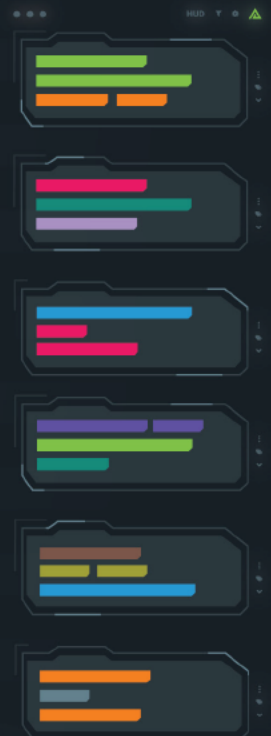




The Fastest Triage & Action Possible

Teams have too many places to search and not enough time. Polarity up-levels analysts by enabling them to triage data faster and take action with less mistakes using augmented reality.



Challenge

Even senior analysts get “IP déjà vu” – Why does something look so familiar, did I see it before? Is it critical that I remember or a distraction?

Sometimes the difference between junior and senior analysts is their intuition, other times it is their long term and short-term memory. Over time, analysts’ memory capacity for certain data types optimizes. Polarity enables this superpower for even the most junior analysts and amplifies it for the senior ones.

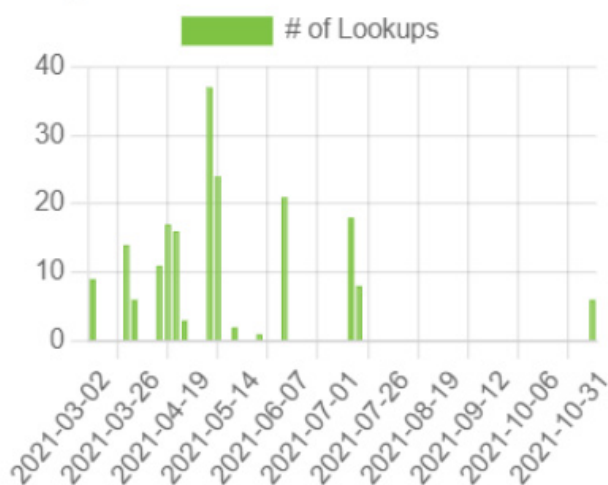
Feature/Use: Analyst Telemetry Integration

With no action from the user, Polarity eliminates IP déjà vu with its telemetry data feature.

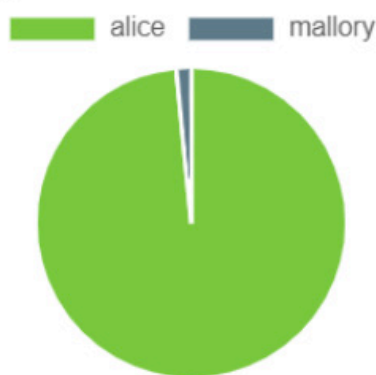
TEL 193 lookups, first seen 9 months ago by you in Mitigate Microsoft Exchange Server Vulnerabilities | CISA - Google Chrome, last seen a month ago

Whether it is an IP or any other investigation artifact, Polarity can inform an analyst the first time they saw something, where they saw it, how many times they have seen it, and who else on their team has looked at the same thing.

Lookups over Time



Lookups by User



Summary

Total Lookups: 193
 First Seen: 9 months ago [03/03/2021 18:00:00]
 First Seen Window Title: Mitigate Microsoft Exchange Server Vulnerabilities | CISA - Google Chrome
 Last Seen: a month ago [11/01/2021 09:56:15]
 Last Seen Window Title: Mitigate Microsoft Exchange Server Vulnerabilities | CISA - Google Chrome

First and Last Seen By

Username: alice
 Full Name: Alice Analyst
 Email: alice@polarity.io

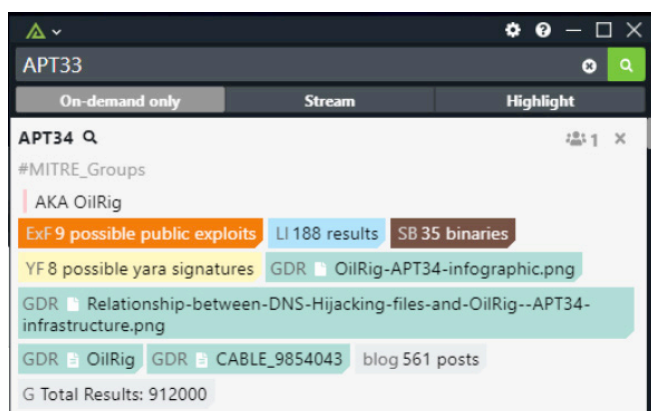
Challenge

Where to start searching? Data and systems within an organization continuously change making it difficult to know where to search or if a search is even worth the effort and time required. It is traditional when onboarding a new team member to train them on how and where to find data. Polarity makes this type of discovery natural and part of daily work.

