Thematic synthesis of DevSecOps definitions from WL

Category	Themes (14)	Codes (49)	Study quotes the definition mentioning the code	Count	Subtotals
Organization, People, & Culture	Expansion to DevOps	expansion to DevOps	S1_IEEE_01, 08, S1_SC_02, 04, 21	5	7
		extension to DevOps	S1_SC_01, 02	2	
	Dev, Sec & Ops	development, operations and security teams	S1_IEEE_01, 05, 08, 12, S1_SC_02, 04, 10, 21, S1_ACM_68	9	11
		developers and operators by involving security experts	S1_SC_02	1	
		dev/sec/ops	S1_IEEE_26	1	
	Culture	culture	S1_ACM_45	1	4
		cultural approach	S1_IEEE_26	1	
		cultural shifts	S1_ACM_50	1	
		shift the mindset	S1_IEEE_10	1	
	Collaboration	collaboration/collaborate	S1_IEEE_01, 08, 12, 26, S1_SC_02 (2 times), 04, 10, 21, S1_ACM_45, 68	11	11
	Breaking silos of security	breaking silos of security	S1_IEEE_08, 24, 26	3	4
		break down the barrier	S1_IEEE_22	1	
	Sharing knowledge	sharing that knowledge	S1_IEEE_08	1	3
		giving that knowledge to the different teams	S1_IEEE_ 24, 26	2	
Process Capabilities	Integration of security into DevOps	incorporating security practices in the DevOps processes	S1_IEEE_01, 08, S1_SC_21	3	22
		incorporation of security practices in a DevOps environment	S1_SC_10, 11	2	
		integrate security controls and processes into DevOps	S1_SC_02, 04	2	
		integration of security practices into DevOps	S1_SC_03, S1_ACM_53	2	
		IT processes with security approach	S1_ACM_04, S1_IEEE_21	2	
		integration of security with development and operation	S1_SC_09	1	
		integrating security principles	S1_IEEE_12	1	
		integration of security processes and practices	S1_IEEE_10	1	
		introduction of more security-oriented processes	S1_SC_22	1	
		integrates continuous security into the original DevOps process	S1_IEEE_03	1	
		inclusion of security into DevOps	S1_SC_01	1	
		including security mechanisms into all phases DevOps workflow	S1_SC_01	1	
		injection of security principles and controls into the DevOps	S1_ACM_50	1	
		including modern security practices that can be	S1_SC_02	1	

		incorporated in the fast and agile world of DevOps			
		integrating secure development best practices and methodologies into development and deployment processes	S1_IEEE_44	1	
		integrating the software development and operation processes considering security and compliance requirements	S1_SC_11	1	
	Agile	agile	S1_SC_02, S1_ACM_45, S1_IEEE_03	3	4
		smart and lightweight approach	S1_SC_31	1	
	Security is the main concern throughout the SDLC	security is the main emphasis	S1_SC_14	1	7
		security is given high priority throughout the SDLC	S1_ACM_07	1	
		a key concern throughout all phases of the development lifecycle and even post deployment	S1_SC_31	1	
		security practices are implemented at each stage of the cycle	S1_ACM_07	1	
		security is implemented at the right level and at right time	S1_IEEE_24	3	
	Shifting security to the start	puts security at the forefront of requirements	S1_IEEE_24	1	2
		shifting security to the early stages	S1_IEEE_06	1	
	Time reduction & Efficiency improvement	time reduction	S1_ACM_04, S1_IEEE_21	2	4
		increase deployment rates	S1_IEEE_22	1	
		increase the rate of testing feedback	S1_IEEE_22	1	
	Security assurance	maintaining a secure operational atmosphere	S1_IEEE_22	1	4
		safeguard application from any potential threats	S1_SC_01	1	
		identifying security vulnerabilities	S1_SC_31	1	
		responsible for application security	S1_IEEE_05	1	
Technology	Reliance on operational tools	reliance on operational tools	S1_ACM_45	1	1
Business	Quality	without lost quality	S1_ACM_04, S1_IEEE_21	2	3
		quality affirmation	S1_SC_14	1	
	Authors of common definitions	Mohan & Othmane	S1_IEEE_01, 08, 26, S1_SC_02, 04, 09, 10, 11, 21, 22, S1_ACM_45, 68	12	25
		Rahman & Williams	S1_IEEE_08, 12, 44, S1_SC_22	4	
		Myrbakken & Colomo-Palacios	S1_SC_02, 03, S1_IEEE_10, S1_ACM_53	4	
		Carter	S1_IEEE_24, 26	2	
		Carturan & Goya	S1_ACM_04, S1_IEEE_21	2	
		Mohan, Othmane, & Kres	S1_SC_11	1	

