Customer Success Story

magellan netzwerke GmbH

SOC Prime has helped **magellan netzwerke GmbH** supercharge the company's cyber defense capabilities whilst freeing up resources for threat hunting and research for their in-house SOC staff.

Industry	Region	Company Size	SIEM & XDR in Use
Computer & Network Security Services	**Central Europe**	**Up to 500 employees**	**Splunk, Elastic Stack, QRadar**

Dr. Ralf Stodt
Head of Security Operations

"Flexibility and providing fresh content for different platforms, like SIEM systems, is something I really appreciate about the Threat Detection Marketplace."

Highlights

- Access to the world's largest threat detection marketplace offering the latest SOC content aligned with the MITRE ATT&CK® framework
- Hundreds of hours saved on content conversion to SIEM, EDR, and XDR language formats with the online Sigma translation engine
- Overcoming the data schema complexity for various SIEM systems in use
- Continuous detection coverage with the most up-to-date content from SOC Prime's Content Team and the global threat hunting community

Challenges

The company **magellan netzwerke GmbH** delivers professional services to customers in various industries, which requires spending a great deal of time on identifying the risks and detecting critical vulnerabilities tailored to the customer-specific threat profile. Providing support for organizations in various industry sectors requires looking from different perspectives at multiple attack vectors to identify what is highly critical for the particular business area. It also means timely addressing these detected vulnerabilities with custom-specific use cases. The organization employs a growing SOC Team who are continuously developing, researching and analyzing content on the latest threats, vulnerabilities, and leading Threat Actors for the company's customers. This requires significant efforts from the SOC Team since keeping up, let alone staying ahead of the ever-changing cybersecurity landscape, is a tough challenge when supporting multiple organizations.

Another challenge magellan had to face as a MSSP was spending a great deal of time on translating detection content between different Security Incident and Event Management (SIEM) solutions, for example from Splunk to the Elastic Stack, or from Elastic to QRadar, and vice versa. These content conversions were time-consuming due to a large number of SIEMs and other security tools used by the company's various customers. The company needed to find a way to streamline threat detection for multiple SIEMs and automate some of the time-intensive processes in finding, customizing, and deploying threat detection content.

Solution

To ensure a premium service was offered to their customers, **magellan netzwerke GmbH** decided to invest in the Threat Detection Marketplace as part of the SOC Prime's Detection as Code platform and take advantage of the following platform capabilities included in the subscription:

- Unlimited access to the Community and Premium content aligned with the MITRE ATT&CK® framework
- An automated service to translate content into the industry-standard Sigma language, ready for customization
- Continuous content support including guided interactions with experts in SIEM, EDR, and XDR technologies
- Search Profile for streamlined search for detections based on a pre-configured content profile tailored to the company's environment
- Custom Field Mapping tool to enable smooth on-the-fly conversions based on the customized data schema solution

Straight away magellan could accelerate the process of content development from research to its implementation right into the organization's infrastructure. The global SOC content library allows covering organization-specific threats and continuously keeping SIEMs updated on the latest detection and response scenarios.

Achievements

Saved Time Translating Content Between SIEMS

Due to the SOC Prime's platform flexibility, it automatically translates content using generic languages, like Sigma and Yara-L formats, as well as content created in the SIEM-native languages. Cross-platform content can be easily convertible to various formats, which helps save hundreds of hours on translating use cases for customers who use different SIEM, EDR, and XDR tools.

Platform Filtering

Threat Detection Marketplace enables streamlined content search tailored to the organization's threat profile, platforms in use, and the cybersecurity professional role. The SOC Prime's platform filtering capabilities have often come in handy to seamlessly search for content applicable to the specific security solutions, attributed to certain Threat Actors, or covering particular Techniques and other ATT&CK parameters.

Custom Field Mapping

This tool helps adopt basic data schemas to the custom ones and tailor them to various industry standards, including ECS, OSSEM, CIM, or CEF.

Reduced MTTD and MTTR

As part of magellan's security strategy, the company has already boosted detection and response capabilities with the platform subscription enabling continuous threat coverage for the company's customers. The magellan's SOC Team can now search for detections much faster and more efficiently, leveraging curated content written by SOC Prime's Content Team and Threat Bounty Program developers.

Content Categorization

What can be seen as next steps in the company's partnership with SOC Prime is enabling content categorization based on the customers' environment, the industry-specific threat profile, as well as ATT&CK coverage details with related links. Search for content based on such pre-configured customer profiles with an ability to export this information can become a valuable enhancement for MSSPs.

About magellan netzwerke GmbH

The company **magellan netzwerke GmbH** is a Managed Security Service Provider (MSSP) with almost 30 years of experience in delivering professional services in IT security and IP networking, data analytics and forensics, including 24/7 support to enable an end-to-end customer journey. The company has operated since 1992 and today provides security services for several hundred customers across Germany. The company name was inspired by the explorer Ferdinand Magellan and it's his pioneering spirit which drives the company to look for innovative solutions to safely navigate them through the world of cybersecurity.