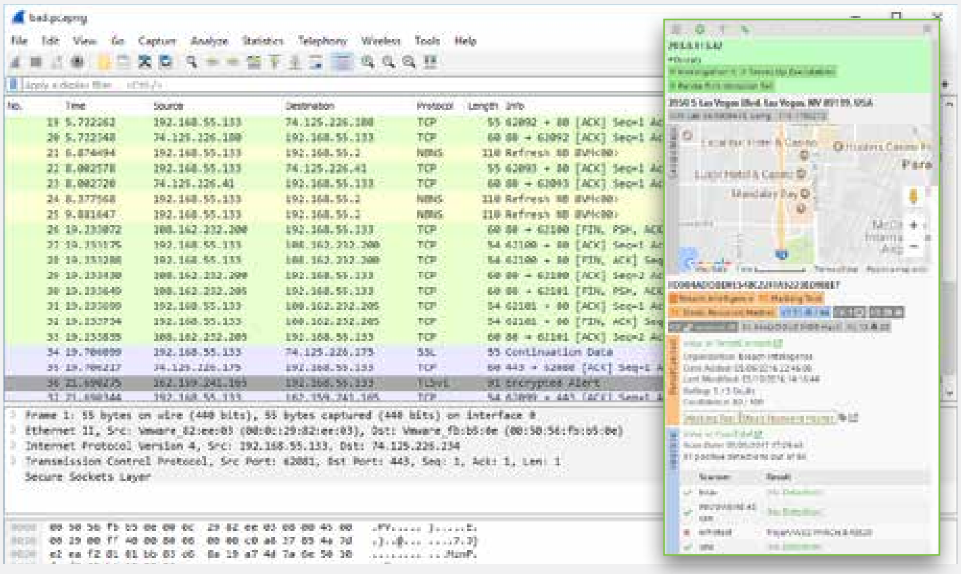
POLARITY

Polarity for Incident Responders


bad.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time        Source           Destination      Protocol  Length Info
   19 5.722262    192.168.55.133   74.125.226.180   TCP       55 62092 → 80 [ACK] Seq=1 Ac
   20 5.722548    74.125.226.180   192.168.55.133   TCP       60 80 → 62092 [ACK] Seq=1 Ac
   21 6.874494    192.168.55.133   192.168.55.2     NBNS     110 Refresh NB BVHC00>
   22 8.002578    192.168.55.133   74.125.226.41    TCP       55 62093 → 80 [ACK] Seq=1 Ac
   23 8.002720    74.125.226.41    192.168.55.133   TCP       60 80 → 62093 [ACK] Seq=1 Ac
   24 8.377568    192.168.55.133   192.168.55.2     NBNS     110 Refresh NB BVHC00>
   25 9.881647    192.168.55.133   192.168.55.2     NBNS     110 Refresh NB BVHC00>
   26 19.233072   108.162.232.200  192.168.55.133   TCP       60 80 → 62100 [FIN, PSH, ACK
   27 19.233175   192.168.55.133   108.162.232.200  TCP       54 62100 → 80 [ACK] Seq=1 Ac
   28 19.233288   192.168.55.133   108.162.232.200  TCP       54 62100 → 80 [FIN, ACK] Seq
   29 19.233430   108.162.232.200  192.168.55.133   TCP       60 80 → 62100 [ACK] Seq=2 Ac
   30 19.233640   108.162.232.205  192.168.55.133   TCP       60 80 → 62101 [FIN, PSH, ACK
   31 19.233699   192.168.55.133   108.162.232.205  TCP       54 62101 → 80 [ACK] Seq=1 Ac
   32 19.233734   192.168.55.133   108.162.232.205  TCP       54 62101 → 80 [FIN, ACK] Seq
   33 19.233859   108.162.232.205  192.168.55.133   TCP       60 80 → 62101 [ACK] Seq=2 Ac
   34 19.704099   192.168.55.133   74.125.226.175   SSL       55 Continuation Data
   35 19.706217   74.125.226.175   192.168.55.133   TCP       60 443 → 62080 [ACK] Seq=1 A
   36 21.690275   162.159.241.165  192.168.55.133   TLSv1     61 Encrypted Alert
   37 21.690344   192.168.55.133   162.159.241.165  TCP       54 62099 → 443 [ACK] Seq=1 A

> Frame 1: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface 0
> Ethernet II, Src: Vmware_82:ee:03 (00:0c:29:82:ee:03), Dst: Vmware_fb:b6:0e (00:50:56:fb:b6:0e)
> Internet Protocol Version 4, Src: 192.168.55.133, Dst: 74.125.226.234
> Transmission Control Protocol, Src Port: 62081, Dst Port: 443, Seq: 1, Ack: 1, Len: 1
  Secure Sockets Layer

0000  00 50 56 fb b6 0e 00 0c  29 82 ee 03 08 00 45 00   .PV..... ).....E.