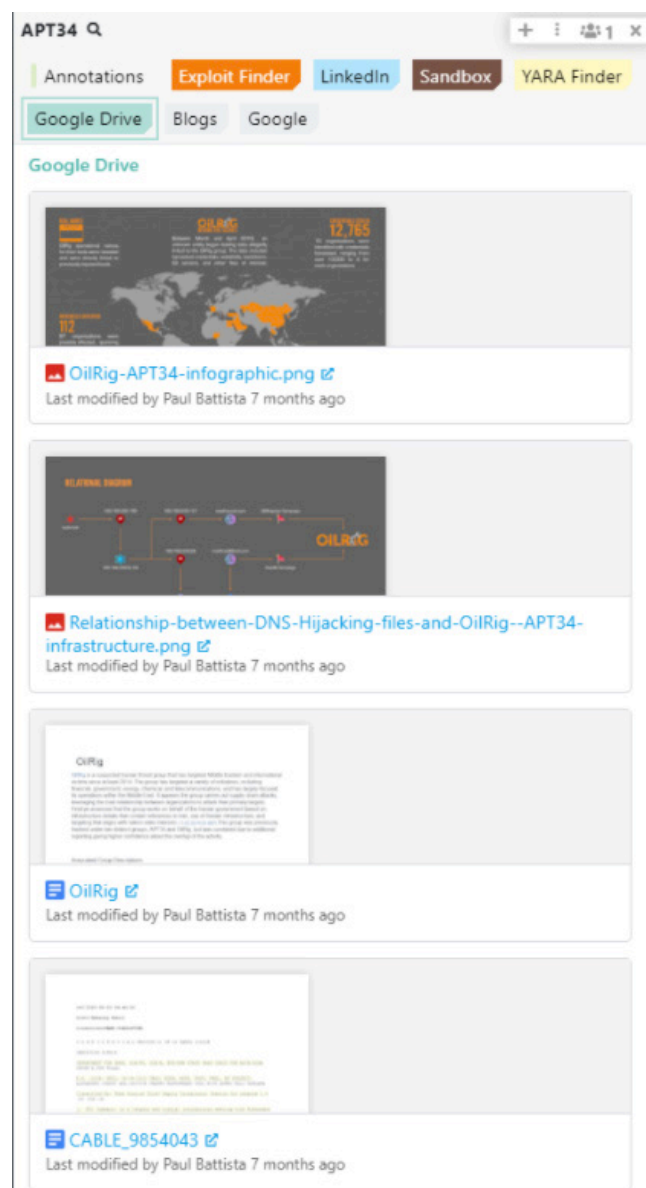
Feature/Use: Federated Search

When a user searches in Polarity, Polarity federates out that search to all the relevant sources and provides three levels of information.

1. Summary View on all the results



2. Detailed View on any specific result



Polarity makes this type of discovery natural and part of daily work.

Feature/Use: Federated Search

3. Summary View on all the results

APT34 Q

Annotations Exploit Finder LinkedIn Sandbox YARA Finder

Google Drive Blogs Google

Blogs

View search options

561 public posts found from 33 of 33 sources

Result #1 from www.fireeye.com
[New Targeted Attack in the Middle East by APT34, a Suspected ...](#)
 APT34 uses a mix of public and non-public tools, often conducting spear phishing operations using compromised accounts, sometimes coupled with social ...

Result #2 from www.fireeye.com
[Hard Pass: Declining APT34's Invite to Join Their Professional ...](#)
 APT34 is an Iran-nexus cluster of cyber espionage activity that has been active since at least 2014. They use a mix of public and non-public tools to ...

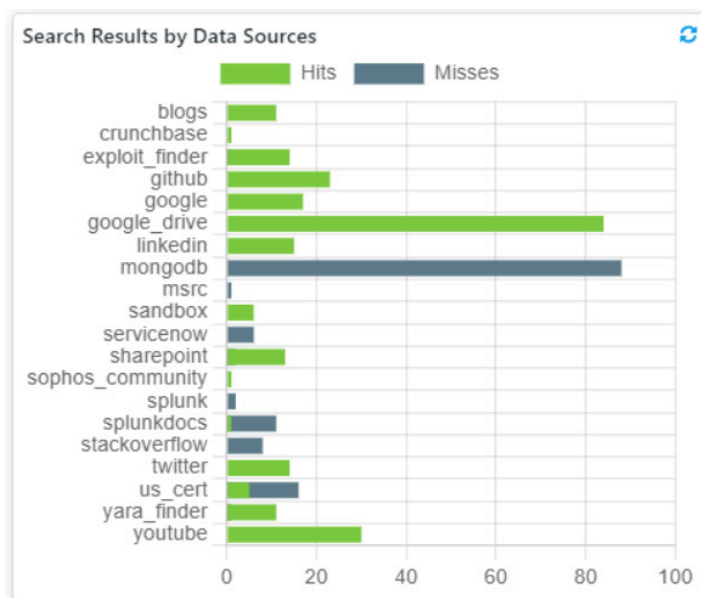
Result #3 from threatpost.com
[Iran-Linked APT34 Invites Victims to LinkedIn for Fresh Malware ...](#)
 Jul 19, 2019 ... APT34, a.k.a. OilRig or Greenbug, specializes in cyber-espionage activity, and is known for attacks targeting a variety of organizations ...

Result #4 from www.darkreading.com
[APT34 Toolset, Victim Data Leaked via Telegram](#)
 Apr 19, 2019 ... Hacking tools, victim data, and identities of the elite Iranian hacker group APT34, also known as OilRig and Helix Kitten, have been leaked ...

