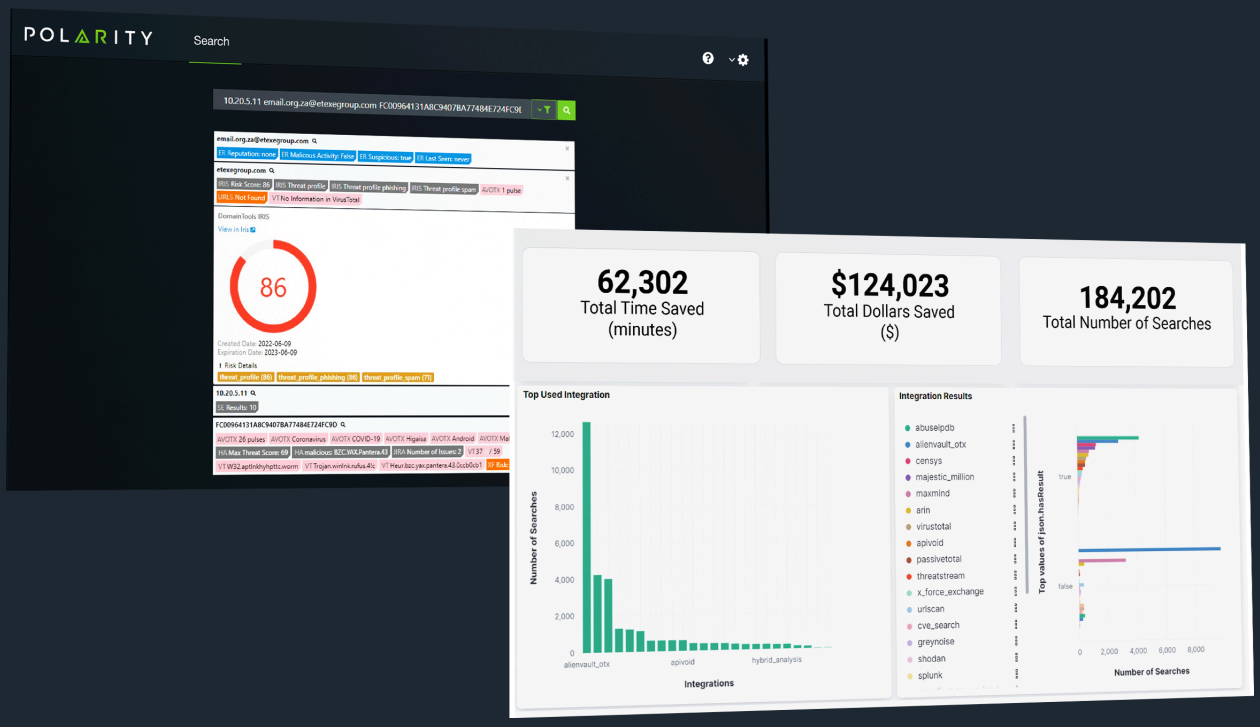
POLARITY

+ ThreatConnect.



Use Cases and Quick Wins for Threat Intelligence Teams

Introduction

Polarity fuses together knowledge and data from across an organization with an expansive integration and annotation framework, enabling Threat Intelligence teams to make one search to find information across all of their tools, internal data sets, communication platforms, and team/cross-department knowledge. Polarity enables:

- Immediate knowledge delivery for informed decision making
- Full data visibility and asset awareness
- Improved team communication and automated knowledge transfer for team member onboarding

Users can connect to over 180 different tools inside of their environment or to external open source information. With Polarity's integration framework, anyone can develop an integration quickly and get visibility into any data set.

Polarity not only enables knowledge delivery through the integration framework, but also through our annotation framework. Polarity allows users to add and enrich any information so they and their entire team/organization can make better informed decisions.

With Polarity Source Analytics, Polarity's telemetry feature, leaders are able to understand what tools deliver value, make informed spending decisions, and remove process deficiencies.

