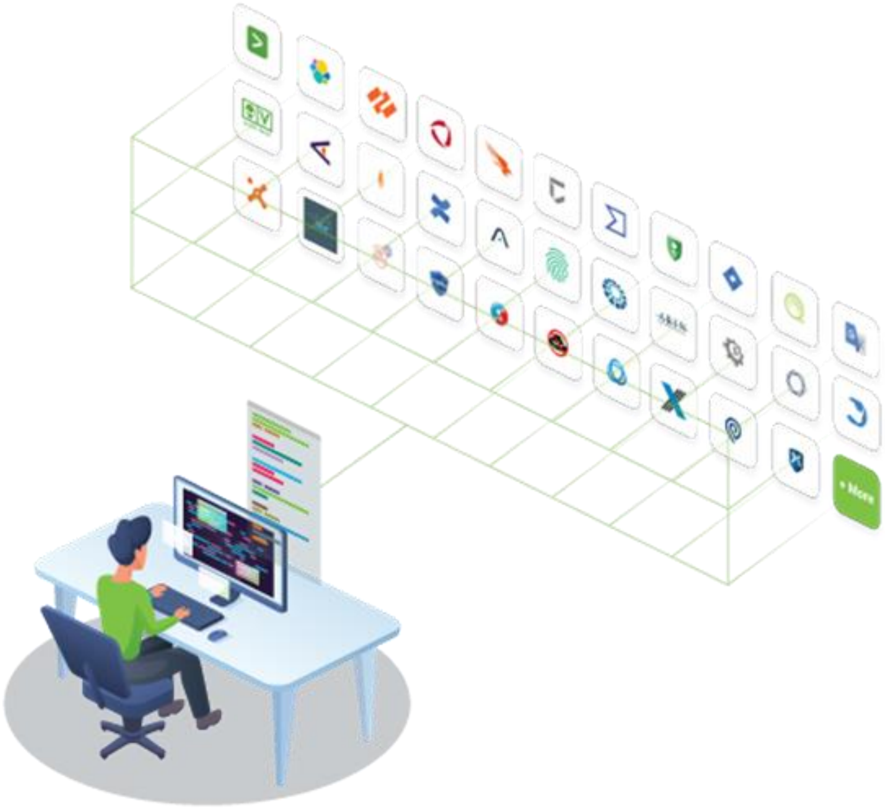
POLARITY

+ ThreatConnect.

MSSP and MDR Use Cases



Background

Managed Services Teams often run lean and take forward-looking and innovative approaches to supporting their customer bases. However, with growing and varying customer bases, there are mounting complexities and nuances in supporting each customer and operating as a seamless extension of the team.

With these complexities, there are traditional challenges that arise from operating a SOC. Managed Services Teams too are overwhelmed with the never-ending flood of events and with gathering the context they need to respond to those events from too many places.

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.

As one Polarity customer stated, Polarity can be their "secret sauce," as it empowers them to optimize their resources, time, and gain further efficiencies which in turn helps them grow their business and helps them have a leg-up on their competitors who are also offering services.

For additional resources regarding Polarity's Managed Service or Managed Detection and Response (MDR) customer's use cases - see the following:

- Practical Use of AI in Cyber Security Analysis with Polarity & Ventech Solutions
- Security Team Works Faster for 200% ROI with Polarity

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

Polarity is a "*unified view*" on top of your team's existing workflow. An MSSP / MDR practitioner that uses Polarity will find that they are better equipped to perform their day-to-day tasks. Managers of analyst teams can expect these representative outcomes:

- The new analyst can know every customer CIDR range(s) on day one
- The consultant can know every employee ID when they first look at the SIEM
- Everyone can see the difference between users, hosts, and IPs
- Teams can maximize the value of licensed tools/subscriptions that enable analyst work
- Reduction in overall alert/event analysis time and increased closure rates
- Everyone will have access to all the necessary data sources in the MSSP/MDR

Polarity is committed to continually demonstrating 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 MSSP/MDR offerings and their team’s ability to triage, contain, and remediate both events and incidents.