Result #5 from threatpost.com
[Iran-Backed APTs Collaborate on 3-Year 'Fox Kitten' Global Spy ...](#)
 Feb 18, 2020 ... The APT34 connection stems from the fact that part of the attack infrastructure used by the group in previous campaigns has been reused for Fox ...

View more

4. In one view, users can see all the places there have been results over time across their whole team:

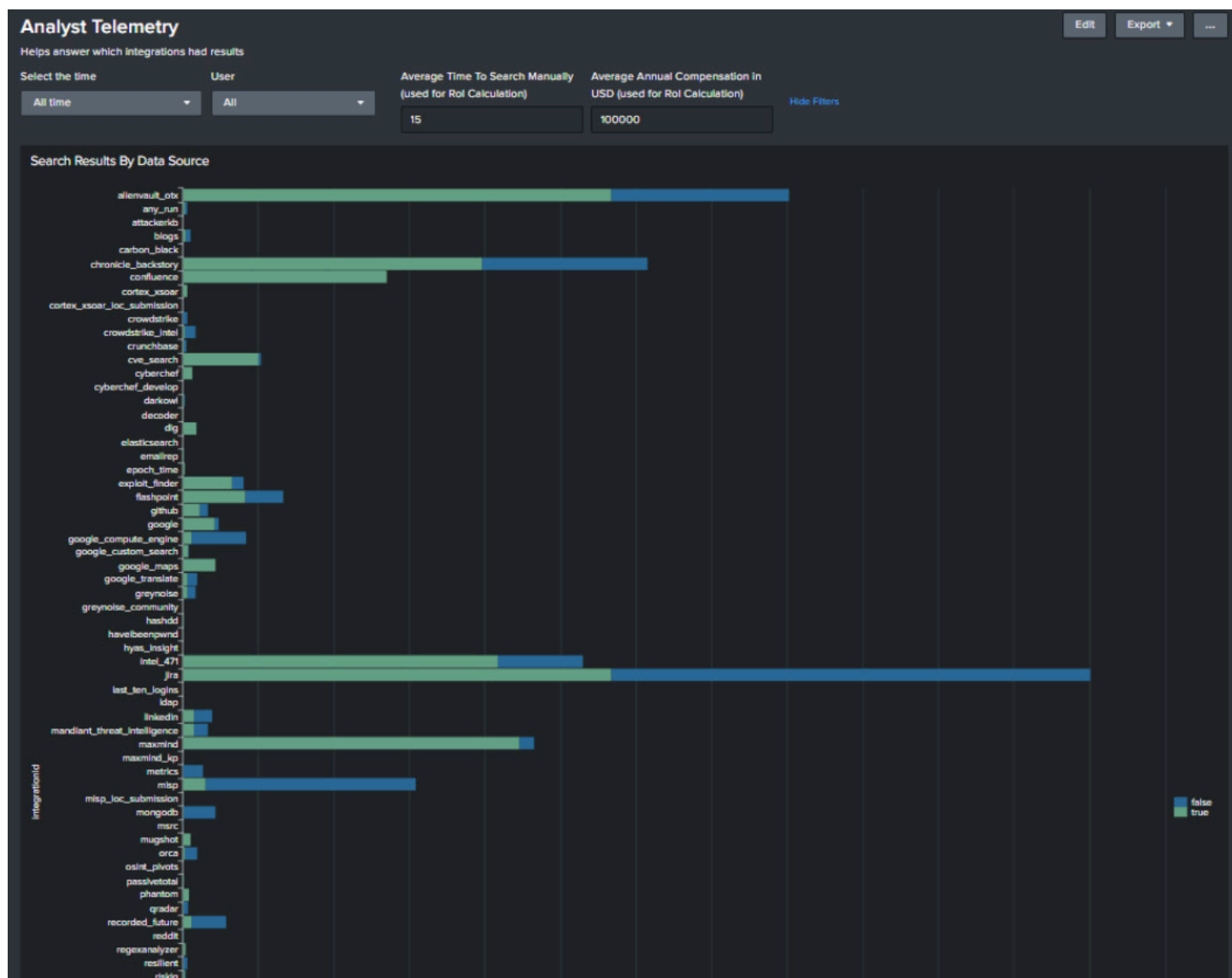


Challenge

It is often difficult to know what sources are the most valuable or overlap with a team's workflow because data is often spread across different systems and changes over time.

Feature/Use: Analyst Telemetry Search Metrics

Polarity's analyst telemetry enables teams and leadership with a data driven approach to identify the most valuable sources used across the team.



Challenge

Even when an analyst knows where to search, they might not know the proper search syntax. Polarity gives even the most junior analysts access to the results of complex searches. Without Polarity this is often attempted using dashboards or saved queries. Inevitably this approach results in too many dashboards and analysts forget or are too busy to search them all.

Feature/Use: Democratization of Complex Queries

With Polarity's integration framework, even the most complex queries are available automatically or at the push of a button reducing friction and enabling consistent information across the entire team and across all workflows.

