Bridewell Consulting

Case Study

SOC implementation bolsters MAG's resilience in turbulent times

Background

As a key CNI sector, security in aviation is paramount. But when the Covid-19 pandemic hit, aviation became one of the worst affected sectors. With revenues plummeting, organisations such as Manchester Airport Group (MAG) were forced to review their budgets and look at areas where substantial savings could be made.

When the scale of the pandemic became apparent in March 2020, MAG were already in negotiations with their existing managed security services provider that ran the organisations outsourced security operations centre (SOC) externally. The initial contract was coming to an end and it was becoming increasingly apparent that in order to remain fit for purpose, the relationship was going to be a lot more costly and complex moving forwards. The incumbent provider wanted to move MAG to a different technology platform which would require substantial CAPEX upfront and would mean an increase in operating costs.

MAG, which is the largest UK owned airport operator and sees over 60 million passengers flying through its airports including Manchester, East Midlands and Stansted each year, were looking to find a solution to the SOC services being provided by its incumbent provider that better met the business' needs. "We decided that now was the time to put a business case together and highlight that we could get a better value service by bringing the SOC in-house," commented Tony Johnson, Head of Cyber Security Operations at MAG.

Case Study

Bridewell Consulting

Case Study

Bridewell CONSULTING
Above. Beyond. Always.

Finding Expert Guidance

Setting up the outsourced SOC had been a gruelling project and the thought of taking on another project of this scale was daunting for MAG, especially in terms of the time it would take. Tony had been looking at different solutions and sought advice from peers across the UK aviation sector. Through these conversations he was invited to a conference at a leading UK airport that had undergone a similar transformation and migration from a slow incumbent. It was here where Tony learned about the airport's own journey building a more modern, agile outsourced SOC with Bridewell as its security partner.

The peer airport had already moved away from having an incumbent fully managed service provider running its SOC and Bridewell as its outsourced partner had deployed the SOC technology stack for the airport which is a blend of Microsoft Sentinel and Microsoft Defender XDR. MAG was impressed by how much was done in such a short amount of time, including onboarding new services.

"The team spoke highly of Bridewell," says Tony. "Bridewell represented themselves very well when we met them there. We had a really productive conversation and could have easily mistaken them for our peers own in-house security team as they had so much knowledge of the business and its infrastructure."

Getting the project off the ground

The progress that had been made at the peer airport and the strong relationship between the airport operator and Bridewell put MAG's fears to rest concerning the scale of their own project. Tony got to work on the business case for MAG, following the model Bridewell had developed using the Microsoft Defender XDR and Microsoft Azure Sentinel stacks. He began to engage with Microsoft to develop a pilot SOC solution and Microsoft offered to fund the pilot and provide necessary resources but stressed the importance of having a cyber security partner involved in the project. Tony already had Bridewell in mind.

"We had the technical capabilities to do this on our own but we wanted to work with a company that had been there and done that. We knew that Bridewell had the relevant experience in aviation as well as ASSURE accreditation so could avoid the pitfalls and complications which can arise in this sector," says Tony.

Once Bridewell understood MAG's business objectives, its dedicated team got to know the organisation with the same level of depth they had demonstrated with previous projects, acting as a value-adding partner that truly understands the customer rather than just another third-party provider.

An assessment phase followed in which Bridewell performed a gap analysis, and then a design phase where it looked at the resources that were already available within MAG and highlighted any further resource that would be required. At this point Bridewell could decide upon the people, processes and technology required for the project. With a significant percentage of MAG's staff furloughed due to the pandemic, resource was a challenge but Bridewell were able to fill these gaps and keep the project running smoothly and, crucially, on-schedule. The SOC was then moved seamlessly in-house with Bridewell offering a Hybrid model ready for the pilot period to begin.

MAG AFTER WORKING WITH BRIDEWELL

TIME DESTINATION FLIGHT STATUS

95% VISIBILITY OF THEIR ESTATE

80,000 EVENTS PER SECOND

7 MAN-HOURS A WEEK SAVED

IN-HOUSE MANAGEMENT OF TOOLS

IDENTITY INSIGHTS

A Resounding Success

The pilot period lasted eight weeks and was a resounding success, completed ahead of deadline with all success criteria met. The project has also been delivered on budget with MAG spending no more than they were with the incumbent provider. "Bridewell really impressed us with how organised they were when it came to getting the pilot SOC underway and they drove the team which was exactly what we needed," says Tony. "There was no reason not to take it to the next stage."

Phase one of the rollout needed to be completed by Christmas Eve which was when the existing contract with incumbent provider ended. The incumbent provider had 70% coverage of MAG's estate and this was the coverage target for phase one. "Bridewell was completely successful in meeting the target and we had exceeded the 70% coverage," says Johnson.

Case Study

Bridewell Consulting

Case Study

Bridewell also provided a dedicated SOC analyst who acted as an honorary team member, sharing the skills and knowledge with MAG's internal team to give them the best success in running the SOC in-house. This resulted in significant cost savings as MAG would otherwise have had to invest heavily in training with an external provider to get their team up to speed. Phase two was completed in March 2021 and Bridewell's SOC analyst and hybrid team has been in place the whole time helping the MAG team move forward providing expert guidance and instilling the in-house team with the confidence required.

Prior to working with Bridewell, MAG only had 70% visibility of their estate and could only see 5,000 events per second. MAG now has visibility of 80,000 events per second and over 95% of endpoints and servers visible to the SOC. MAG's team were flooded with a lot of unnecessary noise from the incumbent provider which would constantly notify them of potential issues that they had detected. It would then be down to the MAG team to investigate the issues which often turned out to be normal behaviour which required no action. "We're very confident that we're delivering a better service internally than the incumbent provider ever could. We can see the outcomes. We can see the incidents that are getting raised and that we're solving," says Tony.

Uncompromisingly Powerful Cyber Security

MAG has seen the biggest impact in dealing with phishing attacks. Like many organisations, MAG has experienced a significant increase in phishing attacks over the last 12 months and attackers are continually trying out new approaches to trick recipients into opening malicious links. The previous solution would entail a lengthy manual process that required MAG to contact other internal technical teams to undertake these tasks every time a phishing attempt was reported. The new SOC will automatically spot a phishing attempt, check that nobody in the organisation has clicked the links, and remove the phishing attempt from inboxes across the organisation.

The organisation had also been considering a SOC assurance audit from a third party to demonstrate the strength of the new solution, but initial conversations with assurance providers revealed this would be costly and time consuming. Tony's internal conversations with senior stakeholders within MAG have led to the conclusion that the positive impact of the Bridewell solution is so clear that an assurance audit will not be necessary.