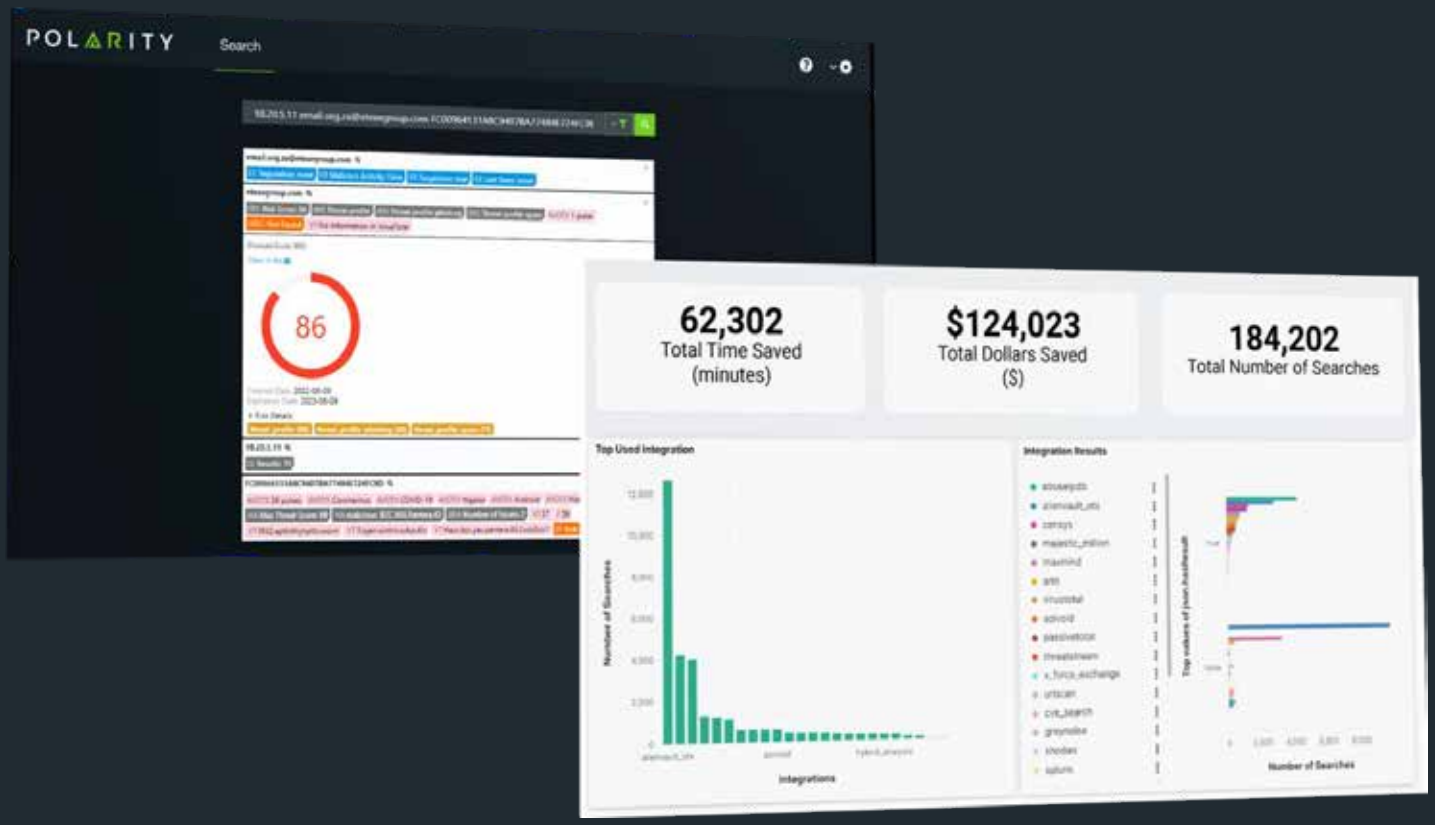
POLARITY

BY ThreatConnect.



Creating Channels that Matter

What is Polarity?

Knowledge and data are spread across disparate systems. Polarity fuses them together in one unified view.
The Polarity platform was created on the principle that people are the most integral component of data analysis.

