SUCCESS STORY

COOPERATION BETWEEN

sure[secure]
your security operations center

OQEMA

Kurzvorstellung des Partners

OQEMA Deutschland, known as Overlack until 2017, is one of the leading chemical distributors in Germany. Just over 1,600 employees currently work for the OQEMA Group at 50 locations in 25 countries.

At the interface between chemical manufacturers and the chemical processing industry, OQEMA provides services along the supply chain. From procurement, product development and individual blending to logistics and recycling.

OQEMA

OQEMA AG

Industry:	Chemical distribution
Employees:	1.600
Founded:	1922
Revenue:	1,7 billion EUR

These topics are part of the success story

- IT security in connection with mergers & acquisitions
- Security Operations Center as a Service

What challenges did the partner face?

The Group is growing steadily. This growth is taking place both organically and through mergers and acquisitions. For this reason, new IT infrastructures must be connected to the core of OQEMA IT in parallel with organic growth. This integration of external infrastructures harbors the risk of a possible infection for the entire IT network of the Group. It must therefore be ensured that the essential business processes are protected in the best possible way.

In addition, OQEMA is affected by the NIS2 directive and must therefore prove that it can detect cyber attacks 24/7 and respond appropriately. The company has therefore evaluated solutions that can cover these challenges.

In this mixed situation, it is important to evaluate at the outset whether implementation with internal resources seems realistic. It is also important to consider that scalability plays a major role in the choice of technology due to rapid and international growth. This applies to the main technologies identified, SIEM and SOAR. If possible, this implementation should be accompanied by a predictable cost structure.

For us at the Cyber Defense Center, these complex and dynamic structures are very challenging, but also totally exciting.

Due to the strong dynamics, we are constantly developing new playbooks and detection rules together with our partner.

Philip Schildein
Head of Cyber Defense Center
suresecure GmbH

How did we solve the challenge?

In the end, our SOC service came out on top because it covers all the challenges. Our SOC is based on the Google SecOps platform, which is provided as SaaS from the cloud.

This means that new infrastructures can be connected at any time within a very short space of time. Even if the new systems to be connected have not yet undergone an in-depth check, OQEMA is able to detect any compromised systems at an early stage and prevent further infections before they occur.

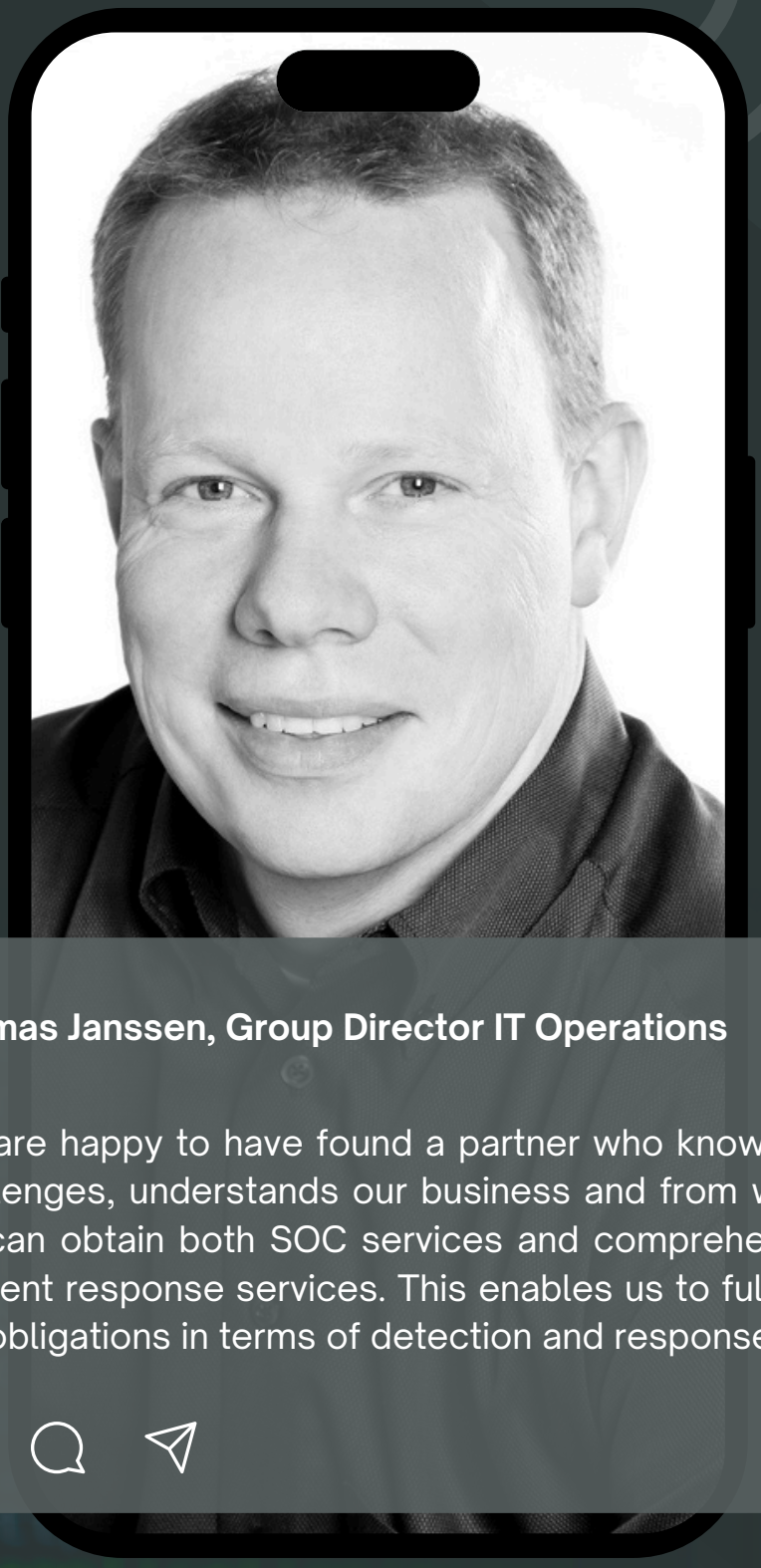
The calculation is based on the number of employees to be protected. The log volume and the number of IT assets are irrelevant and provide the perfect framework for cost-neutral scaling. It is precisely these two points that are usually difficult to define at the start of a SOC project. More systems and log volumes then quickly lead to a completely new price structure, which can then lie outside the set budget.

