Journal of Engineering Science *Vol. XXXIII, no. 1 (2026), pp. 70 - 80*
Fascicle *Electronics and Computer Science* *ISSN 2587-3474*
Topic *Computers and Information Technology* *eISSN 2587-3482*

https://doi.org/10.52326/jes.utm.2026.33(1).05
UDC 004.9.056:004.738.5:378.147.018

A LAB-ORIENTED CURRICULUM MODEL FOR CLOUD-NATIVE SECURITY AUTOMATION: FROM IMAGE SCANNING TO RUNTIME POLICY ENFORCEMENT

Ludmila Peca*, ORCID: 0000-0002-4394-2933,
Andrian Prisacaru, ORCID 0000-0001-7809-0868,
Pavel Nistiriuc, ORCID: 0000-0001-5189-7987,
Svetlana Cojocaru, ORCID: 0000-0002-1187-4294,
Marius Dumitraşcu, ORCID: 0009-0006-3547-4558,
Rostislav Călin, ORCID: 0000-0002-2672-1717

Technical University of Moldova and National Institute of Innovations in Cybersecurity CYBERCOR, 168, Stefan cel Mare Blvd., Chisinau, Republic of Moldova
* Corresponding author: Ludmila Peca, *ludmila.peca@isa.utm.md*

Received: 02. 03. 2026
Accepted: 03. 18. 2026

Abstract. The accelerating adoption of cloud-native architectures has created a critical gap between academic cybersecurity training and operational industry demands. This paper applies a *design-based research (DBR)* methodology to propose a lab-oriented curriculum model for cloud-native security automation, structured around the complete *build-deploy-run* lifecycle. The model integrates progressive static and dynamic security controls aligned with Cloud Workload Protection Platform (CWPP) and Cloud-Native Application Protection Platform (CNAPP) industry practices. Four curriculum modules produce verifiable deliverables, namely scan reports, compliance checklists, runtime policies, and incident analyses, enabling objective competency assessment through a structured rubric. Preliminary validation with 22 master-level students achieved a module completion rate of 90% and an overall competency score of 78%, demonstrating significant improvement over theory-focused approaches. The model offers a replicable framework for both academic programs and professional continuous education, contributing to reducing the global cybersecurity skills gap estimated at 4.76 million professionals worldwide as of 2024.

Keywords: *cybersecurity education, cloud-native security, CNAPP, CWPP, Kubernetes, DevSecOps, container scanning, runtime protection, CVE, compliance.*

Rezumat. Adoptarea accelerată a arhitecturilor cloud-native a creat un decalaj critic între formarea academică în domeniul securității cibernetice și cerințele operaționale ale industriei. Această lucrare aplică o metodologie de *cercetare bazată pe design (DBR)* pentru a propune un model curricular orientat pe laborator pentru automatizarea securității cloud-native, structurat în jurul ciclului complet *build-deploy-run*. Modelul integrează controale de securitate statice și dinamice progresive, aliniate la practicile industriale Cloud Workload Protection Platform (CWPP) și Cloud-Native Application Protection Platform (CNAPP). Patru module curriculare produc livrabile verificabile, respectiv rapoarte de scanare, liste de

verificare a conformității, politici runtime și analize de incidente, permițând evaluarea obiectivă a competențelor printr-o rubrică structurată. Validarea preliminară cu 22 de studenți de nivel master a atins o rată de finalizare a modulelor de 90% și un scor global de competențe de 78%, demonstrând o îmbunătățire semnificativă față de abordările centrate pe teorie. Modelul oferă un cadru replicabil atât pentru programele academice, cât și pentru formarea profesională continuă, contribuind la reducerea deficitului global de specialiști în securitate cibernetică, estimat la 4,76 milioane de profesioniști la nivel mondial în 2024.

Cuvinte-cheie: *securitate în cloud, securitate containerizată, Kubernetes, serverless; automatizarea securității în DevSecOps, scanarea vulnerabilităților, conformitate cloud, protecție la runtime, IAM și guvernanță.*

1. Introduction

The rapid adoption of cloud-native architectures has generated a structural transformation of IT infrastructure, driving the transition from monolithic models to distributed systems based on microservices, containers, and dynamic orchestration. In this context, security can no longer be treated as a perimeter mechanism but must be integrated continuously into development and operational processes.

