Use Cases and Quick Wins for Security Operations Centers

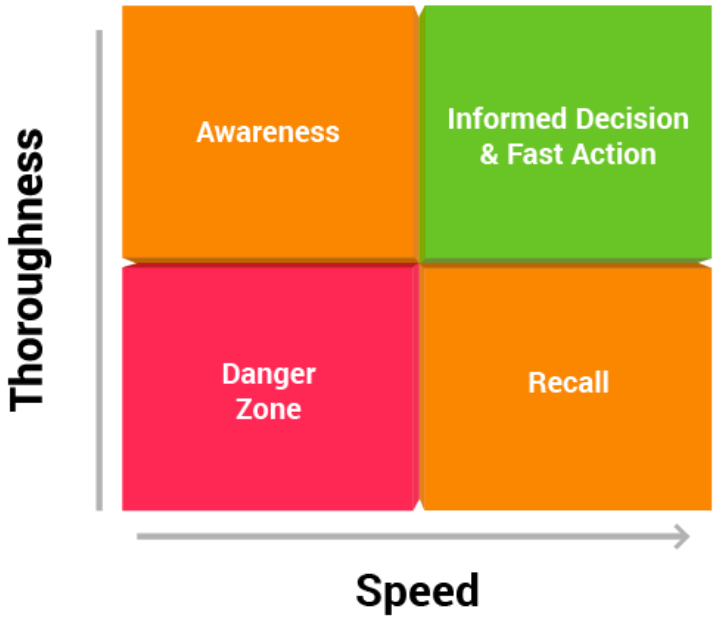
Introduction

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
- Pragmatically Apply Threat Intelligence
- Analyst Coordination / Shift Transition
- Ensure Consistency and Quality of Analyst Workflows
- Enable Effective Application of SOAR Playbooks

Environmental / Asset Awareness

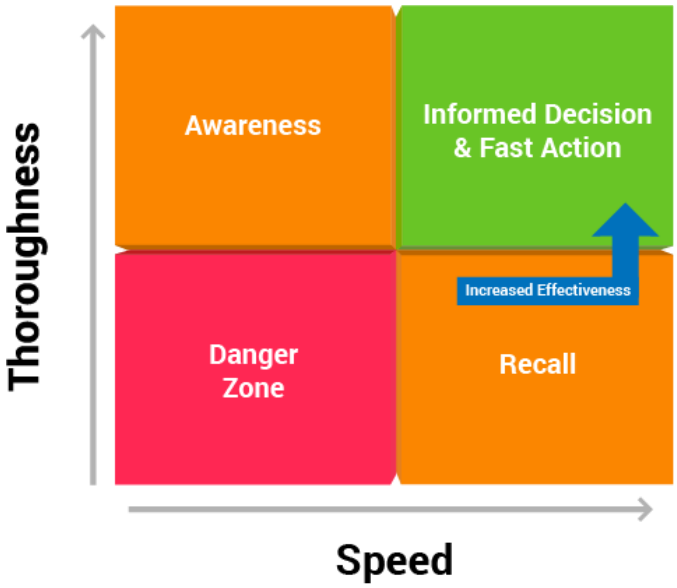
Description:

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:

- 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 AwarenessChart

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:

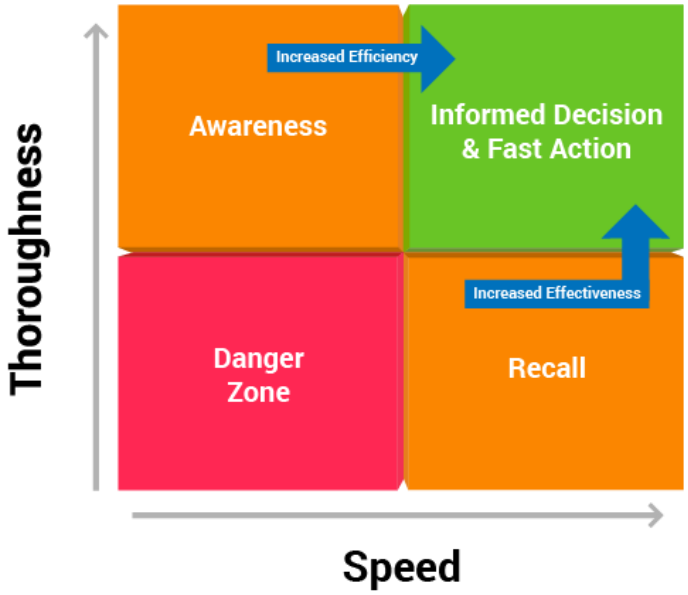
Domains tend to be a key area of focus for Security Operations Centers. There are multiple resources to validate integrity and determine an organization's historical relationship with a domain prior to making a high-quality decision. Polarity enables analysts to execute searches against multiple points 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 – **Free Integrations (www.polarity.io/integrations)**
Representative Channel – **Partner Domains**
Polarity Use Case Frequency – **High**
Core Value prop – **Efficiency**
Customer Time Commitment to Establish Capability – **Very Low**

