POLARITY BY ThreatConnect.

Leveraging AI Integrations to Enhance Organizational Effectiveness

Executive Summary

Polarity connects users to their data and tools, including AI platforms utilizing LLMs, to enhance the ability of users to analyze, visualize, and interpret data from any data source all in one unified view. This makes users more effective by giving them access to disparate data sets, multiple LLMs, all through a no-code user interface. Polarity improves decision making by allowing users to analyze, capture, recall, and share intelligence across any existing workflow, utilizing already in place toolsets, as well as future toolsets like ChatGPT, Google, Azure and even on-premise AI platforms.

Polarity has **over 200 pre-built integrations**, that include AI tools to help users easily:

- Query and Answer
- Summarize
- Interpret
- Extrapolate information from multiple data sources

This brings next generation capabilities to your users. In addition, Polarity supports the establishment of a mechanism to train LLMs and implements a user-driven feedback loop, such that process and algorithms can be enhanced to support specific mission or overarching strategic objectives.

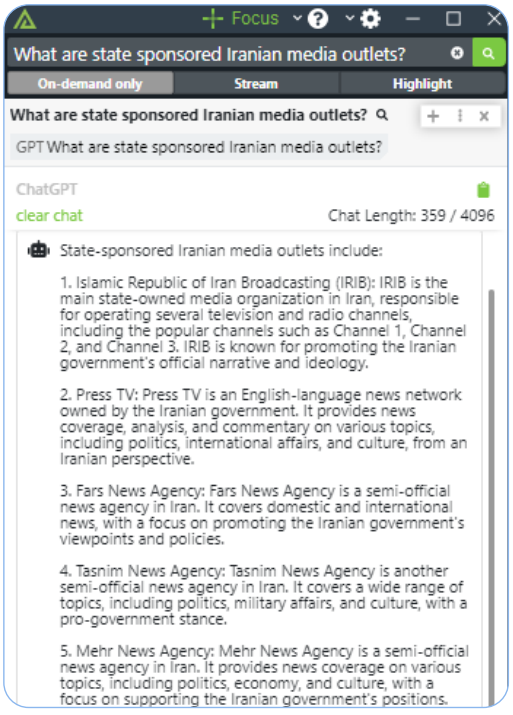
AI Integration Capabilities

Above all else, Polarity is an analyst capability that was developed to support operators in the direct achievement of their responsibilities through more effective and efficient decision making. Polarity includes a suite of capabilities that align directly with enhancing user's capabilities through integrations with AI. The following are some of those chief capabilities.

Query and answer

Polarity integrates out of the box with AI platforms like ChatGPT, Azure and Google, to allow users to ask questions of the various LLMs and receive answers back without having to become AI or prompt engineers themselves. This easy-to-use integration allows users with no data science or prompting background to easily utilize the power of LLMs.

In the example to the right, the analyst can ask a very simple question (e.g. "What are state sponsored Iranian media outlets?") and get a simple answer back from an LLM. It also allows the analyst to ask additional questions and export the responses for information sharing.



ThreatConnect.

ThreatConnect.com
3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com
+1.703.229.4240

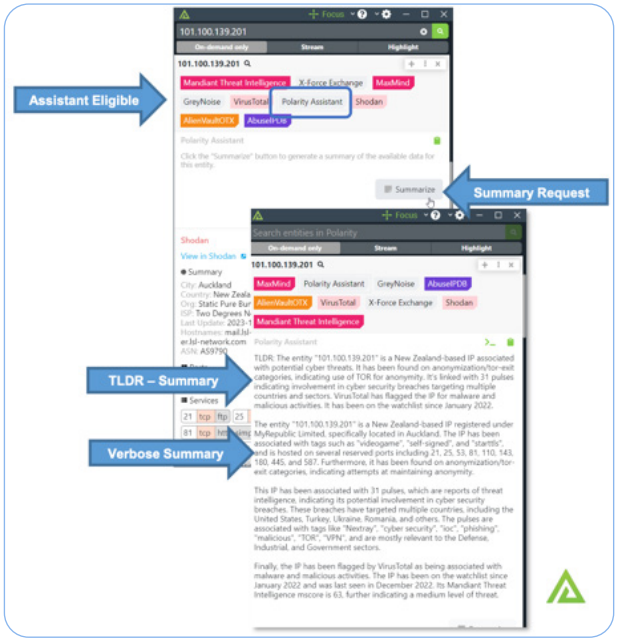
This integration will not make decisions for analysts, but it will help answer questions that would otherwise be time-consuming to investigate. Polarity also allows the user to gather information from sources such that the time associated with hunting and pecking OSINT sources, Publicly Available Information (PAI) can be spent on synthesizing and sense making, rather than searching.

Summarize

The purpose of the Polarity AI Assistant is to provide users with concise and helpful summaries of information, leveraging the capabilities of Large Language Models (LLMs), to assist in understanding and processing data and intelligence from disparate data sources.

