POLARITY

Use Cases and Quick Wins for Security Operations Centers

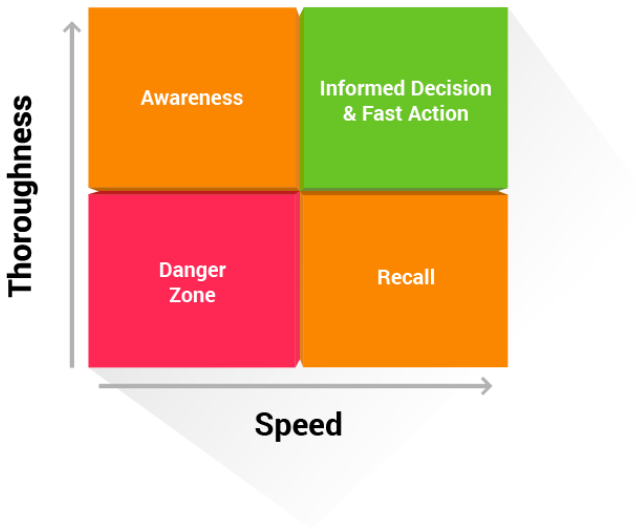
Introduction

Security Operations Teams are overwhelmed with the never-ending flood of events and with context they need to gather from too many places. To reduce the time analysts spend looking up contextual information, attempts are made to integrate it directly into the SIEM. This becomes another never-ending problem of not enough development cycles and not enough screen real estate. The last thing analysts want is another place to search or another dashboard to open—they already have 20+ browser tabs open and too many plugins. Successful teams find the balance of integrating the critical context and relying on analyst intuition to decide the right rabbit holes to dive down (good thing the 86 billion neurons that support human intuition are not that bad) but it is not perfect.

Top performing teams use Polarity and have a comprehensive understanding of their data, knowing how to access the best data available, having the context to see how it is relevant to their work, and seamlessly sharing it between teammates. Polarity is Augmented Reality on top of your team's existing workflow, a way they can see the data better:

- The new analyst can know every CIDR range on day one
- The consultant can know every employee ID when she first looks at the SIEM
- Everyone can see the difference between users, between hosts, between IPs

Polarity does not replace their intuition, it does not work against it by asking them to open another dashboard, Augmented Reality feeds their intuition with data so they can see the full story and see it faster. It is NOT a new place to search, it is an overlay on top of all existing technology and tools used by the SOC today.



Security teams are often forced to balance between being thorough and getting the job done quickly. The image left illustrates this relationship. Consider the analyst who thoroughly investigates every detail (i.e. upper left quadrant); fully **aware** by the time he finishes the job, but too late to act soon enough to make a difference. Similarly, there is the analyst who works on intuition. She speeds through the investigation (i.e. lower right quadrant), **recalling** some details, but missing others that may be important to the investigation.

Polarity overlays contextual information as you work for thoroughness and speed. Software-based Augmented Reality gives you the right data at the right time to make informed decisions and act with speed (i.e. upper right quadrant). With Polarity, teams are no longer forced to balance between being thorough and getting the job done quickly.

How to use this Document

Polarity is committed to continually demonstrating value and increasing the value it provides to its customers.

This document is intended to illustrate popular use cases that Polarity customers are using to enhance their security operations team's ability to triage, contain, and remediate both events and incidents. These use cases include:

- Environmental / Asset Awareness
- Domain Analysis
- Identity Awareness
- Hash Analysis
- Analyst Coordination / Shift Transition
- Consistency and Quality of Analyst Workflows
- Effective Application of SOAR Playbooks

