SANS

QUICK WINS IN CLOUD SECURITY

SOME QUICKER THAN OTHERS

Written by Serge Borso

ENFORCE 2 FA

If you must have user accounts, enforce Two-Factor Authentication (2 FA) – and make sure your default password policy enforces at least 15 characters.

ENCRYPT

Encrypt everything you have the ability to encrypt: Traffic, Disks, Storage, Containers, Keys, Data... Everything!

DISABLE ACCESS

Disable all public read access on S3 buckets and storage containers of any kind; and if you already did this, go back and double check.

BACKUP

Get Serious about backups; if it's mission critical, it should be backed-up per corporate policy. Did you know: If an adversary has sufficient privilege, a ransomware attack can render your backups unusable?

ENABLE TOOLS

Enable AWS Security Hub or Microsoft Defender for Cloud, and learn how to use these tools to identify weak spots in your implementation.

sans.org/cloud-security
sans.org/sec388
#SANSCloudAce