Thematic synthesis of DevSecOps definitions from GL

Category	Themes (20)	Codes (35)	Study quotes the definition mentioning the code	Count	Subtotals
Organization, People, & Culture	Culture	culture	S1_GL_10, 13, 26	3	4
		cultural shift	S1_GL_11	1	
	Philosophy	philosophy	S1_GL_02, 19 (2 times), 26	4	4
	Extension of the DevOps	extension of the DevOps	S1_GL_33	1	1
	Combination of DevOps and SecOps	combination of DevOps and SecOps	S1_GL_13	1	1
	Dev, Sec & Ops	development, operations, and security	S1_GL_15, 19, 27	3	3
	Collaboration	collaboration	S1_GL_26	1	2
		team work	S1_GL_02	1	
	Communication	communication	S1_GL_19	1	1
	Shared responsibility	shared responsibility	S1_GL_10, 33	2	6
		everyone's responsibility	S1_GL_10	1	
		security is a part of everyone's job	S1_GL_12	1	
		make everyone accountable for security	S1_GL_27	1	
		at the top of every developer's mind	S1_GL_12	1	
Process Capabilities	Integration of security into DevOps	integrating security methods into a DevOps process	S1_GL_02	1	6
		integrating security practices within the DevOps process	S1_GL_26	1	
		integration of security practices into a DevOps	S1_GL_10	1	
		adding security components to each step of the DevOps	S1_GL_23	1	
		bake security into the rapid-release cycles	S1_GL_11	1	
		integrating security into a continuous integration, continuous delivery, and continuous deployment pipeline	S1_GL_16	1	
	Agile	agile	S1_GL_05	1	1
	Emphasis on security	emphasizes the importance of sound information security practices	S1_GL_01	1	1
	Shifting security to the start	security from the start	S1_GL_04, 15	2	6
		from the beginning	S1_GL_33	1	
		integrate security objectives as early as possible	S1_GL_10	1	
		avoids any risk of security being an afterthought	S1_GL_01	1	
		placing security practices early during the SDLC	S1_GL_05	1	
	Adoption of security through the entire SDLC	adoption of security through the entire SDLC	S1_GL_19	1	1

	Built-in security	built-in security	S1_GL_04	1	1
	Scalability	scalability	S1_GL_19	1	1
	Shorten the SDLC	shorten the SDLC	S1_GL_23	1	1
Technology	Tooling	tooling	S1_GL_10	1	1
	Security-as-Code	security as code	S1_GL_26	1	1
	Automation	automation/automating	S1_GL_04, 19	2	2
Business	High software quality	high software quality	S1_GL_23	1	1

Thematic synthesis of DevSecOps challenges from WL

Category	Themes (36)	Codes (74)	Study mentions the code	Count	Subtotals
Organization, People, & Culture	Resistance to change	resistance to change in the organization's culture and people mindset	S1_SC_02	1	4
		developer resistance to integrate security protocol	S1_IEEE_08, S1_ACM_05	2	
		developers lose autonomy	S1_IEEE_06	1	
	Challenges of collaboration, communication & coordination	teams working in isolation	S1_SC_02	1	12
		no communication, collaboration and sharing	S1_SC_02	1	
		synchronization and transparency issues	S1_SC_02	1	
		teams working towards conflicting objectives	S1_SC_08	1	
		insufficient monitoring of collaboration	S1_ACM_01	1	
		challenge of unrestricted collaboration	S1_IEEE_08, S1_ACM_05	2	
		coordination of security team and DevOps team	S1_IEEE_08, S1_ACM_05	2	
		un-trusted inputs causing isolation	S1_IEEE_08, S1_ACM_05	2	
		conflict between security and development	S1_IEEE_06	1	
	Challenges in decision level	lack of clarity and transparency in strategy	S1_SC_02	1	2
		lack of commitment of leadership and senior management for DevSecOps adoption	S1_SC_02	1	
	Lacking confidence	low or no confidence in DevSecOps	S1_SC_02	1	2
		lack of trust and skepticism	S1_SC_02	1	
	Neglecting security	management does not prioritize security	S1_IEEE_06	1	2
		security is often not a business priority	S1_SC_49	1	
	Lack of security awareness and responsibility	lack of understanding and awareness of DevSecOps	S1_SC_02	1	5
		improving security awareness	S1_IEEE_06	1	
		nobody is responsible for security	S1_IEEE_06	1	
		security in the team and to the left	S1_IEEE_06	1	
		security push-pull	S1_IEEE_06	1	
	Lack of security knowledge and skills, need for training	lacking security education	S1_IEEE_06	1	4
		lacking knowledge and training	S1_IEEE_06	1	
		lack of skills	S1_SC_02	1	
		lack of knowledge	S1_IEEE_08,	1	
	Boundary between specialist & generalist	the boundary between a specialist and generalist	S1_IEEE_06	1	1
	Insufficient level of governance on DevSecOps adoption	insufficient level of governance on DevSecOps adoption	S1_SC_08	1	1
Process Capabilitie	Neglecting change control in security	neglecting change control in security	S1_IEEE_08	1	1
	Lacking security standards	need for new standards for security prevention,	S1_SC_02	1	2

		detection and response			
		lack of secure coding standards	S1_IEEE_08	1	
	Difficulties in integrating security into DevOps without losing speed	difficulties in integrating security practices into a fast moving DevOps pipeline without slowing down the process	S1_SC_08	1	1
	Difficulties in transforming to DevSecOps without affecting current process	difficulties in running current product and services in parallel to its transformation to DevSecOps	S1_SC_08	1	1
	Ignoring processes and security essentials leading to technical and security debt	ignoring processes and security essentials leading to technical debt and security debt	S1_SC_08	1	1
	Lacking process and platform for communication, collaboration, and sharing information and feedback	lack of common process and platform for communication, collaboration, and sharing information and feedback	S1_SC_08	1	1
	Out-of-sync domains and cross team dependencies causing issues in adopting DevSecOps	out-of-sync and conflicting domain specific bureaucratic processes for development, operation and security activities causing issues	S1_SC_08	1	2
		cross team dependencies and some domains don't allow or cause difficulties in adopting DevSecOps	S1_SC_02	1	
	Using unsuitable metrics	using unsuitable performance metrics for security evaluation	S1_IEEE_08	1	3
		use of unsuitable metrics	S1_ACM_01	1	
		using unsuitable metrics	S1_ACM_05	1	
	Inconsistent security polices design	inconsistent security polices design	S1_ACM_05	1	2
		lacks with consistence security polices design	S1_IEEE_08	1	
	Compliance requirements	compliance requirements	S1_IEEE_07,S1_IEEE_08, S1_IEEE_11,S1_ACM_05	4	4
	Tradeoff between security measures and CI system performance	the tradeoff between increased security measures, and the ability to access and modify the CI system as needed	S1_ACM_95	1	1
Technology	DevSecOps is mistaken for a set of tools	misleading understanding about DevSecOps transformation as implementation of set of tools	S1_SC_02	1	1
	Lack of tool standards	no standard set of recommended tools or mechanism for selection of fit-for-purpose and fit-for-use tools	S1_SC_02	1	2
		lack of tool standards	S1_IEEE_06	1	
	Lack of mature tools for automation and security	incomplete tool set for automation	S1_SC_02	1	13
		lack of automated testing tools	S1_IEEE_06,S1_IEEE_08, S1_ACM_05	3	

