

Contents

| | |
|---|----------|
| 1. Introduction | 1 |
| Why This Book? | 1 |
| Scope Of The Book | 1 |
| The Audience | 2 |
| How Can I Contribute? | 2 |
| 2. Cloud Native Security Foundations | 3 |
| Identity | 3 |
| Authentication | 4 |
| Authorization | 4 |
| Good Practices | 5 |
| Attack Vectors | 5 |
| 3. Containers | 6 |
| Basics | 6 |
| Container Images | 6 |
| Building Container Images Securely | 6 |
| Distributing Container Images Securely | 6 |
| Using A Container Registry | 6 |
| Continuous Delivery | 6 |
| Image Signing | 6 |
| TUF and Notary | 6 |
| Tooling | 6 |
| Good Practices | 6 |
| Attack Vectors | 6 |
| 4. Container Orchestrators | 7 |
| Basics | 7 |
| Kubernetes | 7 |
| ECS | 7 |
| Nomad | 7 |
| Good Practices | 7 |
| Attack Vectors | 7 |
| 5. Policies | 8 |
| Basics | 8 |
| Open Policy Agent (OPA) | 8 |
| Networking | 8 |

CONTENTS

| | |
|---|-----------|
| Workflow | 8 |
| Good Practices | 8 |
| Attack Vectors | 8 |
| 6. Sensitive Data | 9 |
| Basics | 9 |
| AWS | 9 |
| Kubernetes | 9 |
| ECS | 9 |
| Good Practices | 9 |
| Attack Vectors | 9 |
| 7. Service Mesh Security | 10 |
| Basics | 10 |
| Envoy-based systems | 10 |
| Istio | 10 |
| AWS App Mesh | 10 |
| Linkerd | 10 |
| Service Mesh Interface | 10 |
| Good Practices | 10 |
| Attack Vectors | 10 |
| 8. Container Penetration Testing | 11 |