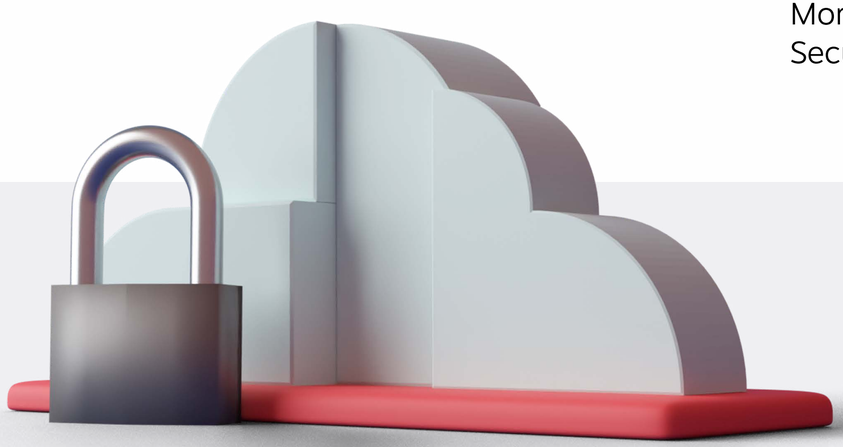
REBURA

A Tenth Revolution Group Company

WILL DEVOPS PROTECT YOU FROM YOUR NEXT DATA BREACH?

DevOps cultures are quickly proliferating within technology organisations, with this new tools are being introduced into technology organisations that help speed up deployments, increase observability and improve the overall quality of infrastructure and product design.

With the introduction of CI/CD pipelines and a DevOps culture, DevOps teams are able to introduce new security tools that can improve the security posture in an organisation, tools that may ultimately protect you from your next data breach.



USING CI/CD PIPELINES TO PROTECT WHAT GETS PUSHED TO PRODUCTION

AWS tools such as AWS CodeBuild give DevOps engineers the platform to introduce new security automation tools into the pipeline with minimal overhead. As development teams push code to production faster and as product complexity increases so does the security risk inherent in products. Simple changes to the way CI/CD pipelines are configured can reduce the overall risk, resulting in a better security posture.

A good first step to increase security is to include developer security tools into the CI/CD pipeline. There are a number of excellent developer security tools on the AWS marketplace for organisations to choose from, with varying levels of functionality. A basic feature that most tools (including open source tools) include is dependency scanning. Dependency scanning prevents third party dependencies with vulnerabilities being shipped to production as part of the product code base. By scanning dependencies, vulnerable dependencies can be picked up automatically and code pushes with vulnerable dependencies prevented.

More details on the tools available through AWS Marketplace can be found **here** - navigating to ‘Application Security’. As part of improving your security posture as an organization in cloud it is worth looking at these tools.

aws PARTNER Advanced Tier Services

- Immersion Day
- Solution Provider
- Migration Services Competency
- Well-Architected Partner Program
- Cloud Operations Services Competency
- Digital Workplace Services Competency
- AWS Marketplace Skilled Consulting Partner
- AWS Microsoft Workloads Services Competency

USING CLOUD SECURITY POSTURE MANAGEMENT TOOLS

With application security increased, DevOps engineers should look to Cloud security products (**www.aws.amazon.com/marketplace/solutions/security** - navigate to 'Cloud Security' to look at products that look at Cloud Security.) These tools look at a number of configurations across a cloud environment and can report back to customers (sometimes in real time) when security issues are present within the operational environment. The scanning of these environments can take place before and after deployments (in some cases) as part off the product deployment - to look at the security posture changes between product deployments - an invaluable tool in evaluating the security posture of your cloud environment.

Whilst the tools mentioned are not an exhaustive list of tooling to look at introducing as part of a DevOps culture they are a good place to start in introducing tooling to improve an organisation's security posture.

WHY DEVOPS?

Whilst security tooling implemented as part of a CI/CD pipeline alongside cloud security posture management tools does not protect your organisation from every threat - by adopting a DevOps culture within your organisation the threat footprint can be reduced with comparatively low effort, without the need for additional resourcing.