The complexity of cloud-native environments derives from their ephemeral, scalable, and automated nature. Resources are created and destroyed dynamically, configurations are defined as code, and security responsibilities are shared between the cloud provider and the user. This dynamic amplifies risks associated with vulnerabilities in container images, misconfigurations in Kubernetes clusters, excessive Identity and Access Management (IAM) permissions, or the absence of behavioral monitoring at runtime.

The scale of the challenge is illustrated by recent workforce data: according to the ISC2 Cybersecurity Workforce Study (2024), the global active cybersecurity workforce stalled at 5.5 million professionals, while the total workforce needed reached 10.2 million, yielding a deficit of **4.76 million professionals**, a 19.1% increase year-on-year [1]. Furthermore, 88% of organizations reported at least one significant cybersecurity consequence due to skills deficiencies [2], and organizations with insufficiently staffed security teams paid on average USD 550,000 more per breach [3]. These figures underscore the urgent need for curriculum models that systematically develop applied cloud security competencies.

To address these risks, the industry has developed integrated Cloud Workload Protection Platform (CWPP) and Cloud-Native Application Protection Platform (CNAPP) solutions, which consolidate static scanning, vulnerability analysis, compliance verification, and real-time behavioral protection across the entire application lifecycle: build-deploy-run. Gartner (2024) defines CNAPP as a unified set of security and compliance capabilities covering artifact scanning, configuration management, risk prioritization, and behavioral analytics [4].

Research problem: how can a curriculum model be designed that reproduces the operational logic of cloud-native security used in industry, progressively integrating static and dynamic controls within an automated framework?

The working hypothesis is that a lab-oriented, progressively structured syllabus based on an integrated enterprise suite can reduce the gap between academic competencies and the operational requirements of cloud-native security. The contributions are: (1) an integrated curricular framework for cloud-native security aligned to DevSecOps; (2) a pedagogical progression from static controls to dynamic protection mechanisms; (3) a rubric-based assessment system with verifiable deliverables; and (4) preliminary quantitative validation results.

2. State of the art

The transformation towards cloud-native architectures has been analyzed extensively in the literature, particularly in the context of containerization and Kubernetes orchestration. Studies on container security highlight that container images represent a major source of vulnerabilities, as they frequently include libraries with known Common Vulnerabilities and Exposures (CVEs) and insecure default configurations [5], [6]. Improper Role-Based Access Control (RBAC) configuration can lead to privilege escalations and unjustified expansion of the attack surface [7].

Recent empirical data confirm the scale of these threats. According to Red Hat's State of Kubernetes Security Report 2024, 89% of organizations experienced at least one Kubernetes-related security incident, with 40% detecting issues specifically in container or Kubernetes configurations [8]. In 2024 alone, 52 new vulnerabilities at various severity levels were added to the CVE database for Kubernetes and its ecosystem [9]; Table 1 summarizes the five most significant.

Table 1

Most significant CVEs in the Kubernetes and container ecosystem (2024)

CVE ID	CVSS	Severity	Description
CVE-2024-3094	10.0	Critical	Malicious code injected in XZ Utils: full Secure Shell (SSH) compromise
CVE-2024-31989	9.0	Critical	Argo CD: unauthenticated Redis instance allows cluster-level privilege escalation
CVE-2024-21626	8.6	High	runC: container escape granting access to host node filesystem
CVE-2024-6387	8.1	High	OpenSSH (sshd): race condition exploitable by unauthenticated remote users
CVE-2024-10220	8.1	High	gitRepo volume: arbitrary command execution on host node with root privileges

Source: Fairwinds Security Report 2024 [9]; Upwind Security 2025 [10].

In parallel, the DevSecOps literature supports the early and continuous integration of security controls in Continuous Integration/Continuous Delivery (CI/CD) pipelines [11]. The 'shift-left security' concept is frequently mentioned as a mechanism for risk reduction through early detection [12]. However, real integration remains difficult due to lack of specialized skills and tool fragmentation [13]. Regarding cloud security education, curricula are predominantly theoretically oriented, with limited exposure to modern protection mechanisms [14]. Research emphasizes the need for laboratory- and scenario-based learning models [15]. Three major limitations are identified: (1) absence of an integrated curriculum model covering the full build-deploy-run lifecycle; (2) lack of progressive integration of static and dynamic controls; and (3) insufficient use of enterprise platforms for educational simulation of real conditions.