SPLNK Results: 2

SPLNK bluecoat_events

SPLNK Victor

SPLNK Vincent

Splunk

[Run Search in Splunk](#)

Fields

[_source](#)

[Table](#)

[JSON](#)

Destination: 185.250.151.72

Domain: fjois.com

Protocol: HTTPS

User: Victor

Extracted source: 192.168.2.44

Host: bluecoat_proxy

Index: bluecoat_events

Fields

[_source](#)

[Table](#)

[JSON](#)

Destination: 185.250.151.72

Domain: fjois.com

Protocol: HTTPS

User: Vincent

Extracted source: 192.168.2.33

Host: bluecoat_proxy

Index: bluecoat_events

Challenge

Senior analysts often take notes in physical form or on a file on their desktop. Although their notes are often tactical, they are extremely valuable to both the analyst who took them and the team they are collaborating with.

Feature/Use: Notes Across All Team Members and Workflows

Polarity amplifies the power of analyst notes by disseminating them to the right team members at the right time, no matter what tools they are using. Even the most junior analyst, day one on the job, can know when they are looking at something important.

?

—

□

×

Annotate

Import Annotations (CSV)

Entities *

Clear all entities

103.228.53.155 ✕

Annotations * (case sensitive)

Clear all annotations

TOR exit node being used by APT34, ✕
If you are reading this, please call me at 555-555-5555
|


Channels *

#Investigation_42 ✕

▼

Cancel

Annotate

103.228.53.155 Q  1 X


#Investigation_42

TOR exit node being used by APT34,
If you are reading this, please call me at 555-555-5555

MM Petaling Jaya, Selangor (Malaysia) MM [AS55720] ASGigabit Hosting Sdn Bhd

SB 1 binaries GN Classification: malicious GN Tor Exit Node

GN Country: Malaysia GN Org: Gigabit Hosting Sdn Bhd

GN  Cobalt Strike SSH Client + 3 others AVOTX 50 pulses AVOTX tsec

AVOTX tpot19 AVOTX honeypot AVOTX la-safe.org AVOTX TOR

AVOTX +1 tags G Total Results: 49 VT 6 / 90 VT Malicious RF Suspicious

RF Risk Score: 45 RF Rules: 9/64 DIG ns1.thegigadns.com.

DIG hostmaster.thegigadns.com. PH No Events Found

RIQ GIGABIT-MY Gigabit Hosting Sdn Bhd RIQ ASN: 55720 RIQ REP Count: 10

XF Risk: 8.6 XF Malaysia MTI MScore: 70 (suspicious)

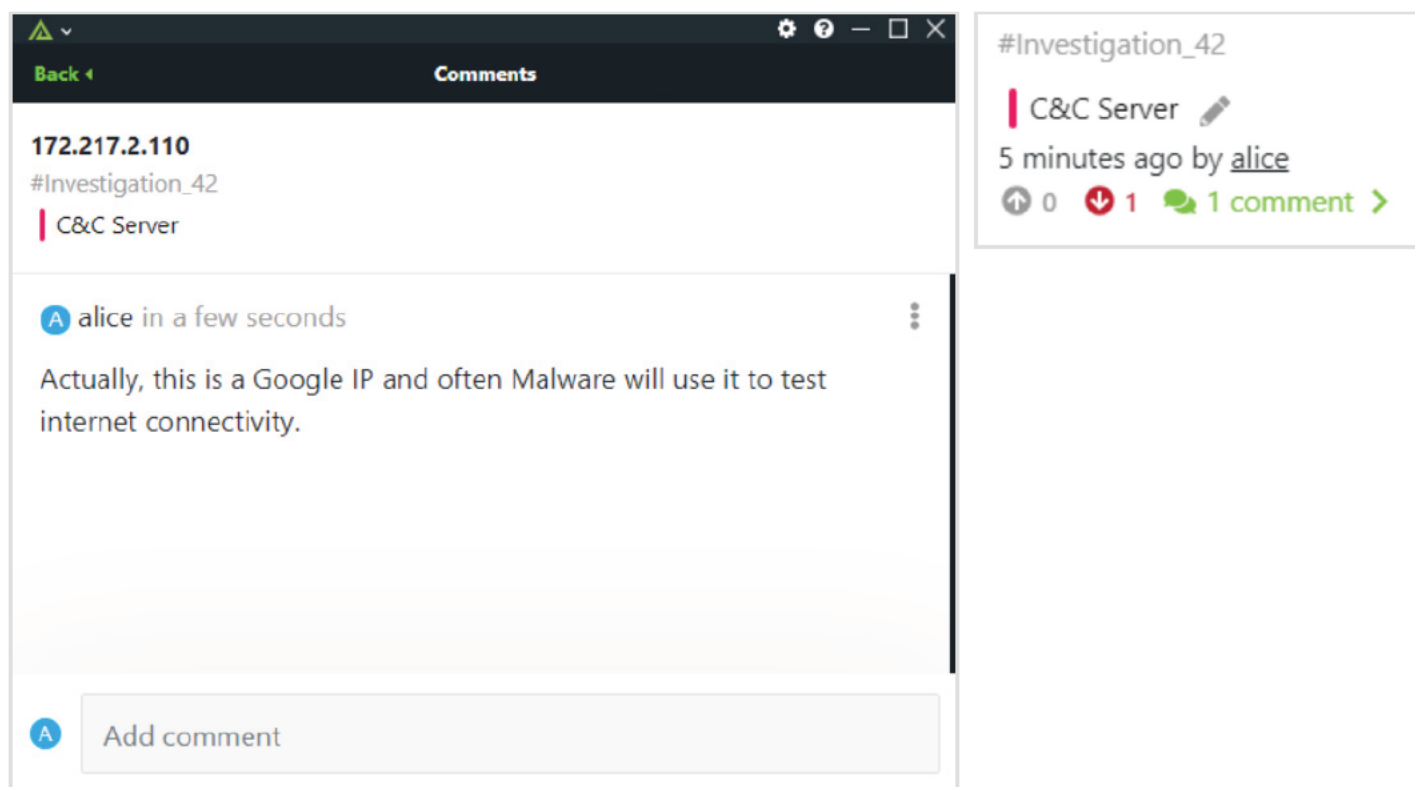
PT Resolutions: 0, Articles: 0, Certs: 0, Hashes: 0, Host Pairs: 0, Projects: 0, Trackers: 0, Components: 1

