DIRECTV Latin America

Partnership with SOC Prime enabled DIRECTV Latin America to enhance the company's threat detection capabilities by leveraging curated detection content tailored for Splunk, IBM QRadar, and SentinelOne formats. Leveraging high-quality alerts from SOC Prime Platform helped the company effectively address alert management and prioritization challenges. DIRECTV Latin America relies on SOC Prime as a confident partner to maximize the value of SIEM migration to IBM QRadar striking the right balance between detection coverage and risk minimization. Through collaboration with SOC Prime, the company continues to maintain high standards for the quality and efficiency of its services while strengthening defenses.

Industry	Region	Company Size	SIEM & XDR in Use
Telecommunications/ Entertainment	**Latin America**	**10,000+ employees**	**Splunk, QRadar, SentinelOne**

Germán Miotti
Blue Team Lead at DIRECTV Latin America

"Our partnership with SOC Prime elevated our Splunk system's capabilities. Leveraging the MITRE ATT&CK® framework, SOC Prime not only enhanced our alert management but also acted as a true partner, adeptly navigating challenges and exceeding expectations. As we confidently transition from Splunk to IBM QRadar SIEM, their proven track record of consistent excellence gives us peace of mind. We are assured of maintaining the highest standards in both quality and efficiency, thanks to the value of our collaboration with SOC Prime."

Highlights

- Advancing proactive threat detection capabilities with access to verified detection algorithms enriched with relevant threat intelligence
- Improving threat detection coverage leveraging curated use cases aligned with MITRE ATT&CK®
- Optimizing alert management for enhanced resilience against emerging threats
- Enabling a rapid QRadar SIEM implementation with the best possible balance between detection coverage and risk minimization

Challenges

Detection Coverage Gaps in a Globally Distributed Setting

As one of the world's largest satellite television providers, DIRECTV Latin America curates a globally distributed team with people managing diverse business operations, working in different time zones, and speaking multiple languages. DIRECTV Latin America also has remote teams along with an extensive partner ecosystem accessing the company's assets outside the corporate network. To ensure cybersecurity resilience in such a diversified environment without downtime and delays, the company was looking for a partner who could provide follow-the-sun cybersecurity operations and help navigate operational challenges.

Zero-Trust Adoption Hurdles

Over the years, DIRECTV Latin America has been deploying core solutions for a zero-trust strategy and is currently redesigning the implementation of the SIEM as the core of the company's defensive security.

The company has been looking for a cybersecurity partner that shares a similar innovative mindset and builds solutions on zero-trust architecture to drive more value from shared expertise.

SIEM Migration Challenges

DIRECTV Latin America is currently transitioning from Splunk to IBM QRadar navigating the challenges of multiple data source migration inherent in the SIEM transition process. As the cyber threat landscape is constantly evolving, the company's engineering team has been looking for ways to ensure continuous improvements in alert handling and prioritization for ongoing SIEM management in QRadar. DIRECTV Latin America has been in search of a partnership as an opportunity to collaborate on a comprehensive value proposition, facilitating the smooth implementation of new configurations.

Solution

DIRECTV Latin America relies on SOC Prime as a trusted partner that helps tackle the company's cybersecurity challenges backed by its **SaaS platform for collective cyber defense** that fuses threat intelligence, open-sourcing, zero-trust, and generative AI. Access to SOC Prime's world's largest library of detection ideas for emerging threats and adversary TTPs enables the company to streamline content R&D operations and free up the engineering team for other value-added activities. Partnership with SOC Prime empowers DIRECTV Latin America to consistently meet high standards of quality and efficiency while enriching its entertainment services with innovative cybersecurity solutions.

DIRECTV Latin America can further rely on the partnership with SOC Prime leveraging **Uncoder AI** and backed by the guidance and support of SOC Prime's Professional Services Team to smooth out migration to IBM QRadar and optimize the transition of log sources and custom use cases, maximizing resource effectiveness.

Achievements

24-Hour Threat Coverage

DIRECTV Latin America relies on SOC Prime's follow-the-sun detection engineering operations that ensure round-the-clock protection and proactive defense, leaving no chance for emerging threats, critical exploits, or adversary TTPs to go undetected regardless of the time zone differences.

Improved Alert Management & Prioritization

Through partnership with SOC Prime, DIRECTV Latin America managed to improve alert handling leading to reduced risk exposure and contributing to an improved cybersecurity posture. Leveraging prioritized high-quality and verified detections from SOC Prime Platform enabled the company's engineering team to focus on incident investigation rather than analyzing overwhelming volumes of alerts while minimizing false positive rates.

Access to Ready-to-Deploy Behavior-Based Detections

DIRECTV Latin America relies on SOC Prime Platform as a library of predefined use cases and for consulting best peer-driven practices to build research on and streamline rule coding based on thousands of threat hunting ideas and detection engineering guidance.

Leveraging behavior-based and vendor-agnostic Sigma rules has saved DIRECTV Latin America time and effort on content R&D, translation, and fine-tuning to Splunk, QRadar, and SentinelOne language formats in use.

Improved Visibility Into Threats

With access to an extensive rule feed on the latest adversary TTPs based on ATT&CK, DIRECTV Latin America has managed to increase threat detection coverage. The company is also seeking guidance through an ongoing partnership with SOC Prime to streamline and optimize QRadar implementation while keeping an optimal balance between detection coverage and risk minimization.

Streamlined & Resource-Efficient Adoption of New Configurations

SOC Prime has enabled DIRECTV Latin America to prioritize the implementation of new configurations and facilitated the adoption of a revised cybersecurity strategy backed by a zero-trust model and based on the implementation of the SIEM at its core for reduced time to market.

About DIRECTV Latin America

DIRECTV Latin America has been at the forefront of entertainment for nearly three decades. Since the company's launch in 1994, DIRECTV Latin America has continually evolved its product, best-in-class content, and service to provide customers with an industry-leading video offering. When it comes to the best in entertainment, the company offers nearly every Latin American the ability to beam it or stream it. Focused on people, vendors, and customers, DIRECTV Latin America seeks to deliver innovative entertainment experiences where, when, and how people want it. A shared passion for the joy of television defines the company's mission to offer the content, service, and reliability that allows their customers to connect, unwind, and indulge their inner superfan by watching what they love on any screen, anywhere.

As a leader in entertainment, DIRECTV Latin America never stops innovating and continues to embrace emerging technologies. As the company moves into a bright future, it is committed to achieving the mission of aggregating, curating, and delivering entertainment with its exceptional and innovative services.