3. Research methodology

The design of the proposed curriculum model is based on a design-based research (DBR) approach, frequently used in applied educational research in technological domains [16]. DBR enables the simultaneous pursuit of theoretical grounding and empirical validation, through the design and iterative refinement of an educational artefact, in this case a lab-oriented syllabus, followed by pilot implementation and analysis.

Curriculum design was guided by four principles: (1) alignment with the build-deploy-run operational cycle following DevSecOps practices [11], [13]; (2) progressive integration of static and dynamic controls, consistent with container and microservice security recommendations [5], [12]; (3) laboratory- and real-scenario-based learning [15], [16]; and (4) evaluation based on verifiable deliverables and a structured rubric for objective competency measurement.

In technical terms, the model is grounded in National Institute of Standards and Technology (NIST) SP 800-190 container security guidelines [17] and CIS Kubernetes Benchmark best practices. The pedagogical foundation also draws on prior e-learning and network security work developed at UTM [19–21].The development process comprised four stages: (1) analysis of operational requirements against Association for Computing Machinery/Institute of Electrical and Electronics Engineers (ACM/IEEE) curriculum guidelines [14] and the European Union Agency for Cybersecurity (ENISA) cybersecurity skills framework [15]; (2) modular structuring aligned to the build-deploy-run lifecycle; (3) definition of deliverables and assessment rubric; and (4) pilot implementation with 22 master-level students and preliminary quantitative validation.

The operational requirements analysis drew on competency frameworks from ACM/IEEE guidelines for computing programs [14] and from ENISA's 2022 report on cybersecurity skills development in the EU [15]. The modular structure was validated against the build-deploy-run lifecycle, yielding four modules aligned with progressive security controls as summarized in Table 2 below2 below.

Table 2

Curriculum module structure: lifecycle alignment and verifiable deliverables

Modul	Titlu	Faza DevSecOps	Livrabile principale
M1	Static Image Analysis	Build	CVE scanning, Dockerfile audit, registry signing
M2	Cloud Compliance & Configuration	Deploy	CIS Benchmark, RBAC audit, secrets mgmt.
M3	Agent Deployment & Runtime Protection	Run	Defender install, behavioral policies, alert tuning
M4	Incident Response & Governance	Run / Audit	Log analysis, snapshot forensics, IAM audit

Source: Authors' design, aligned with NIST SP 800-190 [17] and CIS Kubernetes Benchmark.

4. Model description

The proposed curriculum model is built on an operational architecture that reproduces the complete build–deploy–run cycle, using an integrated cloud-native protection suite (CWPP/CNAPP type) as the implementation environment. The model's technical structure

follows the progressive integration of static and dynamic controls, consistent with NIST recommendations for container security [17] and CIS best practices for Kubernetes.

