CYBERNEST HUB · FREE RESOURCE

The 10-Point AWS Security Baseline Checklist

The exact checklist we run on every AWS Startup Security Baseline sprint before we touch anything else. Five categories, ten checks, about twenty minutes. Check each box as you confirm it.

---

1. Root Account & MFA

- [ ] MFA is enforced on the root account, not just recommended.
- [ ] Root has not been used for day-to-day work in the last 90 days.

2. IAM Users & Roles

- [ ] No active credentials belong to former contractors or employees.
- [ ] No policy uses a wildcard (*) action or resource without a documented reason.
- [ ] Every access key in use is less than 90 days old, or has a documented rotation plan.

3. CloudTrail & Logging

- [ ] CloudTrail is enabled account-wide, in every region, not just the primary one.
- [ ] Every AWS account you operate (not just the main one) has logging enabled.

4. S3 & Data Protection

- [ ] S3 Block Public Access is enabled at the account level.
- [ ] Every bucket has encryption enabled at rest.

5. Backup & Recovery

- [ ] Automated backups are running for every production database and critical data store.
- [ ] At least one restore has been tested in the last 90 days, not just configured and assumed to work.

Found more than a couple of unchecked boxes? That's normal, not alarming. The AWS Startup Security Baseline sprint closes these gaps in a fixed 7 to 14 day engagement, with two live working sessions where fixes happen together instead of just getting written down for later.

cybernesthub.com/aws-startup-security-baseline · deandre.wilson@cybernesthub.com · CyberNest Hub, a DBA of D.E. Wilson LLC