Sorint.SEC

SOC Prime has helped Sorint.SEC accelerate their threat hunting capabilities and enable proactive threat detection. Overall, the company has managed to save up to one hundred hours per quarter per each SOC team member.

Industry
Information Technology & Services

Region
Southern Europe

Company Size
1,000+ employees

SIEM & XDR in Use
Microsoft Sentinel, QRadar, Splunk, Microsoft Defender ATP, SentinelOne

Claudio Colombo
Chief Technology Officer at Sorint.SEC

“We bought the subscription to the SOC Prime Threat Detection Marketplace to improve our threat hunting capabilities and enable proactive threat detection, so we could provide at least one tuned, tailored and dedicated custom rule for each client per week. With SOC Prime, we can obtain already tuned rules ready to deploy to different SIEM platforms, gaining the right visibility in just a matter of hours rather than in a matter of days.”

Highlights

- Increased visibility into threats with the continuously updated threat detection content aligned with the MITRE ATT&CK® framework
- Accelerated delivery of detections based on specific log sources and TTPs highly anticipated by the company’s customers
- On-the-fly cross-platform translations matching the security toolkit in use
- Privacy-conscious approach to content development compliant with best security practices

Challenges

Lack of SOC Team Hours on Cross-SIEM Content Development and Rule Customization. Security Analysts are frequently overwhelmed with tuning and generating new high-quality rules and their deployment on different SIEM platforms. Otherwise, this can generate a lot of noise and low-quality alerts forcing the SOC team to fix possible false positives and false negatives, increasing effort with low efficiency. In addition to customization challenges of the existing content stack, organizations have to keep pace with the ever-changing attack vectors and continuously deliver new detections to enhance threat visibility. Before collaborating with SOC Prime, Sorint.SEC had to devote sufficient hours to research into the current threat landscape, followed by content development. First, the company produced detections for Splunk, their top security tool in use, and then the in-house SOC team was involved in producing translations to other SIEM systems, which was both a costly and time-consuming process.

Need for Custom Behavior Content Matching Both Legacy On-Premises SIEMs and Cloud-Native Solutions. The majority of customers are challenging MSSP organizations to obtain behavior-based detection content, which causes minimum false positives while preventing missed threats and alert fatigue.

Sorint.SEC was long in search of a cybersecurity vendor that could provide a valuable high-quality solution providing access to behavior-based detections that needed minimum fine-tuning and could be easily deployed to both legacy and next-gen cloud solutions depending on the customers' infrastructure.

Increased Need for Security Awareness in Cloud Environments. Cloud solutions are highly scalable, offer accelerated speed and performance, still, they are more exposed to cyber threats and require more efficient security controls. Sorint.SEC was looking for a trusted SaaS product vendor that could deliver security-conscious threat detection capabilities aligned with best security practices and industry standards on data privacy protection.

Solution

Sorint.SEC has long been searching for a partnership with the trusted cybersecurity vendor to help the company take their cyber defense capabilities to the next level. With SOC Prime, Sorint.SEC has gained access to the world's largest Threat Detection Marketplace that contains 130,000+ detections aligned with the MITRE ATT&CK framework and continuously updated allowing the company to defend against attacks easier, faster and more efficiently. SOC Prime's Detection as Code platform delivers custom use cases tailored to the organization's SIEM and XDR stack and an industry-specific threat profile, which enables Sorint.SEC to provide their customers with ready-to-use solutions following the privacy-focused cybersecurity standards.

Achievements

Enhanced Visibility into the Organization-Specific Cyber Threats

Sorint.SEC has been looking for ways to improve visibility into the continuously evolving threat landscape and help their customers proactively defend against digital threats. Partnership with SOC Prime has helped Sorint.SEC to enable proactive threat detection providing the company's clients with custom use cases available in a matter of hours and covering the latest exploits.

Streamlined Delivery of Curated Behavior-Based Detections Matching the Customers' Needs

With SOC Prime, Sorint.SEC has managed to obtain detection content covering specific log sources and ATT&CK parameters highly relevant to the customers' needs. Access to the SOC Prime Threat Detection Marketplace enriched the company's content stack with the latest Sigma-based threat detections easily convertible to different SIEM and XDR formats. In addition, leveraging the automated capabilities of the SOC Prime's Continuous Content Management (CCM) module, Sorint.SEC can now easily reach the most relevant content based on the pre-configured parameters, like Microsoft data sources and related Event IDs.

Saved SOC Team Hours and Effort with High-Quality Cross-Tool Translations

SOC Prime's support for on-the-fly content translations has helped Sorint.SEC significantly reduce their SOC team's time and effort on converting and fine-tuning detections from Splunk to the Microsoft Sentinel, QRadar, and other SIEM-native formats applied by the company's customers. Overall, Sorint.SEC has managed to save up to one hundred hours per quarter per security engineer enabling the SOC team to contribute with maximum productivity to high-quality and high value security operations.

Improved Threat Modelling Based on the MITRE ATT&CK Framework

Prior to using the SOC Prime's Detection as Code platform, Sorint.SEC was leveraging the ENISA threat taxonomy. With access to the SOC Prime Threat Detection Marketplace content aligned with the latest MITRE ATT&CK framework version, Sorint.SEC has gained more opportunities for threat-centric selection of detections based on the customers' threat profile.

High Security Standards and Privacy Risk Mitigation

Looking for a third-party vendor to augment the company's Managed Security services, Sorint.SEC was highly concerned about security and data privacy protection. SOC Prime's commitment to high security standards, including the use of best data encryption practices and privacy-centric approach to content delivery, ensures that leveraging the Detection as Code platform is secure and reliable in terms of data privacy protection.

About Sorint.SEC

Sorint.SEC is the CyberSecurity Company of the Sorint.LAB group, a leader in Digital Transformation delivering consultancy and Managed Security services in Europe for over 35 years. Backed by its CyberSecurity Operation Center, Sorint.SEC provides 24/7 world-class Managed Security services, including Managed Detection and Response and Managed XDR. Sorint.SEC helps organizations enable continuous monitoring and threat protection by providing Design and Delivery services tailored to the customers' infrastructure, as well as Evolution services delivered by architecture specialists to help the customers augment their investments and extract more value from the existing technological stack according to the business directives.

© SOC Prime, Inc. All Rights Reserved

Explore SOC Prime's Detection as Code platform to defend against attacks easier, faster and more efficiently than ever.

EXPLORE PLATFORM