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

This document is intended to illustrate some of the use cases in which Polarity customers are enhancing their threat intelligence operations with Polarity. Use cases include:

- *Collection Support*
- *Indicator Analysis / Triage Support*
- *Exposure Assessment*
- *Investigation Collaboration*
- *Threat Intelligence Dissemination & Enablement*

Threat Intelligence - Use Cases

Collection Support

- Description:
  - Polarity enables on-the-fly ***collection*** and ***ingestion*** of intelligence into threat intelligence repositories.

- Capabilities:
  - Once entities are populated in the overlay window, an analyst can observe what is in a threat repository (See Indicator Analysis / Triage Support Use Case) as well as observe what entities are not currently represented in the repository.
  - Polarity allows for the bulk submission of indicators into threat repositories
  - Polarity allows for tagging and organization of indicators from the screens the analyst is working from, rather than needing to log into a threat platform.

- Benefits:
  - Coverage - Polarity allows for this collection and ingestion from ***any screen***, not just limited to browser content. The efficiencies associated with historical browser-only plugins are now extended to all platforms leveraged by the threat analyst. For example:
    - Indicators observed in OSINT gathering
    - Indicators observed within a VM
    - Indicators observed within a mail client
    - Indicators contained in within write/copy protected content
    - Indicators presented via community sharing web session
  - Clarity - Analyst can understand if there are evolving threats associated with historically investigated indicators
  - Consistency - for structured population of a channel/integration and avoid out of structure annotations
  - Quality - Analysts can marry additional sources of public and private intelligence data sources via the Polarity overlay, allowing for the most thorough submissions (e.g. verbose tags, proper classifications) of intelligence into their threat repository.

Delivery term – Short (2-3 Weeks for Anomali)
Dependencies – Threat Repository | Polarity Channel Designated for Intelligence
Polarity Use Case Frequency – High
Core Value Prop – Efficiency
Customer Time Commitment to Establish Capability – Very Low

Indicator Analysis / Triage Support

- Description:
  - Polarity enables **real-time analysis** of indicators **observed** via the threat analysis process. This can be delivered via on-demand or optical modes.

- Capabilities:
  - Situational delivery of indicators already contained within existing threat repositories (e.g. Threat Intelligence Platform (TIP) or proprietary backend)
    - Awareness of indicators status
    - Awareness of indicators status
  - Interaction between connected platform(s) (e.g. apply / remove a tag, add a note)
  - Analysts can link to additional sources of intelligence
  - Analysts can view comments associated with the IOC

- Benefits:
  - Analysts become immediately aware as to the relevance or significance of an indicator on their screen
  - Analysts can immediately determine the relevance of indicators to the enterprise
  - Analysts achieve efficiencies as a by product
    - Reduction of duplicative analysis
    - More collaborative and/or contributory analysis
  - Prioritization of analysis based on organizational context delivery enabling teams to determine the relevance of the threat to the enterprise. (e.g. Query EDR, vulnerability scanners, asset platforms).

Delivery Term – Immediate (Hours/Days)
Dependencies – Threat Repository
Polarity Use Case Frequency – High
Core Value prop – Efficiency & Effectiveness
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 as to the availability of exploit code.
  - Polarity provides real time access into vulnerability scan data that can inform the analyst as to 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 as to 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 as to viability of threats or threat actors that might seek to exploit the vulnerability
  - Analysts can pursue mitigations more rapidly and with more certainty given the confidence of making the most informed decision.

Delivery term – Immediate (Hours/Days)
Dependencies – None
Customer Deployment – Deployed with Top 3 U.S. consumer bank
Core value prop – Effectiveness
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 investigatory process - this will lead to **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 screen. Once applied, those annotations can be shared across analyst pools, 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. 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 action / in action of their peers, they can collaborate not only on the end result, but foster mindshare that can be applied for higher quality analysis in the future.

Delivery term – Immediate (Hours/Days)
Dependencies – None
Customer Deployment – Deployed with Top 3 U.S. consumer bank
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 provision of the right information at the right time to the right people.

Delivery term – Immediate (Hours/Days)
Dependencies – Threat Repository
Customer Deployment – Deployed with Top 3 U.S. consumer bank
Core Value Prop – Effectiveness
Customer Time Commitment to Establish Capability – Very Low