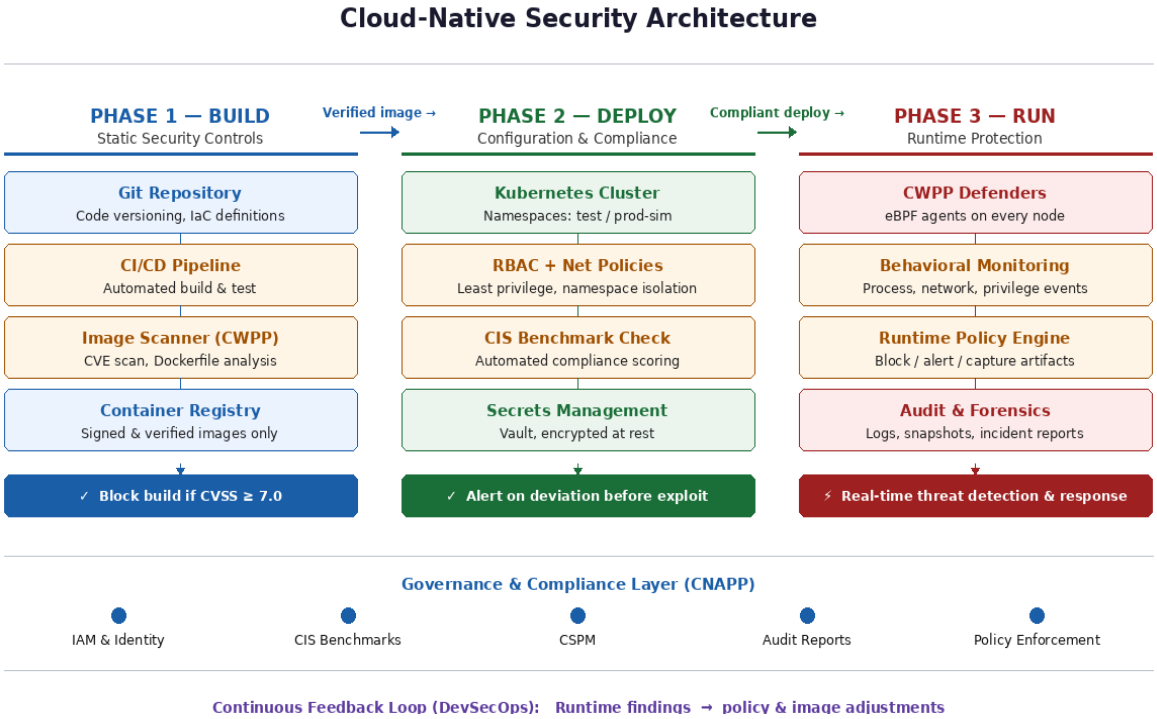

Figure 1. Cloud-Native Security Architecture: Integrated Build–Deploy–Run Model with continuous feedback loop.

Source: Authors' design, based on NIST SP 800-190 [17] and CIS Kubernetes Benchmark.

4.1. Technical architecture of the laboratory environment

Level 1 – Build (static controls and supply chain security). The build phase integrates a Git repository, an automated CI/CD pipeline, and a container image registry. Automated image scanning is implemented before publication, including CVE identification and Dockerfile configuration analysis. Blocking the build when severity thresholds are exceeded operationalizes risk policy and transforms security into a formal acceptance criterion for the software artifact, reflecting DevSecOps 'shift-left security' principles [13].

Level 2 – Deploy (configuration validation and compliance). The application is deployed to a Kubernetes cluster organized in distinct namespaces (test/production-simulated). Configurations are evaluated against the CIS Kubernetes Benchmark. The literature documents that the majority of Kubernetes incidents are caused by configuration errors rather than critical software vulnerabilities [7], making automated compliance checks at deploy time essential to reduce the operational attack surface.

Level 3 – Run (behavioral protection and incident response). Dynamic controls are introduced through installation of CWPP protection agents (defenders) at node level, monitoring process behavior and container network traffic. Detection mechanisms identify unauthorized executions, unjustified privilege escalations, and suspicious external connections. A feedback mechanism allows runtime monitoring results to determine adjustments to container images and build-phase configurations, closing the continuous security cycle.

Governance and compliance layer. A transversal governance layer, implemented through the Cloud-Native Application Protection Platform/Cloud Security Posture Management (CNAPP/CSPM) capabilities of the enterprise suite, covers IAM policy evaluation, cloud account compliance checks, and audit report generation across all three phases. This

layer correlates technical controls with compliance frameworks and supports policy-as-code enforcement.

4.2. Security workflows

The architecture is operationalized through three main security workflows, integrated in a cyclic continuous feedback mechanism. Figure 2 provides a detailed flowchart of each workflow, including decision gates and inter-workflow handoffs.

