Assurance in DevSecOps Pipelines

Marco Anisetti[1,3][0000−0002−5438−9467], Alex Della Bruna[1,2][0009−0000−6775−2897], and Giandonato Inverso[1]

[1] Università degli Studi di Milano, Milan, Italy
marco.anisetti@unimi.it, alex.dellabruna@studenti.unimi.it, giandonato.inverso@studenti.unimi.it
https://www.unimi.it
[2] Consorzio Interuniversitario Nazionale per l'Informatica, Rome, Italy
https://www.consorzio-cini.it
[3] Moon Cloud, Crema, Italy
marco.anisetti@moon-cloud.eu
https://www.moon-cloud.eu

Abstract. Today's data-intensive workflows executed in the continuum are increasingly designed using DevSecOps pipelines to cope with their complexity in terms of i) composition of tasks involved and ii) deployment procedures in the continuum. Security is becoming one of the prominent concerns to be addressed in this scenario, in most of the cases made of i) intrinsically vulnerable IoT devices, ii) sensitive data, and iii) wide use of ML. Although DevOps pipelines and CI/CD solutions are largely used, the DevSecOps manifesto is currently not fully adopted given the lack of solutions to embed security assurance controls in the Dev(Sec)Ops pipelines. In this paper, we present a platform to integrate security assurance in DevSecOps pipelines. Our contribution also includes a novel model for IoT/specific pipelines where the staging branch mimics the real IoT scenario using virtualization.

Keywords: Assurance · DevSecOps · Continuos Integration/Continuos Delivery

1 Introduction

Current DevOps technologies pave the way for a much more reactive and efficient data-intensive development process with unprecedented advantages in terms of time and deployment effort. However, they also pose numerous challenges in the integration of assurance techniques, which makes it difficult to have effective non-functional checks [5]. In the last decade, to address these challenges, DevSecOps [2] have come in place. While some literature works presented how to integrate assurance in DevSecOps [3,4], the full adoption of DevSecOps principles is still in its infancy and business-ready solutions are far from being available. In this paper, we propose an innovative solution to assess non-functional properties on DevSecOps pipelines using assurance controls with the goal of *i)* minimum adaptation effort for the developer and *ii)* providing the base structure for an efficient and scalable DevSecOps pipeline assurance process. We consider

a challenging IoT scenario where *i)* DevSecOps pipelines need to mimic IoT devices and *ii)* compliance to a set of non-functional properties is requested [7]. To achieve this goal, our approach integrates *i)* a IoT specific CI/CD staging system that closely mirrors the operational environment, *ii)* specific controls at each pipeline stage reporting assurance results on an external assurance platform featuring advanced data aggregation and analysis.

2 The DevSecOps Assurance Methodology

Our DevSecOps assurance methodology is articulated on three main components:

- `Moon Cloud`: an assurance platform to assess CI/CD pipelines. It implements *probes* (assurance controls) whose results, called *evidence*, are evaluated by compliance evaluation rules. For instance, a probe can search for vulnerabilities on a given target (e.g., source code) while the evaluation rule filters the vulnerabilities by severity. In case of severity higher than a threshold, the *probe* returns a negative output.
- `Injector`: a set of custom-built programs that provides the assurance capabilities to the DevOps process.
- `Pipeline`: the real target of the probes execution, hosted on a CI/CD provider.

Figure 1 shows the proposed assurance process. First, it first configures the evaluation rule on the Moon Cloud platform (1). Next, the Injector instruments the pipeline (2) generating the instrumented pipeline (3). The instrumented pipeline is executed and produces an artifact for every stage that needs to be assessed (4). Finally, the probe(s), triggered by the instrumented pipeline (5), connects to the CI/CD provider, analyzes the necessary artifacts (6), and writes the collected evidence (7). Evidence is then evaluated according to the evaluation rule returning a positive or negative output. The assurance execution report is finally available both on the pipeline stage and on the Moon Cloud dashboard.

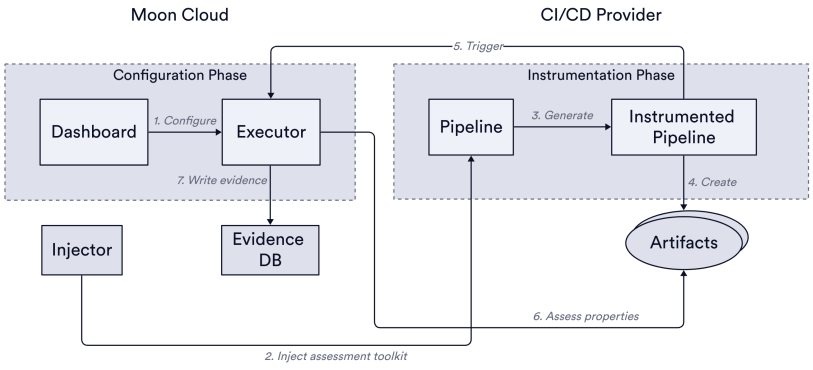

Fig. 1: Assurance Process

3 IoT-specific DevSecOps

IoT DevOps pipelines are commonly developed without taking into consideration security assurance. An inappropriate real/world staging phase can further worsen the situation, bridging upstream vulnerabilities directly into final operation environment, whose resolution often involves the manual intervention. To settle the issue, we injected a new assurance phase on each stage of the pipeline: it ensures the compliance at every pipeline stage. The resulting pipeline in Figure 2 is composed of the following stages:

