

Customer Success Story: Hospitality

Wyndham Hotels and Resorts Reduces Threat Detection and Response Times While Scaling Security Operations

WYNDHAM
HOTELS & RESORTS

Background

Wyndham Hotels and Resorts has 9,100+ hotels in 95 countries across 25 brands. Its security team spans threat and vulnerability management, security operations, risk and compliance, cloud and app security, and digital fraud. Wyndham has long been a power user of both the ThreatConnect TI Ops Platform and Polarity.

Challenges Faced

Before implementing ThreatConnect and Polarity, the security team faced a variety of challenges that limited their response times and efficiency:

- ◆ Analysts had to context switch between a “sea of chrome tabs” to investigate and triage events using multiple tools, intel sources, and knowledgebases.
- ◆ Data from all of those tools and sources was manually collected and correlated, taking precious time and effort.
- ◆ Searching for IOCs across their security tools and data sources was manual and time-consuming.
- ◆ SOC analysts struggled to operate consistently and efficiently.
- ◆ Feeding new intel and knowledge back into the TI Ops platform was cumbersome and time consuming, limiting the ability to memorialize findings.

Why They Choose ThreatConnect and Polarity

The combination of ThreatConnect TI Ops and Polarity enables Wyndham to respond faster, more precisely, and with greater efficiency. The combination allows security operators to leverage threat intelligence in-line with context from a wide range of security tools and knowledge sources at the point of analysis, decision, and action.

Key Benefits

- ◆ Automated the real-time collection of context across a range of sources in a single view
- ◆ Frictionless access to threat intel where and when it's needed, regardless of where it lives.
- ◆ Improved cross-team collaboration using a common set of data sources.



- ◆ Analysts have a dedicated workspace to augment their work reducing the need for dozens of browser tabs, enabling them to triage and respond to alerts faster
- ◆ Automated external and internal data is used across every phase of the alert and event triage process to provide consistent and comprehensive context for security events and alerts
- ◆ Every analyst saves hours daily using Polarity's federated data search
- ◆ Incident response is now a highly collaborative, "one team" effort
- ◆ In-app automation eliminated the need to implement and manage a complex SOAR tool

"Using Polarity with the ThreatConnect Platform is a force multiplier for our security team. Together, these solutions give us confidence that all our most valuable information is delivered to our analysts, cross-references against multiple sources, and acted upon by the right people at the right time."

Michael Francesse – Senior Manager, Cyber Security Advanced Threat

Benefits of ThreatConnect TI Ops Platform and Polarity

The ThreatConnect TI Ops Platform lets organizations truly operationalize and evolve their cyber threat intel program, enabling cybersecurity operations teams to improve their organization's resilience to attacks measurably. The TI Ops Platform enhances collaboration across teams to drive proactive threat defense and improve threat detection and response. The AI- and automation-powered TI Ops Platform enables analysts to perform all their work effectively and efficiently in a single, unified platform, allowing threat intel to be aggregated, analyzed, prioritized, and actioned against the most relevant threats.

Polarity enables frictionless federated search, correlation, and analysis for CTI and security operations teams that augments analyst tools with a unified view of data and context aggregated in real-time from over 200 decentralized data sources (threat intel, logs, knowledge bases, security tools, and contextual sources). Users can take action directly in the app, eliminating context-switching and missed data points by dramatically reducing the number of consoles and browser tabs analysts require.

Learn how ThreatConnect TI Ops and Polarity can make you and your team more effective, decisive, and collaborative:

+1.800.965.2708 – or – threatconnect.com/request-a-demo



ThreatConnect enables threat intelligence operations, security operations, and cyber risk management teams to work together for more effective, efficient, and collaborative cyber defense and protection. With ThreatConnect, organizations infuse ML and AI-powered threat intel and cyber risk quantification into their work, allowing them to orchestrate and automate processes to get the necessary insights and respond faster and more confidently than ever before.

More than 200 enterprises and thousands of security professionals rely on ThreatConnect every day to protect their organizations' most critical assets.

www.threatconnect.com

3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com

+1.800.965.270