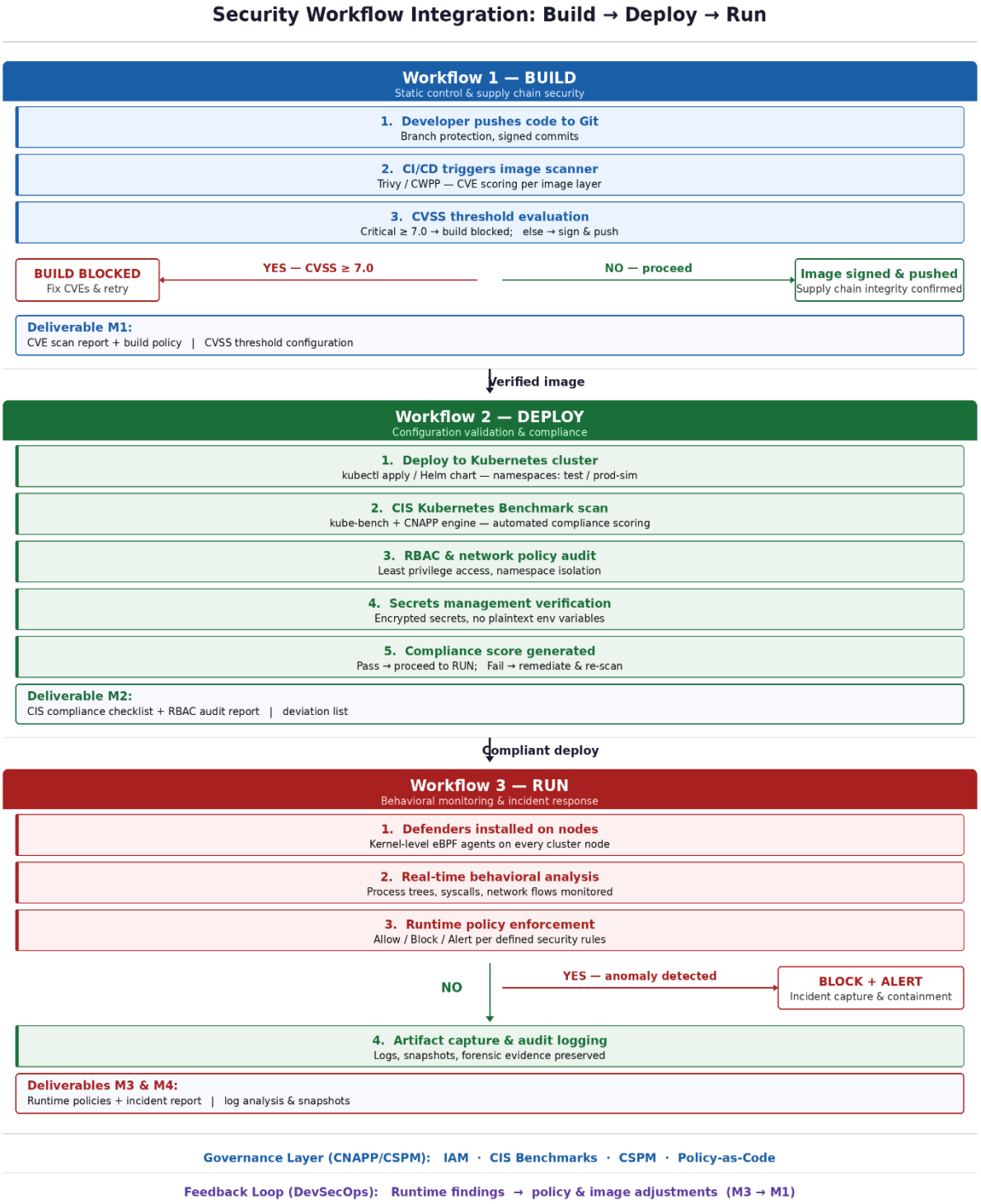

Figure 2. Security Workflow Integration: Static → Compliance → Behavioral Protection with decision gates and feedback loop.
Source: Authors' design.

Workflow 1, static control in the build phase. The build workflow integrates automated mechanisms for static analysis of container images and associated configurations. Scanning is triggered within the CI/CD pipeline, and results are evaluated based on the severity of identified vulnerabilities (CVE scoring). If a preset risk threshold is exceeded, the build process is interrupted, preventing the propagation of a compromised image to the registry.

Workflow 2, validation and compliance in the deploy phase. In the deploy stage, the application is implemented in the Kubernetes cluster, and configurations are evaluated against security policies and CIS standards. This workflow verifies RBAC configuration compliance with the 'least privilege' principle; restrictive network policies; namespace isolation; and secure secrets management.

Workflow 3, behavioral monitoring in the run phase. The run workflow introduces dynamic monitoring of container and active process behavior. Protection agents collect system-level events, network calls, and privilege modifications, comparing them with previously defined policies. Anomaly detection enables identification of unauthorized executions, blocking of suspicious processes, alert generation, and capture of artifacts for subsequent analysis.

