

OPERATOR^X

The First AI Hunt Kit
Assistant Optimized for
Defensive Cyber Operations



Written By
Nate Delgado
Software Product Lead

I. The Need to Strengthen Team-Wide Expertise

Today's defensive cyber operators are tasked with outmaneuvering adversaries while navigating a sprawling toolset and oceans of data. Even experienced operators may not be familiar with every tool and syntax in the arsenal and the disconnected nature of many mission environments means it's difficult to impossible to supplement training with research in the field.

Operator X, powered by SealingTech, is a revolutionary AI Hunt Kit Assistant designed specifically for the cyber warfighter and to run 100% offline. By unifying an operator's entire toolkit into a single conversational interface, Operator X automates complex tasks and amplifies team-wide expertise, empowering operators to command their mission environment with unparalleled speed and accuracy.

II. The Solution: An AI Assistant for the Cyber Warfighter

Operator X is a Large Language Model (LLM) powered chat application that serves as an intelligent, conversational layer between the operator and their tools. For the first time, warfighters can simply talk to their defensive cyber operations (DCO) tech stack, expressing intent in plain English and letting Operator X translate it into precise, effective action.

The platform unifies the operator's entire toolkit by automating complex tasks across an expanding suite of integrations. Instead of memorizing syntax, operators can now focus on their objective, commanding their arsenal with powerful agents, analyzing data with a mission-tuned AI, and querying a dynamic knowledge base that learns and adapts from their unique operational data.

III. Core Capabilities: A Unified and Intelligent Arsenal

Operator X's power lies in its ability to seamlessly integrate three pillars of modern AI applications: natural language interaction, expert agent frameworks, and a dynamic, context-aware knowledge base.

a. Natural Language Command and Control

At its core, Operator X is an intuitive chat interface. Operators can issue commands, ask questions, and describe desired outcomes in natural language. The system parses this intent and executes the correct actions. This simple interface democratizes detection engineering and eliminates the syntax bottleneck, allowing an operator to ask questions in plain English instead of needing to craft the query manually.

b. Operator X Agents: Automating Complex Tasks

Operator X employs a suite of specialized agents, each an expert in a specific tool or function. These agents utilize sophisticated prompt chaining and prompt templates to intelligently break down complex problems into multi-step tasks that are executed automatically. **Key agents include:**

Threat Hunting and Network Detection (SIEM, Suricata, Vectra AI): Seamlessly query SIEM data in Splunk or Elastic, investigate real-time detections from Vectra AI, and automatically generate complex Suricata detection rules based on findings.

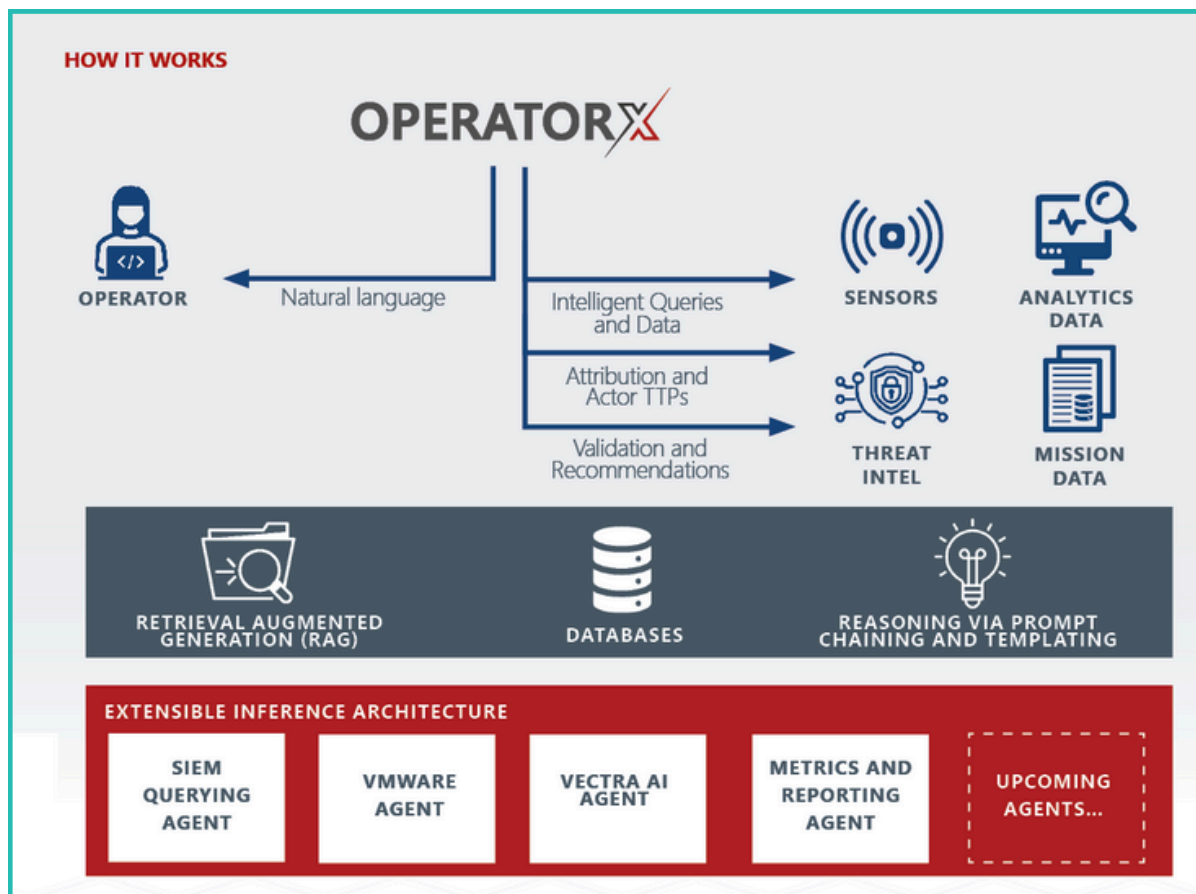
Infrastructure, Case Management and Host Analysis (VMware, Security Onion, osquery): Manage virtual infrastructure, find and create Cases in Security Onion, and leverage the full power of osquery without needing to memorize its hundreds of tables.