> ***“You can, with proper context, come up with the conclusion without having to jump and skip into so many different platforms. It’s nothing overly complex and that’s the beauty about it. It keeps it simple and allows your analysts to really take a deep dive. It’s a combination of things that will actually lower the cost of your SOC and make your team more efficient. It’s a combination of automation and contextualization. Automation to remove those manual steps and contextualization to lower the effort of manual actions that your SOC has to take.”***
>
> *Alexander Sinno, SOC Leader*

Capabilities: Traditional Operational Security Quick Wins

Selector Analysis

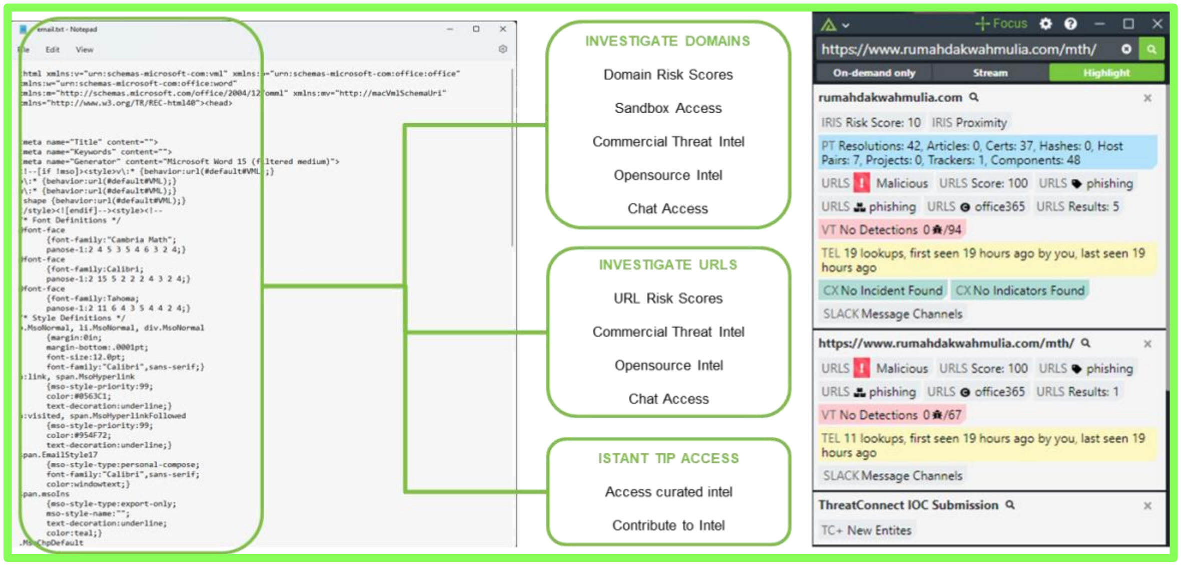
There are multiple resources to validate integrity and determine an organization’s historical relationship with a selector prior to making a high-quality decision. Polarity enables analysts to execute searches against multiple points of reference and actions to be taken.

Sourcing High Value Data Sets:

Polarity enhances analyst views by:

- Sourcing information directly from multiple intelligence platforms.
- Overlaying open source / commercial threat intelligence specific to a selector.
- Delivering the most recent information to teams, not only information sourced at the time of ingestion.
- Automatically demonstrating historical relationships between enterprises and the selector (e.g., via immediate query to proxy logs).

