THE PROJECT · STEP-BY-STEP BUILD GUIDE

SOC 2-READY AWS CLOUD

One project for your cybersecurity resume. You build a small AWS environment as code, scan it against SOC 2 controls, fix what fails, and put the proof on GitHub.

1	2	3	4
AWS	TERRAFORM	SCAN	GITHUB

WHAT YOU NEED · ALL FREE TO START

AWS account new accounts get credits
aws.amazon.com/free

Terraform infrastructure as code
developer.hashicorp.com/terraform/install

Prowler open-source compliance scanner
github.com/prowler-cloud/prowler

GitHub where the project lives
github.com

AWS credits: $100 at sign-up and up to $100 more, up to $200 in total, on a free plan that lasts 6 months. Source: aws.amazon.com/free

ABOUT VANTA

In the video I name Vanta. That is what companies pay for, and it has no free plan. Prowler is the free tool that runs a SOC 2 check on your own account, so this guide uses Prowler.

START TODAY · 5 MINUTES

Open the AWS link above, create your account on the free plan, and switch on MFA for the root user. That is your first control passed.

1 Create the AWS account

FREE PLAN · NO CHARGE UNLESS YOU UPGRADE

- Sign up at aws.amazon.com/free and pick the free plan. You are not charged unless you upgrade.
- Turn on MFA for the root user, then stop using root.
- Create an IAM user for daily work and give it MFA too.
- Install the AWS CLI and connect it to that user:

```
aws configure
aws sts get-caller-identity   # shows who you are
```

2 Build it as code with Terraform

IaC · REPO: aws-soc2-terraform

Make a folder called aws-soc2-terraform. In main.tf, write these yourself, one at a time:

- A VPC with one private subnet (aws_vpc, aws_subnet)
- An S3 bucket with encryption, versioning and public access blocked (aws_s3_bucket_server_side_encryption_configuration, aws_s3_bucket_versioning, aws_s3_bucket_public_access_block)
- CloudTrail writing audit logs to that bucket (aws_cloudtrail)
- A strong IAM password policy (aws_iam_account_password_policy)
- Encrypted disks by default (aws_ebs_encryption_by_default)

Then deploy it:

```
terraform init
terraform plan      # read what it will build
terraform apply
```

WHY THIS MATTERS

Anyone can click around the console. A Terraform repo shows you can build the same secure setup again, the same way, every time. That is the skill.

3 Run the SOC 2 compliance scan

GRC · PROWLER, OPEN SOURCE

- Install Prowler and scan your account against its SOC 2 framework:

```
pip install prowler
prowler aws --compliance soc2_aws
```

- Open the report it saves in the output folder. Save a copy. This is your BEFORE.
- Pick the failed checks. Fix each one in main.tf, not in the console.
- Run terraform apply, then scan again. Save that report. This is your AFTER.

The four checks from the video, and what passes them:

Encryption at rest	S3 and EBS encryption
MFA on root account	Step 1
Audit logging on	CloudTrail
No public buckets	public access block

MAKE IT AUTOMATED

Scan after every change you apply. To go further, add a GitHub Actions workflow that checks your Terraform on every push. Checkov is a free scanner for that.

SAY IT RIGHT

Write SOC 2-aligned, not SOC 2 compliant. SOC 2 is an audit report a CPA firm issues to a company. Your project proves you can build and check the controls behind it.

4 Push it to GitHub, put it on your resume

PACKAGE · PUSH · RESUME

- Add a .gitignore first. Never push state files or keys:

```
.terraform/
*.tfstate
*.tfstate.backup
*.tfvars
```

- Write a README: what you built, a simple diagram, the BEFORE and AFTER scan, and what you fixed.
- Push it:

```
git init
git add .
git commit -m "soc2 baseline"
git branch -M main
git remote add origin <your repo URL>
git push -u origin main
```

- When you are done, run terraform destroy so your credits last.

YOUR RESUME LINE

Built AWS infrastructure as code with Terraform (VPC, S3, IAM, CloudTrail) and automated SOC 2-aligned compliance scanning with Prowler. Fixed [your number] failed controls.
github.com/you/aws-soc2-terraform

5 Pair it with the cert

CERT + PROJECT BEATS CERT ONLY

The project is the proof. Security+ is the cert I name in the video. Put the two together. Check where you stand before you pay for anything:

Try 15 Security+ questions free, no sign-up

`getuprep.com/comptia/sy0-801`

Built this? Tell me which step you got stuck on. @getuacademy