By utilizing LLMs, the Polarity AI Assistant can generate summaries that capture the key points and main ideas of the information and intelligence gathered from the user's data sources. The Polarity AI Assistant takes care of all the prompting within the integration code, so there is no need to train the model, or the users.

The LLM can be hosted locally, so there is no need to share the data searched outside of your organization. Also as important, Polarity presents authoritative data from sources leveraged in production in the summary, so that analysts can trust, but verify the content produced.



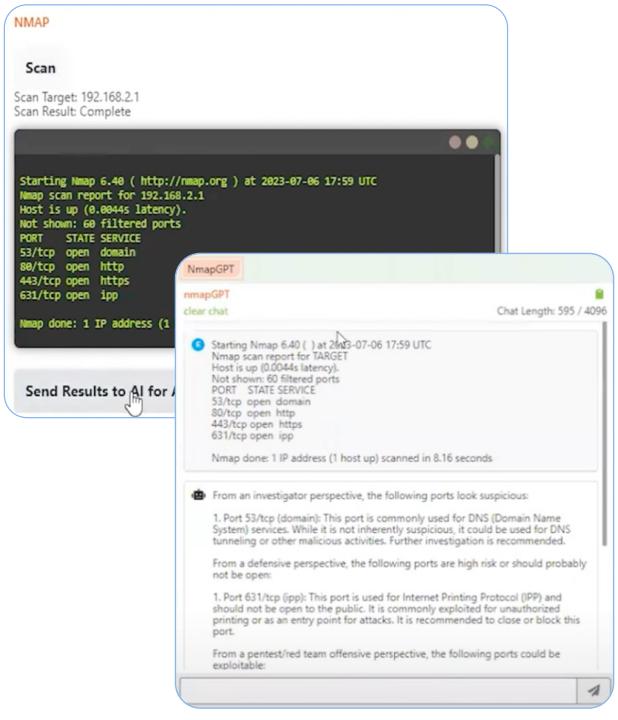
Interpretation

Polarity's open integration framework allows integrations to connect with AI platforms for advanced analysis to interpret content, enhance the findings, and contextualize information for greater understanding by the analyst.

This allows analysts to get multiple perspectives, granting both junior and senior personnel greater speed and confidence in their decisions without having to learn any prompts or queries, and without pivoting out of their workflow.

In the example to the right, an analyst is presented with system output (e.g. NMAP scan result). To an inexperienced analyst, the output is a simple presentation of ports, services, and their status. With Polarity, raw results in this form can be presented back to the analyst with suggestions. In this example suggestions are made for next steps from defensive, offensive and investigative perspectives.

This use case can be expanded to inputs of any variety (code, system events, foreign language, sentiment analysis, combatant weapons capabilities, and more) giving broad mission support.



ThreatConnect.

ThreatConnect.com
3865 Wilson Blvd., Suite 550
Arlington, VA 22203

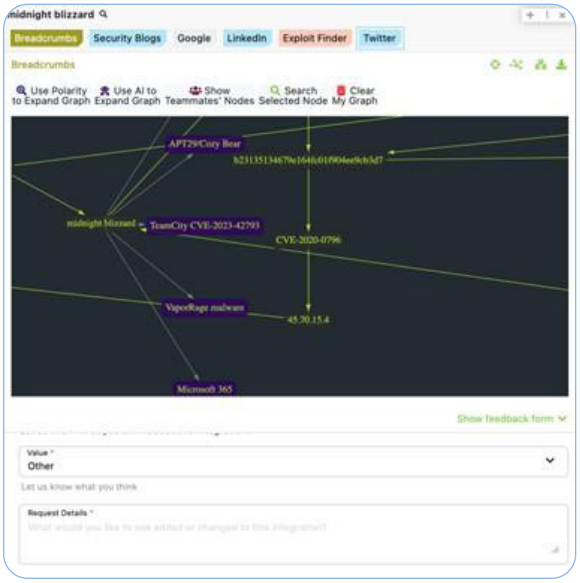
sales@threatconnect.com
+1.703.229.4240

Extrapolation

Polarity enables users to perform federated searches, which means it searches across both internal enterprise sources and/or external open sources. Polarity can run on closed networks.

Polarity can plot these search results on a graph, providing a visual representation of the data and their relationships to one another insofar as investigative history. Users can then perform subsequent searches based on the plotted results and visualize them on the same graph.

The search results can be further refined using an LLM that helps reduce "noise", improve the accuracy and relevance of results discovered with Polarity.



Establishing Feedback Loops

While use and application of capabilities such as those previously described can be powerful, there must be an established mechanism for leadership, key decision makers and technical stakeholders to understand the effectiveness of the capability. This will allow teams to iterate, improve and constantly strive for more optimal outcomes. For a technology that will influence analyst decision making, the likelihood of finding a feedback mechanism stronger than the analysts that consume and action based on these capabilities is unlikely.

Polarity allows for the rapid creation of an online or offline feedback mechanism that can be supplied out of band (e.g. sending feedback to stakeholders via a ticketing solution), in the LLM lifecycle (feeding the response directly back the to an LLM directly) or supporting other methods of feedback collection via the Polarity UI. This is accomplished via feedback collection forms, buttons, and actions that can be introduced into the Polarity UI for engagement by end users. In the image above, see how user can provide feedback to stakeholders via the feedback dropdown included directly below LLM driven results.