Example: Header Analysis with Polarity



```
html xmlns:v="urn:schemas-microsoft-com:vml" xmlns: ="urn:schemas-microsoft-com:office:office"
mlns:w="urn:schemas-microsoft-com:office:word"
mlns:m="http://schemas.microsoft.com/office/2004/12 omml" xmlns:mv="http://macVmlSchemaUri"
mlns="http://www.w3.org/TR/REC-html40"><head>


meta name="Title" content="">
meta name="Keywords" content="">
meta name="Generator" content="Microsoft Word 15 (f ltered medium)">
!--[if !mso]><style>v\:* {behavior:url(#default#VML ;}
\:* {behavior:url(#default#VML);}
\:* {behavior:url(#default#VML);}
shape {behavior:url(#default#VML);}
/style><![endif]--><style><!--
* Font Definitions */
font-face
	{font-family:"Cambria Math";
	panose-1:2 4 5 3 5 4 6 3 2 4;}
font-face
	{font-family:Calibri;
	panose-1:2 15 5 2 2 2 4 3 2 4;}
font-face
	{font-family:Tahoma;
	panose-1:2 11 6 4 3 5 4 4 2 4;}
* Style Definitions */
.MsoNormal, li.MsoNormal, div.MsoNormal
	{margin:0in;
	margin-bottom:.0001pt;
	font-size:12.0pt;
	font-family:"Calibri",sans-serif;}
:link, span.MsoHyperlink
	{mso-style-priority:99;
	color:#0563C1;
	text-decoration:underline;}
:visited, span.MsoHyperlinkFollowed
	{mso-style-priority:99;
	color:#954F72;
	text-decoration:underline;}
pan.EmailStyle17
	{mso-style-type:personal-compose;
	font-family:"Calibri",sans-serif;
	color:windowtext;}
pan.msoIns
	{mso-style-type:export-only;
	mso-style-name:"";
	text-decoration:underline;
	color:teal;}
.Ms ChpDefault
```

https://www.rumahdakwahmulia.com/mth/

rumahdakwahmulia.com

IRIS Risk Score: 10 | IRIS Proximity

PT Resolutions: 42, Articles: 0, Certs: 37, Hashes: 0, Host Pairs: 7, Projects: 0, Trackers: 1, Components: 48

URLS ! Malicious | URLS Score: 100 | URLS phishing

URLS phishing | URLS office365 | URLS Results: 5

VT No Detections 0/94

TEL 19 lookups, first seen 19 hours ago by you, last seen 19 hours ago

CX No Incident Found | CX No Indicators Found

SLACK Message Channels

https://www.rumahdakwahmulia.com/mth/

URLS ! Malicious | URLS Score: 100 | URLS phishing

URLS phishing | URLS office365 | URLS Results: 1

VT No Detections 0/67

TEL 11 lookups, first seen 19 hours ago by you, last seen 19 hours ago

SLACK Message Channels

ThreatConnect IOC Submission

TC+ New Entites

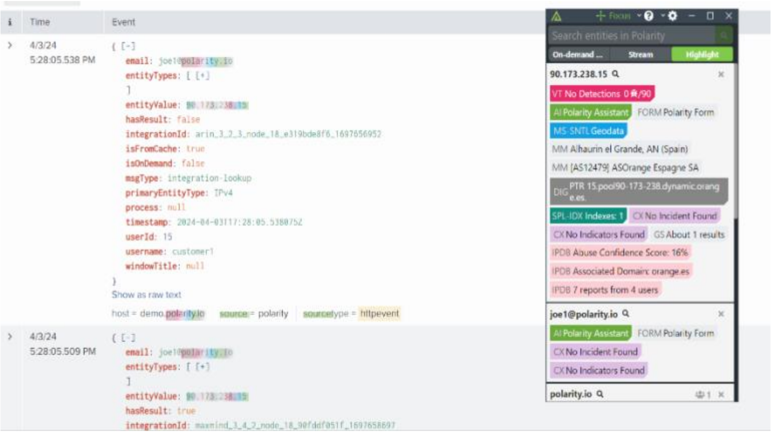
Adding Context:

- Via channels or integrations, Polarity creates awareness of business relationships between selectors and enterprises (e.g., Entity: “Polarity.io” Annotation: “trusted partner”).
- Polarity allows for the capture of valuable information regarding other strings integral to the investigation process. For example:
  - Commonly used binaries in the MITRE ATT&CK chain
  - Hosting providers leveraged by adversaries
  - Banners/nomenclature used in the propagation of malware
  - Language leveraged in phishing campaigns

Enhancing SIEM

Whether you are consolidating events into a single platform, or bouncing from one SIEM solution to the next, there are real pain points associated with working within a SIEM platform. The following are well documented SIEM challenges:

