How to keep your startup's cloud secure

(when your security team is just you)

Ryder Damen, Developer Advocate, Indeni Cloudrail
Conf42 - DevSecOps, December 5, 2021

cloudrail

You can’t.

But we’ll do our best.

Overview

What We’re Going To Talk About

- About Me
- Who This Is For
- “DevOps” Engineering
- Your Startup’s Security Landscape
- Application Security
- Infrastructure Security
- Other Security
- Best Practices
- Conclusion

About Me

Ryder Damen

- Developer Advocate at Indeni Cloudrail
- DevOps Engineer
- Web Developer
- Biomedical Engineering Background

Who this is for

- Me, when I was first getting into the field
- DevOps Engineer
- Not from a security background
- At a scaling startup
- Growth mindset

“DevOps”

“DevOps”

A list of things I’ve been asked to do as a DevOps Engineer

- Create cloud resources
- Write infrastructure as code
- Respond to incidents
- Provision new services
- Manage SOC2 certifications
- Organize penetration tests
- Run penetration tests
- Open a data centre
- Assemble servers
- Provision new accounts for employees
- Run background checks for new employees
- Create an employee annual security test course
- Manage GSuite / Google Workspace
- Migrate all cloud services to AWS
- Migrate all cloud services to GCP
- Migrate things off Azure
- Reduce the cost of cloud billing
- Negotiate with vendors for contracts
- Monitor application vulnerabilities
- Monitor infrastructure vulnerabilities
- Deal with DNS
- Install Kubernetes bare-metal
- Try to run spark on Kubernetes in its infancy
- Manage engineers
- Write for the company blog
- Help people reset their passwords
- Help people understand their computers
- Contribute to the code base
- Design graphics
- Fix application vulnerabilities
- Fix infrastructure vulnerabilities
- Fix low level vulnerabilities
- Containerize, then un-containerize services
- Negotiate product discounts
- Talk to customers
- Product manage
- Project manage
- UX design
- Catch an uber with a company server in the trunk
- Connect a fibre optic trunk line in the basement of a building
- Reset the breakers after the machine learning engineers blew the power by all training at the same time

It’s a lot.

You might not be from a security background - I’m not.

Security Landscape At Your Startup

Application / Infrastructure / Other

Application Security

Application Security

- Anything involving the application
  - Secure Code; OWASP Top Ten
  - Application Composition
  - Penetration testing

Application Security Tools

Application Security

- Implement the tools into your pipeline
  - Don’t fail the pipeline just yet
  - Set a deadline, then fail the pipeline
- Set aside time, and create an adhoc team
  - Triage the issues
  - Double the estimation

Infrastructure Security

Infrastructure Security

- Are you in a public cloud?
- Cloud Security Posture Management (CSPM) tools
- Implement Infrastructure as code & configuration management
- Infrastructure vulnerability scanning tools
- Consider initial implementation
  - How much work will this take for you to manage? Is it worth the investment of your time?

Cloud Security Posture Management Tools

Infrastructure-as-Code Security Tools

“Other” Security

“Other” Security

Anything not application or infrastructure

- What is your device management policy?
  - Are devices running an endpoint monitoring service?
- SOC2 related guidelines
- Use a SOC2 management tool

SOC Security Tools

Recommended Practices

Things you can do to make your life easier

- Bring infrastructure down to its most simple version
- Use managed services wherever possible
  - AWS ECS Fargate, instead of AWS ECS EC2
- Use Infrastructure as code
- Recruit other members of your team for feedback
- “Shift left”

In Conclusion

Keeping your startup's cloud secure by your lonesome

- Simplify everything
- Use managed services
- Use infrastructure as code
- Implement application security tools in your deployment pipeline
- Implement infrastructure security tools in your deployment pipeline
- Involve as many others in the security process as possible
- Continuously demonstrate that more people in this role is valuable

“The real DevOps was the friends we made along the way”

Ryder Damen, Developer Advocate, Indeni Cloudrail
Conf42 - DevSecOps, December 5, 2021
ryder.d@indeni.com
twitter.com/ryderlikestacos
linkedin.com/in/ryderdamen