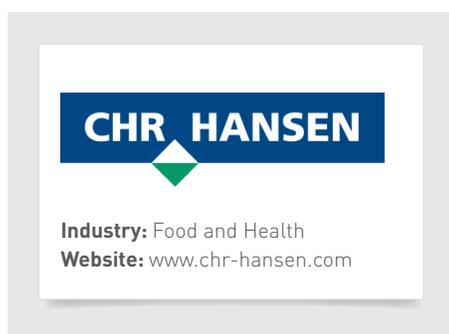


Ezenta and Rapid7 Help Chr. Hansen Gain Security Visibility



Chr. Hansen, a 140-year old company headquartered in Denmark with offices worldwide, develops natural ingredient solutions for the food, nutritional, pharmaceutical and agricultural industries.

Søren Hansen is the IT Security Manager there, overseeing standard security operations and reporting to the CIO. He remembers when he was first appointed to the position: “I had a strong technical background, but needed someone to partner with from a prioritization standpoint, with regards to the day-to-day management of the security program.”

Enter Ezenta, a highly specialized IT security company dedicated to forging strategic partnerships through a combination of technology, consulting, and reporting. Søren was able to leverage his organization’s preexisting relationship with Ezenta to great effect. “They’re our external security advisors, and they’ve been extremely helpful in ensuring that our security program remains top notch,” he explains. “I outlined some of the security challenges we were having, which mostly centered on the need for

“I’d have to waste hours going in, looking at the infected machine, and collecting information that UserInsight now gives me right out of the box.”

greater visibility. Ezenta recommended Rapid7 UserInsight.”

Søren required greater visibility into what users were doing on the network, along with an intruder

analytics solution that would alert on suspicious network activity and streamline incident investigation. UserInsight seemed to meet those needs, and so Chr. Hansen moved forward with a proof of concept, with input from Ezenta.

Since the Ezenta team was familiar with both the environment at Chr. Hansen as well as the product itself, their guidance was integral to ensuring that the proof of concept ran smoothly. “Immediately, the information began flowing in a very manageable way. It was easy to see the value in the product – it alerted us to the presence of malware that was easily eliminated, but that we might not otherwise have known about.”

Once UserInsight was deployed, Søren continued to see results. By detecting stealthy attack methods, such as stolen credentials and lateral move-

“Immediately, the information began flowing in a very manageable way. It was easy to see the value in the product – it alerted us to the presence of malware that was easily eliminated, but that we might not otherwise have known about.”

—**Søren Hansen** , IT Security Manager, Chr. Hansen

ment, UserInsight provided visibility into anomalous behavior. “I wanted a product that would flag specific things which we might not otherwise know about, and that’s exactly what UserInsight does. If it generates an alert that is a false positive, I can create a rule to correct that – so we can fine tune the system to meet our needs. I find value because the alerts tell me when I need to investigate something in greater depth to determine whether it is, in fact, a security incident. For example, I may need to ask my colleague whether they really did log in with administrator credentials on a machine that they don’t typically use.”

The team at Chr. Hansen didn’t have time to spend sifting through mountains of information – in that regard, UserInsight has delivered not just on the quality of alerts, but also the quantity. “The product sends me an

appropriate amount of alerts – about three to five per day,” says Søren. “That’s definitely not an unmanageable amount of noise. I also liked the fact that we didn’t have to deploy another agent on the endpoint. We deployed it agentlessly and haven’t had a single complaint from IT.

“UserInsight also flagged a malicious process that our virus scanners missed.” This was because UserInsight uses the results of over 50 virus scanners to detect known malware, which covers some of the blind spots that can be found in antivirus solutions.

“UserInsight is also helpful when it comes to communicating with other groups – such as the server or network teams. If I’m asking for assistance with an investigation, I can take the information which UserInsight provides and can tell them where to

look. For example, ‘This is a known piece of malware, can you please clean this machine? Here’s the file name.’ That’s brilliant because otherwise I’d have to waste hours going in, looking at the infected machine, and collecting information that UserInsight now gives me right out of the box.”

At the end of the day, Chr. Hansen has benefited from its relationship with Ezenta and Rapid7. “We didn’t just choose Ezenta because we need extra manpower,” Søren says. “They’re trusted advisors who actively assist us with our security program development. You can’t over prepare when it comes to security. Rapid7, meanwhile, has been very impressive with developing features and incorporating customer feedback into UserInsight. I wouldn’t hesitate to recommend them.”