5. Operational Integration in the DevSecOps literature [6]

The proposed technical model is designed to reproduce the complete operational lifecycle of cloud-native applications, consistent with the lifecycle structure defined in NIST SP 800-190 [17]. The architecture is organized on three functional levels corresponding to the build, deploy and run phases, ensuring progressive integration of static and dynamic controls.

Through the coherent integration of controls across the entire build-deploy-run lifecycle, the proposed model surpasses the fragmented approaches identified in the literature and offers an operational framework aligned with internationally recognized standards [13], [17]. The architectural structure allows both reproduction of enterprise conditions in a controlled academic environment and the assessment of technical competencies based on the effective implementation of controls.

Industry adoption data supports the relevance of this approach: Gartner projected that by 2025, 60% of enterprises would have consolidated CWPP and CSPM capabilities with a single vendor, up from 25% in 2022. Meanwhile, the Cloud Security Alliance reported that 75% of organizations are using or planning to use CNAPP solutions [4]. These trends reinforce the need for academic programs to integrate CNAPP/CWPP operational practices.

6. Results and discussions

The implementation of the proposed curriculum model in a master-level university program aimed to assess students' ability to operate real security controls in cloud-native environments. Preliminary validation was carried out through analysis of technical deliverables generated in each module, including scanning reports and vulnerability prioritization, RBAC policy configuration and testing, runtime protection rule definition, and simulated incident documentation based on collected logs and artifacts.

The results obtained indicate a visible increase in technical autonomy compared to theory-centered approaches. Students demonstrated the ability to implement and adjust functional policies in an orchestrated environment, not just describe abstract concepts. The integration of build-deploy-run workflows in a unified framework contributed to understanding the relationship between vulnerability, misconfiguration, and active exploitation, consolidating a systemic perspective on cloud-native security.

Compared to traditional teaching models, in which container security and runtime protection are treated separately, the proposed model ensures logical continuity of controls and reflects the operational structure recommended in NIST SP 800-190 [10] and in the DevSecOps literature [13]. The correlation of laboratory activities with standards such as the CIS Kubernetes Benchmark anchors the educational process in practices effectively used in industry, reducing the gap between academic competencies and real operational requirements.

Table 3 presents a comparative analysis of the proposed model against traditional curriculum approaches across key evaluation criteria.

Table 3

Comparative analysis: traditional approaches vs. the proposed lab-oriented model

Comparison criterion	Traditional approaches	Modelul propus (lab-based)
Pedagogical orientation	Predominantly theoretical	Practical, based on real scenarios
Control integration	Fragmented (container + runtime treated separately)	Full build-deploy-run cycle
Use of enterprise platforms	Rare or absent	CWPP/CNAPP suite as reference environment
Competency assessment	Examene teoretice, proiecte izolate	Verifiable deliverables, functional policies
Alignment with industry standards	Limited (general concepts only)	NIST SP 800-190, CIS Kubernetes Benchmark
Feedback mechanisms	Absent or manual	Cyclic, automated (runtime to build)

Source: Authors' analysis based on [14], [15], [16].

The cybersecurity workforce data further contextualizes the contribution of this work. With a global deficit of 4.76 million professionals as of 2024 [1], and 88% of organizations reporting skill-related security consequences [2], lab-oriented models that develop verifiable operational competencies represent a direct response to industry needs. The IBM Cost of a Data Breach Report 2024 found that organizations with understaffed security teams paid an average of $550,000 more per breach [3], illustrating the financial stakes of inadequate practical training.

Table 4

Global cybersecurity workforce gap indicators (2023–2024)

Indicator	Value (2023)	Value (2024)	Change
Active cybersecurity workforce (global)	5,5 mil.	5,5 mil.	+0,1%

Continuation Table 4

Professional workforce deficit	3,99 mil.	4,76 mil.	+19,1%
Total workforce needed (global)	9,5 mil.	10,2 mil.	+7,4%
Organizations with staffing deficit	69%	67%	-2 p.p.
Average cost of a security breach	$4,45 mil.	$4,88 mil.	+9,7%

Source: ISC2 Cybersecurity Workforce Study 2024 [1]; IBM Cost of a Data Breach Report 2024 [3].