Code commit: where the developer push code updates.
Static code analysis: executes a series static code vulnerability probes.
OCI image build: stage where the related container image are built from i) base image (usually external), ii) static code dependencies and iii) previously committed code.
OCI image analysis: assesses the vulnerabilities related to the built container image.
Staging: deploys beta software is to a pre-production environment. The software is executed in a VM which emulates real/world conditions.
Firmware analysis: assesses vulnerabilities related to the staging environment at bare-metal level, including the firmware. This step is completely automated thanks to virtualization.
Deploy: deploys final software to the operation environment.
Operation: continuously executes a set of *probes* against the operation environment [5].

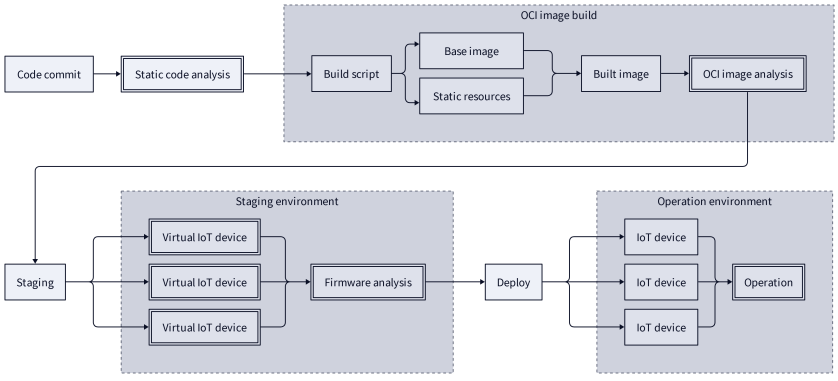

Fig. 2: Proposed IoT-specific DevSecOps pipeline

4 Discussion and Conclusions

We preliminarily evaluated the proposed approach leaving the discussion of the results in our future work. Our evaluation showed that our assurance methodology for IoT-specific DevSecOps pipelines generates insightful information which can significantly reduce the time needed to notice new vulnerabilities and trace back security events. The high modularity can consistently simplify traditional DevSecOps pipelines and speed up the transition to new security-conscious development approaches. For instance, modern ML applications strongly need to comply to regulations (i.e., EU AI Act [1,6]), from ML development to production. Finally, the decoupling between the pipeline and the assurance platform makes it possible to combine results from heterogeneous systems in the same data analysis tool, that is, Moon Cloud.

Acknowledgments. This work is partly supported by the project MUSA – Multilayered Urban Sustainability Action – project, funded by the European Union – NextGenerationEU, under the National Recovery and Resilience Plan (NRRP) Mission 4 Component 2 Investment Line 1.5: Strengthening of research structures and creation of R&D "innovation ecosystems", set up of "territorial leaders in R&D" (CUP G43C22001370007, Code ECS00000037). It is also partially supported by Università degli Studi di Milano via the program "piano sostegno alla ricerca" and "One Health Action Hub: University Task Force for the resilience of territorial ecosystems", – PSR 2021 – GSA – Linea 6.

References

1. Eu ai act: first regulation on artificial intelligence (2024), https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01_EN.pdf
2. Akbar, M.A., Smolander, K., Mahmood, S., Alsanad, A.: Toward successful devsecops in software development organizations: A decision-making framework. Inf. Softw. Technol. **147** (2022), https://www.sciencedirect.com/science/article/pii/S0950584922000568
3. Anisetti, M., Ardagna, C.A., Gaudenzi, F., Damiani, E.: A continuous certification methodology for devops. In: Proc. of MEDES 2019. Limassol, Cyprus (Nov 2019)
4. Anisetti, M., Bena, N., Berto, F., Jeon, G.: A devsecops-based assurance process for big data analytics. In: Proc. of IEEE ICWS 2022. Barcelona, Spain (Jul 2022)
5. Ardagna, C.A., Bena, N., Hebert, C., Krotsiani, M., Kloukinas, C., Spanoudakis, G.: Big data assurance: An approach based on service-level agreements. Big Data **11** (2023)
6. Floridi, L., Holweg, M., Taddeo, M., silva, j., Mokander, J., Wen, Y.: capai: A procedure for conducting conformity assessment of ai systems in line with the eu artifcial intelligence act. In: capAI (2022)
7. Judvaitis, J., Nesenbergs, K., Balass, R., Greitans, M.: Challenges of devops ready iot testbed. In: Proc. of IEEE/ACM MDE4IoT/ModComp@MoDELS. Munich, Germany (Sep 2019)