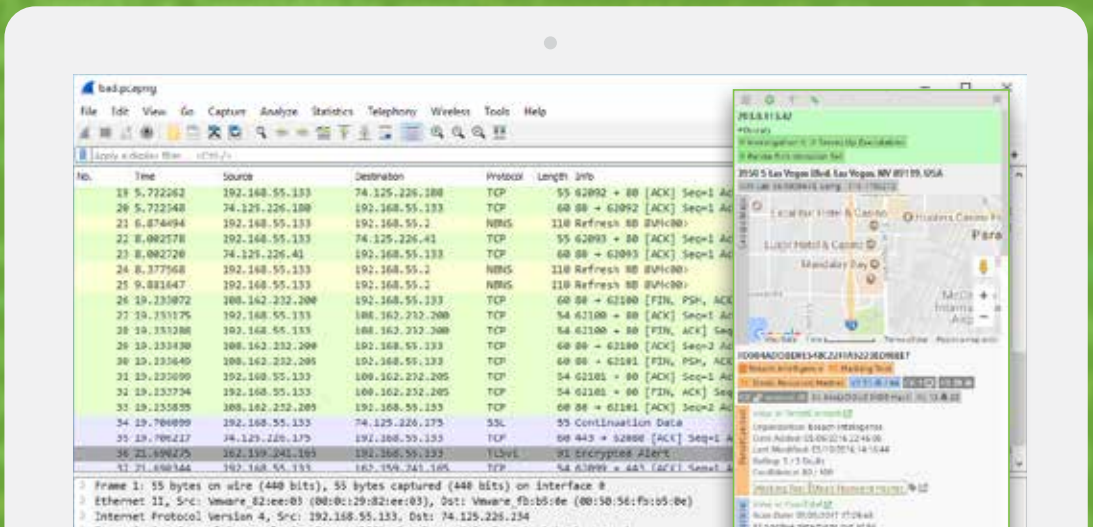
POLARITY

Polarity for SOC



WHAT IS POLARITY?

Polarity is a memory augmentation platform created on the principal that people are the most integral component of data analysis. It provides a new way for IT and Security Professionals 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 analysts 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 SOC analysts never miss the critical intelligence that could have prevented a devastating data breach.

SOC CHALLENGES

Context Information is Dispersed

To accurately assess threats, SOC analysts need to continuously gather context information from a wide range of sources including their colleagues, the Internet, and internal knowledge repositories. This process is time consuming and forces analysts to sacrifice thoroughness for the need to keep up with an ever increasing barrage of intrusion attempts. Incomplete context information due to time constraints, data silos, and tools that cannot interoperate result in undiscovered threats, intrusions, and data breaches.

WITH MEMORY AUGMENTATION

Polarity Delivers Context Information

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

Work Effort is Duplicated

Work efforts are consistently duplicated as multiple analysts 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

Analysts using Polarity have total data awareness as Polarity automatically notifies them of intelligence generated by co-workers in the previous shift, last week, last month, or even last year. For example, if one analyst is investigating a spear phishing email and they flag a malicious URL, Polarity will automatically notify another analyst reverse engineering malware that uses the same URL.

Analyst Fatigue Contributes to Mistakes

Hours of monotonous look-ups, queries, and data entry reduces the quality and speed of human decision making leading to mistakes of habit. Quality pattern recognition degrades to cognitive shortcuts to clear the queue of "false positives".

Polarity Increases Productivity

Polarity combats analyst fatigue by automating the most repetitive and time consuming components of an analyst's daily workflow. Reduced lookups and automatically delivered context data speeds up the decision making process letting analysts do analysis.

ALICE'S FAILURE WITHOUT MEMORY AUGMENTATION

Alice, a SOC analyst who has been with the organization for a year, churns her way through alert after alert marking them as false positives until one stands out, Five Different Users Logged in from One IP Address. She pulls up her browser to lookup the IP and discovers it is a hotel in London. She has seen this false positive before, employees all traveling together, logging in from the same WiFi connection to catch up on email, plus she tells herself "we have two-factor authentication." She checks the box that says false positive, adds her comment, and closes the event.

What Alice does not realize is that she just made a bad decision that will not be uncovered for three months. It turns out only one of the five employees was actually traveling to London. His system was compromised and used to authenticate to the other users' email.

Despite integration of threat intelligence, IP geolocation, human resources, and asset management data into the SOC workflow, Alice still made a bad decision because she did not have access to the relevant institutional intelligence. This knowledge gap allowed the intruder to access pricing information on a 300 million dollar buyout deal currently being negotiated. This insider information allowed the intruder's client to out-negotiate Alice's organization.

THE TEAM'S SUCCESS WITH MEMORY AUGMENTATION

Now what if Alice had Polarity, how would her decision process change? When Alice views the alert for Five Different Users Logged in from One IP Address, Polarity recognizes the IP address and username on her screen and automatically delivers the following intelligence:

- A message from the threat intelligence team letting her know that the users all have access to sensitive buyout deal information and are regularly targeted by a persistent threat.
- A message from the helpdesk team letting her know that one of the users had a virus earlier that day and because he was traveling just ran antivirus to remove it.
- A message from one of her SOC teammates letting her know that the IP address is a London Hotel where employees regularly stay.

Instantly and automatically armed with additional context, Alice decides to confirm travel schedules of the five users and quickly realizes only one of the users had traveled to London. She reaches out to her colleagues on the threat intelligence and helpdesk teams and they contain the threat before sensitive emails are read.

ABOUT POLARITY

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