Exposure Assessment

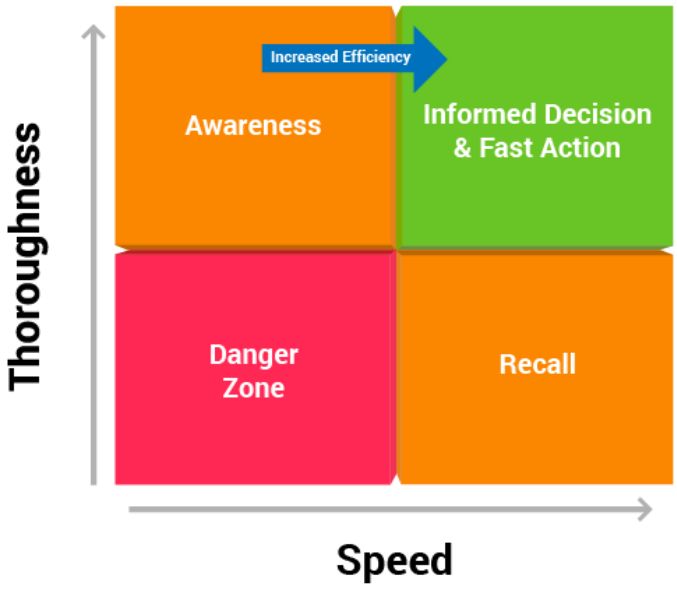
Description
To understand the risk that threat actors pose to an enterprise, analysts must have strong understanding of their vulnerability and exposure to exploitation by threat actors. Polarity allows for both a rapid and thorough assessment of vulnerabilities exposure through on-screen overlays.

Capabilities:

- Polarity allows for the triage analysis of Common Vulnerability and Exposure (CVE) designations. Additional information regarding the CVE can be queried from public records or from commercial data sources.
- Polarity allows for the retrieval of OSINT and commercial threat intelligence regarding the CVE.
- Polarity allows for the retrieval of information that informs an analyst of the availability of exploit code.
- Polarity provides real time access into vulnerability scan data that can inform the analyst of the presence of a specific exposure within their environment.
- Via Polarity's annotation framework, analysts can document known mitigating controls specific to their enterprise as it relates to historical CVEs under investigation.
- Ticket and other workflow platforms can be queried in real time to inform the analyst of work that is complete, incomplete or inflight regarding a CVE.

Benefits:

- Analysts can more quickly understand their exposure to published vulnerabilities.
- If the exposure exists, analysts can immediately tap into insights related to the viability of threats or threat actors that might seek to exploit the vulnerability.
- Analysts can pursue mitigations more rapidly and with more certainly given the confidence of making the most informed decision.



Exposure Assessment Chart
Delivery term – **Immediate (Hours/Days)**
Dependencies – **None**
Polarity Use Case Frequency – **High**
Core value prop – **Efficiency**
Customer Time Commitment to Establish Capability – **Very Low**