		lack of integrated testing tools to secure DevOps	S1_IEEE_08,S1_ACM_05	2	
		wrong automated deployment tools	S1_ACM_01,S1_IEEE_01, S1_IEEE_12	3	
		use of immature automated deployment tools	S1_ACM_01,S1_ACM_05, S1_IEEE_08,S1_IEEE_12	4	
	Complexity in managing different tools	complexity in managing different tools	S1_SC_02	1	1
	Difficulty in simulating production	difficulty in simulating production	S1_SC_02	1	1
	Availability and reliability of infrastructure resources, tools, automation, and network bandwidth for fast deployment cycle	availability and reliability of infrastructure resources, tools, automation, and network bandwidth for shorter and frequent deployment cycle	S1_SC_02	1	1
	Challenges of legacy system refactoring	refactoring or maintaining monolithic (legacy) system	S1_SC_02	1	2
		challenging to automate legacy system	S1_IEEE_06	1	
	Threat modeling scalability issue	threat modeling scalability issue	S1_IEEE_08,S1_ACM_05	2	2
	Remaining manual security testing and need for automated testing performance measures	security manual testing	S1_IEEE_08,S1_ACM_05	2	4
		lack of automated testing performance measures for security	S1_IEEE_08,S1_ACM_05	2	
	Use of cloud and serverless computing brings security complications	move security to the cloud	S1_IEEE_06	1	18
		cloud security complications	S1_SC_05,25,28,44, S1_IEEE_16,25,39, S1_ACM_19,52,59.66	11	
		attacks due to miss-configured cloud environments	S1_IEEE_33,S1_IEEE_42	2	
		security smells in Infrastructure as Code (IaC)	S1_ACM_06,S1_IEEE_28, S1_SC_26	3	
		invading VMs or containers	S1_ACM_52	1	
Business	Restructuring due to high cost and considering ROI (return on investment)	restructuring organization and implementing DevSecOps practices can lead to high cost such as salaries for security experts, costs on new tools	S1_IEEE_04	1	2
		risk and cost battle	S1_IEEE_06	1	
	Customer readiness for frequent releases	customer readiness for applying frequent releases to production setup	S1_SC_02	1	1
	Difficulty in training users for using advanced tools	users need to be properly trained when using advanced tools	S1_SC_02	1	1
	Insufficient resource is not	insufficient number of resources	S1_SC_02	1	3

	able to cope with abundance of information	abundance of information	S1_ACM_05, S1_IEEE_08	2	
	Dilemma in selection of business processes for DevSecOps transformation	dilemma in selection of business processes in product and service delivery for transformation to DevSecOps	S1_SC_08	1	1
	Conflicting approaches to security and business requirements	security and business objectives are implemented using conflicting approaches	S1_ACM_64	1	1

Thematic synthesis of DevSecOps challenges from GL

Category	Themes (16)	Codes (49)	Study mentions the code	Count	Subtotals
Organization, People, & Culture	Cultural resistance and organizational opposition	resistance to change	S1_GL_15	1	4
		challenge of the shifting role of security	S1_GL_37	1	
		organizational opposition	S1_GL_24	1	
		cultural resistance	S1_GL_20	1	
	Challenges of collaboration, communication & coordination	collaboration challenges	S1_GL_28,29	2	8
		failing to collaborate with the InfoSec team	S1_GL_18	1	
		lack of coordination between InfoSec team and developers	S1_GL_19	1	
		gaps between DevOps and Security teams	S1_GL_20	1	
		disconnect between security and development	S1_GL_39	1	
		friction between development and security teams	S1_GL_13	1	
		communication requirements	S1_GL_15	1	
	Urging velocity but neglecting security	developers are focused on velocity, not security	S1_GL_17	1	4
		DevOps teams neglect security	S1_GL_30	1	
		conflicting aims	S1_GL_38,40	2	
	Lack of security knowledge and skills, need for training	developers are not security specialists	S1_GL_15	1	6
		being unfamiliar with common security risks	S1_GL_18	1	
		the skills gap	S1_GL_37	1	
		not enough company stakeholders are security savvy	S1_GL_39	1	
		lack of security knowledge	S1_GL_38,40	2	
	Recruiting challenges	recruiting challenges	S1_GL_24	1	3
		understaffing InfoSec teams	S1_GL_18	1	
		engaging too late with the InfoSec team	S1_GL_18	1	
Process Capabilities	Fast changes and DevOps process conflict with slow security testing	rapid pace of change	S1_GL_29	1	6
		faster development process	S1_GL_28	1	
		security teams struggle to keep up with the pace of DevOps	S1_GL_30	1	
		DevOps velocity	S1_GL_37	1	
		Slow security testing	S1_GL_38,40	2	