- **Tuning and False Positives**: SIEMs may generate a significant number of false positives, requiring manual tuning to reduce noise and focus on real threats.
- **Integration Challenges**: Integrating SIEM with existing security tools and systems can be challenging, leading to gaps in visibility and effectiveness.
- **Slow Search Processes**: SIEMs collect data from multiple sources. The sheer amount of information consolidated, combined with advanced correlations can overwhelm these systems and slow down the analysis process.



```
i  Time               Event
>  4/3/24             { [-]
   5:28:05.538 PM       email: joe1@polarity.io
                        entityTypes: [ [+]
                        ]
                        entityValue: 90.173.238.15
                        hasResult: false
                        integrationId: arin_3_2_3_node_18_e319bde8f6_1697656952
                        isFromCache: true
                        isOnDemand: false
                        msgType: integration-lookup
                        primaryEntityType: IPv4
                        process: null
                        timestamp: 2024-04-03T17:28:05.538075Z
                        userId: 15
                        username: customer1
                        windowTitle: null
                      }
                      Show as raw text
                      host = demo.polarity.io   source = polarity   sourcetype = httpevent
>  4/3/24             { [-]
   5:28:05.509 PM       email: joe1@polarity.io
                        entityTypes: [ [+]
                        ]
                        entityValue: 90.173.238.15
                        hasResult: true
                        integrationId: maxmind_3_4_2_node_18_90fddf051f_1697658697
```

90.173.238.15

VT No Detections 0/90

AI Polarity Assistant

FORM Polarity Form

MS-SNTL Geodata

MM Alhaurin el Grande, AN (Spain)

MM [AS12479] ASOrange Espagne SA

DIG PTR 15.pool90-173-238.dynamic.orange.es.

SPL-IDX Indexes: 1

CX No Incident Found

CX No Indicators Found

GS About 1 results

IPDB Abuse Confidence Score: 16%

IPDB Associated Domain: orange.es

IPDB 7 reports from 4 users

joe1@polarity.io

AI Polarity Assistant

FORM Polarity Form

CX No Incident Found

CX No Indicators Found

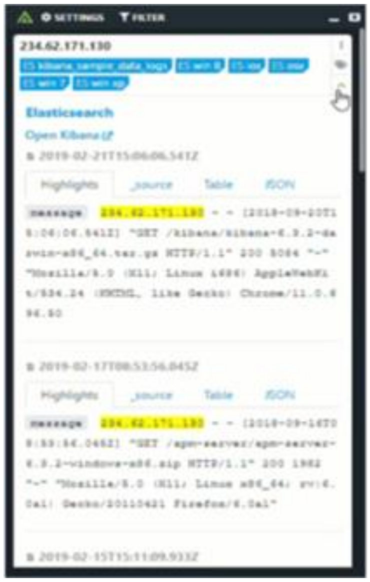
polarity.io 1

Polarity works on top of any tool, making the introduction of integrated content into your analysis process instantaneous.

In the example (left), Polarity introduces commercial and OSINT content right on top of a Splunk event, helping to speed overall time to determination.

Polarity SIEM integrations can maximize searching your important SIEM indices - and return data via the Polarity Overlay Window without replicating data. Polarity searches the data where it lives.

In another example (right), Polarity is used to query critical Elastic indices. Searching your SIEM with Polarity ensures consistency, repeatability, and alignment of your operational practices with organizational priorities.



234.62.171.130

ES kibana_sample_data_logs | ES win 8 | ES xp | ES osx | ES win 7 | ES win xp

Elasticsearch

Open Kibana

2019-02-21T15:06:06.541Z

```
message  234.62.171.130 - - [2018-09-20T15:04:06.541Z] "GET /kibana/kibana-6.3.2-darwin-x86_64.tar.gz HTTP/1.1" 200 3084 "-" "Mozilla/5.0 (X11; Linux i686) AppleWebKit/534.24 (KHTML, like Gecko) Chrome/11.0.696.50"
```

2019-02-17T08:53:56.045Z

```
message  234.62.171.130 - - [2018-09-14T08:53:56.045Z] "GET /apm-server/apm-server-6.3.2-windows-x86.zip HTTP/1.1" 200 1982 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:6.0a1) Gecko/20110421 Firefox/6.0a1"
```