Challenge

Junior (and sometimes senior) analysts make faulty assumptions that are never caught by other team members. When incorrect notes are taken in Polarity, faulty assumptions are easier to spot.

Feature/Use: **Note Feedback**

Mistakes are inevitable, because Polarity works across all tools, faulty assumptions are easy to spot when team members come across them or are reviewing work. Polarity has built in upvoting, downvoting, and commenting:



The screenshot displays the Polarity interface. At the top, there's a dark header with a 'Back' button and a 'Comments' tab. Below this, a note is shown with the IP address '172.217.2.110', the tag '#Investigation_42', and the label 'C&C Server'. A comment by 'alice' is visible, stating: 'Actually, this is a Google IP and often Malware will use it to test internet connectivity.' To the right of the comment, there's a feedback section for '#Investigation_42' showing 'C&C Server' with an edit icon, '5 minutes ago by [alice](#)', and voting options: 0 upvotes, 1 downvote, and 1 comment with a right arrow.

Challenge

In cyber and national defense, we often get stuck in training mode but true learning happens on the job. Polarity creates opportunities for discovery and learning on top of any workflow.

Feature/Use: Portable Learning Content

Beyond learning from co-workers' notes and links to relevant resources, Polarity supports video and other content embedded right in the overlay window. This provides a fast path to shortcuts, documentation, and educational resources.



nmap Q

#Commands

- Scan a specific port: `$nmap [Target] -p [Specific Port]`
- Command to find vulns: `$nmap -v --script vuln [Target]`

Confluence

Display 25 of 169 results.

Pages

- Page: [RFC 0086 - Enterprise Website Search - CE Enhancements](#)
- Page: [August 2021 Integration Updates](#)
- Page: [Polarity Server 4.1.0, Web 4.1.0 New Install on CentOS 8 or RHEL 8](#)
- Page: [Polarity Server 4.1.0, Web 4.1.0 Upgrade for CentOS 8 and RHEL 8](#)
- Page: [Polarity Server 4.1.0, Web 4.1.0 New Install on CentOS 7 or RHEL 7](#)
- Page: [Polarity Server 4.1.0, Web 4.1.0 Upgrade for CentOS 7 and RHEL 7](#)
- Page: [0085 - Enterprise Web Search](#)
- Page: [PX 4.2.0 Test Plan](#)
- Page: [Troubleshooting Polarity Client](#)
- Page: [July 2021 Integration Updates](#)
- Page: [0088 - Polarity Server Re-Write](#)
- Page: [0074 - Ability to add Attachments as an Annotation](#)
- Page: [Minio Deployment & Setup](#)
- Page: [4.1.0-SVR RPM Test Plan](#)
- Page: [Polarity OVA Installation Guide](#)
- Page: [Test Plan CentOS <X> Template](#)
- Page: [PX <x.x.x> Test Plan Template](#)
- Page: [Enabling Polarity Analyst Telemetry](#)
- Page: [Enabling Polarity Telemetry](#)
- Page: [June Integration Updates 2021](#)
- Page: [DHS](#)
- Page: [Customer Support](#)

Attachments

- Attachment: [Polarity Developer Guide.pdf](#)
- Attachment: [Polarity Enterprise Guide.pdf](#)
- Attachment: [text.hbs](#)

Splunk Q

#Commands #contacts

- Default path of forwarder: `/opt/splunkforwarder/bin`
- Start on Boot: `$sudo ./splunk enable boot-start`
- Accept Licence: `$sudo ./splunk start --accept-license`
- Add Monitor: `$sudo ./splunk add monitor [path to logs]`
- Add Forwarder: `$sudo ./splunk add forward-server 192.168.2.8:9997 -auth [username]:[password]`
- + 2 more annotations

Challenge

During a crisis, you never know what tools you will be using or where your work will take you. Polarity's Focus Mode feature lets team members tell Polarity a specific area of the screen to analyze and then triggers searches and actions from there.

Feature/Use: Polarity Focus Mode

Gives analysts the power of Polarity's real time optical character recognition with control over where and when it is run. Maybe it's a specific operational vm/shell or maybe it is a foreign social media website.

