

DevOps Tools and Cloud Connection

1	Problem Space	3
1.1	Why, how and what DevSecOps?	3
1.1.1	Goals and Activities of DevOps	3
1.1.2	Threats and Activities of Security.....	3
1.1.3	Speed vs Security	3
1.1.4	Mobile Considerations	3
2	Solution Space.....	3
2.1	Making a Plan.....	3
2.2	Going Cloud.....	3
2.2.1	Riding SaaS for Security.....	3
2.2.2	Cloud Models	3
2.3	Tool Objectives and Integration Points.....	3
2.4	Planning Phase	3
2.4.1	Threat Modeling.....	3
2.4.1.1	IriusRisk	3
2.4.2	Communication and Issue Tracking	3
2.4.2.1	Confluence	3
2.4.2.2	Jira	3
2.5	Building Phase	3
2.5.1	Protecting Code Repositories.....	3
2.5.1.1	Signing Commits.....	3
2.5.1.2	Protecting Branches	3
2.5.1.3	Backups	3
2.5.2	Writing Custom Security Tests	3
2.5.2.1	Gauntlt	3
2.5.2.2	Live Static Application Security Testing	3
2.5.2.3	SonarQube	3
2.5.2.4	Checkmarx.....	3
2.6	Reviewing and Testing Phase	3
2.6.1	Software Composition Analysis.....	3
2.6.1.1	Veracode	3
2.6.1.2	Black Duck	3
2.6.1.3	Mend.....	3
2.6.2	Application Security Testing.....	3

2.6.2.1	Mobile Security Framework.....	3
2.6.2.2	ImmuniWeb	3
2.6.2.3	CodifiedSecurity	3
2.6.2.4	Container Scanning	3
2.6.2.5	Trivy.....	3
2.7	Deployment Phase	4
2.7.1	Infrastructure as Code Security.....	4
2.7.1.1	Snyk	4
2.7.2	Chaos Engineering.....	4
2.7.2.1	Chaos Monkey.....	4
2.7.2.2	ChaoSlingr	4
2.7.3	Cloud Security	4
2.7.3.1	Evident.IO.....	4
2.8	Observation Phase	4
2.8.1	Security Monitoring	4
2.8.1.1	Alert Logic	4
2.8.1.2	Halo	4
2.8.1.3	Tripwire	4
2.8.2	Runtime application self-protection	4
2.8.2.1	Fortify	4
2.8.2.2	Imperva	4
2.8.2.3	Dynatrace	4
3	Loopback and Conclusion	4