Telecom Multinational Industry Leader

Long-term partnership with SOC Prime has enabled the multinational telecom and digital service provider to constantly keep detection content up to date and cover the industry-specific use cases.

Industry	Region	Company Size	SIEM & XDR in Use
Telecom	**Western Europe**	**Up to 10,000 employees**	**ArcSight, Elastic Stack**

IT Security Manager

"We bought the SOC Prime Threat Detection Marketplace subscription as we were struggling to maintain our rule sets which were putting our company at risk. Since subscribing to the Threat Detection Marketplace we are able to continuously update our security content without increasing resources. SOC Prime is now a critical part of our security infrastructure and increasing the venue from existing SIEM investments."

Highlights

- Continuous security enhancement with access to the curated detection content matching the telecom-specific threat profile
- Enabling continuous threat coverage through content alignment with the MITRE ATT&CK® framework
- Reduced MTTD and increased ROI from the SIEM technologies in use
- Providing strategic advisory on the SIEM architecture optimization and tactical recommendations on enhancing security maturity

Challenges

Telecommunication networks are constantly facing cybersecurity challenges and are in dire need of sophisticated defense tools to withstand DDoS and other attacks typical of this threat landscape.

By taking a holistic approach to the cybersecurity services, telecom companies are constantly looking for all-encompassing SOC solutions that would allow keeping track of the local cybersecurity needs in each country and timely address identified risks. One of the top telecom companies in the EMEA region, which further became SOC Prime's partner, was in search of an integrated security approach that would bring about proactive threat detection, continuous security monitoring, and deliver all sorts of log collection.

This industry leader in the telecom sector was seeking assistance in deploying a scalable infrastructure tailored to the telecom threat environment and continuous maintenance of the related security services, including guidance on scale-up and scale-down architecture solutions, migrations to newer software versions, and ongoing SIEM support.

One of the company's primary concerns was finding a vendor of threat detection content that would offer innovative solutions for threat detection covering the telecom-specific use cases and applicable to various SIEMs, including ArcSight and the Elastic Stack.

Solution

With the purchase of the Premium subscription to the SOC Prime Threat Detection Marketplace, the company has unlocked potential for continuous security enhancement applying the unique rule set keenly focused on the telecom attack profile. Mapping content to the MITRE ATT&CK® framework has brought about the increased content focus on threats the company anticipates most that has significantly improved the overall detection quality. The company's security performers, including SOC Managers, Security Analysts, and Detection Engineers can now obtain value from the Threat Detection Marketplace content that is being constantly updated to meet the latest threats sparing in-house resources targeted at detection.

Through the long-term partnership with SOC Prime, this telecom leader has received support in the transition phase, guidance on scalable architecture solutions and setup recommendations for a hybrid dual-SIEM environment based on ArcSight ESM and the Elastic Stack. SOC Prime has provided strategic advisory on the SIEM architecture, assured 99.99% platform uptime and helped to address the tactical tasks of cost-efficient log source onboarding maximizing threat detection capabilities and thus directly increasing ROI from the SIEM technology and SOC operations.
With the SOC Prime Threat Detection Marketplace, the company has supercharged its strategic detection capabilities and reduced the Mean Time to Detection (MTTD) metrics based on the data collected in the Elastic Stack and powered by the exclusive SOC content.

Achievements

Cost-Efficiency & High-Quality Threat Detection

As a multinational telecom and digital service provider, the company is continuously striving to invest in developing markets while reducing the company's operating costs to maximize shareholder returns. Leveraging the SOC Prime Threat Detection Marketplace enables reasonable cost management along with the delivery of high-quality detection and accompanying security services.

Enhanced Visibility into Industry-Specific Threats

SOC Prime curates a wealth of detection content aligned with the MITRE ATT&CK® matrix, which has enabled the telecom company to gain more visibility into threats most relevant to the organization's security needs. The Threat Detection Marketplace content base is growing exponentially providing access to custom telecom-specific use cases helping the company's SOC team save sufficient time on threat detection and content development.

Increased ROI from SIEM Investments

Through partnership with SOC Prime, the multinational telecom leader has managed to extract more value from the existing ArcSight ESM and the Elastic Stack SIEM systems and maximize the productivity of SOC operations.

Innovation-Driven Security Strategy

The company is looking for ways to level up its local SOC services resonating with their security initiatives and a growing need for innovations. These ambitions can be achieved looking back on the tangible outcomes gained through collaboration with SOC Prime and drawing guidance from this ongoing partnership.

About Telecom Multinational Industry Leader

The industry-leading telecom company in the EMEA market delivers all-encompassing communication and digital services to 210+ million customers with rapidly evolving economic dynamics. The key company’s vision is to empower customer ambitions through technology that can be achieved by guiding their choices and channeling their efforts and resources into the right direction neatly matching their business needs.