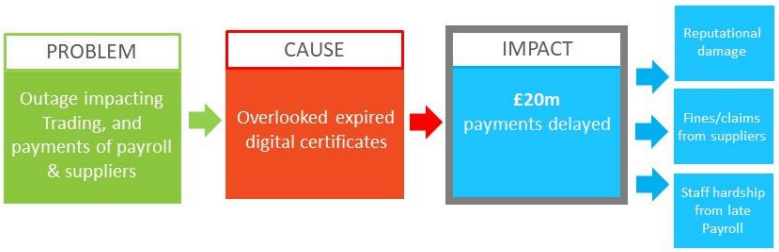
Case study @data*Belt*®

Merchant bank payments and trading processes held up for the sake of an **expired security certificate** – AiM to the rescue!

Situation

A successful London City merchant bank had a significant outage in 2019 which stopped payments of payroll, suppliers and some trading. The impact was £20m of payments held up for a full day together with loss of investments.

Once the IT team had investigated the issue, they found it was down simply to an expired security certificate that had been overlooked. And not only that, but 4 of the key finance and payment systems of the company shared the same certificate. So, when the certificate expired it caused multiple system failures. This caused not only reputation damage, but could have led to fines and claims from creditors, as well as leading to potential hardship of staff if they weren't paid on time.



The company decided to look into an automated tool that would ensure that all certificates were classified and their locations identified – whether structured inside key stores of different platforms or unstructured elsewhere on the network. The company also wanted to ensure that soon to expire certificates were the subject of automated alerts to its service desk system, raising tickets with the relevant system owner to renew the certificate accordingly.

The bank looked at several suppliers in the market that might meet ten required success criteria and approached AiM as a possible candidate for a solution.

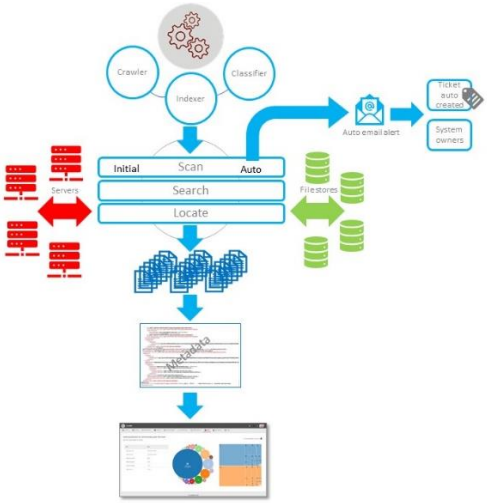
Solution

AiM proposed its AI-powered data governance platform data***Belt***® to deliver its service module ***Certificate Management as a Service*** (CMaaS) solution. AiM delivered a proof of concept project demonstrating on the company's test network how Data***Belt***®'s crawler, indexer and classifier engines scanned, searched and located certificates in all locations, parsed the certificate files and presented the results with all their meta data through a console or report.

t: +44(0) 8448 040 653
e: info@aimltd.uk
w: aimltd.uk

Data***Belt***® was used to schedule auto-scans and to link them to the systems they supported and their owners. AiM also demonstrated how data***Belt***® could integrate with the company's email system to send email alerts, as well as auto-creation of tickets with the relevant system owner for certificate accordingly.

In addition, data***Belt***® was able to undertake an impact assessment to identify operational liabilities where one certificate supported multiple IT systems. This allowed the company to reduce the risk by certificate diversification.



Results

After a successful proof of concept, the company selected AiM to deploy its CMaaS solution. We were informed that data***Belt***® was the only tool considered that more than met each of the success criteria. Other tools in the market failed to meet the functionally rich standards set by data***Belt***® and provide the company with the confidence they needed that the tool could automate the certificate management process.

There have been no certificate failures in the company since implementation 8 months ago, and AiM has extended the governance process to automate the certificate renewal process as well as the company using other services on the platform – cyber security and data protection - to support other governance activities.

t: +44(0) 8448 040 653
e: info@aimltd.uk
w: aimltd.uk