0010  00 29 00 f7 40 00 80 06  00 00 c0 a8 37 85 4a 7d   .)..@... ....7.J}
0020  e2 ea f2 81 01 bb 03 d6  8a 19 a7 4d 7a 0e 50 10   ........ ...MznP.
```

2550 S Las Vegas Blvd, Las Vegas, NV 89109, USA

WHAT IS POLARITY?

Polarity is a memory augmentation platform created on the principle that people are the most integral component of the incident response process. It provides a new way for centralized or distributed incident responders to utilize a collective memory by delivering critical intelligence to the right team members only when it is relevant to what they are working on. Polarity drives responders to make better and faster decisions, increasing productivity, and reducing the risk of a data breach going undetected. Polarity works by analyzing the content of a user's screen and notifying the user about intelligence of interest helping to ensure that incident responders never miss intelligence critical to combating a cyber intrusion.

WHO IS POLARITY?

Polarity Inc. is a software company which focuses on augmenting human analysis with a collective memory. Shared automatic access to intelligence has enabled Polarity's customers to improve a responder's ability to make better and faster decisions. Polarity is the first memory augmentation platform designed for IT and Security professionals.

Challenges, and how Polarity helps solve them.

INCIDENT RESPONSE CHALLENGES

WITH MEMORY AUGMENTATION

IOC Data Capitalization

To accurately assess threats and understand evidence, responders need to continuously gather contextual information from a wide range of sources including response team members, the Internet, and internal knowledge repositories. This process is time consuming and forces responders to sacrifice investigative cycles that could be spent containing cyber incidents. Incomplete contextual information may arise due to time constraints, data silos, and tools that cannot interoperate - resulting in prolonged intrusions, and data breaches.

Polarity Delivers Context Information

Polarity automatically searches for and delivers relevant context to incident responders as they are working. Those responders are less likely to miss critical intelligence because Polarity removes the burden of finding relevant contextual information. Since Polarity operates at the screen level, Polarity enables collaboration across multiple applications, toolsets and workflows. Responders no longer have to choose between working fast and working thoroughly.

Distributed Personnel / Teams

Work efforts are consistently duplicated as multiple responders research the same information over a period of hours, days, months, and years, greatly reducing productivity. The problem is magnified when personnel operate in distributed locations, on shifted schedules, or within different organizational units. The opportunity for collaboration, a key component of a well-functioning SOC, is lost if personnel who are working on related issues are unable to find one another.

