Banking Industry Leader

In 2020, SOC Prime started partnership with the industry-leading rural savings bank and credit union in Southern Europe. In less than 6 months, SOC Prime has helped the company streamline its detection content development process and save up to 600+ SOC team hours.

Industry	Region	Company Size	SIEM & XDR in Use
Banking	**Southern Europe**	**5,000+ employees**	**QRadar**

Project Manager & SOC Analyst

“With SOC Prime Threat Detection Marketplace, we’ve managed to speed up the development of detections aligned with MITRE ATT&CK® Techniques, Tactics, and Threat Actors. Now our SOC Team can focus on other security operations that are a lot more important while constantly keeping our SIEM updated on complex SOC use cases we were not able to deliver before.”

Highlights

- Accelerated threat detection content development mapped to the MITRE ATT&CK framework
- SOC team can now dedicate time to research and complete threat coverage
- More complex SOC use cases now addressed significantly increasing security maturity
- 600+ hours saved on detection development in the first six months

Challenges

Although the company’s SOC Team was growing, the development of detection scenarios from scratch during constantly changing attack vectors was posing challenges for the in-house security engineers. They tried adopting the MITRE ATT&CK framework to solve the problem, but working with the rule logic to address even the most common industry-specific Techniques, Tactics, and Threat Actors became harder to manage considering the constant evolution of threats. The core of the problem was the level of research and development required for the compex use cases along with the time it was taking for testing, fine-tuning, implementation, and analysis of false positives. In addition, finding skilled security specialists in QRadar was becoming increasingly tough.

With the spread of the COVID-19 pandemic, the security of all remote working processes became the company’s priority. The organization’s SOC Team became primarily focused on developing threat detection content based on remote working attacks. Therefore, the company had to cover detection and response scenarios they had not planned, which required even more work from the SOC Team.

Solution

After investigating a number of alternatives, the company invested in the SOC Prime Threat Detection Marketplace to access cross-platform content across various SIEM language formats, including the company's QRadar security solution. They chose the Premium subscription of the Threat Detection Marketplace unlocking access to an impressive library of ready-to-made detection and response scenarios convertible to various platform formats and benchmarked against MITRE ATT&CK.

Threat Detection Marketplace has been licensed for the whole SOC Team with their SOC Analysts, Threat Hunters, Content Developers, and SIEM Engineers — all able to leverage the platform that customizes its user experience based on the professional role.

Achievements

Reduced Burden on SOC Team

Through less than half a year's partnership with SOC Prime, the company has managed to save up to 600+ SOC Team hours by leveraging some of the 3,000+ custom detections tailored to the company's QRadar SIEM solution.

Continuous Threat Coverage

Using the Threat Detection Marketplace, the organization can keep track of all SOC content items deployed into its QRadar instance to keep it constantly updated on new use cases addressing the latest threats and covering some specific ATT&CK Techniques.

More Opportunities with the In-House SIEM management

With SOC Prime, the company's SOC Engineers are now able to devote time to other high-value procedures, like security monitoring and incident response. After subscribing to the SOC Prime Threat Detection Marketplace, the company managed to speed up their threat hunting process and save time for tracking the SIEM health and performance optimization. Later on, the entire SOC team switched to the in-house SIEM management, which also helped reduce costs spent on external SIEM administration services.

Fast and Smooth Cross-Platform Content Conversion

The company has also gained access to 4,500+ behavior-based cross-platform Sigma detections leveraging the Sigma rule repository. With the help of the Sigma UI tool, converting detection content from the generic language to the QRadar SIEM-native format has become much faster and easier, as well as helped avoid parsing errors during content translation to various platforms.

Access to Compliance-Specific Use Cases

The Southern European industry-leading bank has actively leveraged detections addressing compliance and auditory needs to meet all the required regulatory standards. The newly redesigned flow of the Threat Detection Marketplace enabled the company to streamline the search for the compliance-specific content items as a separate use case. Offering more compliance-specific detection content with relevant tagging based on PCI DSS Compliance and other types of compliance, as well as content addressing auditory needs, can be seen as a common SOC content request for organizations in the financial sector.

About Banking Leader in Southern Europe

The company is the leading rural savings bank and credit union in Southern Europe delivering best-in-class banking services to clients in various industries. With 1,000+ offices spread across all Spain, the company pays close attention to cybersecurity and is constantly looking for ways to boost the organization's detection and response capabilities.