Lab Summary

To recap what we have learned:

- **Lab 1 - Security exercises**: Grant and restrict permissions to your S3 buckets with S3 bucket policies. Use AWS Config and Access Analyzer to detect buckets within your account and organization that have public access, and remediate public access where unintended.
- **Lab 2 - S3 Access Grants**: S3 Access Grants complement the existing S3 security management tools to manage permissions for IAM roles/users, AWS services, as well as corporate identities. We encourage exploring S3 Access Grants where you want to scale your fine-grained access control with a simplified model for defining access permissions.
- **Lab 3 - Enabling Malware Protection for S3 by using GuardDuty**: Automatically scan for the potential presence of malware within your S3 buckets to protect your users and applications.
- **Lab 4 - S3 Access Control Lists**: To align with S3's best practices for managing security permissions, we encourage all customers to consider disabling ACLs within their environments. This lab demonstrates how to manage your S3 ACL permissions, detect where they may still be present in your AWS accounts, and disable ACLs on your buckets.

Workshop complete
Congratulations you have completed the the Amazon S3 security workshop.

Previous