Investigation Collaboration

Description

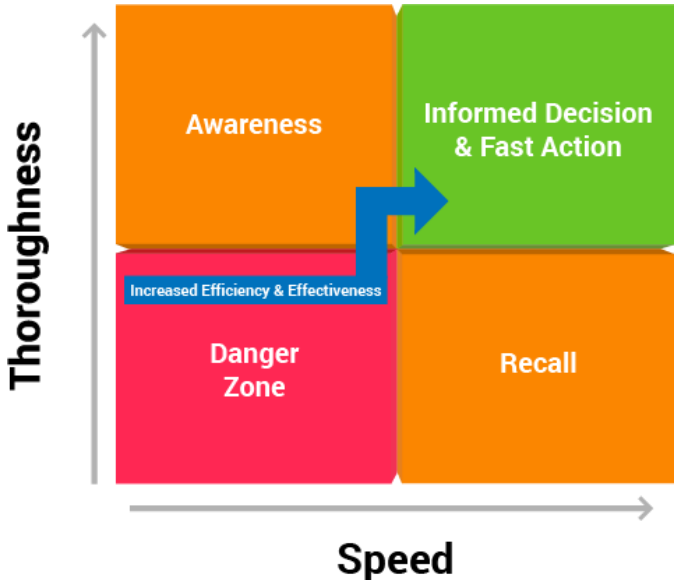
Larger investigations and/or inquiries will inevitably result in **more data** to analyze and **more contributors** to the investigation process - this will lead to a **duplication of efforts**, increased likelihood information failures and delayed time to decision or action if required. Polarity's annotation capability, coupled with team collaboration metrics, can allow team members to better collaborate and capture more opportunities.

Capabilities:

- Polarity allows for the association of annotations to entities that may appear on an analyst's screen. Once applied, those annotations can be shared across analysts, or across access-controlled groups.
- Polarity allows for more granular notes to be applied to annotations in the form of comments. These comments can create awareness surrounding efforts actively being applied or determinations made regarding entities that may be observed many times with an investigatory workstream.
  Polarity is packaged with the means to assess if team members have encountered the same indicator.
- Knowing that it is possibly the first time an indicator has been encountered may prompt an analyst to demonstrate more diligence in analysis.

Benefits:

- Coordination - Analysts can tackle more when they can quickly understand what has been analyzed by the 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. This allows for deeper analysis of the indicator or a fresher perspective with the understanding that certain elements of an investigation have already been accounted for.
- Knowledge Sharing – When analysts become aware of the decision processes or rationalizations for 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.



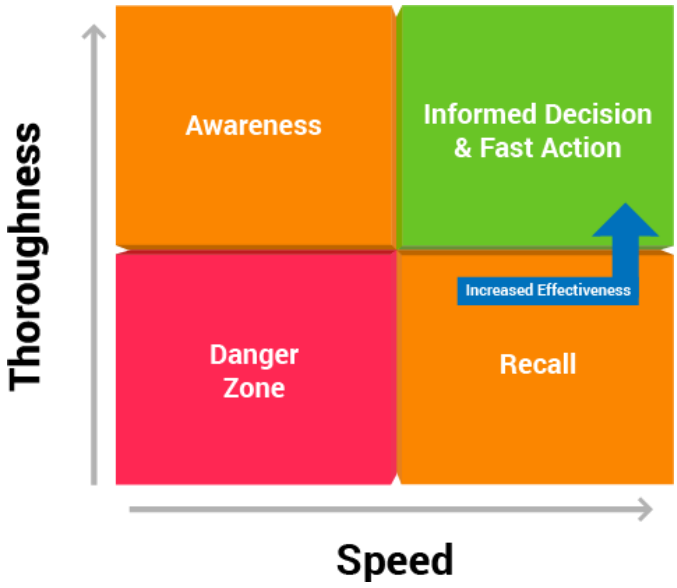
Investigation Collaboration Chart
Delivery term – **Immediate (Hours/Days)**
Dependencies – **None**
Polarity Use Case Frequency – **High**
Core value prop – **Effectiveness**
Customer Time Commitment to Establish Capability – **Very Low**

Threat Intelligence Dissemination & Enablement

Description:
Polarity delivers access-controlled dissemination of intelligence to supported teams. Ensuring that the intelligence curated and products developed for consumption are capitalized upon by those who would leverage it in decision making.

Capabilities:
Information that is collected by intelligence analysts can be exposed to a broader spectrum of analysts (e.g. SOC, IR), such that it can be read when it is applicable to what they are working on.

Benefits:
Dissemination of threat intel is a significant challenge. Polarity enables provisioning of the right information at the right time to the right people.



Threat Intelligence Dissemination & Enablement Chart
Delivery term – **Immediate (Hours/Days)**
Dependencies – **Threat Repository**
Polarity Use Case Frequency – **High**
Core Value Prop – **Effectiveness**
Customer Time Commitment to Establish Capability – **Very Low**