2019-02-15T15:11:09.933Z

Polarity has out of the box integrations with leading SIEMs such as:

- Devo
- Google Chronicle
- Rapid7
- ElasticSearch
- IBM QRadar
- Splunk
- Falcon Logscale
- Microsoft Sentinel
- SumoLogic

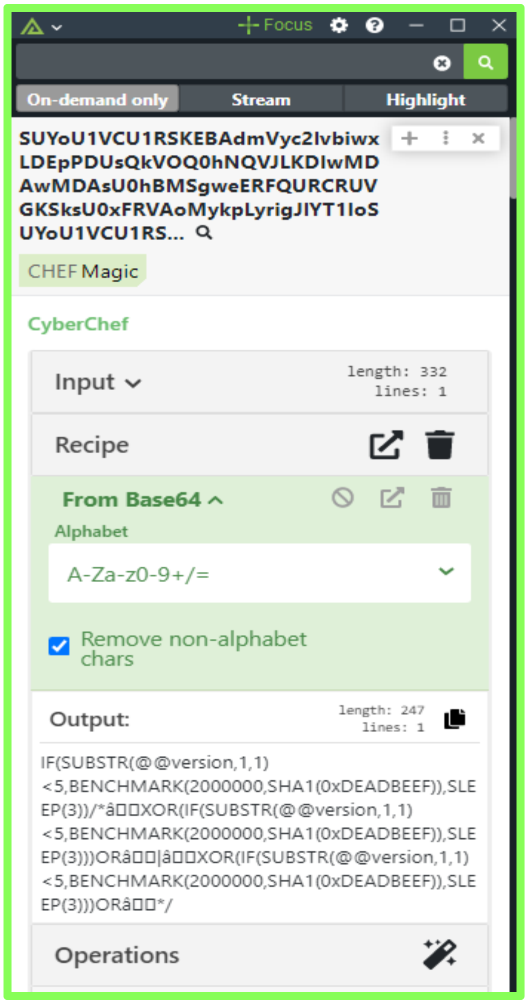
With Polarity, you can connect to one SIEM, many SIEMs – and/or all the other data sets you want to search when investigating. Polarity further enhances your tools capabilities and can limit or eliminate the hunting and pecking that consumes the valuable opportunity time teams have on a day-to-day basis.

Utility / Functionality

The day-to-day work of a security analyst exceeds simply searching details of selectors and making a good decision. Tools of the trade are employed in order to better understand what is being investigated. Oftentimes, the tools are leveraged to deobfuscate or decode the truest representation of the selector that requires investigation.

To enable security analysts in these scenarios, Polarity has developed a class of integration that allows for the transformation or manipulation of data on the Polarity user's screen. When invoked by the Polarity user, transformations can be applied directly to a datapoint. These transformations include language translation, decoding, de-obfuscating, or relationship mapping.

For example, Polarity has a very useful integration with CyberChef. CyberChef is an intuitive web app for carrying out all manner of cyber operations within a web browser. Such operations include simple encoding like XOR (eXclusive OR), Base64 - or more complex operations with AES, DES, and Blowfish. The tool is designed to enable both technical and non-technical analysts to manipulate data in complex ways without having to learn additional complex tools or algorithms.



```
SUYoU1VCU1RSKEBAdmVyc2lvbiwx
LDEpPDUsQkVOQ0hNQVJLKDIwMD
AwMDAsU0hBMSgweERFQURCRUV
GKSksU0xFRVAoMykpLyrigJlYT1loS
UYoU1VCU1RS...
```

Input length: 332 lines: 1

From Base64

Alphabet: A-Za-z0-9+/=

☑ Remove non-alphabet chars

Output: length: 247 lines: 1

```
IF(SUBSTR(@@version,1,1)
<5,BENCHMARK(2000000,SHA1(0xDEADBEEF)),SLE
EP(3))/*â□□XOR(IF(SUBSTR(@@version,1,1)
<5,BENCHMARK(2000000,SHA1(0xDEADBEEF)),SLE
EP(3)))ORâ□□|â□□XOR(IF(SUBSTR(@@version,1,1)
<5,BENCHMARK(2000000,SHA1(0xDEADBEEF)),SLE
EP(3)))ORâ□□*/
```

The Polarity CyberChef Integration allows teams to harness CyberChef's functionality by searching for any string on-demand within the Polarity UI, and then enables execution of recipes based on the data searched.