Environmental / Asset Awareness

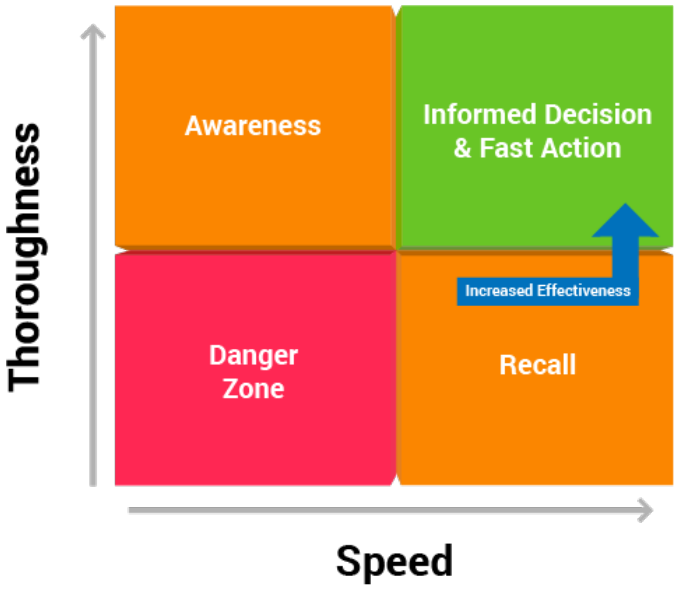
Description:
Polarity enables real-time visibility of assets represented within log analysis tools, SIEMs, SOARs, or other workflow events - well beyond what is included in existing workflow platforms.

Capabilities:

- Polarity overlays asset information sourced from Asset Management or CMDB platforms, conveying the owners, the business risk, and software specifics.
- Polarity overlays segment and network details specific to the asset's environment (e.g. this asset resides within a high-risk CIDR range).
- Polarity overlays the vulnerability exposure of an asset. This can be sourced from:
    - Vulnerability management systems
    - Disparate ticketing systems
    - Spreadsheet outputs uploaded to the Polarity platform
- Polarity overlays existing exceptions applied to the asset.
- Polarity overlays historical tickets related to the asset. This might include:
    - In-flight efforts (that might actually be triggering the event)
    - Historical efforts that might have significant relevance (e.g. an assets exception to password policy)
- Polarity can be leveraged to annotate assets when such assets are:
    - Not included within Asset Management / CMDB
    - Not current within Asset Management / CMDB
    - There is no Asset Management / CMDB

Benefits:

- The number of searches against disparate data sources is significantly reduced, possibly to zero.
- Polarity can promote Asset Management system currency via the integration with ticketing systems whereby analysts can report shadow IT or assets that have less than current records.



Environmental / Asset Awareness Chart
Delivery term – **Immediate (Hours/Days)**
Representative Integrations – **Asset Repository, Vulnerability Scanners**
Representative Channels – **CIDR Ranges, Asset Knowledge Gaps**
Polarity Use Case Frequency – **High**
Core Value Prop – **Effectiveness**
Customer Time Commitment to Establish Capability – **Very Low**

Domain Analysis

Description:
Domains tend to be a key area of focus for Security Operations Centers. There are multiple resources to validate integrity and determine an organization's historical relationship with a domain prior to making a high-quality decision. Polarity enables analysts to execute searches against multiple points of reference and actions to be taken if needed.

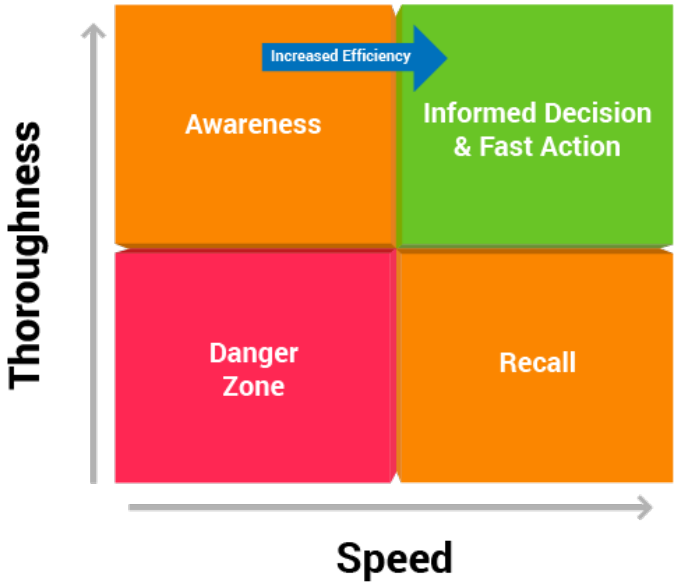
Capabilities:

