Apiko

WEB & MOBILE SOFTWARE DEVELOPMENT COMPANY

INFRASTRUCTURE CHECKLIST

If you are looking for **DevOps services, security infrastructure audit** or **setup**
LET'S GET IN TOUCH

[Talk to a DevOps Engineer]

01 ARCHITECTURE

Apiko

- [ ] 01 Do you follow infrastructure as a code approach (Terraform, CloudFormation, etc)?

- [ ] 02 Do you have infrastructure documentation? Is it up-to-date with your current infrastructure state?

- [ ] 03 Is your infrastructure placed in a private network?

- [ ] 04 Is your infrastructure self-recovery (instances in multiple availability zones)?

- [ ] 05 Do you know all third-party services your application is integrated with?

- [ ] 06 Is there any part of the application that may be a single point of failure?

02 CODE

- [ ] 01 Do you have unit/integrations/e2e/performance tests?

- [ ] 02 Do you have CI/CD pipelines for automated testing and deployment?

- [ ] 03 Do you have configured linter for your application code?

- [ ] 04 Are you running linter/prettier checks for your code before commit changes/merge changes?

- [ ] 05 Are you testing your code using static code analysis tools?

- [ ] 06 Are you using maintained and secure versions of packages in your application?

- [ ] 07 Are you using only industrial standards in cryptography (not your own)?

03 MONITORING

Apiko

- 01 Do you have a website monitoring service set up (Freshping, Pingdom, Downtime Monkey, etc)?

- 02 Do you have CloudWatch / New Relic or other monitoring tools for your infrastructure set up?

- 03 Is APM (Application Performance Monitoring) configured for all services?

- 04 Are application logs available for viewing and retaining?

- 05 Does the application have distributed tracing?

- 06 Are all third-party services monitored?

04 ALERTING

- 01 Are infrastructure budget alerts configured?

- 02 Are anomaly alerts configured?

- 03 Are error alerts configured?

- 04 Do you have responsible people for reacting to alerts?

05 SECURITY

01   Does the AWS root user have Two-Factor authentication enabled?

02   Do all team members have Two-Factor authentication enabled on their accounts?

03   Are you using automated security analysis tools?

04   Is your database not accessible from the public network?

05   Are you using secure storage for secrets and credentials (CI/CD secrets, Keybase, etc)?

06   Does your Dockerfile have no security issues (if it is present)?

07   Are the website SSL certificates updating automatically or is there a notification about certificates update?

08   If you are using cloud computing instances: do the operating systems have the latest security patches installed?

09   Do you know team members who have access to your infrastructure and what permissions they have?

10   Do you follow the least privilege principle for user accounts?

06 BEST PRACTICES

01   If you are using Terraform: are you storing terraform.tfstate file separately from your Git repository?

02   If you are using Docker: are you running an application under a non-privileged user?

03   If you are using Docker: does your Dockerfile follow best practices?

ABOUT APIKO

Apiko is a software development company that enters markets with digital businesses, using a solid process and clever strategies. We merge imagination and technology to help brands grow in the age of constant change and transformation.

SOCIAL LINKS

in Linkedin 🐦 Twitter f Facebook
▶ Youtube Ⓒ Clutch

CONTACTS

Harju maakond, Tallinn,
Haabersti linnaosa, Paevalille tn 6-7, 13517

contact@apiko.com
apiko.com

Apiko