Project Overview

The capstone project divided students into two specialized teams: a Cloud Engineering Team and a Cloud Risk Assessment Team. In order to meet the client requirements, students were placed into training programs covering AWS Cloud Foundations, AWS Cloud Security Foundations, and the NIST Risk Management Framework. Both teams received hands-on experience with Prowler, Qualys Total Cloud, and Amazon Web Services. To support progress and maintain engagement, members of both teams were to complete two weekly one-hour remote review sessions that were held via Microsoft Teams, led by members of Georgia State University's Cloud Security and Compliance team.

Team Structure and Roles

The capstone project was organized into two teams: the Cloud Engineering Team and the Cloud Risk Assessment Team, each consisting of five members with one designated as team leader. The team leader was responsible for being the main contact point to the client. Both teams collaborated closely to complete technical training, participate in scheduled meetings, and submit project updates. They shared responsibilities, addressed challenges together, and ensured the successful completion of all project milestones.

Cloud Engineering Contributions

The Cloud Engineering Team developed a three-tier web architecture in AWS based on client requirements (being highly available and scalable). The architecture included a VPC, six subnets across two availability zones, internet and NAT gateways, route tables, and security groups. Amazon RDS was used for database deployment. In addition, the team completed assigned AWS Cloud Foundations and AWS Cloud Security Foundations training, which prepared them to design and deploy the three-tier architecture.

Cloud Risk Assessment Contributions

As a member of the Cloud Risk Assessment team, we contributed to the development and delivery of an extensive project that assessed cloud security posture using CSPM and CNAPP tools. Our responsibilities included researching and explaining the functions of Cloud Security Posture Management (CSPM) and Cloud Native Application Protection Platform (CNAPP) tools and creating a comparison chart that is side-by-side, highlighting the use cases and main features. We helped define major cybersecurity concepts like compliance frameworks, risk, risk mitigation strategies, and CIS Amazon Web Services Framework Benchmark and NIST 800-171 framework-- going into more depth on the control families and associated security requirements. In addition, our team created two matrices, a 3x3 and 4x4 risk matrix that aligned with Qualys TotalCloud and Prowler severity levels, analyzed by the 4 findings from each tool. Finally, the team assisted with the development of a mitigation plan and schedule for all failed findings and matched them with appropriate risk mitigation strategies based on impact and likelihood.

Challenges and Solutions

Cloud Engineering Team: Throughout the project, there were several difficulties, including incorrect target group registrations, misconfigured security groups, and connection problems. System testing was also delayed by misalignment between the database, application, and web tiers. Students also had trouble with the load of the training materials, and they occasionally had problems using the AWS lab environments. The team overcame these challenges and successfully finished the project by working together, troubleshooting, and stepping up participation.

Cloud Risk Assessment Team: Throughout the project, several major challenges affected the overall execution and outcomes. The compliance mapping and tool integration showed difficulties, as Prowler provided us with exact compliance mappings within its reporting; Qualys TotalCloud required us to research manually to verify each control family and mapping. This increased the time and complexity to complete each task. Additionally, Prowler's setup was a demanding operation; it required us to install Prowler in AWS Cloudshell each session. Another challenge faced was inconsistent team participation during the scheduled meetings, resulting in ineffective collaboration, delayed progress, and ultimately causing stricter grading and evaluations upon project completion. As this was the first semester, the GSU Cloud Security and Compliance team introduced Qualys TotalCloud.

Conclusion

Both the Cloud Engineering and Cloud Risk Assessment teams successfully met all client requirements and delivered the final project deliverables. We concluded our project with a formal presentation to the Professor and Georgia State University's Cloud Security and Compliance team. To close it off, we sought evaluations from the Client after the final presentation to gauge our final grade.

Furthermore, the Cloud Engineering Team suggests a more hands-on system for all team members. Future Cloud Risk Assessment team would benefit from improved documentation and further knowledge of the CSPM and CNAPP tools as they are great to use, clearer team expectations, and greater engagement to support a very efficient and effective project delivery.