Polarity can be seen **(right)** enabling users with the ability to decode complex strings, by way of the Polarity-CyberChef integration.

Polarity has other utility-based integrations that save time and help analysts to immediately obtain new levels of thoroughness in their investigative processes. Other utility class integrations include:

- DNS Dig
- Epoch Time Converter
- Google Translate

- Proofpoint URL Decoder
- Unshorten.me

Complete SOAR Operability / Compatibility

Many MSSP/MDR companies have adopted SOAR in order to drastically reduce the amount of noise that must be sifted through when performing services for a growing customer base, but as the total number of SOAR managed events goes up, so do the number of events that require manual investigation - or otherwise human intervention.

Polarity allows teams to get the most out of their SOAR implementations. The mechanisms for achieving this are best summarized within three main categories.

SOAR Access

- Polarity users can kick off searches/actions from anywhere. Either through the search bar or through OCR.
- Polarity provides an optimized UI for federated search on how results are returned and viewed.
- Polarity can be used to manage access as appropriate or enforce least privilege to run specific playbooks and reduce the need for direct access to SOAR.
- Polarity directs users back to desired work platforms (e.g., SOAR, Ticketing, workflow management), once information is delivered.

SOAR Enablement

- Polarity streamlines investigations initiated outside of a workflow platform.
- Polarity can transform or apply utility to the data, which is not possible in SOAR.
- Users can capture additional evidence and create artifacts to add to an incident (e.g., screen captures, text extracts, exported results).
- Users can kick-off playbooks without having to be in a SOAR console.
- Users can create and update incidents without having to be in a SOAR console.
- Users have the ability to enrich free form text information (username, workstation name, etc.).

Delivery to SOAR

- Polarity enriches information at the point of need. Data is delivered in a “Data Finding the Analyst” format.
- The most recent information is drawn from interconnected data and knowledge bases.
- Deliver Knowledge Access (e.g., JIRA, Zendesk, ServiceNow).
- Deliver finished intel reports (e.g., TI vendor, SharePoint, Custom, etc.).
- Deliver access to multi-soar, multi-playbook, or multi-ticket environments.
- Robust caching for optimal integration with current and legacy data sources.

Capabilities: Customer Onboarding / Record Currency

Polarity enables MSSPs and MDR teams with contextualization when they are investigating cyber security events. Teams are able to seamlessly contribute towards shared bodies of knowledge that give a quick and reliable understanding of what is being investigated by a security analyst.

When onboarding a new customer (or maintaining an existing one) it is vital to understand the specifics of a customer's environment. This is difficult for an enterprise responsible for just one enterprise, let alone many. Polarity allows you to better understand your customer environments.

The following mechanisms are available mechanisms to enable customer environmental awareness:

Customer Asset Awareness

- Automatic ingest of customer asset inventories from a list
- Assets under management
- Critical assets/mission critical assets (e.g., domain controllers)
- High value targets (e.g., contains sensitive information)

Customer Identity Awareness

- Automatic ingest of customer identities
- Service accounts
- High risk/privileged accounts
- Recognition of risky identities

Rapid Cross Reference Against Polarity Integration Framework

- Search SIEM platforms (e.g., network proxy log index) for historical behavior associated with an identity.
- Determine if identities (e.g., email addresses) are known to be compromised.