In the past, the OQEMA Group has already detected and documented various cyber attacks.

The company is an attractive target, particularly due to its international reputation, industry affiliation and strong growth.

That is why a key element in the evaluation of potential service providers was also their expertise in the area of incident response. In the event of an attack, it was important to react quickly and correctly in order to avert potential damage. This is where we were able to score points with our comprehensive incident management framework, which also includes segments such as authority management and crisis communication.

The OQEMA Group is therefore well equipped for future activities and can continue to pursue its growth ambitions without restriction.

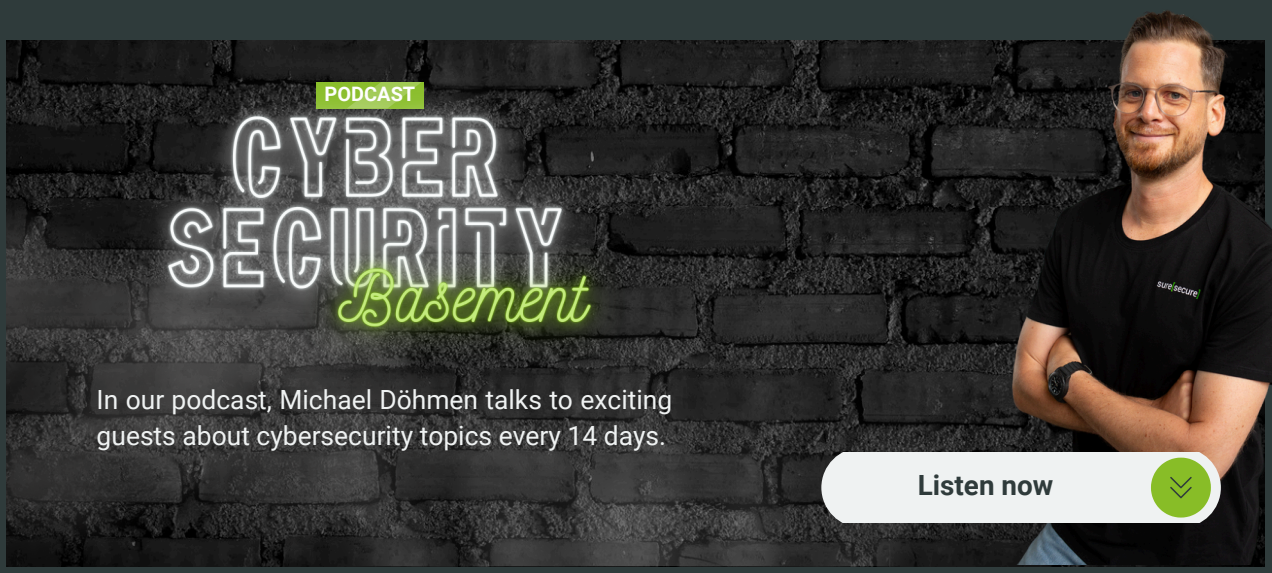


Thomas Janssen, Group Director IT Operations

We are happy to have found a partner who knows our challenges, understands our business and from whom we can obtain both SOC services and comprehensive incident response services. This enables us to fulfill all our obligations in terms of detection and response.

Key Take-Aways:

- Securing important business processes should be a priority. This means that these should be precisely identified, described and secured
- Visibility and transparency are key elements in the defense against cyber attacks
- Securely managing a growing IT network through organic expansion and acquisitions and complying with the NIS2 directive, which requires 24/7 monitoring of cyber threats, is complex
- Implementation of a scalable, cloud-based SOC service based on the Google SecOps platform ensures improved security, regulatory compliance, flexible scalability and cost predictability



suresecure gmbh
Dreischeibenhaus 1
40211 Düsseldorf

Telefon: +49 (0) 2156 974 90 60

E-Mail: kontakt@suresecure.de
www.suresecure.de