The image is a collage of four screenshots demonstrating the Polarity Focus Mode feature. The top-left screenshot shows a Windows Command Prompt with a 'tracert' command being executed, and a green dashed box highlighting the command text. The top-right screenshot shows the Polarity interface with a search bar and a list of search results, with a green dashed box highlighting the search bar. The bottom-left screenshot shows a VMware Workstation window with a terminal running a 'netstat' command, and a green dashed box highlighting the terminal output. The bottom-right screenshot shows a social media post from Inna Smirnova, with a green dashed box highlighting the post content.

Challenge

Some missions require fast action with “guard rails” or an easy button. Polarity’s integration framework supports action at the touch of a button.

Feature/Use: **Actions**

Polarity’s overlay window supports enabling action. That could be kicking off a scan, updating tasking, deconflicting an operation, submitting a report, or running a playbook. Analysts and operators are presented with the most common, recommended, or critical actions so executing them is near frictionless from wherever the mission takes them.

Phantom

- Info

Name: 205.251.242.103

Status: **This Entity does not exist in Phantom**

[Create Event in Phantom Dashboard](#)
- Create Event and Run Playbook

Event Owner:

Severity:

Sensitivity:

Playbook:

CEF Fields:

Create Event & Run

ThreatConnect

- Info

Associations (4)
- Indicator Analytics

Organization: [Polarity](#)

Threat Assess Score: 201/1000

Threat Assess Rating: 2.5

Threat Assess Confidence: 35.5
- Details

Date Added: 12/04/2020 13:37:13

Last Modified: 10/14/2021 14:16:05

Rating: ☐ ☒ ☐ ☐ ☐ ☐ Moderate

Confidence: 31 - Doubtful
- Observations/False Positives

Observation Count: 0

False Positive Count: 0

False Positive Last Reported: 11/29/2021
- Tags
- Available Playbooks

[Archive.org Wayback Machine Query](#)

[Run In Dashboard](#)

Challenge

Sometimes the artifact is right in front of you but it is not easy to spot. Analysts don't always know when or what to look up so augmenting by bringing the data to them up-levels anyone analyzing data.

Feature/Use: Polarity Highlights

Polarity uses software-based augmented reality techniques to highlight data in any application. This enriches any user experience with data they care about or insights that are critical to the mission. Even the most junior or fatigued analyst will have a hard time missing the important information.

DATE 2020-08-05 04:46:00

SOURCE Embassy Kabul

CLASSIFICATION **FAKE CLASSIFIED**

C O N F I D E N T I A L SECTION 01 OF 02 KABUL 004068

SENSITIVE SIPDIS

DEPARTMENT FOR SRAP, SCA/FO, SCA/A, EUR/~~IRM~~ STATE PASS USAID FOR ASIA/SCAA
USFOR-A FOR POLAD

E.O. 12058: DECL: 08/04/2020 TAGS: KDEM, MOPS, PGOV, PREL, AF SUBJECT:
ALEXANDER IVANOV AKA LEZVIYE SHARES RANSOMWARE TOOL WITH **AHMED WALI KAHLAMA**

Classified By: Fake Station Chief Deputy Coordinator Jessica for reasons 1.4
(b) and (d)

1. (FC) Summary: in a lengthy and cordial introductory meeting with Alexander Ivanov (AKA Lezviye, **Sasha Gutrow**), **ROSTEC** Developer and suspected Cyber Operator, and **Ahmed Wali Kahlama**, suspected leader of the **GilRig** (APT34) threat group the two exchanged small talk and then discussed the death of "Suleimani" (presumed Qassem Suleimani). Both Ivanov and Kahlama acknowledged the unwelcomed intrusion of foreign influence. Ivanov transferred a file to arm Kahlama's team with a weapon for revenge. End Summary.

Relationship Building

2. (FC) In an online meeting on August 4th, 2020, **Ahmed Wali Kahlama**, suspected leader of the **GilRig** (HELIX KITTEN, Helminth, Clayslide, APT34, IRN2, threat group met with **Alexander Ivanov** (AKA Lezviye), **ROSTEC** Developer and suspected Cyber Operator. Kahlama initiated the conversation from an internet café at Lamar Internet Cafe (34.5337865, 69.1981253), **Alexander Ivanov**'s location was unknown. The two exchanged small talk and then discussed the death of "Suleimani" (presumed Qassem Suleimani). Both Ivanov and Kahlama acknowledged the unwelcomed intrusion of foreign influence in the region. Ivanov complimented Kahlama's leadership and the success of his team so far. Ivanov said his boss was very impressed with the last operation.

Providing Cyber Weapon

3. Ivanov pledged his support of the cause and said he personally coded a weapon to help in the fight. Ivanov transferred a file to arm Kahlama's team with a weapon for revenge.

