
Table of Contents

Preface.....	vii
1. Introduction to DevSecOps.....	1
Before DevOps: The Software Development Life Cycle	3
What Is DevSecOps?	6
Introducing Automatoonz	7
Cloud Infrastructure: Secure by Default	8
Move Fast, Secure Fast: The Importance of Automation	9
DevSecOps Culture	10
Summary	11
2. Setting Up Your Environment.....	13
What You'll Need	13
Installing and Verifying Your Setup	14
Installing the AWS CLI	14
Installing the Docker Engine	15
Checking Your Python Version	15
Installing Git	16
Installing Kubernetes	16
Creating Your First Bare-Bones Pipeline	17
Summary	18
3. Securing Your Infrastructure.....	21
What Makes Infrastructure Secure?	21
Hands Off! Preventing Unwanted Access with IAM Permissions	22
Detecting Misconfigurations	23
Identifying a Standard	23
Threat Modeling	24

Security Controls	24
Better Than a Cure: Implementing Preventive Controls	26
Implementation	28
Summary	33
4. Logging and Monitoring.....	35
What Are Logging and Monitoring—and Why Do They Matter?	35
Attack Styles	36
Advanced Persistent Threat Attacks	37
Ransomware Strains	38
Passive and Active Attacks	38
Log Types	40
Log Storage	41
Detecting Anomalies	44
Remediation with AWS Config	48
Correlating User Activity with CloudTrail	51
Network Monitoring with an Amazon VPC	53
Summary	55
5. Controlling Access Through Automation.....	57
The Principle of Least Privilege	58
Fine-Tuning Access Controls	60
Use a Tagging System	60
Clarify Team Responsibilities	61
Prevent and Detect	62
The IAM Pipeline	63
Summary	66
6. Fault Injection Test.....	67
Distributed Systems	67
Adaptive Security Controls	68
The True Cost of Downtime	69
Methods for Minimizing Downtime	69
Chaos Engineering	70
Basic Principles	71
Advanced Principles	74
Chaos Engineering in AWS Environments	76
Chaos Engineering at Automatoonz	78
AWS Fault Injection Simulator Experiment Examples	78
Kubernetes Pod Stress Testing	79
Throttling EC2 API Calls	80
Stress Testing the CPU on an EC2 Instance	81

Terminating an EC2 Instance	82
Removing Ingress and Egress Rules from a Security Group	83
Detaching an EBS Volume from an EC2 Instance	84
Summary	85
7. People and Processes.....	87
People: Team Structures and Roles	87
Security Engineers	88
Developers	88
Compliance Team	89
Product Manager	90
Team Structure	90
Processes: Practices and Communication	92
Communicate to the Right People, Consistently	92
Make Product Owners Accountable for Their Security Findings	93
Build Threat Modeling into Your Processes	93
Build Roadmaps to Reach Your DevSecOps Goals	95
What Next?	95
Summary	96
Index.....	99