However, the results presented have a preliminary character and are limited to implementation in a single institutional context. Generalization of conclusions requires validation of the model across multiple cohorts and different environments. Additionally, the use of an enterprise suite presupposes access to infrastructure and specialized licenses, which may influence replicability in resource-constrained institutions. Looking ahead, extending the model through the integration of AI-assisted analysis mechanisms and the use of distributed cyber range environments could consolidate the applied dimension and scalability of the approach.

7. Conclusions and recommendations

This paper proposed a lab-oriented curriculum model for security automation in cloud-native environments, grounded in the progressive integration of static and dynamic controls across the entire build–deploy–run lifecycle. Unlike the fragmented approaches identified in the literature, the proposed model provides a coherent structure that reproduces the operational workflows used in enterprise environments and transposes them into a formalized educational framework.

Through the correlation of the technical architecture and laboratory activities with internationally recognized standards, such as NIST SP 800-190 and the CIS Kubernetes Benchmark, the model ensures the alignment of learning objectives with real security practices. The integration of image scanning, compliance checks, and runtime protection in a cyclic feedback mechanism consolidates the continuous security perspective and contributes to the development of applied operational competencies.

Preliminary results indicate that the approach oriented on the effective implementation of technical controls leads to increased autonomy and incident analysis capability in containerized and dynamically orchestrated environments. The proposed model is not limited to transmitting theoretical knowledge, but creates an evaluable framework for developing competencies in the field of cloud security automation.

Although complete validation requires extending implementation to multiple cohorts and institutional contexts, the conceptual and architectural framework presented offers a replicable basis for integrating cloud-native security in university programs and continuous professional training. Future directions include consolidating quantitative competency assessment mechanisms, integrating AI-assisted analysis techniques for alert prioritization, and extending the model to distributed cyber range environments.

Overall, the contribution of the paper consists in defining an integrated technical and curricular model that reduces the gap between academic training and the operational requirements of cloud-native security, offering a systemic framework for developing competencies in the field of DevSecOps automation.

Acknowledgments: This work was carried out with the support of the bilateral project PN-IV-PCB-RO-MD-2024-0558 TYPHON, 'Training young professionals using an intelligent, optimized cyber range network', implemented in collaboration between the Technical University of Moldova, through the National Institute for Innovation in Cybersecurity CYBERCOR, and the National University of Science and Technology 'Politehnica București'.

Conflicts of interest. The authors declare no conflicts of interest.