Reporting: Collect metrics from across the tech stack to generate custom reports on demand.

c. Interactive Knowledge Base: Your Evolving Expert

Operator X features a powerful retrieval-augmented generation (RAG) pipeline that transforms your data into an interactive knowledge base. Operators can upload files like mission orders, threat intelligence, or tool documentation, which the system intelligently indexes, making it instantly available for summarization and analysis.

This allows operators to chat directly with their data, correlating detections with intelligence, troubleshooting infrastructure issues, or learn how to use tools they're unfamiliar with. This mission-tuned AI enables Operator X to go beyond general cyber helper to an evolving expert on your specific mission.

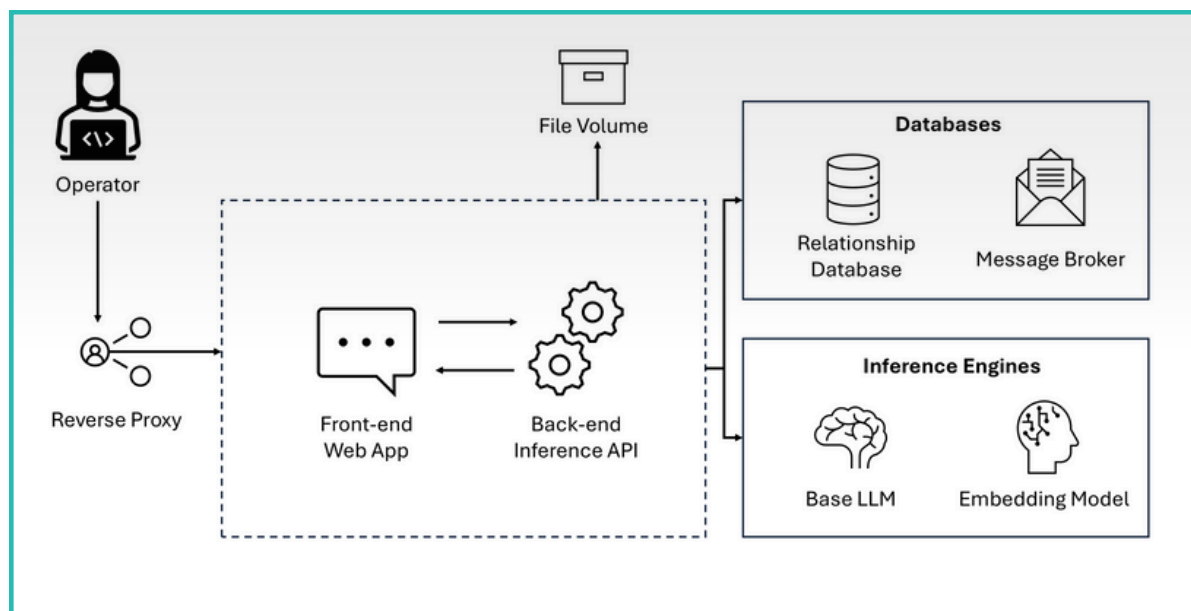


IV. Secure by Design

Operator X is designed to run 100% offline. The LLM model, agents, and data reside locally. It requires no internet connectivity and makes no external API calls, ensuring operational security and control in fully air-gapped environments.

V. Flexible and Extensible

Built on a containerized microservices architecture, the platform is inherently flexible. This allows for the rapid development of new agents to integrate additional tools and the continuous evaluation and deployment of new and improved LLM models to optimize for speed and performance.



VI. Hardware Requirements

The platform is designed to run on a single server with at least one GPU with 24GB of vRAM. While optimized for SealingTech's industry-leading Cyber Fly-Away Kits, it can be installed on customer hardware or cloud instance that meets the minimum GPU requirements.

VII. Amplifying Team-Wide Expertise, Speed, and Accuracy for Mission Readiness

Operator X unifies a cyber operator's entire toolkit into a single conversational interface.

It automates complex tasks and transforms junior operators into senior-level experts through its expanding suite of custom agents and powerful capabilities. It empowers operators to command their toolset with greater accuracy and speed. It troubleshoots in real-time, letting teams focus on the mission at hand. Deployable anywhere from a Kit laptop and fully offline, Operator X is built mission-ready to halt cyber adversaries in their tracks.

**To schedule a demonstration of Operator X,
contact our team or visit sealingtech.com/operatorx**

About SealingTech

Sealing Technologies (SealingTech), a Parsons Corporation company, is a trusted partner in providing powerful edge computing hardware and defensive cybersecurity solutions to protect the Federal Government and private enterprise. Veteran-founded in 2012, SealingTech continues to use its vast cyberspace expertise and knowledge to provide cutting-edge research, engineering, and integration services that support the US and its allies. For more information, visit www.sealingtech.com.