Polarity Base Capabilities

KNOWLEDGE Capture

With the touch of a keystroke, you can annotate any string with information worth sharing or remembering. This could be notes on a target, evidence from an investigation, or intelligence on a threat. Polarity's integration framework allows data that has been already captured or available in other tools like Splunk, Elastic, or any other Data Platform to be automatically available to users that are using tools like SOAR, ticketing systems, or other solutions to make informed, high confidence decisions.

Computer Vision

Polarity can enable data collection and collaboration across any workflow. Polarity instantly integrates the collective memory data and internal data sources through the integration framework with your entire team and across existing toolsets. Because it functions at the pixel level — Polarity can recognize any arbitrary string, even data that would not typically be identified with traditional entity extraction or natural language processing techniques.

ThreatConnect.com
3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com
+1.703.229.4240

Overlay

The HUD - Polarity incorporates your team's annotations, LLM(s), log platforms, custom data sets, intelligence platforms, ticketing systems and other software solutions into an actual heads-up display for their desktops that is an overlay directly on their screens to deliver data and context in real-time.

Channels

The collective memory grows over time and users choose what channels of data they subscribe to that are relevant to their workflow. The organization can configure the overlay colors to identify what institutional knowledge is actionable vs informational. Channels can also be user driven and prepopulated. Imagine you are an intelligence analyst investigating a target. How would you find out if another analyst somewhere in your vast organization is investigating the same target? In the event that each user has a unique piece of the analytic puzzle, not collaborating can result in an intelligence failure. Polarity reduces the required actions from two users down to one. When one user captures their notes in Polarity, Polarity automatically shares those notes with other users on the team. Channels can be used for:

- Standard Operating Procedure Awareness;
- Personas Information Capture and Retrieval;
- Threat Actor Groups;
- System References;
- "Hot" Words or Phrases.

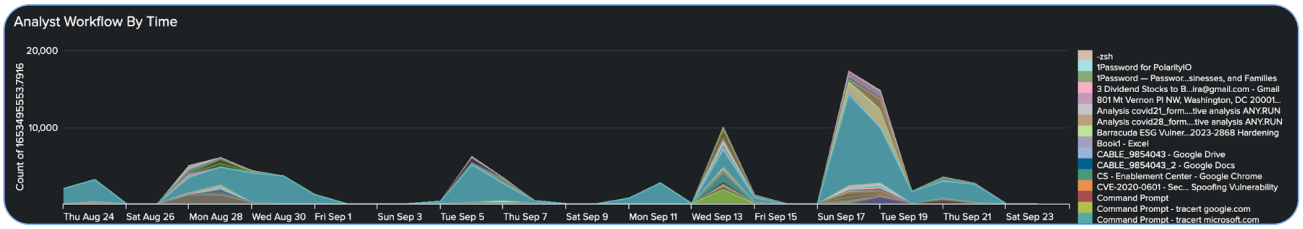
Polarity Source Analytics

Polarity Source Analytics (PSA) offers insights into security operations that have never been seen before. PSA gives visibility across teams', or departments' entire workflows, showing what is searched, what is analyst observed, and what context was actually available at the time your teams are conducting investigations.

ThreatConnect.

ThreatConnect.com
3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com
+1.703.229.4240



PSA allows you to define virtually any dashboard based on your organization's needs. Some of the most powerful dashboards help to show where the blind spots in your data are, where your process bottlenecks are, and which of your tools are delivering value to your team.

By utilizing Polarity, leadership can achieve operational awareness and establish a historical record of operations.

Polarity can foster a culture of continuous learning, knowledge transfer and improvement - mitigating the impact of analyst turnover and ensuring that the entire team benefits from the expertise of their peers.

Learn More

To learn more about Polarity by ThreatConnect and request a custom demo, please connect with us via chat on threatconnect.com or request a demo at threatconnect.com/request-a-demo.

ABOUT THREATCONNECT + POLARITY

ThreatConnect enables threat intelligence operations, security operations, and cyber risk management teams to work together for more effective, efficient, and collaborative cyber defense and protection. With ThreatConnect, organizations infuse ML and AI-powered threat intel and cyber risk quantification into their work, allowing them to orchestrate and automate processes to get the necessary insights and respond faster and more confidently than ever before. More than 200 enterprises and thousands of security professionals rely on ThreatConnect every day to protect their organizations' most critical assets.

Polarity was founded by former intelligence officers and incident responders who built a solution for the challenge they saw cybersecurity teams facing everywhere: knowledge and data is spread across disparate systems, which results in teams making bad decisions based on incomplete comprehension. They didn't want to create just another tool, but a system that fuses all of your disparate data, tools, and knowledge into one unified view. In July 2024, ThreatConnect acquired Polarity.

ThreatConnect.

ThreatConnect.com
3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com
+1.703.229.4240