	Interconnectedness of the DevOps process	interconnectedness of the DevOps process	S1_GL_28	1	1
	Implementing security in CI/CD	implementing security in CI/CD	S1_GL_28	1	1
	Continuous deployment chaos	continuous deployment chaos	S1_GL_19	1	1
	Poor visibility of security track record	poor visibility of security track record	S1_GL_19	1	1
	Compliance at risks	compliance at risks	S1_GL_39	1	1
	Inadequate privileged credentials and access controls causing cyber attacks	inadequate controls provide an opening for attack	S1_GL_30	1	2
		privileged credentials used in DevOps are targeted by cyber attackers	S1_GL_17	1	
Technology	Lack of mature tools for automation and security	mismatched tools	S1_GL_15	1	4
		tool-centric approaches to secrets management create security gaps	S1_GL_17	1	
		inefficient Static AST tools (SAST)	S1_GL_19	1	
		manual pen-testing becomes a bottleneck	S1_GL_19	1	
	Legacy systems need for cloud support for scalability	lack of cloud support	S1_GL_19	1	3
		systems are not scalable	S1_GL_19	1	
		legacy infrastructure	S1_GL_24	1	
	Containers and other tools come with their own risks.	container and other tools can often be the reason for security concerns	S1_GL_20	1	3
		workload containerization	S1_GL_29	1	
		tools come with their own risks	S1_GL_30	1	
	Use of cloud and serverless computing brings security complications	security vulnerabilities in the Cloud	S1_GL_24	1	6
		server less computing	S1_GL_28	1	
		cloud security	S1_GL_29	1	
		cloud security complications	S1_GL_38,40	2	
		cloud and open source environments lead to compromise of critical information, configuration errors, compliance issues and security breaches	S1_GL_20	1	

Thematic synthesis of DevSecOps practices from WL

Category	Themes (41)	Codes (86)	Study mentions the code	Count	Subtotals
Organization, People, & Culture	Collaboration	continuous collaboration	S1_SC_04	1	16
		enhanced collaboration	S1_ACM_02	1	
		work collaboratively	S1_ACM_02	1	
		cross-departmental collaboration	S1_IEEE_04	1	
		collaborating development, operation and security	S1_IEEE_04	1	
		increased collaboration between development, operations and security teams	S1_IEEE_12	1	
		close collaboration	S1_IEEE_12	1	
		collaboration within and between different teams	S1_IEEE_12	1	
		collaboration amongst different departments	S1_IEEE_12	1	
		collaboration between Dev&Ops	S1_IEEE_12	1	
		collaboration between Dev&Sec	S1_IEEE_12	1	
		collaboration between Sec&Ops	S1_IEEE_12	1	
		team collaboration	S1_IEEE_15	1	
		close collaboration of the teams	S1_IEEE_15	1	
		strong collaboration	S1_IEEE_15	1	
		collaboration between the security team and the development and operations teams	S1_IEEE_15	1	
	Communication	communication occurs at the right time and the delivery ability is continuous	S1_SC_04	1	9
		close communication	S1_ACM_02, S1_IEEE_09	2	
		good communication	S1_ACM_02	1	
		communication of security requirements	S1_ACM_02	1	
		virtual communication	S1_ACM_02	1	
		face-to-face communication	S1_ACM_02	1	
		physical communication	S1_ACM_02	1	
		strong communication	S1_IEEE_15	1	
	Trust	trust	S1_ACM_02, S1_SC_04, S1_IEEE_29	3	9
		trustworthy	S1_ACM_02	1	
		trusted relationships	S1_ACM_02	1	
		mutual trust	S1_ACM_02	1	
		implicit trust	S1_ACM_02	1	
		fully trusting each other	S1_SC_04	1	
		trust within the teams	S1_IEEE_29	1	
	Security champions	security champions	S1_SC_04, S1_ACM_02	2	2
	Knowledge sharing	knowledge sharing	S1_ACM_02, S1_SC_04	2	2
	Shared responsibility for	shared responsibility for security	S1_ACM_02, S1_SC_04	2	2

	security				
	Shameless retrospectives	shameless retrospectives	S1_SC_04, S1_IEEE_09	2	2
	Continuous improvement mindset	continuous improvement mindset	S1_SC_04	1	1
	Leadership	leadership	S1_SC_04	1	1
	Commitment & Agreement	commitment	S1_IEEE_29	1	2
		commitment and agreement	S1_SC_04	1	
	Hiring new personnel	hiring new personnel	S1_SC_04	1	1
	Enhance transparency	transparency	S1_SC_04, S1_IEEE_29	2	3
		clear transparency	S1_SC_09	1	
	Feedback loop	feedback (continuous and immediate)	S1_SC_04	1	3
		feedback loop between developers, security professionals, and operations team members	S1_SC_04	1	
		feedback loops	S1_ACM_15	1	
Process Capabilities	Shifting security to the left	shifting security to the left	S1_IEEE_04, 24, 26, S1_SC_02, 03, 08, 11, S1_ACM_50, 81	9	9
	Security-by-Design	security by design	S1_SC_07, 08, 18, 20, 22, S1_IEEE_16, 29, 30, 36, S1_ACM_45, 69	11	11
	Risk management	risk management (including risk assessment, risk treatment and risk control)	S1_SC_03, 05, 11, 18, 20, 22, 26, 40, 41, S1_ACM_03, S1_IEEE_34	11	11
	Compliance control	compliance control	S1_IEEE_11, S1_SC_27	2	2
	Continuous certification for DevOps	continuous certification for DevOps	S1_ACM_08	1	1
	Increase the visibility	increase the visibility	S1_SC_09	1	1
	Good documentation and logging	good documentation and logging	S1_IEEE_15	1	1
	Least privilege controls	least privilege controls	S1_IEEE_33	1	1
	Software process maturity	software process maturity - maturity models have emerged that let you link the degree of software security to the quality of the process	S1_SC_32	1	2
		Building Security In Maturity Model (BSIMM) model and The ISO/IEC 27035 Incident Management Cycle	S1_ACM_01	1	
	MUSA security DevOps framework for multi-cloud applications	MUSA DevOps framework for security assurance in multi-cloud applications	S1_IEEE_16, S1_IEEE_40	2	3
		MUSA Security DevOps (SecDevOps) framework	S1_ACM_52	1	

