RAPID7

CASE STUDY

# Rapid7 InsightVM and InsightIDR Integrate to Drive 60% Time Savings and Ease Compliance for Energie Suedbayern

**INDUSTRY:**
Energy/Utilities

**SIZE:**
350 employees

**PRODUCTS:**
InsightVM*, InsightIDR

## CHALLENGE

- Needed to remain compliant with Germany's IT Security Act.
- Required a technical solution that had the intelligence, not just rules, to detect anomalous activity in their IT infrastructure.

## SOLUTION

- Since ESB could prove the technology was used for security purposes, it was approved by the works council.
- Rapid7 InsightVM and InsightIDR offered "one agent to rule them both" for simplified management and centralized reporting.

Germany's large energy sector is a sizeable target for hackers. Today's cybercriminals, hacktivists, and state-sponsored operatives have both the motive and the capabilities to strike with attacks designed to steal sensitive operational and customer information, hold organizations to ransom, or disrupt and destroy key control systems.

These are just some of the threats that keep Benjamin Nawrath awake at night. Benjamin Nawrath is the information security officer at Southern Bavarian energy provider Energie Suedbayern (ESB), which supplies natural gas and electricity to 120,000 households in the south of Germany. The largest operator of its kind in the region, ESB has around 350 employees, with 14 staff working alongside Benjamin Nawrath in IT.

### The compliance burden

One of Benjamin Nawrath's biggest challenges is maintaining compliance with Germany's IT Security Act (ITSG), which became law in 2015 but applies from July 2017 onward. The law requires all critical infrastructure providers to run an advanced cybersecurity program designed to ensure the availability, integrity, authenticity, and confidentiality of their IT infrastructure. It also demands that organizations regularly provide certification proving their compliance. Failure to do so could result in a fine of hundreds of thousands Euro.

With a large and complex environment to monitor (including 2,000 IP addresses), limited IT staff resources, a growing compliance burden, and ever-determined hackers to keep at bay, Benjamin Nawrath needed robust technology solutions to help overcome these major challenges.

*Our award-winning Nexpose product has evolved into InsightVM, which utilizes the power of the Rapid7 Insight platform, our cloud-based security and data analytics solution.

Learn more at:
www.rapid7.com/insightvm

## Getting the green light

ESB IT had been using Rapid7's leading vulnerability management solution Nexpose* previously, so expanding their portfolio with Rapid7 was a natural choice. To fill the need for an incident detection and response solution, a Proof of Concept (PoC) with Rapid7 InsightIDR was quickly and easily to set up to provide that all-important confirmation of the product's industry-leading capabilities.

"I needed a solution that had intelligence inside it—not just a technical solution to create rules. I buy the intelligence, not the rules. That's what Rapid7 really made successful for us in this evaluation," says Benjamin Nawrath. "Splunk and similar solutions just collect the logs, and I needed to keep track of them myself. But I want to know if something strange or irregular is happening, which InsightIDR tells me. It was the best solution to provide the intelligence I need for a reasonable price."

ESB moved forward with the combination of InsightVM (the evolution of Rapid7 Nexpose) and InsightIDR—both powered by the Rapid7 Insight platform—to offer industry-leading vulnerability management and incident detection and response. Benjamin Nawrath states that both solutions were easy to set up and maintain, and that they provide "one agent to rule them both"—simplifying management and centralizing reporting. ESB has been a keen adopter of cloud services, so there were no roadblocks in terms of delivery. And since it was for security purposes, the monitoring of IP addresses was given the green light by representatives from the German works council.

## Accelerating incident response

InsightIDR has saved ESB IT time and helped them respond to incidents far more quickly. Unifying SIEM, user behavior analytics (UBA), and endpoint detection and response (EDR), it was designed from the ground up to detect intrusions as early on in the attack chain as possible, leaving nowhere for the bad guys to hide.

"Honestly, I didn't have any incident response process in place before InsightIDR. I would just get a report from users saying 'something is not as expected.' I would then have to dig in and collect logs myself, which took a huge amount of time," says Benjamin Nawrath. "InsightIDR has really helped me be able to respond to incidents more quickly. It's really easy to use and the agents provide great insight."

Benjamin Nawrath is leveraging the live dashboard functionality to track failed log-ins by special users. "One of the many good things is, I don't have to tell InsightIDR what is a service account—it just recognizes it," he says.

The easy-to-manage portal allows him to keep an eye on any unusually high values, if remote users are logging in from other countries, or any other metrics that might indicate non-compliance. Email alerts complete the picture and are also sent to other members of the IT team, allowing them to respond if anything malicious is found.

## Lowering risk with InsightVM

With a complex IT environment to monitor, including highly sensitive industrial control systems, Nawrath also needed enterprise-grade vulnerability management tightly integrated into InsightIDR. Rapid7's InsightVM automatically collects, monitors, and analyzes any vulnerabilities on the corporate network, featuring advanced analytics and reporting to allow users to prioritize and remediate risk.

For ESB, success is measured in terms of lowering risk over time, something InsightVM has been great at driving.

"I scan regularly and with user credentials, so I get as much information as I need. We have nearly no false positives, which is great," says Benjamin Nawrath. "InsightVM also helps us to identify old systems which need to be refreshed, upgraded, or even abandoned. It provides great insight in how I can evaluate the risk. It's great to see how risk decreases by implementing remediations."

"InsightIDR has helped me be able to respond to incidents more quickly. It's easy to use and the agents provide great insight."

The agents have also helped save time over regular scans, and the benefit of tight integration with InsightIDR has boosted efficiency by enabling highly accurate correlations between incidents and vulnerabilities.

## Looking ahead

Ultimately, the combined power of InsightIDR and InsightVM has saved Benjamin Nawrath as much as 60% of his and his team's time. This in turn allows him to spend more time on verifying the vulnerabilities themselves, and to prepare for an upcoming OSCP examination. What's more, the value of the data generated by Rapid7 has even helped him increase his standing within the organization.

"Upper management isn't overly involved with security, but with both products I'm able to convince them of the real risks we face. It helps me get more respect for my work," he says. "And because the solutions weren't that expensive there was no problem convincing the management to free up the budget."

As for the future, Benjamin Nawrath plans to extend the capabilities of his investments even further by implementing InsightVM's Remediation Workflow to delegate tasks to his colleagues. But most importantly, he's confident the combination of InsightIDR and InsightVM will provide all the reassurance needed to meet its obligations under the IT Security Act—keeping ESB safe, secure, and compliant for the years to come.