- Polarity augments the analyst view with information sourced directly from **multiple** domain intelligence platforms. Examples of integrations with free sources include:
  - URLScan
  - URLHaus
  - VirusTotal
- Polarity overlays open source and commercial threat intelligence that is specific to the domain.
- Polarity ensures that the **most recent** information is pulled, not only the information that was pulled at the time of ingestion.
- Polarity automatically demonstrates historical relationships between the enterprise and the domain (e.g. via immediate query to proxy logs).
- Polarity highlights whether the IP addresses associated with the domain have been observed from enterprise firewalls.
- Via channels or integrations, Polarity creates awareness for the business relationships between the domain and the enterprise (e.g. Entity: "Polarity.io" Annotation: "Is a trusted partner.").
- Polarity initiates actions against domains. For example:
  - If integrations support scan requests (e.g. URLScan), scans can be kicked off.
  - If SOAR playbooks exist, drive by simulations may be initiated.

Benefits:

- Higher quality decisions as a direct result of available context sourced from multiple sources.

- Increased efficiencies as the effort to perform disparate searches no longer monopolizes opportunities for more scrutiny and detail-oriented analysis.
- Analysts can immediately determine the relevance of domain to the enterprise.



Domain Analysis Chart

Delivery term – **Immediate (Hours/Days)**
Representative Integrations – **Asset Repository, Vulnerability Scanners**
Representative Channels – **CIDR Ranges, Asset Knowledge Gaps**
Polarity Use Case Frequency – **High**
Core Value Prop – **Effectiveness**
Customer Time Commitment to Establish Capability – **Very Low**

Identity Awareness

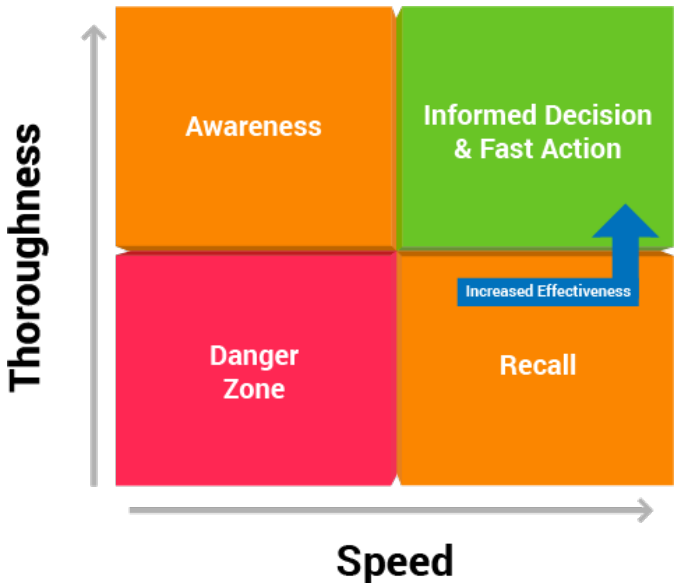
Description:
Polarity enables visibility into user profiles and other attributes commonly viewed within log analysis tools, SIEMs, SOARs, or other workflow events - well beyond what is included in existing workflow platforms.

Capabilities:

- Polarity overlays user information sourced from LDAP platforms.
- Polarity provides insights into historical user tickets (e.g. user deprovisioning requests overlaying on top of successful authentication event).
- Polarity overlays the risk exposure of a user. This can be sourced from:
  - Public sources that associate the user's information to data loss events (e.g. immediate references against https://haveibeenpwned.com)
  - Data Loss Prevention (DLP) event logs
  - Insider threat management systems "base risk" scores
  - Insider threat management system baselines
- Polarity overlays VPN log events to allow the analyst to determine the region the user has logged in from.

Benefits:

- Analysts can make much more informed decisions regarding the true severity of an event based on the contextual user information that is overlaid on their screen.
- Correlations that might not have otherwise been possible, or possible only with significant ETL, development, and added mouse clicks, are now available on the fly.



