POLARITY BY ThreatConnect

Case Study

End-to-End Triage of Atomic Indicators with Polarity

Challenge

The Wyndham Security team covers a wide range of functions including Threat & Vulnerability Management, Security Operations, and Identity Management. It's a highly collaborative environment where analysts routinely work with other departments at Wyndham and with a Managed Security Service Provider that assists with Level 1 events in the SOC.

As with many security teams, Wyndham uses a number of different products to protect their business with each providing a wealth of data for analysis. For example, when triaging an event, an analyst may access more than a dozen different tools to enrich an IP address or hash. Even for experienced analysts, it's a challenge to keep track of all the available resources, and it takes time to pivot from product to product when doing the job. In the best circumstances, the approach can be inefficient, and in lesser cases it might even result in output that is inaccurate or inconsistent across analysts.

While it's important to be thorough in security, speed is also critical. Even the best teams are challenged to find the right balance between being accurate and working fast. For example, when the team at Wyndham is triaging a system that may have been compromised, it is important to consider all data that may be relevant. Yet even sourcing basic data such as user account details from LDAP can introduce delays that slow response times. Similarly, gathering context from a proprietary system that uses property IDs assigned to each hotel often introduces inefficiency as the team pauses for look-ups when triaging an event.

The team at Wyndham saw an opportunity to save time when dealing with repetitive tasks and to improve consistency as well as accuracy in the way events were triaged. They turned to Polarity for help.

Solution

Data tells a story, Polarity helps you see it with software-based Augmented Reality overlaying 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 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.

At Wyndham, Polarity has helped the team 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 investigating a system that may have been compromised, relevant context like user account details from LDAP are automatically displayed by Polarity on screen. This saves time and improves accuracy since all the information available to work an investigation is available exactly when it is needed versus searching across several different sources.
The Polarity open-source integration framework supports more than 100 security

WYNDHAM HOTELS & RESORTS

About Wyndham

Wyndham Hotels & Resorts makes travel possible for all. From big cities and small towns to beachfront resorts and highway hotels, their 20 iconic brands bring a diverse perspective to the travel experience. With friendly service, thoughtful amenities, and a range of options for the everyday traveler, Wyndham will be there to welcome you wherever you go.

"Polarity is a force-multiplier for our security team whether its threat hunting or another discipline. With Polarity in Highlight or On-demand mode we have confidence that all of our most valuable information is delivered to our analysts, cross referenced against multiple sources, and is acted upon by the right people at the right time. "

Michael Francess
Manager, Cyber Security Advanced Threat

products enabling Wyndham to connect their SIEM, TIP, EDR, NDR, LDAP, 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 Wyndham to support proprietary applications and even customize the way results appear.

Polarity also helps you get the data needed to act quickly. It's about working fast; having the ability to retrieve relevant context exactly when it is needed to make a decision.

With Polarity the team at Wyndham sees relevant context overlaid on screen as they are working. For example, instead of searching the proprietary system to map a property code to a specific hotel, this information is instantly displayed for any property codes on the analyst's screen. The team also uses Polarity On-Demand searches to quickly query all security products for information that is needed in an investigation. For example, simply pasting a hash into the Polarity search window, returns everything that is known about the hash based on prior work completed by the team as well as any details available from the security products connected through the integration framework.

The relationship between Wyndman 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 data could impact their work.

Result

With Polarity, Wyndham has a single platform for end-to-end triage of atomic indicators. Polarity brings together all the context known by the team based on prior investigations, plus what's known by all the security products connected through the integration framework.

Armed with Polarity, the thoroughness and speed of the team's work has improved. Overlooking relevant context during an investigation, swiveling between multiple products to enrich an event, and losing valuable time searching for important details is now a distant memory. Polarity has helped deliver the right data needed to complete the job, exactly when it is needed.

While everyone on the security team at Wyndham has benefited, Polarity has delivered an added value to less experienced analysts. Because it enables the team to seamlessly share the results from prior investigations, less experienced analysts are able to tap this collective memory to improve their skills. Similarly, the Polarity Community on Slack has been a helpful resource for seeking answers to questions and tapping the experiences of other users.

Working from a great foundation, the team at Wyndham is evaluating additional use cases for Polarity for Risk & Compliance, Application Security, and even departments beyond the scope of security like the Hotel Support Team.

POLARITY BY ThreatConnect

About Polarity

Data tells a story, Polarity helps you see it with software-based Augmented Reality overlaying contextual information as you work. No glasses or goggles are needed. When analysts use Polarity, they are better equipped to make thorough decisions and take action with speed.