CheckScan+ Aryza Case Study

Aryza is a global provider of case management and process automation software solutions for regulated industries, serving insolvency practitioners, lenders, and regulators.

Aryza's solutions automate a wide range of back and middle office activities including customer data collection, administration, and payment processing. Its scalable technology platform is capable of meeting high volume, high complexity needs and helps customers significantly increase efficiency while ensuring compliance with local legislation.

The breadth and quality of Aryza's software and service proposition is reflected in its strong and long-term customer relationships. Since its foundation in 2002, the business has grown rapidly both organically and through M&A. Today it is the market leader in the UK, Canada, and Ireland with a growing international presence.

THE CHALLENGE

Aryza operates within a highly regulated, and compliance-driven financial services industry. The company also develops applications for their financial services clients so it's of the utmost importance to show rigorous security testing through the SDLC (software development life cycle). They are required to show that they regularly monitor, detect, and resolve IT security issues.

Historically Aryza availed of standalone penetration testing on an ad hoc basis. This method was providing the company with some confidence; however, it wasn't giving them the full picture to their IT security health. When security is approached as an occasional project, scanning tools are often not engaged frequently enough to accurately evaluate potential risks.

Because Aryza develop B-to-B-to-C applications, including debt management and advice solutions, they could be subject to a client audit at short notice. Having access to highly detailed vulnerability reports and illustrating how vulnerabilities were dealt with over time was a real concern. Organisations in highly regulated industries rely on detailed reporting, as well as executive level analysis. Often, scanning tools in the market today make report generation time consuming.

Vulnerability scanning has been relied upon for years to mitigate risks. However, many scanning tools in the marketplace today lack ease of use and protection required for organizations to defend against potential security breaches.

THE SOLUTION

From speaking to the team at CommSec, Aryza's CTO realised they needed a solution that was fully managed, integrated with their infrastructure and gave them a high level of reporting. Gary Walsh remarks," Aryza *required automated security testing that was frequent, fully integrated and gave them in-depth reporting into system vulnerabilities, particularly within their app development environment in the cloud*".

CommSec's solution in this space leverages an internationally recognised web application and infrastructure scanning tool through AppCheck. This technology, combined with manual scan validation formed the basis of our CheckScan+ - Vulnerability Scanning service. The platform is used to conduct host discovery and vulnerability scans on external (internet facing) and internal IP-based systems and networks. CheckScan+ employs a variety of scanning techniques built on a proprietary scanner application to survey the security posture of the target IP-based systems and networks. These scans proactively test for both known and unknown vulnerabilities and the existence of mainstream industry practice security configurations. CommSec assigns each CheckScan+ client a Security Analyst (SA) within the SOC who serves as the client's primary point of contact for more involved technical questions. The SA provides the client clear, consistent security consulting advice on their Managed Vulnerability Scanning program. The consistent quality of this advice is achieved by providing the SA access to a common technology platform kept up to date by dedicated teams of security analysts and vulnerability researchers.

"Aryza have been using the CommSec CheckScan+ managed service since early Q2 2021. Although this is a relatively new component within the Aryza information security landscape, we are already finding the CheckScan+ service to be very beneficial. Working with the CommSec team has been easy, the reporting in-depth and support whenever required is readily available.

The CheckScan+ service provides us additional confidence in a world where the external information security threats to all financial technology companies and customers are increasing all the time."
Paddy Keating, CTO, Aryza

The CTO at Aryza along with their wider team selected CheckScan+, and the team at CommSec, to manage their vulnerability management program. The CommSec vulnerability management team completed a demo scan and followed a risk-based onboarding methodology that allowed Aryza to begin to onboard their chosen critical applications to be entered into a vulnerability management program over the 12 months to come.

BENEFITS OF CHECKSCAN+ TO THE CLIENT:

- Reduction in the likelihood of a cyber-attack, which would have a negative impact on the company's reputation. With CheckScan+, organisations can provide clients security assurance and the peace of mind needed to put their trust in them.
- Reduced Scan Times – CheckScan+ Scanning Engine reduced scan times by almost 80% and in turn offered a much more structured approach to security testing.
- Fewer False Positives – the ability to reconcile and correlate recurring security assessments produces more accurate assessment data and requires less time and fewer resources to validate false positives.
- CommSec's complete management of the scanning process from Schedule, Configure and Manage.
- Quick Deployment – from initial contact, onboarding, to initial scanning all within 6 weeks.
- High-Level Detailed Reporting, Technical Support, and Remediation Advice provided via Security Analysts.
- Testing is more regular, to a larger scope of area giving Supply chain reassurance. This in turn has allowed for Aryza and other corporate clients who deliver services within a supply chain framework to gain peace of mind that not only are their applications constantly assessed but if an external audit were to be requested formal historical reporting can be produced with ease.
- Critical apps are tested once every quarter and reported on every quarter – this allows them to show progression with their IT security health and present a narrative to their clients.
- CheckScan+ Integrates into their app development tools – meaning when using certain Continuous Integration and Continuous Development (CI/CD) tools such as Azure Dev Ops, Jenkins, Team City and GitLab etc they have functionality to run "on demand" vulnerability scans at various stages of the development lifecycle to suit business requirements.
- CheckScan+ reports save a lot of time and effort when it comes to Regulatory Compliance and information needed for international security standards such as ISO 27001 and Cyber Essentials Plus.

Book a Demo Here