Identity Awareness Chart
Delivery Term – **Immediate (Hours/Days)**
Representative Integrations – **LDAP, User Log Indices**
Representative Channel – **Service/Admin Accounts, VIPs, Compromised Accounts**
Polarity Use Case Frequency – **High**
Core Value Prop – **Effectiveness**
Customer Time Commitment to Establish Capability – **Very Low**

Hash Analysis

Description:

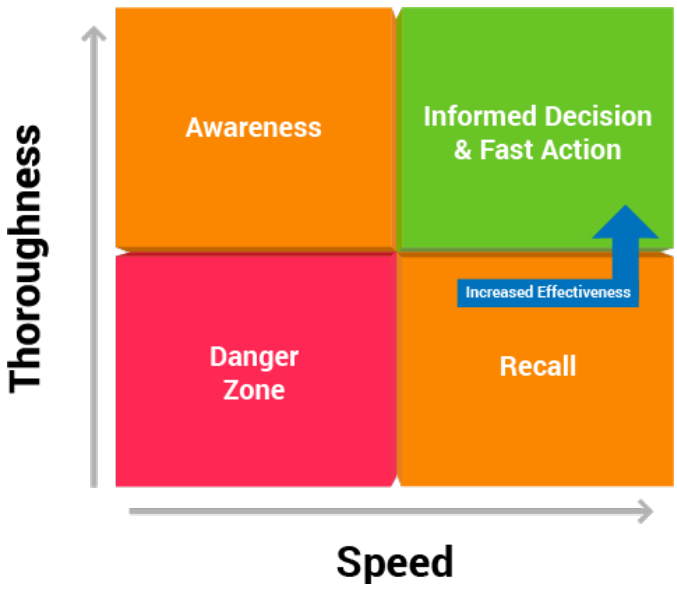
Polarity enables **real-time analysis** of hashes that are present and displayed across workflow systems or captured as part of isolated information security events.

Capabilities:

- Polarity overlays information sourced from public repositories regarding the malicious or non-malicious nature of the hash.
- Polarity overlays open source and commercial threat intelligence over a hash as it is displayed on a screen. Note: In security operations this can be access controlled to read-only.
- Polarity can allow for the overlay of internal information related to the hash that analysis might be re-reviewing. For example:
  - Collisions with "known-good" hashes
  - Historically reported false positives
  - Procedures associated with handling the hash
- Polarity allows for immediate reference against a gold-build hash set.
- Analysts can leverage Polarity as the means for contribution to internal databases of known hashes.
- Polarity allows for immediate retrieval of historical events associated with the hash that are present within connected logging or log consolidation / aggregation platforms.
- Polarity can initiate submissions of hashes to platforms (e.g. sandboxes) for analysis.
- Polarity will automatically query Endpoint Detection and Response platforms presence of the hash within an enterprise.
- Jointly with integrated SOAR platforms, Polarity will initiate pre-defined containment activities.

Benefits:

- Earlier identification of malicious or potentially malicious hashes.
- Immediate understanding of a hash's presence or lack thereof in the remainder of the enterprise.
- Immediate understanding of historical events involving the observed hashes.
- Avoidance of costly investigations into previously investigated or benign hashes.



Hash Analysis Chart
Delivery Term – **Immediate (Hours/Days)**
Representative Integrations – **Threat Intelligence, OSINT Hash Data (e.g. Virus Total)**
Representative Channel – **Known Collisions, Gold Build Hash Inventory**
Polarity Use Case Frequency – **Medium**
Core Value prop – **Effectiveness**
Customer Time Commitment to Establish Capability – **Very Low**