Technology	Automation	Automation	S1_ACM_01, 09, 30, 49, 71, 72, 81, 95, S1_IEEE_01, 06, 07, 09, 10, 12, 13, 15, 20, 21, 26, 38, 41, 54, 57, S1_SC_02, 03, 08, 09, 11, 17, 18, 20, 22, 26, 27, 28, 32, 40	37	104
		Automated/automating test/testing	S1_ACM_01, 09, 30, 49, 81, 95, S1_IEEE_01, 06, 07, 09, 10, 12, 15, 21, 26, 38, 41, 54, 57, S1_SC_02, 03, 08, 09, 11, 17, 18, 22, 26, 27, 28	30	
		Automated monitoring	S1_ACM_01, 71, 72, 81, S1_IEEE_01, 07, 12, 13, 15, 21, 26, 38, S1_SC_03, 08, 09, 18, 20, 26, 40	19	
		automated/automating/automatic deployment	S1_ACM_01, 09, 30. 95, S1_IEEE_01, 12, 15, 26, S1_SC_02, 03, 08, 28	12	
		automated/automating scans	S1_IEEE_01, 07, S1_SC_32	3	
		automated/automating code review	S1_IEEE_01, 07, 12	3	
	Fault injection (chaos engineering)	Fault injection (chaos engineering)	S1_IEEE_13	1	1
	Security-as-Code	Security-as-Code	S1_SC_03, 08, 09, 18, S1_IEEE_06,	5	5
	Continuous monitoring	misleading understanding about DevSecOps transformation as implementation of set of tools	S1_IEEE_01, 07, 12, 13, 15, 21, 26, 38, S1_SC_03, 08, 09, 18, 20, 26, 40, S1_ACM_01, 15, 71, 72, 81	20	20
	Threat modeling	threat modeling/analysis	S1_IEEE_02, 04, 07, 11, 30, 36, 39, 61, 71, S1_SC_03, 26	11	11
	Red team security drills	red team security drills	S1_IEEE_04, S1_SC_03	2	2
	Detect existing security flaws	detect existing security flaws	S1_SC_09	1	1
	Make sure the basics of host and network security are in place	make sure the basics of host and network security are in place	S1_SC_09	1	1
	Container security	Container/Containerization security	S1_ACM_52, S1_IEEE_01, 55	3	10
		run container as non-root users	S1_SC_09, 34, S1_IEEE_55	3	

		use the latest version of image	S1_SC_42	1	
		conduct deep scanning of container image	S1_IEEE_04	1	
		enhance security of Docker	S1_IEEE_31	1	
		security practices in Kubernetes to manage containers safely	S1_IEEE_18	1	
	DAST	Dynamic Application Security Testing (DAST) techniques integrated into a CI/CD pipeline.	S1_IEEE_10	1	1
	RASP	Runtime Application Self-Protection (RASP) controls	S1_SC_32.	1	1
	Combination of static and dynamic analytical methods	A combination of static and dynamic analytical methods.	S1_IEEE_15	1	1
	Immutable-as-Code	Immutable-as-code can be used to ensure the immutability of infrastructure and avoid accidental configuration drifts	S1_IEEE_33	1	1
	Policy-as-Code	Policy-as-Code is an attempt to code the policy itself	S1_IEEE_33.	1	1
	Design-as-Code	Design-as-code: CAIRIS (Computer Aided Integration of Requirements and Information Security) model.	S1_IEEE_36	1	1
	Micro-segmentation	Micro-segmentation.	S1_SC_38.	1	1
	Advanced malware detection	Advanced malware detection - employs machine learning & deep learning	S1_SC_32	1	1
	Adopting DevSecOps in microservices-based applications	Adopting DevSecOps in microservices-based applications	S1_IEEE_17, 43, 52, 57, 84, 86, S1_SC_15, 33, 36	9	9

Thematic synthesis of DevSecOps practices from GL

Category	Themes (54)	Codes (106)	Study mentions the code	Count	Subtotals
Organization, People, & Culture	Cultural shift to security	cultural shift	S1_GL_41	1	2
		change the security mindset	S1_GL_32	1	
	Improving collaboration, communication & cooperation	cross-functional collaboration	S1_GL_30	1	7
		foster collaboration between security and development	S1_GL_25	1	
		open contribution and collaboration	S1_GL_24	1	
		collaboration and integration	S1_GL_02	1	
		communicate and collaborate	S1_GL_32	1	
		improving empathy and cooperation	S1_GL_10	1	
		reducing friction	S1_GL_10	1	
	Collective responsibility for security	collective responsibility	S1_GL_02	1	2
		assign security responsibility to one person from your DevOps team	S1_GL_28	1	
	Shared knowledge	learn from each other	S1_GL_32	1	2

