Transforming Nationwide's security operations

VIDEO TRANSCRIPT

Nationwide Building Society is headquartered in the UK. It's the largest of its kind in providing retail banking services globally. We are a mutual, so we are owned by our customers and recently we've acquired the Virgin Money brand that allows us to move beyond retail banking into the arena of business banking as well. To put it in context, one in ten pounds of deposits that our retail customers hold across the country is with Nationwide. So we are a systemically significant institution in the UK. We needed to ensure our teams could prepare for evolving threats, including those driven by Artificial Intelligence, and this meant modernising our security monitoring tooling. We wanted a unified solution, utilising a single set of tools and one language, to reduce our time to detect and respond to security incidents, as well as optimising our costs. We knew that a migration of Nationwide's Security Operations Centre from Splunk Cloud to Microsoft Sentinel was the right call. But this was set to be the most complex migration we'd ever completed. There were terabytes of daily data and hundreds of analytics rules and automation playbooks – as well as processes and rules that had to be redefined. This attention to detail would mean that Nationwide had a solution that would last it into the future. And we partnered with Microsoft to ensure we could deliver it smoothly. It is a tall order, and the clockwork coordination between multiple teams. And all of this, while ensuring we're also maintaining the service stability. This was an innovation-led approach – while most clients were experimenting with generative AI, we had put it to practical use as part of query language translation, which acted as a catalyst to help us accelerate the migration. It was a highly collaborative process, with colleagues from Nationwide, Accenture and Microsoft all working as one team with a shared goal. We took an agile approach to delivery, starting work on new parts of the project at 50-60% completion to accelerate the schedule. Our product engineering teams were embedded from the start. This meant we could provide direct technical support whenever it was needed and also pick up valuable learnings as we progressed. Together with Accenture, we also pioneered the large-scale deployment of our joint generative AI Splunk to Sentinel migration tool – with use on the Nationwide migration being a worldwide first. This delivered a 40% in time

saving for manual effort spent interpreting and converting Splunk rules to Kusto Query Language (or KQL). It actually worked so well, we've now made it a standard part of the Microsoft product set. The project was a complete success. It was delivered on time and handled a huge 430 custom detection use cases. As well as being a successful delivery for Nationwide, we're proud to have played our part in roadtesting the new generative AI KQL tool that is now being used by other Microsoft customers to protect their own organisations. Now, we're set up for further adoption of automation and AI in our security operations. That gives us the tools to handle emerging threats, with flexible cloud scale protection and integration with the wider Microsoft security ecosystem. So ultimately, we believe now we've got a really robust method of defending the fort for our customers. So while we take care of their money and make it work harder for them, they can rest assured that their personal and financial details are safe and secure with us