It provides a new way for IT and Security Professionals to utilize a collective memory by delivering critical intelligence to the right team members only when it is relevant to what they are working on. Polarity drives analysts to make better and faster decisions, increasing productivity, and reducing the risk of a data breach going undetected. Polarity works by analyzing the content of a user's screen and notifying the user about intelligence of interest helping to ensure that security analysts never miss the critical intelligence that could have prevented a devastating data breach.

But "intelligence" takes on many forms. One of the most common but least leveraged forms is the tribal knowledge and know-how learned by team members across a distributed team.

This document is intended to help teams understand how to capture this tribal knowledge and share it in a meaningful way.
Topics include:

- What is a Polarity Channel?
- Why do I Need Polarity Channels?
- Types of Channels
- Channels and Roles
- Channel Suggestions – Investigation Specific
- About Polarity

What is a Polarity Channel?

Channels in Polarity provide a way to organize Entities and Annotations into logical groups. You can subscribe or unsubscribe to different channels to customize the intelligence you receive.

Why do I Need Polarity Channels?

Organizations strive to submit information into common knowledge repositories. However, the repositories are generally meant for longer term preservation of information that is of high confidence. In the process of performing analysis, analysts may make any number of judgments based on information at the time that are not meant for long term retention and/or are of lessor confidence in the early workings of the analytic process. In other scenarios, analysts may have information that is of high confidence, but lack the repository from where judgments can be easily recalled. In summary, these are the core rationalizations for Polarity channels:

- Exist as a context-rich repository for shorter term analytic judgments
- Allow for situational referencing of lower confidence artifacts
- Enable awareness and recall for annotations that have no authoritative or accessible repository.

By encouraging users to capture a brief summary of their analytic judgements in Polarity as an annotation, the collective memory of an organization is expanded, and duplicate work is avoided.

When subscribed to a relevant Channel, Polarity automatically informs users of relevant contextual information based on those annotations enabling other users to draw on the judgements, insights, and knowledge of their team.

Types of Channels

Channels can typically be categorized into the following two types:

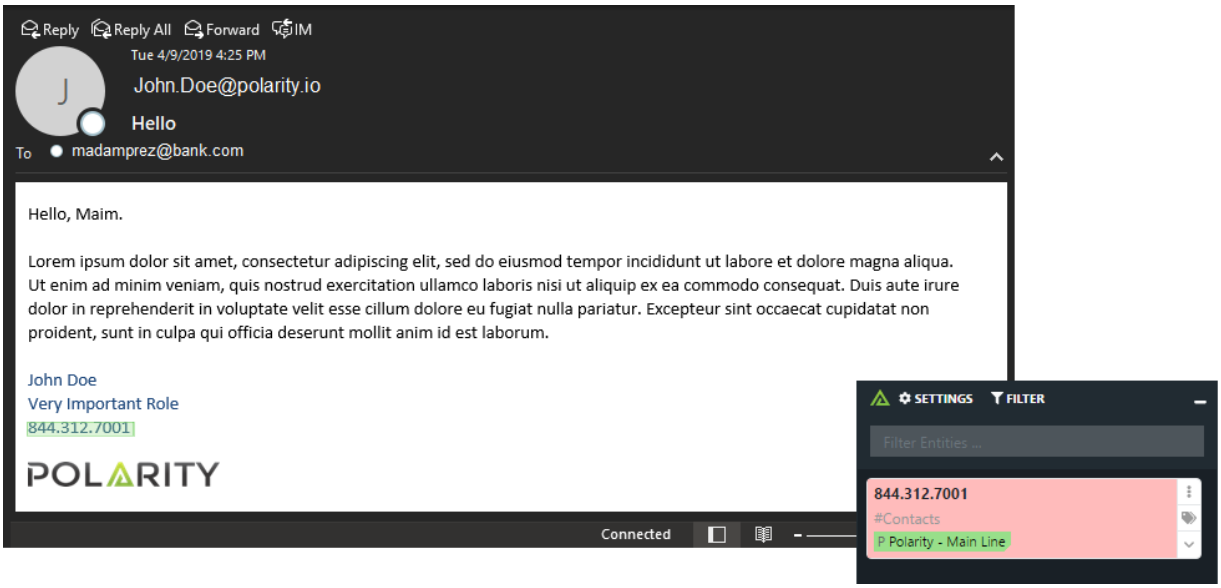
- **Reference Channels** – A Reference Channel is a Channel that has been pre-populated with information that has relevance under certain conditions and workflows. Information in these channels tends to be static or evolves slowly. (Example: Country Codes, Zip Codes)

- **Collaborative Channels** – A Collaborative Channel is organically contributed to over time with the experiences and judgements of analysts that subscribe and contribute to the Channel. Information within these Channels is dynamic and expected to evolve over time. (Example: Contacts)

There are no hard and fast rules for when to create a Polarity Channel. If the user values remembering the relationship between Entities and Annotations, then creating a Channel to manage those relationships will provide a surefire mechanism for enabling situational awareness and recall within Polarity.

