Customer Success Story

evoila GmbH

Partnership with SOC Prime allowed **evoila GmbH** to enrich the company's Managed Security Services and significantly reduce MTTD. Access to the broad collection of SIEM and EDR algorithms mapped directly to the MITRE ATT&CK® framework helped the company boost its cyber defense capabilities.

Industry
Information Technology & Services

Region
Central Europe

Company Size
11-50 employees

SIEM & XDR in Use
Elastic Stack

Christoper Knöll
Head of Security at evoila GmbH

"With the Threat Detection Marketplace and SOC Prime's SOC Workflow App, we've integrated a toolset into our Managed Security Service that allows us to massively reduce the mean time to detect (MTTD) cyber attacks. The rules created and validated by SOC Prime and its large developer community allow us to map the most up-to-date attack vectors directly into our service"

Johannes Hiemer
CEO of the evoila group

"With our Managed Security Service SIEM, customers of all sizes can profit from the possibilities of using Security Information and Event Monitoring (SIEM) without having to make large up-front investments. We are also intending to participate in the SOC Prime Developer Program to actively develop the platform further."

Highlights

- Improved cybersecurity posture
- Reduced MTTD metric
- Empowering Managed Security Services via integration with SOC Prime's products
- Extensive opportunities for collaborative cyber defense and research

Challenges

As an innovation-driven managed security service provider (MSSP), **evoila GmbH** has always been looking for ways to enhance automation solutions that will give the company's customers a competitive edge with an improved speed, scalability, and a keen focus on their core business needs.

The company prioritized the need for enriching Managed Security Services with a cloud first approach that required focusing resources on strengthening the security portfolio. With this in mind, **evoila GmbH** was striving to extend the existing scalable and innovative log management based on Elasticsearch leveraging SIEM functionalities and detection mechanisms.

The company was in search of a reliable cybersecurity vendor that could offer state-of-the-art threat detection content applicable to multiple SIEM and XDR platforms. The key concern was investing in a scalable solution that would be in line with the company's existing security portfolio and help **evoila GmbH** enhance the cyber defense capabilities of the customers' cloud environments.

Solution

In September 2019, **evoila GmbH** found a perfect match for supercharging the security portfolio by starting a partnership with SOC Prime. With the SOC Prime Threat Detection Marketplace and the SOC Workflow App, a native Elastic Stack add-on for advanced security analytics, **evoila GmbH** has accelerated its Managed Security Services, enhancing cybersecurity performance and significantly reducing Mean Time to Detect (MTTD) metrics.

Achievements

Enhanced Platform Support

Ability to integrate and enrich threat intelligence and attack data for 20+ SIEM, EDR, and XDR platforms.

Threat-Centric Selection of Detection Content

Threat detection content alignment with the MITRE ATT&CK® framework enabling reaching the most relevant rules, alerts, and queries matching the customers' threat profile.

Automation

Linking information from SIEMs, threat intelligence, vulnerability management, and APT scanners for quick-wins in security analytics.

API Integration

Automated streaming of detection algorithms to on-premises, hosted and cloud-native SIEM platforms.

The company is also channeling its resources into cybersecurity research and continuous development of threat detection content that can help withstand the most sophisticated attacks. Collaborating with the SOC Prime Threat Bounty Program, which enables researchers to monetize their own detection content, is one of the company's goals for ongoing partnership.

With SOC Prime, **evoila GmbH** has enriched its Managed Security and Consulting Services through the use of scalable and high-performance SIEM tools. Using a wealth of SOC content available in the Threat Detection Marketplace, including 130k+ SIEM and XDR algorithms, search queries, Snort and YARA rules and more types of curated content, has helped **evoila GmbH** to take its cybersecurity services to the next level.

About evoila GmbH

As a cloud-focused MSSP, **evoila GmbH** specializes in the product development of new ideas and concepts related to cloud integration. Since 2012, the owner-managed company has faced every challenge in the IT market with great passion, excellent know-how, and a pronounced awareness of quality, while striving for a good balance between employees, customers, and the company. From its two locations in Mainz and Nuremberg, **evoila GmbH** with around 30 employees, contributes to technological progress and supports its customers. The company is now building its Managed Security Services with a cloud first approach, aligning the customers' security portfolios with the clear trend of using multi and hybrid cloud scenarios in the IT infrastructure.