Polarity Provides Total Data Awareness

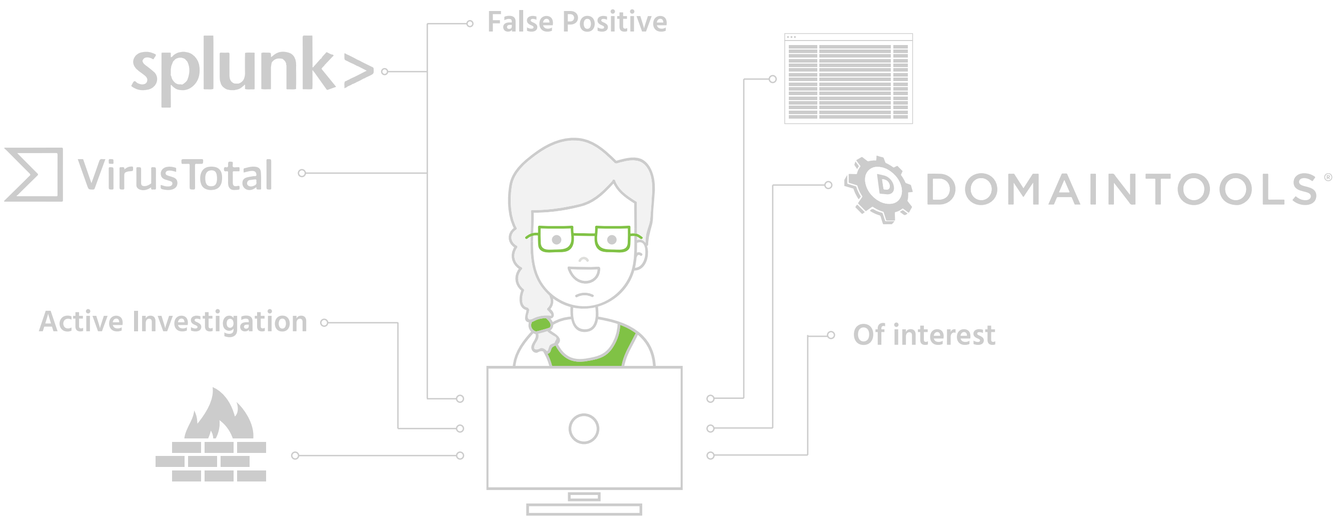
Responders using Polarity have total data awareness as Polarity automatically notifies them of intelligence generated by co-workers across the globe, in the previous shift, last week, last month, or even last year. For example, if one responder is investigating a Distributed Denial of Service (DDoS) and they flag a malicious IP address range, Polarity will automatically notify another responder about malicious IP addresses within that range when they are present on the responder's screen.

Demanding Conditions

Responders are typically working under stressful and demanding work conditions. These conditions, coupled with long hours, the monotony of certain investigative work-streams, repeated queries and data entry, reduces the quality and speed of human decision making leading to mistakes of habit.

Polarity Increases Productivity

Polarity combats responder fatigue by automating the most repetitive and time consuming components of a response effort. Reduced lookups and automatically delivered contextual data speeds up the decision-making process letting responders apply their efforts where it is needed most.



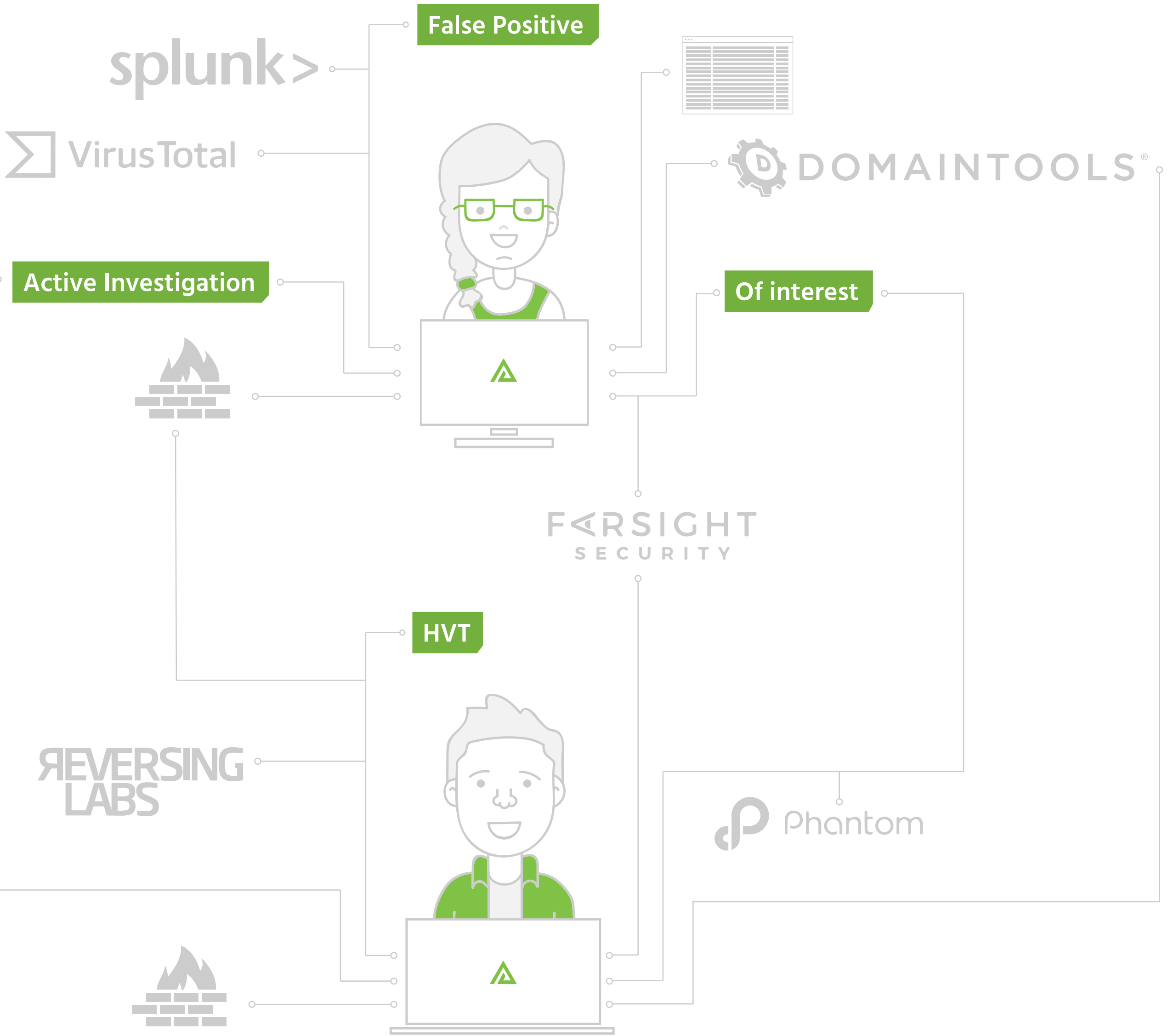
ALICE'S FAILURE WITHOUT MEMORY AUGMENTATION

Alice is an incident responder who is deployed on investigations primarily throughout the eastern United States. On a data compromise investigation, she requests firewall and IDS event logs from the time frame surrounding the event in question and begins her review. Throughout the course of the investigation, she identifies over 50 IP addresses sourced from more than 30 well-known hosting providers that have executed broad TCP scans against her client's address space within that time frame. Given her investigation time constraints and executive pressure to achieve containment, she notes these IPs but continues to look for evidence of successful authentication outside of the norm that might have been the source of the data compromise. In her continued investigation, Alice identifies a smaller set of IP addresses, hosted by provider in the state of Florida, attempting single form submissions against her client's address space. Her attention quickly transitions to these IP addresses.