		shared threat intelligence	S1_GL_24	1	
	Training, learning and education for security	provide training	S1_GL_06	1	6
		get training	S1_GL_10	1	
		enabling through training	S1_GL_32	1	
		cross-training	S1_GL_35	1	
		educate developers	S1_GL_25	1	
		security learning	S1_GL_14	1	
	Recruiting success	recruiting success	S1_GL_10	1	2
		invite InfoSec to demos	S1_GL_18	1	
	Security champions	security champions	S1_GL_10	1	1
	Pragmatic implementation	pragmatic implementation	S1_GL_02	1	1
	Be reactive and responsive	be reactive and responsive	S1_GL_32	1	1
	Make security a priority	get buy-in from stakeholders	S1_GL_32	1	2
		make security a priority	S1_GL_32	1	
	Continuous feedback loop	continuous feedback loop	S1_GL_09, 13, 15, 22, 35	5	5
Process Capabilities	Integrate security early	integrate security during the planning phase	S1_GL_35	1	3
		take a proactive approach to security	S1_GL_17	1	
		include security early in the life cycle	S1_GL_28	1	
	Secure-by-Design	secure by design	S1_GL_31	1	3
		embed security into each release	S1_GL_31	1	
		embedded security	S1_GL_19	1	
	Moving security to the left	moving security to the left	S1_GL_08, 09, 13, 15, 18, 31, 35, 36	8	8
	Define security requirements	define security requirements	S1_GL_06	1	2
		security requirements and design	S1_GL_14	1	
	Security reviews	conduct security reviews	S1_GL_18	1	2
		integrate security review into every phase	S1_GL_18	1	
	Security evaluation	security evaluation	S1_GL_14	1	2
		proactive security assessments	S1_GL_10	1	
	Enhance visibility	enhance visibility	S1_GL_41	1	1
	Better reporting	report	S1_GL_02	1	2
		better reporting	S1_GL_19	1	
	Measurement	define metrics	S1_GL_06, 19	2	3
		measurement	S1_GL_02	1	
	Policies	impose policy and governance	S1_GL_41	1	2
		implement security policies	S1_GL_30	1	
	Compliance	compliance	S1_GL_10	1	4
		compliance operations	S1_GL_24	1	
		identify compliance requirements beforehand	S1_GL_28	1	
		bridging the divide between compliance and development	S1_GL_02	1	
	Vulnerability and incident management	vulnerability and incident management	S1_GL_14	1	5
		Incident management	S1_GL_08, 10	2	

		vulnerability management	S1_GL_23, 30	2	
	Privileged access management	privileged access management	S1_GL_30	1	2
		secure access via secrets management	S1_GL_41	1	
	Version control, metadata, and orchestration	version control, metadata, and orchestration	S1_GL_10	1	1
	Common weaknesses enumeration (CWE)	common weaknesses enumeration (CWE)	S1_GL_08	1	1
	Operational controls validation and improvement	operational controls validation and improvement	S1_GL_14	1	1
	Keep credentials safe	keep credentials safe	S1_GL_06	1	1
Technology	Software Composition Analysis	software composition analysis and governance	S1_GL_06	1	2
		software composition analysis	S1_GL_23	1	
	Automation	automation	S1_GL_02, 04	2	15
		use tools and automation	S1_GL_06	1	
		automate protection of business logic flaws	S1_GL_19	1	
		automated code review	S1_GL_23	1	
		automate as much as possible	S1_GL_25, 28	2	
		automate tools and security processes	S1_GL_30	1	
		use automated security tools	S1_GL_41	1	
		automate security processes	S1_GL_17	1	
		automated security testing	S1_GL_08,11,13,15, 35	5	
	Threat modeling	threat modeling	S1_GL_06, 10, 14, 25, 28	5	5
	Continuous monitoring	continuous monitoring	S1_GL_06	1	5
		monitoring	S1_GL_02	1	
		24×7 proactive monitoring	S1_GL_24	1	
		monitor and scale	S1_GL_25	1	
		security monitoring	S1_GL_31	1	
	Secure coding	source code repository and scanning	S1_GL_10	1	6
		Secure coding	S1_GL_14	1	
		secure coding practice	S1_GL_10, 28	2	
		build preapproved code	S1_GL_18	1	
		conduct code dependency checks regularly	S1_GL_25	1	
	Sensitive information scan	sensitive information scan	S1_GL_23	1	1
	SAST	Static Application Security Testing (SAST)	S1_GL_02, 08, 23, 25	4	4
	DAST	Dynamic Application Security Testing (DAST)	S1_GL_02, 08, 23, 25	4	4
	IAST	Interactive Application Security Testing (IAST)	S1_GL_02, 08, 19, 25	4	4
	RASP	Runtime Application Self-Protection (RASP)	S1_GL_02, 08, 25	3	3
	Security-as-Code	Security-as-Code	S1_GL_32	1	1
	Compliance-as-Code	Compliance-as-Code	S1_GL_23	1	1
	Policy-as-Code	Policy-as-Code	S1_GL_17	1	1
	Consumable security services with APIs	Consumable security services with APIs	S1_GL_24	1	1