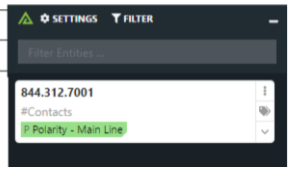
Channels and Roles

The value proposition of specific Channels will vary based on the role of the analyst and their workflows. Take for example a Reference Channel that identifies phone numbers as an entity and overlays the identity associated with the phone number. This phone number Channel has very little value for a security analyst that is reading email that already has the associated identity in a signature line.



The same Channel, however, may be extremely valuable when the identity information is not present on the screen. For example, if an analyst is evaluating phone records as part of an investigation.

Mar 26	11:09 AM	571.444.4444	Fairfield, CT	Leesburg, VA	9	--	--
Mar 26	11:40 AM	844.312.7001	Fairfield, CT	Incoming, CL	3	--	--
Mar 26	11:55 AM	443.444.4444	Fairfield, CT	Elkton, MD	19	--	--
Mar 26	12:19 PM	443.444.4444	Fairfield, CT	Elkton, MD	7	--	--
Mar 26	12:33 PM	781.444.4444	Fairfield, CT	Dedham, MA	3	--	--
Mar 26	1:03 PM	877.444.4444	Fairfield, CT	Toll-Free, CL	23	--	--
Mar 26	2:23 PM	917.444.4444	Fairfield, CT	Incoming, CL	23	--	--
Mar 26	2:47 PM	571.444.4444	Fairfield, CT	Leesburg, VA	1	--	--
Mar 26	3:00 PM	443.444.4444	Fairfield, CT	Elkton, MD	21	--	--
Mar 26	3:28 PM	571.444.4444	Fairfield, CT	Leesburg, VA	23	--	--
Mar 26	3:50 PM	860.444.4444	Fairfield, CT	VM Deposit, CL	1	--	--
Mar 26	3:51 PM	443.444.4444	Fairfield, CT	Elkton, MD	49	--	--
Mar 26	4:40 PM	860.444.4444	Fairfield, CT	Old Saybrk, CT	8	--	--
Mar 26	4:51 PM	844.312.7001	Fairfield, CT	Incoming, CL	1	--	--



In cases where the Channel has limited value given the workflow of an analyst at the time, the analyst can unsubscribe from the Channel until the Channel is needed again.

Channel Suggestions – Investigation Specific

For some, the selection or decision to create a Channel may be apparent; for others, Polarity has created the following to serve as suggestions for those in specific Cyber Security Roles.

Collaborative Channels

Channel Name	Description
Investigation Notes	Annotations indicating investigative judgement or status as it pertains to an investigated domain or other IOCs. • Annotations as to the legitimate business relationship with a domain • Annotations regarding file names • Annotations regarding the user who has been targeted with the potential malware. (e.g., "Executive") • Historical investigation activities taken against a specific indicator.
Temporary Operating Procedures	In the event of a prolific attack affecting the company or the industry, specific operating procedures can be annotated to allow for dissemination of those operating procedures to analysts when relevant to what they are working on. For example: • "badguyz.com" –> Per X-ISAC communication, currently being leveraged in targeted remote access tool distribution.

Reference Channels

Channel Name	Description
Top Level Domains	A Channel that serves as a repository for domain extensions representing the country associated with the domain.
Enterprise Domains	For large organizations, there may be registered domains numbered in the 100s or 1000s. Establishing a reference channel for business domains will allow analysts to quickly determine whether certain indicators identified during an investigation are legitimate.

About Polarity

Polarity fuses knowledge and data together into one unified view, enabling immediate information delivery, automating knowledge transfer across teams, and allowing leaders to understand which of their data sources deliver value. Polarity revolutionizes how teams work, what they spend their time doing (completing tasks, not searching for context), and how informed their day-to-day decisions are.