SUCCESS STORY

FROM THE COLLABORATION

sure[secure]
your security operations center

BSW

Brief Introduction of the Partner

Badische Stahlwerke GmbH (BSW) is a steel manufacturer based in Germany. Up to 2.4 million tons of steel are produced annually at its Kehl site. In the electric steel plant, steel is not manufactured from iron ore and coke. Instead, the secondary raw material steel scrap is recycled in a resource-efficient manner and then melted down in an electric furnace to produce new steel, a circular process that can be repeated indefinitely.

This process results in products such as reinforcing steel bars and wire rod. With annual revenues of more than one billion euros and around 900 employees, Badische Stahlwerke GmbH is a key contributor to the German steel industry and the broader industrial sector.

Badische Stahlwerke GmbH

Industry:	Steel industry
Employees:	approx. 880
Founded:	1955, since1968 as BSW
Steel p.a.:	2.4 million tons
Insured:	> EUR 1 billion

These topics are part of the success story

- Incident Response Retainer
- Incident Response Management
- The Importance of Trust in the Security Environment

Incident Response Retainer: When the worst-case scenario becomes reality

“We hoped we would never need the retainer. But when it mattered, it proved invaluable.”
- Ralf Butsch, CISO, Badische Stahlwerke GmbH

As a steel producer, Badische Stahlwerke GmbH has always relied on forward-looking IT security. If steel production were to come to a halt due to IT issues, the consequences could be severe.

For this reason, at the end of 2022, the company decided to enter into an IR retainer agreement, as it lacked the in-house expertise to handle a cyberattack internally. We looked back on this exceptional case in an interview with CISO Ralf Butsch, who joined BSW only after the security incident. He is familiar with every detail.

Fotos: Carsten Görling

Initial Situation:
Prevention Instead of Remorse

After the decision had been made to engage an incident retainer, the evaluation of relevant providers followed. Looking back, Ralf emphasizes that the following points were particularly important to him:

- a dedicated point of contact with crisis experience
- German-speaking support
- a resilient, trust-based interpersonal relationship
- regular crisis exercises

Is it surprising that the primary focus is on the interpersonal aspect? Not really, because when you are operating together at the very heart of a company during an incident, you are grateful to know the “doctor” and to be confident that they have performed this procedure several times before. And yet, in such an operation, everyone is working at the limit of their capacity.

When the steel producer engaged the Incident Response Retainer with suresecure GmbH, it did so with the quiet hope of never having to activate it. After all, who wishes for an IT security incident within their own company?

What no one could have anticipated, however, was that at the time the contract was signed, the attacker was most likely already active within the network. Although projects to strengthen cyber resilience were underway in parallel, they came too late.

The Emergency: An Attack from the Inbox

DThe attack began several weeks before the ransomware was deployed, starting with a classic phishing email. The attacker moved through the system unnoticed, gathered privileges, and was able to place the malware. By the time the systems were ultimately encrypted, it was too late for countermeasures:

Nothing worked anymore. No logins, no communication.

“We brought the fax machine up from the basement just to be able to communicate at all,” Ralf Butsch quotes a colleague.

Trucks lined up in front of the factory gates, customer inquiries went unanswered, and internal communication broke down. The company’s digital infrastructure was completely paralyzed.

And then?

“Then we immediately called you - the emergency number was posted at the front desk. And 15 minutes later, help was there. For us, that was a turning point.”

He was particularly impressed by the speed and the clear communication:

“Everyone was relieved that someone was there who knew what to do.”

The Turning Point: From Firefighting to a Firewall

The incident was a turning point, but also the starting point for significantly strengthened cyber and business resilience. After the retainer was activated, several workstreams were launched immediately. In addition to the forensic investigation, it was essential to address reporting obligations and to thoroughly review the entire communication process.

To avoid reputational damage, targeted and proactive communication is crucial. After all, all stakeholders have a legitimate interest in the situation. Our incident framework covers the following topics:

- **Incident Management**:
  Organization, planning, and coordination of all workstreams
- **Containment**:
  Limiting the damage, where possible
- **Communication**:
  Targeted crisis communication tailored to specific audiences
- **Legal**:
  Legal support and guidance
- **Desaster Plan:**
  Creation of a structured roadmap through the incident
- **Recovery**:
  Immediate initiation of system restoration and infrastructure cleanup
- **Forensics**:
  In-depth analysis and reconstruction of the cyber kill chain

A single point of contact for all relevant components - even though BSW certainly has its own resources for communication and legal matters:

"A sparring partner with experience is simply invaluable in such a situation, helping to build confidence in dealing with the multitude of issues," says Ralf.