	Red and blue team exploit testing	red and blue team exploit testing	S1_GL_24	1	1
	Integrate security issues within your general bug tracker	Integrate security issues within your general bug tracker	S1_GL_19	1	1
	Configuration management	configuration management	S1_GL_10	1	1
	Host hardening	host hardening	S1_GL_10	1	1
	Application-level assessment	application-level assessment	S1_GL_10	1	1
	CI/CD for patching	CI/CD for patching	S1_GL_10	1	1
	Container security	Docker security	S1_GL_10	1	4
		Kubernetes security	S1_GL_10	1	
		Leverage containerization	S1_GL_28	1	
		Harden the container	S1_GL_41	1	
	Verify cloud infrastructure	verify cloud infrastructure	S1_GL_28	1	1
Business	Separation of duties	separation of duties	S1_GL_14, 17	2	2
	Business-driven security	business-driven security	S1_GL_24	1	1
	Availability and business continuity management	availability and business continuity management	S1_GL_14	1	1
	Linear scalability and affordable cost	linear scalability and affordable cost	S1_GL_19	1	1

Thematic synthesis of DevSecOps metrics from WL

Category	Themes (15)	Codes (41)	Study mentions the code	Count	Subtotals
OPC	Security-trained rate	number of developers that have gone through security-training	S1_IEEE_06	1	1
Business	Business metrics	business metrics	S1_SC_02	1	3
		revenue	S1_SC_02	1	
		key performance indicators	S1_SC_02	1	
Process Capabilities	Top vulnerability	number of mistakes in different security categories	S1_IEEE_06	1	5
		OWASP top 10	S1_IEEE_06	1	
		top vulnerability types	S1_SC_03	1	
		the most recurring	S1_SC_03	1	
		helps planning training	S1_SC_03	1	
	Time spent correcting mistakes in each category	time spent correcting mistakes in each category	S1_IEEE_06	1	1
	Number of continuous delivery cycles per month	number of continuous delivery cycles per month	S1_SC_03	1	3
		Number of successful deploys to production per month	S1_SC_03	1	
		how quickly changes can be deployed to production	S1_SC_03	1	
Technology	Penetration test pass rate	systems that are affected by internal and external penetration testing	S1_IEEE_06	1	1
	Security test pass rate	security test pass rate	S1_IEEE_57	1	3
		identify security vulnerabilities	S1_IEEE_57	1	
		ratio of failed-versus-pass static security source code scans	S1_IEEE_57	1	
	Code scanning detection rate	code scanning detection rate	S1_IEEE_57	1	3
		number of security scans identifies a problem in each timeframe or given process phase	S1_IEEE_57	1	
		also include the number of problems	S1_IEEE_57	1	
	Defect density	defect density	S1_SC_03	1	3
		number of confirmed defects detected in software component during a defined period of development/operation divided by the size of the software/component	S1_SC_03	1	
		negotiate reasonable goals to reduce defect density over time	S1_SC_03	1	
	Defect burn rate	defect burn rate	S1_SC_03	1	3
		how quickly the team is addressing defects	S1_SC_03	1	
		Measuring development team productivity solving defects	S1_SC_03	1	
	Critical risk profiling	critical risk profiling	S1_SC_03	1	3
		the relation between issue criticality and the value of that vulnerability to possible attackers	S1_SC_03	1	
		prioritize the order development teams should address issues	S1_SC_03	1	
	Number of adversaries per application	how many adversaries an application might have	S1_SC_03	1	3
		associated with the practice of Threat Modeling & Risk Analysis	S1_SC_03	1	

		identify the applications are more exposed to possible attacks and prepare accordingly	S1_SC_03	1	
	Adversary return rate	adversary return rate	S1_SC_03	1	3
		how often an adversary will use the same strategy and procedures	S1_SC_03	1	
		helps define appropriate training	S1_SC_03	1	
	Point of risk per device	point of risk per device	S1_SC_03	1	3
		number of vulnerabilities per server	S1_SC_03	1	
		helps prioritize these vulnerabilities	S1_SC_03	1	
	Number of issues during red teaming drills	number of issues during red teaming drills	S1_SC_03	1	3
		number of found issues and fixed by Red Team	S1_SC_03	1	
		red team effectiveness	S1_SC_03	1	

Thematic synthesis of DevSecOps metrics from GL

Category	Themes (6)	Codes (16)	Study mentions the code	Count	Subtotals
Process Capabilities	Whether features undergo a security review	whether features undergo a security review	S1_GL_18	1	3
		the percentage of features that undergo security review early in the design process, percentage should go up over time	S1_GL_18	1	
		know the current state and progress of security reviews	S1_GL_18	1	
	Whether security review slows down the development cycle	Whether security review slows down the development cycle	S1_GL_18	1	3
		how much time the reviews add to the development process, the time should go down until it reaches an agreed-to minimum	S1_GL_18	1	
		the efficiency of security reviews	S1_GL_18	1	
	How well security is integrated into the delivery lifecycle	how well security is integrated into the delivery lifecycle	S1_GL_18	1	3
		number of security reviews captured at stages of the SDLC (design, develop, test, and release), this number should go up until it reaches a value that suggests that InfoSec is fully integrated	S1_GL_18	1	
		Know the degree of InfoSec team's involvement in each step of the SDLC	S1_GL_18	1	
Technology	Whether automated testing covers security requirements	whether automated testing covers security requirements	S1_GL_18	1	3
		the number or percentage of security requirements that are included in the automated testing process, this percentage should go up over time	S1_GL_18	1	
		Know the degree of InfoSec team's involvement in writing automated tests	S1_GL_18	1	
	The use of preapproved libraries, packages, tool	use of preapproved libraries, packages, tool chains, and processes	S1_GL_18	1	3

	chains, and processes	Initially, measure whether InfoSec is engaged in tools development. As work progresses, the number of InfoSec-approved libraries, packages, and tool chains that are available, or the number of these resources that are used by the development and operations teams. Engagement should increase over time until the organization agrees that InfoSec oversight of tools is at the correct level. Similarly, the percentage or number of preapproved tools in use should increase until the team uses all the tools that InfoSec has created or approved.	S1_GL_18	1	
		Know the degree of InfoSec team's engagement in tools development and the usage of preapproved libraries, packages, tool chains	S1_GL_18	1	
	Using SAFe DevOps Health Radar	SAFe DevOps Health Radar measures DevOps performance, by assessing the maturity of four aspects and 16 activities of the CI/CD pipeline	S1_GL_01	1	1