Finally, Alice observes two isolated IP addresses from an ISP in eastern Europe, attempting password sweep attacks against validated accounts associated with the client's web application. Several of those accounts correspond to initial customer reports of data loss and the client is thrilled that Alice and her team has cracked the case.

What Alice does not realize is that she just made a bad decision that will not be uncovered for three months. Amongst the scanning IPs were systems that had identified an externally facing code repository that contained several valuable artifacts leveraged by the attack, including, amongst other things, the account names leveraged in the sweep identified by Alice.

While a review of this system's web logs had been conducted by another member of the investigation team, Bob, the activity had not been noted as "of interest" as the requests were coming from a reputable hosting provider in a state where the client has a concentrated remote workforce.



THE TEAM'S SUCCESS WITH MEMORY AUGMENTATION

Now what if Alice and Bob had Polarity, how would the investigation have changed? Alice would have been able to effortlessly tag or otherwise associate the initially observed IP addresses with reconnaissance behavior. Then, when other members of the incident response team, conducting separate efforts under the boarder investigation, came across those IP addresses, they would have been made aware of this intelligence. Specifically, Polarity would have recognized the IP address on Bob's screen and automatically delivered the following intelligence:

- A comment from Alice that the IP had been associated with reconnaissance behavior.
- Immediate insight from a 3rd party intelligence provider that the IP has been associated with malicious activity.

Instantly and automatically armed with additional context, Bob decides to further investigate web traffic from these IPs and determines that they've been leveraged in accessing various web resources for the past several months. He requests a broader history of the web logs and determines a more significant scope of intellectual property and sensitive data that were collected by the attacker.