References

1. ISC2. 2024 Cybersecurity Workforce Study. ISC2: Clearwater, FL, USA, 2024. Available online: https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study (accessed on 20 February 2026).
2. ISC2. 2025 ISC2 Cybersecurity Workforce Study. ISC2: Clearwater, FL, USA, 2025. Available online: https://www.isc2.org/Insights/2025/12/2025-ISC2-Cybersecurity-Workforce-Study (accessed on 1 March 2026).
3. IBM Security. Cost of a Data Breach Report 2024. IBM: Armonk, NY, USA, 2024. Available online: https://www.ibm.com/reports/data-breach (accessed on 5 February 2026).
4. Gartner. *Market Guide for Cloud-Native Application Protection Platforms 2024*. Gartner: Stamford, CT, USA, 2024.
5. Combe, P.; Martin, A.; Di Pietro, R. (2016) To Docker or Not to Docker: A Security Perspective. *IEEE Cloud Computing 3*(5), 54–62. Available online: https://doi.org/10.1109/MCC.2016.100 (accessed on 11 February 2026).
6. Shu, R.; Gu, X.; Enck, W. A (2017) Study of Security Vulnerabilities on Docker Hub. In: *Proceedings of the ACM Conference on Data and Application Security and Privacy (CODASPY)* 2017, Scottsdale, AZ, USA, pp. 269–280. Available online: https://doi.org/10.1145/3029806.3029832 (accessed on 21 February 2026).
7. Rahman, M.; Williams, L.; Johnson, P. (2021) Security Analysis of Kubernetes Deployments. *IEEE Access 9*, 102401–102415. Available online: https://doi.org/10.1109/ACCESS.2021.3098280 (accessed on 02 February 2026).
8. Red Hat. State of Kubernetes Security Report 2024. Red Hat: Raleigh, NC, USA, 2024. Available online: https://www.redhat.com/en/resources/state-kubernetes-security-report (accessed on 15 February 2026).
9. Fairwinds. The Top 5 High/Critical Kubernetes CVEs of 2024. Fairwinds: Boston, MA, USA, 2024. Available online: https://www.fairwinds.com/blog/the-top-5-high-critical-kubernetes-cves-of-2024-have-you-patched-them-yet (accessed on 10 February 2026).
10. Upwind Security. Understanding & Securing Kubernetes: Key Vulnerabilities. 2025. Available online: https://www.upwind.io/glossary/what-are-kubernetes-vulnerabilities (accessed on 5 March 2026).
11. Fitzgerald, J.; Stol, K.-J. (2017) DevOps: A Software Architect's Perspective. *IEEE Software 34*(3), 16–20. Available online: https://doi.org/10.1109/MS.2017.62 (accessed on 04 February 2026).
12. Humble, J.; Farley, D.(2010) *Continuous Delivery: Reliable Software Releases through Build, Test, and Deployment Automation*; Addison-Wesley: Boston, MA, USA.
13. Myrbakken, S.; Colomo-Palacios, R.(2017) DevSecOps: A Multivocal Literature Review. *IEEE Access 5*, 135–148. Available online: https://doi.org/10.1109/ACCESS.2017.2762696 (accessed on 09 February 2026).
14. Association for Computing Machinery (ACM); IEEE Computer Society. *Computer Science Curricula 2013: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science*; ACM Press: New York, NY, USA, 2013. Available online: https://www.acm.org/binaries/content/assets/education/cs2013_web_final.pdf (accessed on 11 January 2026).
15. European Union Agency for Cybersecurity (ENISA). *Cybersecurity Skills Development in the EU*; ENISA: Heraklion, Greece, 2022. Available online: https://www.enisa.europa.eu/publications/cybersecurity-skills-development-in-the-eu (accessed on 02 January 2026).

16. Reeves, T. C. (2006) Design-Based Research and Educational Technology: Rethinking Technology and the Research Agenda. *Educational Technology & Society* *9*(1), 1–5. Available online: https://www.jstor.org/stable/jeductechsoci.9.1.1 (accessed on 25 February 2026).
17. National Institute of Standards and Technology (NIST). *Application Container Security Guide (SP 800-190)*; NIST: Gaithersburg, MD, USA, 2017. Available online: https://doi.org/10.6028/NIST.SP.800-190 (accessed on 25 February 2026).
18. Cloud Security Alliance (CSA); Microsoft. Cloud Native Application Protection Platform Survey Report 2023. CSA: Seattle, WA, USA, 2023. Available online: https://cloudsecurityalliance.org/research/topics/cnapp (accessed on 1 March 2026).
19. Dumbraveanu, R., Peca, L. (2022) E-learning in Developing ICT Skills of Future Engineers. In: 1st International Online Scientific Conference ICT in Life [online]: conf. proceedings, August 2022, Osijek, Croația. Osijek. 2022, pp. 86-95ISSN 2939-3930. Available online: https://www.researchgate.net/profile/a-Dumbraveanu/publication/362791467. Available online: (accessed on 22 February 2026).
20. Peca, L.; Țurcanu, D. (2023) Network security: Practical examples solved to be introduced in network security. Tehnica-UTM, Chisinau, 2023, pp. 7–232. Available online: https://www.researchgate.net/publication/370943880 (accesed on 6 February 2026).
21. Peca, L.; Dumbrăveanu, R. (2022) Learning Management System, Trends in E-Learning [In Romanian]. In: Proceedings of the National Scientific Conference with International Participation. Republican Conference of Teaching Staff. UST, Chisinau, Republic of Moldova, 2022. pp. 124-130. Available online: https://ibn.idsi.md/vizualizare_articol/153353 (accessed on 01 February 2026).

Citation: Peca, L.; Prisacaru, A.; Nistiriuc, P.; Cojocaru, S.; Dumitraşcu, M.; Călin, R. (2026). A lab-oriented curriculum model for cloud-native security automation: from image scanning to runtime policy enforcement. *Journal of Engineering Science*. 2026, 33 (1), pp. 70-80. https://doi.org/10.52326/jes.utm.2026.33(1).05.

Submission of manuscripts: jes@meridian.utm.md