Analyst Coordination / Shift Transition

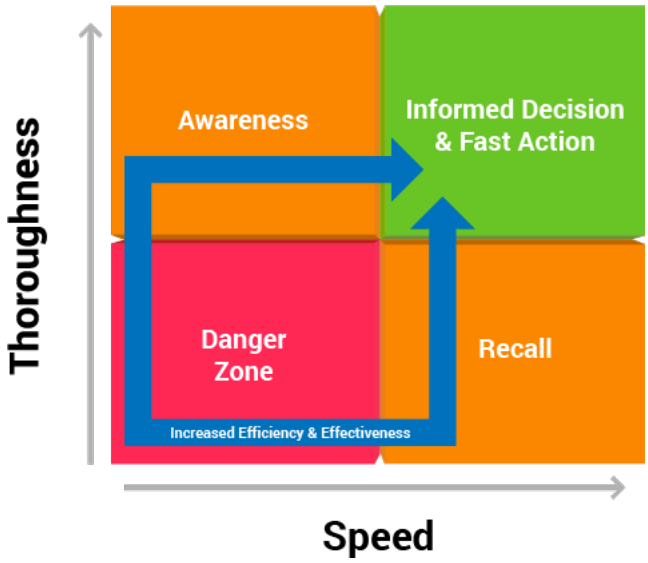
Description:
Polarity empowers analysts not only with the **right information** to conduct their investigations, but **strengthens the collaborative fabric** between analysts, allowing them to **reduce fatigue** and **minimize duplicative efforts**.

Capabilities:

- Polarity allows analysts to contribute towards a shared knowledge base that is accessed into in a just-in-time format, such that the lessons learned by one analyst can be shared immediately as it becomes relevant. The knowledge base extends across:
    - Time zones
    - Shift changes
    - Universal overlays on all tools
- Polarity allows analysts to understand if others have encountered similar data points and entities on their screen, allowing them to tap into the **organizations most value assets – <u>its people.</u>**
- Polarity has basic integrations that allow for instant language translation, allowing for analysts to gain viability into historical exchanges applicable to their investigations that contain foreign languages. For example:
    - Developer notes within code bases
    - Historical email interaction
    - Tickets submitted to updated in foreign languages
    - Websites that contain foreign text
    - Intelligence feeds / OSINT analysis that require translation

Benefits:

- Coordination - Analysts can tackle more when they can quickly understand what has been analyzed by their colleagues as well as what determinations have been made and why.
- Contribution – Instead of duplicating analysis, analysts can complement or contribute to the analysis of their peers, allowing for deeper analysis of the indicator or fresher perspective with the understanding that certain elements of an investigation have already been accounted for.
- Knowledge Share – When analysts become aware of the decision processes or rationalizations for the action / inaction of their peers, they can collaborate not only on the end result, but foster mind-share that can be applied for higher quality analysis in the future.



Analyst Coordination / Shift Transition Chart
Delivery Term – **Immediate (Hours/Days)**
Representative Integrations – **Google Translate, Analyst Metrics**
Representative Channel – **Investigated, False Positives, SOPs**
Polarity Use Case Frequency – **Medium**
Core Value prop – **Efficiency & Effectiveness**
Customer Time Commitment to Establish Capability – **Very Low**

Consistency and Quality of Analyst Workflows

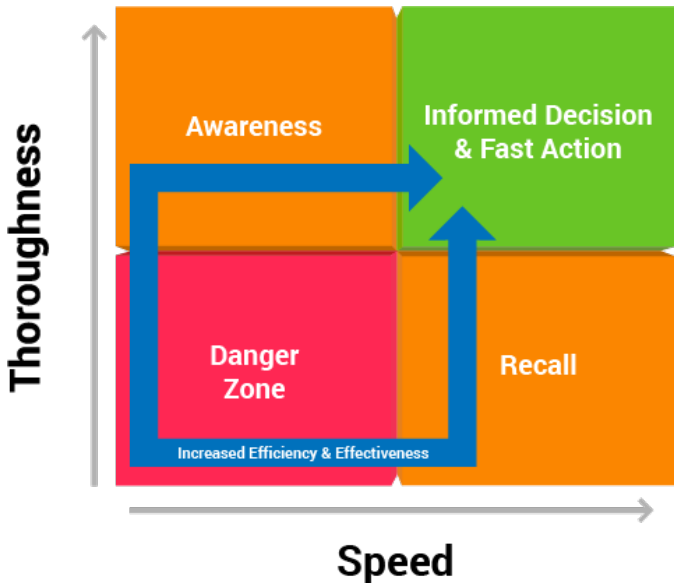
Description:
SOC leadership must balance speed of analysis with quality of analysis. Turnover of analysts also means knowledge and experience loss and a continual skill set disparity among team members. A SOC leader must ensure that all events and incidents are handled to the same expectations across team members irrespective of tenure.