RAW TECHNICAL EXCHANGE

```
46.72.177.4 - - [12/Dec/2015:18:31:08 +0100] "GET /administrator/ HTTP/1.1" 200 4263 "-" "Mozilla/5.0 (Windows NT 6.0; rv:34.0) Gecko/20100101 Firefox/34.0" "-"
46.72.177.4 - - [12/Dec/2015:18:31:08 +0100] "POST /administrator/index.php HTTP/1.1" 200 4494 "http://almhuette-raith.at/administrator/" "Mozilla/5.0 (Windows NT 6.0; rv:34.0) Gecko/20100101 Firefox/34.0" "-"
83.167.113.100 - - [12/Dec/2015:18:31:25 +0100] "GET /administrator/ HTTP/1.1" 200 4263 "-" "Mozilla/5.0 (Windows NT 6.0; rv:34.0) Gecko/20100101 Firefox/34.0" "-"
83.167.113.100 - - [12/Dec/2015:18:31:25 +0100] "POST /administrator/index.php HTTP/1.1" 200 4494 "http://almhuette-raith.at/administrator/" "Mozilla/5.0 (Windows NT 6.0; rv:34.0) Gecko/20100101 Firefox/34.0" "-"
95.29.198.15 - - [12/Dec/2015:18:32:10 +0100] "GET /administrator/ HTTP/1.1" 200 4263 "-" "Mozilla/5.0 (Windows NT 6.0; rv:34.0) Gecko/20100101 Firefox/34.0" "-"
95.29.198.15 - - [12/Dec/2015:18:32:11 +0100] "POST /administrator/index.php HTTP/1.1" 200 4494 "http://almhuette-raith.at/administrator/" "Mozilla/5.0 (Windows NT 6.0; rv:34.0) Gecko/20100101 Firefox/34.0" "-"
109.184.11.34 - - [12/Dec/2015:18:32:56 +0100] "GET /administrator/ HTTP/1.1" 200 4263 "-" "Mozilla/5.0 (Windows NT 6.0; rv:34.0) Gecko/20100101 Firefox/34.0" "-"
109.184.11.34 - - [12/Dec/2015:18:32:56 +0100] "POST /administrator/index.php HTTP/1.1" 200 4494 "http://almhuette-raith.at/administrator/" "Mozilla/5.0 (Windows NT 6.0; rv:34.0) Gecko/20100101 Firefox/34.0" "-"
91.227.29.79 - - [12/Dec/2015:18:33:51 +0100] "GET /administrator/ HTTP/1.1" 200 4263 "-" "Mozilla/5.0 (Windows NT 6.0; rv:34.0) Gecko/20100101 Firefox/34.0" "-"
91.227.29.79 - - [12/Dec/2015:18:33:52 +0100] "POST /administrator/index.php HTTP/1.1" 200 4494 "http://almhuette-raith.at/administrator/" "Mozilla/5.0 (Windows NT 6.0; rv:34.0) Gecko/20100101 Firefox/34.0" "-"
```


Challenge

Traditional entity extraction or natural language processing is not flexible enough for real work. There is always an artifact or indicator that does not fit the mold. Polarity support recognition of any string.

Feature/Use: Entity Extraction

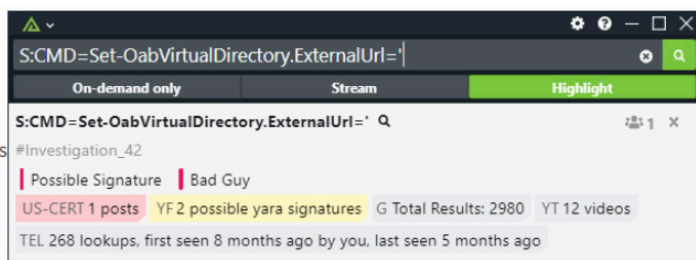
Although Polarity supports adding custom entity types with a regular expression, Polarity goes beyond that and can actually recognize any string with proprietary entity recognition techniques. Whether that is a string of bytes, a name in a foreign language, or a malware signature, Polarity can recognize it when it matters.

- /owa/auth/Current/themes/resources/owafont_ko.css
- /owa/auth/Current/themes/resources/SegoeUI-SemiBold.eot
- /owa/auth/Current/themes/resources/SegoeUI-SemiLight.ttf
- /owa/auth/Current/themes/resources/lgnbotl.gif

Administrators should search the ECP server logs for the following string (or something s

`S:CMD=Set-OabVirtualDirectory.ExternalUrl=`

The logs can be found at `<exchange install path>\Logging\ECP\Server\`.

