVERITY] severity"
- "Count incidents by [FIELD] for [TIMEFRAME]"
- "Investigate incident [ID]"

Alert Queries

- "Show alerts since [TIMEFRAME]"
- "Count alerts with [SEVERITY] severity in [TIMEFRAME]"
- "Group alerts by [FIELD] from [TIMEFRAME]"
- "Show details for alert [ID]"

Documentation Queries

- "How to [ACTION] in Seqrite XDR?"
- "What is [FEATURE/CONCEPT]?"
- "Best practices for [ACTIVITY]"
- "Steps to [PROCESS]"

By following this guide, you'll be able to effectively leverage SIA's capabilities to enhance your security operations with Seqrite XDR. Please consider that SIA undergoes persistent advancements, and its capabilities may be refined and expanded over time.