For additional resources regarding the ability to import content into Polarity for immediate distribution and awareness to analysts – see the following:

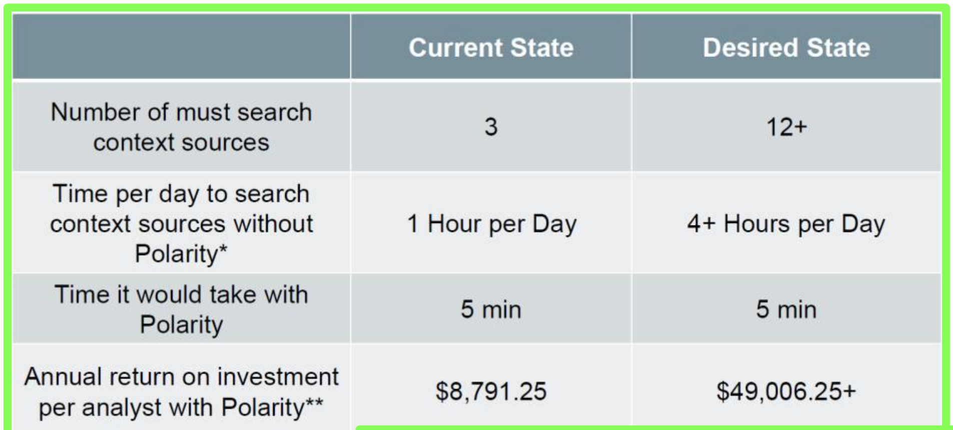
- Leveraging Channels in Polarity
- Polarity User Tips: Reference Channels

Performance Impacts

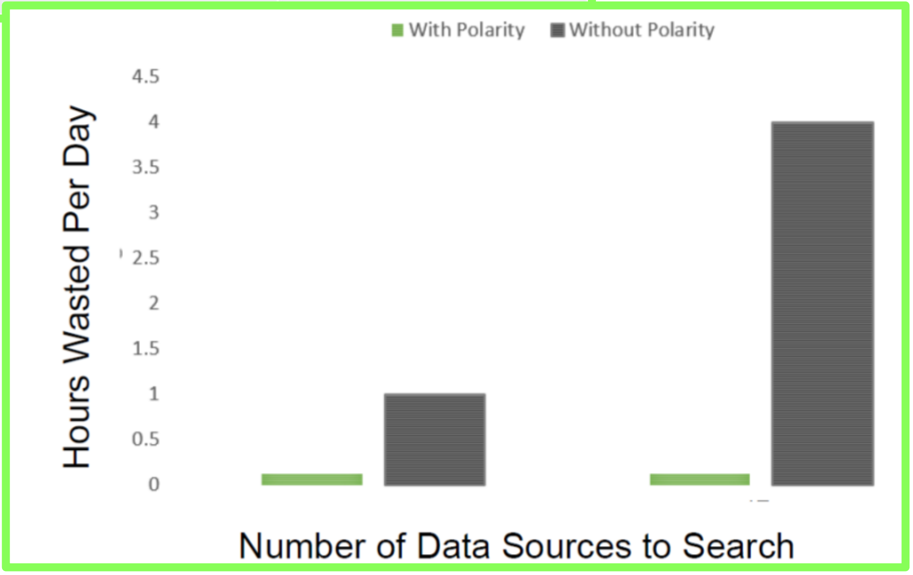
When performing detailed ROI analysis based on time study comparisons, teams find that there is a clear advantage of employing Polarity.

In one documented example, the ROI analysis showed that time spent gathering context when investigating IOCs from a phishing email or SIEM alert could be reduced by more than 60%. Similarly, time spent on subnet or asset name lookups related to building reference sets could be reduced by nearly 90%. Polarity's annual ROI was calculated at 200%, and the project yielded a 6-month payback period.

In another study performed by a large MSSP, they forecasted the following savings when promoting Polarity out to their distributed MSSP team members.



	Current State	Desired State
Number of must search context sources	3	12+
Time per day to search context sources without Polarity*	1 Hour per Day	4+ Hours per Day
Time it would take with Polarity	5 min	5 min
Annual return on investment per analyst with Polarity**	$8,791.25	$49,006.25+



Polarity helps deliver the right data required to complete the job, exactly when it is needed without breaking the analysts' workflow.

Conclusion

Though investigative speed is paramount, so is thoroughness - getting the job done fast but incorrectly only multiplies the speed of making errors. With Polarity, MSSPs and MDRs can multiply their efficiency in responding to incidents while maintaining a high standard of quality, thoroughness and accuracy in their investigations, improving the scalability of their businesses, and providing a better customer experience.

Book a demo with our team at threatconnect.com