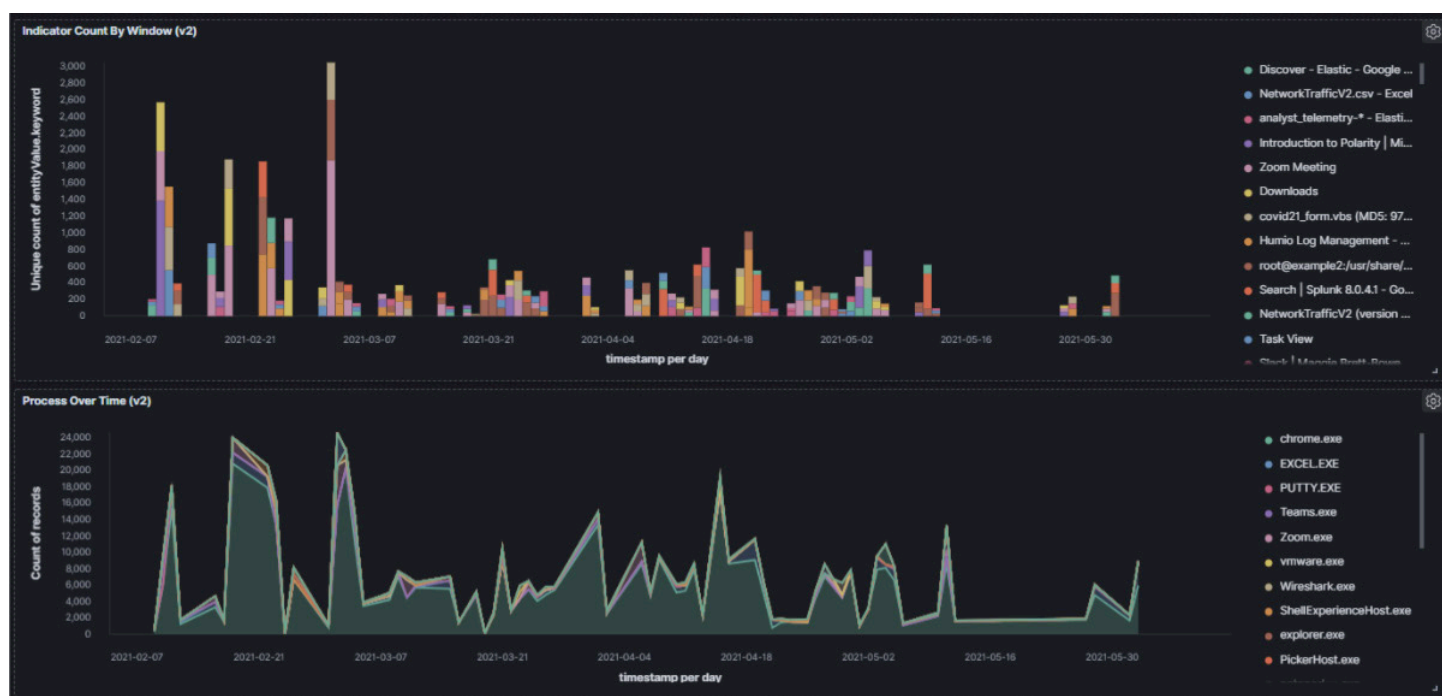


Challenge

It is sometimes difficult to understand the difference between senior and junior analyst workflows. What causes some analysts to have different results than others.

Feature/Use: Analyst Tool Telemetry

Polarity's analyst telemetry enables teams and leadership to understand the different tools and workflows used across different members of a team. Leadership can get a qualitative answer to what are the most common tools used by the team, where does the team spend most of their time, and what are common/uncommon workflows between tools.



Challenge

The threshold of friction that users are willing to put up with is low. Add to that a critical mission and you will have a very difficult time getting an analyst to adopt a new tool or workflow. Polarity does not work against an analyst's workflow. Polarity works on top of it with only a couple easy key strokes.

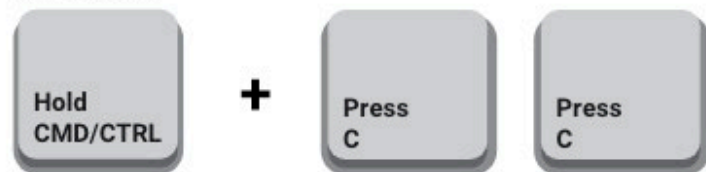
Feature/Use: Simple Short-Cut Keys

With less than an hour of instruction and a couple shortcut key sequences, analysts will never work the same way again. Polarity reduces friction for analysts and operators to search, take notes, or take action.

On-demand



Annotate



Focus Mode - Windows and Linux



Focus Mode - macOS



Other Enterprise Features

Problem

Different teams leverage or have access to different data

Other Enterprise Features

Polarity supports role based access controls to streamline deployment with security in mind.

Polarity supports SAML and other enterprise security user configurations and deployment methodologies.

Enterprise Security Features

Team Users Groups			
Group Name			Users
Description			Actions
Hunt_Team			2 Settings
Red_Team			2 Settings
Malware_Investigatio...			1 Settings
DLP			1 Settings
Financial_Analyst_Team			1 Settings
Threat_Intel_Team			1 Settings
SOC			2 Settings
eCrimes			1 Settings
Operations_Team			0 Settings

Custom Development

Polarity has a robust integration development framework with over 175 integrations built to date. Polarity has been optimized for you to easily add custom data sources.

Community

Polarity has thousands of users across enterprise and government. Polarity has over 175 open source integrations <https://github.com/polarityio> developed by users, partners, and the Polarity team.

Support

Polarity is consistently complimented on having the best support of any vendor the customer has ever worked with.

Other Enterprise Features

Deployment, maintenance, and staff augmentation.

Although Polarity is easy to deploy and maintain, we understand many organizations are short-handed so Polarity has resources to support deployment, maintenance, and custom development if needed.

Programmatic Access To Polarity Functionality/ Search

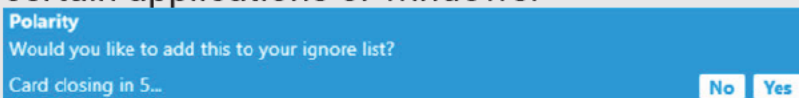
Polarity supports API and web based access to Polarity's features that do not require the client software. This means you can enable teams to search and leverage Polarity before the client software is installed. It also opens the door for you to embed Polarity into other applications where appropriate.

Polarity Search awareness at any time

Polarity enables users to not just get information through our different recognition and on-demand modes, but also enables users to just search for information at any point through our web

All investigations have noise.

Polarity has robust features to filter out noise or ignore certain applications or windows.



Search

