CYWARE™

Cyware Quarterback AI Features

Cyware's product portfolio weaves the power of AI into advanced threat intelligence operationalization capabilities to help security teams act faster and more effectively. AI is embedded across all offerings through Cyware Quarterback AI, the unified AI fabric that supports threat intelligence end-to-end workflow from threat automation through response automation.

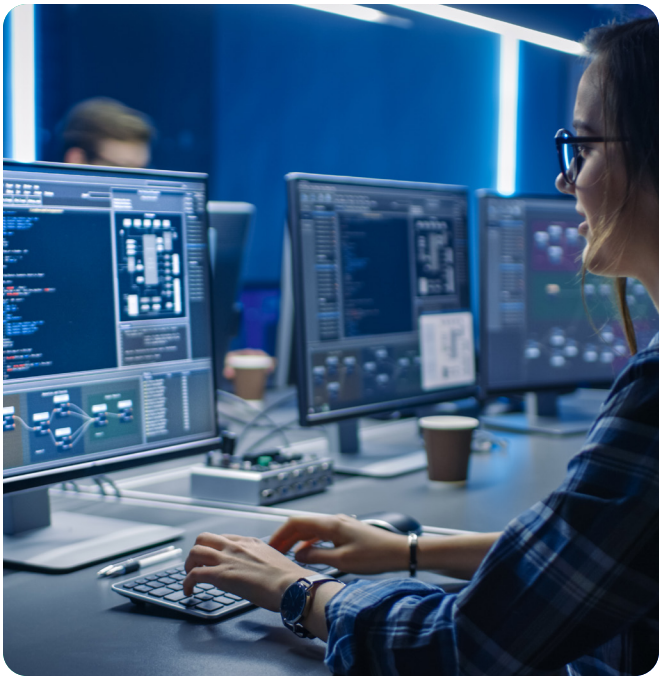
General Availability Capabilities (Already Available and Upcoming):

- **AI Capabilities in Cyware Intel Exchange:**
  - » AI-Powered Threat Intelligence Parser in Quick Add **(Available)**
  - » AI-Powered Report Summarization **(Available)**
  - » AI-Powered Cyware Advanced Threat Intel Crawler (Browser Plugin) **(Available)**
  - » AI-Powered Threat Data Search using Natural Language Processing (NLP) **(Upcoming)**
- **AI Capabilities in Cyware Orchestrate:**
  - » AI Action Node **(Available)**
  - » AI-Powered Playbook Builder **(Available)**
  - » AI-Powered Custom Code Generator **(Available)**
  - » AI-Powered Playbook Runlog Debugger **(Available)**

Key Capabilities and Features

Cyware Intel Exchange

- **AI-Powered Threat Intelligence Parser in Quick Add:** Parses and extracts Indicators of Compromise (IOCs), Tactics, Techniques, and Procedures (TTPs), threat actors, malware, vulnerabilities, and courses of action directly from text, documents, or websites. This eliminates the manual effort of fetching and entering data into Cyware Intel Exchange by integrating seamlessly with the Quick Add Intel module. Powered by OpenAI 4o mini.
  - » ***Limitation:*** *Metadata coverage is not as extensive as feed ingestion, and accuracy depends on the underlying model.*
- **AI-Powered Report Summarization:** Provides instant summaries of threat intelligence reports and related objects (e.g., IOCs, malware), helping analysts cut through lengthy descriptions and avoid alert fatigue. By accelerating knowledge discovery, it enables faster incident response.



Integrated into the Threat Object details page in Cyware Intel Exchange and powered by OpenAI 4o mini.

- **AI-Powered Cyware Advanced Threat Intel Crawler (Browser Plugin):** Transforms threat intelligence from websites into structured, enriched data in real time. By eliminating manual scraping, reducing human error, and minimizing ingestion delays, this extension delivers fast, reliable threat data capture. Compatible with Google Chrome and Microsoft Edge, with backend services hosted on AWS.
  - » ***Limitation:*** *Currently supports a maximum of 50,000 characters per extraction (subject to revision).*
- **AI-Powered Threat Data Search using Natural Language Processing (NLP):** Enables analysts to search threat objects using natural language queries instead of filters or Cyware Query Language (CQL). This dramatically simplifies data discovery, making threat hunting faster and more intuitive. Powered by Cyware MCP server and Claude Sonnet 4.

Cyware Orchestrate

- **AI Action Node:** Introduces a new type of playbook node that embeds Large Language Models (LLMs) for intelligent alert analysis, data normalization, and threat intelligence summarization. By automating complex tasks, it reduces manual effort and accelerates response. Supports multiple AI providers, including OpenAI, Mistral, Meta Llama, Gemini, and Anthropic
- **AI-Powered Playbook Builder:** Simplifies playbook creation through an intuitive, LLM-assisted interface that generates workflows from natural language descriptions. By leveraging Cyware's extensive library of actions and integrations, it accelerates security automation. Available exclusively for Cyware cloud deployments with a pre-configured OpenAI instance.
- **AI-Powered Custom Code Generator:** Automatically generates custom code blocks for playbooks from natural language prompts, eliminating the need for advanced coding expertise. This reduces development time while empowering broader teams to customize workflows. Exclusive to Cyware cloud deployments and powered by a pre-configured OpenAI instance.
- **AI-Powered Playbook Runlog Debugger:** Assists in debugging failed playbook runlogs by identifying root causes and providing step-by-step remediation guidance. Embedded directly within the playbook runlog interface, it streamlines troubleshooting and accelerates error resolution. Powered by a pre-configured OpenAI instance.

About Cyware

Cyware is leading the industry in Operationalized Threat Intelligence and Collective Defense, helping security teams transform threat intelligence from fragmented data points to actionable, real-time decisions. We unify threat intelligence management, intel sharing and collaboration, as well as hyper-orchestration and automation—eliminating silos and enabling organizations to outmaneuver adversaries faster and more effectively.

Learn More

Request a Demo Today