KALLES GROUP
IT Professional Services

Uplifting Security using Systematic Code Scanning Processes

Microsoft Corporation

Challenge

The Security team within the Artificial Intelligence and Research (AIR) sector at Microsoft supports research teams as they develop innovative technologies. The team was tasked with empowering research teams to complete their security assessment code scanning seamlessly.

Ideally, running of code scanning tools would become systematic, if not automatic. This would require integration of the coding platform, the build process, and the scanning tools. There is a great deal of variability in all three, so the team would be solving for a large number of use cases and decision-trees between them.

Ultimately, the goal was to keep the company secure by assuring applications are built to Microsoft security standards and industry best practices and taking as little time as possible to do so.

Approach

Kalles Group began the engagement by first defining the business objectives of the project, eliciting all available use cases, and interviewing the hiring manager to incorporate their vision.

Identifying the solution took several weeks as the team worked to obtain the necessary permissions and access, define and understand the tools available, interpret the needs of the business, and reach out to research teams to see what they were doing in practice.

Major challenges included a lack of standardization throughout the organization, a changing vision as they dove deeper into the processes, not understanding all resources available to the team, and looking for patterns while evaluating use cases to assure they could reduce the set of cases to the smallest set possible. Kalles Group was asked to perform scans and communicate with the research teams as they were doing the development work.

Because of the challenges experienced, a large portion of the engagement included helping to define resources, goals, and vision while architecting the solution.

Kalles Group
www.kallesgroup.com

601 Union Street, Suite 4200
Seattle, Washington 98101

solutions@kallesgroup.com
206.652.3378

Solution

VSTS (Visual Studio Team System) was researched and identified as the final solution. Based on this decision, the team designed and architected Securebuild Web App V1, which would easily onboard product teams to VSTS for builds and continuous integration, with the security tools built-in. The Web App would also solve the problem of reactively doing security, and instead make it proactive.

In addition, it would remove the security team from trying to replicate the build and manual scan, and empower product teams to scan quickly and consistently. Various scanning and build tools were used to support the solution such as Release Tracker Tool, Outlook, Skype, Word, Visio, and PowerBI.

Results

While the project required a great deal of flexibility and initiative to obtain the necessary answers and resources, the manual effort of moving security assessments through a queue (assuring that all security tasks are completed and logged in the release tracker tool, scheduling meetings, accessing code and scan output in an established repository) is no longer required. The client can now engage code scanning tools quickly and put the output into the established repository.

Other benefits include:

- The process of running the scans is faster
- The client has far more data now than before
- Scans are being run more consistently
- VSTS is now a known option and teams have been guided on how to use it

Ultimately, there is a much quicker turnaround on security assessments for the organization.

While the project required a great deal of flexibility, the manual effort of moving security assessments through a queue is no longer required.

Kalles Group
www.kallesgroup.com

601 Union Street, Suite 4200
Seattle, Washington 98101

solutions@kallesgroup.com
206.652.3378