Thematic synthesis of DevSecOps tools from WL

Category	Themes (11)	Codes/Tools (33)	Study mentions the code	Count	Subtotals
Technology	Automation tools	Chef	S1_IEEE_07, S1_SC_12, 20, 26	4	11
		Jenkins	S1_SC_12	1	
		Ansible	S1_SC_20	1	
		Puppet	S1_SC_20	1	
		Gauntlt	S1_IEEE_01, 06	2	
		SaltStack	S1_SC_01, 20	2	
	Automated code review tools	Veracode Greenlight	S1_SC_01	1	1
	Threat modeling tools	IriusRisk	S1_SC_01	1	2
		Microsoft threat modeling tool	S1_IEEE_39	1	
	Containerization tools	Docker	S1_SC_09, 18, 20, 29, 34, 42, 45, 48, S1_ACM_95, 99, S1_IEEE_31, 55	12	18
		Kubernetes	S1_ACM_52, 76, 89, S1_SC_20, 29, S1_IEEE_18	6	
	Cloud security tools	Terraform	S1_SC_12, 20, S1_IEEE_33	3	4
		Snorby threat stack	S1_IEEE_01	1	
	Cyber security tools	Tripwire	S1_IEEE_01	1	2
		Snort	S1_IEEE_01	1	
	Monitoring and alerting tools	New Relic	S1_IEEE_01	1	9
		Nagios Icinga	S1_IEEE_01	1	
		Graphite	S1_IEEE_01	1	
		Ganglia	S1_IEEE_01	1	
		Cacti	S1_IEEE_01	1	
		Pager Duty	S1_IEEE_01	1	
		Sensu	S1_IEEE_01	1	
		Boundry	S1_IEEE_01	1	
		Pingdom	S1_IEEE_01	1	
	Logging tools	PaperTrail	S1_IEEE_01	1	5
		Logstash	S1_IEEE_01	1	
		Loggly	S1_IEEE_01	1	
		Splunk	S1_IEEE_01	1	
		SumoLogic	S1_IEEE_01	1	
	SAST tools	Kiuwan	S1_SC_01	1	1
	DAST tools	OWASP ZAP	S1_IEEE_01	1	2
		Arachini	S1_IEEE_01	1	
	Advanced malware detection tool	CodeAI	S1_SC_01	1	1

Thematic synthesis of DevSecOps tools from GL

Category	Themes (14)	Codes/Tools (45)	Study mentions the code	Count	Subtotals
Technology	Automation tools	Ansible	S1_GL_04	1	1
	Containerization tools	Docker	S1_GL_03, 10	2	4
		Kubernetes	S1_GL_03, 10	2	

	Container security tools	Twistlock	S1_GL_42	1	3
		Notary	S1_GL_42	1	
		Aqua Security	S1_GL_42	1	
	Cloud security tools	AppScan on Cloud	S1_GL_42	1	4
		AWS Security service	S1_GL_42	1	
		ThreatModeler Cloud Edition	S1_GL_42	1	
		Trend Micro Cloud One	S1_GL_42	1	
	Automated code review tools	PMD	S1_GL_23	1	3
		DevSkim	S1_GL_23	1	
		FindSecBugs	S1_GL_23	1	
	Sensitive information scanning tools	TruffleHog	S1_GL_23	1	3
		GitSecrets	S1_GL_23	1	
		Talisman	S1_GL_23	1	
	SAST tools	Flawfinder	S1_GL_23	1	6
		Graudit	S1_GL_23	1	
		Bandit	S1_GL_23	1	
		Spotbugs	S1_GL_23	1	
		SonarQube	S1_GL_23, 42	2	
	DAST tools	OWASP ZAP	S1_GL_23	1	7
		BDD Security	S1_GL_23	1	
		Arachini	S1_GL_23	1	
		Nikto	S1_GL_23	1	
		Radamsa	S1_GL_23	1	
		FuzzDB	S1_GL_23	1	
		Fortify Webinspect	S1_GL_42	1	
	RAST tools	Fortify Application Defender	S1_GL_42	1	1
	Software composition analysis tools	Retire.js	S1_GL_23	1	3
		OSSAudit	S1_GL_23	1	
		OWASP Dependency-Check	S1_GL_23	1	
	Compliance-as-code tools	nspec	S1_GL_23	1	3
		ServerSpec	S1_GL_23	1	
		OpenSCAP	S1_GL_23	1	
	Vulnerability management tools	Defect Dojo	S1_GL_23	1	8
		ArcherySec	S1_GL_23	1	
		Snyk	S1_GL_10, 21	2	
		HackerOne,	S1_GL_21	1	
		Claire	S1_GL_21	1	
		Stethoscope	S1_GL_21	1	
		Rapid7 Nexpose	S1_GL_21	1	
	Monitoring and alerting tools	Suricata	S1_GL_21	1	2
		NewRelic	S1_GL_42	1	
	DevOps performance measuring tool	SAFe DevOps Health Radar	S1_GL_01	1	1