POLARITY BY ThreatConnect

Case Study

Security Team Works Faster for 200% ROI with Polarity

Challenge

The customer operates a lean security organization within a multi-billion dollar Financial Services company with a global SOC and US-based Incident Response team. The team works in a highly collaborative “Fusion Center” model where efficiency is an important driver. The industry is competitive, so optimizing the output from the team is key to aligning with the corporate strategy.

It’s not unusual for the team to handle hundreds of events per day working across more than twenty-five different security products. Integration between these disparate products is limited, which affects the efficiency and effectiveness of collaboration across the team.

For example, when researching an IOC, an analyst might need context from different tools. Even for an experienced analyst, it’s a challenge to keep track of all the sources, and it takes time to pivot from product to product when doing the job.

While speed or efficiency is critical, it’s also important to be thorough. The skill set of the team is mixed with seasoned analysts who are well versed at handling events, plus less experienced analysts who are learning on the job. It’s important to share knowledge across the team as a means of developing the less experienced analysts and balancing the load for the seasoned pros.

Solution

Data tells a story, Polarity helps you see it though a unified view that provides an overlay with contextual information as you work. When analysts use Polarity, they are better equipped to make thorough decisions and take action with speed.

Polarity helps you seach beyond human scale to find the right data to make better decisions. It’s about being thorough; knowing what is available from past analysis completed by you and your teammates, as well as all the context provided by the security products used day-to-day.

Polarity has helped the client integrate security products from a wide range of vendors, so context is overlaid during analysis and action is seamlessly taken once decisions are made. For example, when researching an IOC, an analyst can right click the URL in the ServiceNow ticket to quickly pivot back into Splunk, ThreatQuotient, or other products for further context. This saves time and improves accuracy since all the information available to research an IOC is available exactly when it is needed versus searching across several different sources.

“We use a wide range of tools in the SOC. Polarity gives a unified platform that automatically searches all of them in parallel to speed up analysis and enrich every tool and workflow...”

Cybersecurity Executive
Healthcare Company

The Polarity open-source integration framework supports more than 170+ security products enabling the team to connect their SIEM, TIP, ticketing system, Vulnerability Scanner, and a number of other products. Though the team is technical, Polarity's ability to integrate these products without requiring them to write code is an important advantage over other approaches. The integration framework also enables the team to support proprietary applications and even customize the way results appear.

With Polarity the team gets relevant context for events as they are working them without needing to pivot between products to repeat searches. The team is also planning to use Polarity Annotations which will allow an analyst to easily recall important details from a past investigation as well as share those same details across the entire global team.

The relationship between the client and Polarity began with a Proof of Concept, and quickly moved into production as the team realized how improved thoroughness and speed when working with security data could impact the efficiency and effectiveness of their work.

Result

The team created a detailed ROI analysis based on time study comparison data they were able to collect during the Proof of Concept with our telemetry feature. The results clearly showed an advantage when using Polarity. For example, the 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%.

With a team that handles hundreds of IOCs and reference sets each day, the ROI from working faster and more thoroughly adds up. Polarity's annual ROI was calculated at 200%, and the project yielded a 6 month payback period. Although Polarity was not budgeted in the team's annual plan, they were able to support the purchase based on the strength of the business case and support for corporate initiatives tied to efficiency.

Though the initial business case was based only on a few use cases, the team has since found dozens of ways to use Polarity. The efficiency gains are so pronounced that management has even noticed performance differences between analysts; those using Polarity are able to meet time and quality SLAs more consistently than those who do not use it.

Working from a great foundation, the team continues to evaluate additional use cases for Polarity including those associated with Risk Management, and even how Polarity could be used by departments beyond the scope of security, such as overlaying information on contracts for the Legal team. Polarity has helped deliver the right data needed to complete the job, exactly when it is needed.