From my perspective, I can only express my deepest respect for the entire incident team. What is accomplished during these times is, in part, truly beyond human limits.

I am very pleased, and also proud, that we were able to build a truly strong partnership as a result of the incident at BSW.

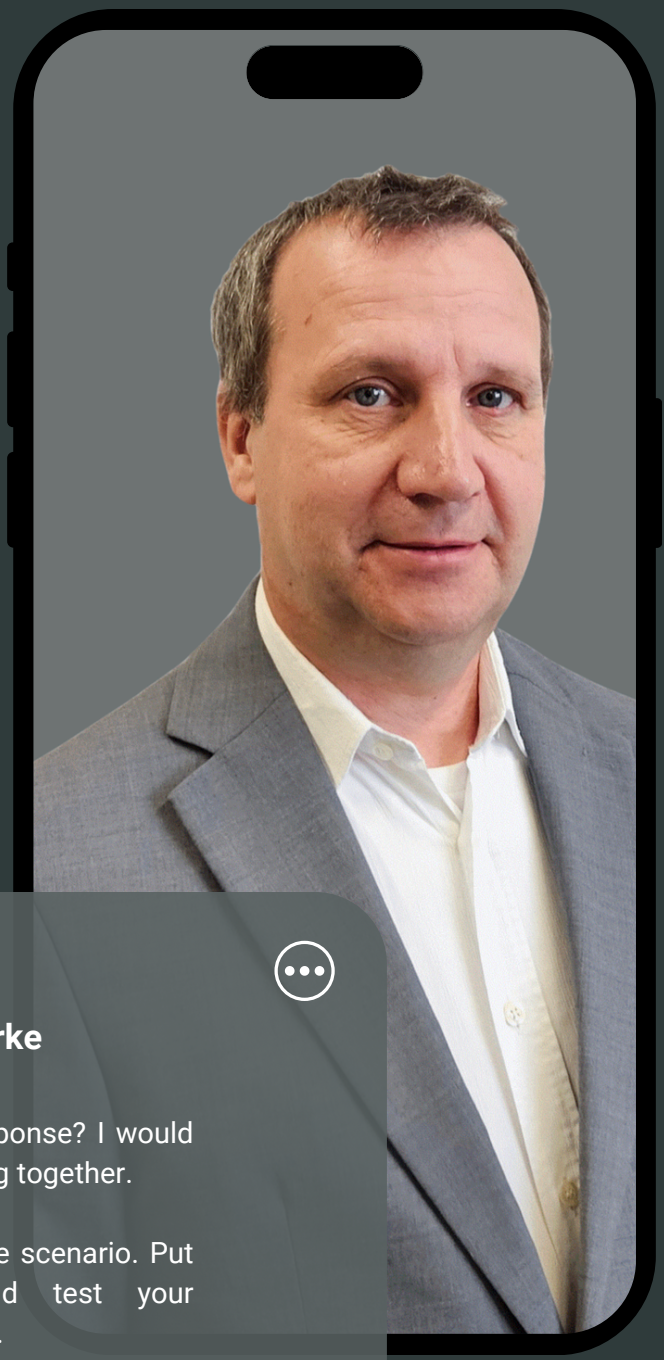
Filip Krauß
Enterprise Account Executive
suresecure GmbH

The Turning Point: From Firefighting to a Firewall

Following the incident, a comprehensive Security Operations Center (SOC) was established, processes were redefined, and the ISMS was refined. Today, the company is positioned more broadly and robustly, viewing cybersecurity as a continuous development process. In the services area in particular, BSW relies on strong partnerships.

SafeGuard, suresecure's Incident Response Retainer, is more than a contract - it is proof that, in an emergency, every second counts…

His advice to colleagues in the industry is clear:



Ralf Butsch
CISO Badische Stahlwerke

A SOC without Incident Response? I would never do that. The two belong together.

Don't wait for the worst-case scenario. Put safeguards in place and test your processes while you still can.

Key Take-Aways:

- Preparation Determines the Outcome in an Emergency
- Trust Outperforms Technology
- Resilience Emerges from the Attack

suresecure gmbh
Dreischeibenhaus 1
40211 Düsseldorf

Phone: +49 (0) 2156 974 90 60

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