Capabilities:

- Polarity Channels provide real-time Knowledge Repositories, replacing time consuming and frustrating knowledge expeditions into Confluence, Jira, SharePoint, etc.
- Annotations promote real-time collaboration and retention of analysis and decision making.
- SOC leaders determine what authoritative data sources analysts will use to draw conclusions.

Benefits:

- Senior Analysts' experience and previous conclusions are provided to all other team members, allowing them to directly benefit from this experience in real-time.
- Turnover doesn't mean loss of knowledge; experience and decision making is retained by Polarity.
- Analysts don't have to "Google" information when they need data to make an informed decision. Approved and curated data is provided in real-time at the point of analysis.
- Workflow checklists are enabled with the curated data provided by Polarity.
- SOC leaders can view the decision making of their team members and conduct QA/QC spot checking by reviewing Annotations and Channels.



Analyst Workflows Chart
Delivery Term – **Immediate (Hours/Days)**
Representative Integrations – **All**
Representative Channel – **"Investigated", "False Positives", "Hash Collisions"**
Polarity Use Case Frequency – **High**
Core Value prop – **Effectiveness**
Customer Time Commitment to Establish Capability – **Low**

Enable Effective Application of SOAR Playbooks

Description:
Enable effective application of SOAR Playbooks. Despite the power and promise of SOAR capabilities, the fact remains that operation impact awareness is still often left to humans. Just because one "can" automate and take action, does not always translate to "should" take action. Humans remain in the loop when containment and remediation actions have the potential to cause operational impact.

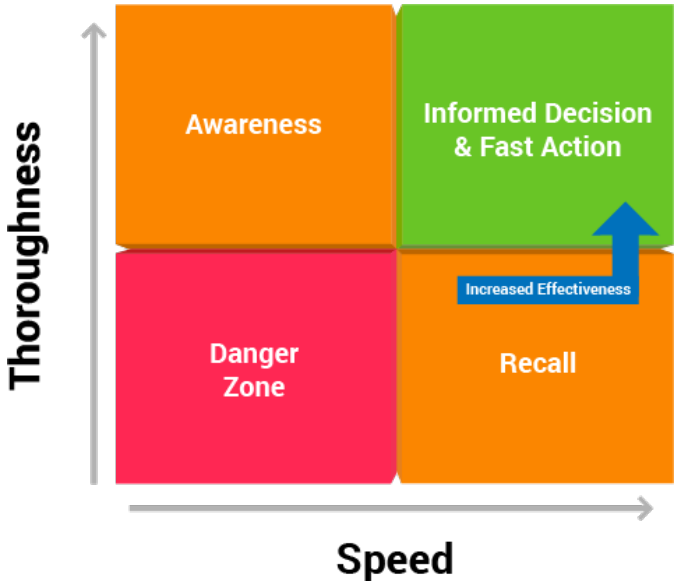
Capabilities:

- SOAR playbooks are selected and run from the Heads-Up Display.
- The operational context needed to understand an assets criticality, connectivity and location are provided in the same field of view as the playbook trigger.

- Analyst telemetry and workflow can be collected with Polarity to use data to prioritize the best playbooks to invest time in building.

Benefits:

- Polarity helps ensure that an action enabled by a SOAR capability is a fully informed one.
- Operational impacts can be minimized or eliminated when analysts know what function an asset serves prior to launching containment and remediation actions.
- Environmental awareness is in the same field of view and the trigger to launch the action.



SOAR Playbooks Chart

Delivery Term –

Representative Integrations – **Phantom, Swimlane, XSOAR,**

Representative Channel – **"Playbook Guidance"**

Polarity Use Case Frequency – **Moderate**

Core Value prop – **Efficiency**

Customer Time Commitment to Establish Capability – **Low**