Journal of Harbin Engineering University
ISSN: 1006-7043
Vol 45 No. 9
September 2024

Shift-Left Security Integration: Automating Vulnerability Detection in Container Images

Pradeep Chintale, Rajashekhar Reddy Kethireddy,
Lead DevOps Engineer, SEI Investment Company, Downingtown, PA, USA, chintale.pradeep@gmail.com
Cleveland State University,Cleveland,Ohio, USA rajashekhar.kethireddy@gmail.com
Gopi Desaboyina, SEI Investment Company, Phoenixville , Pennsylvania, USA, gopidesaboyina@gmail.com

Abstract - Containerization completely changed the ways applications are being deployed and managed into an approach that is efficient and based on consistent delivery across various environments. It is true that as more containers are used, so do the requirements for strong security solutions. One of the crucial components of container Image security is identifying vulnerabilities in the images through automation.
Container images with all the required elements, including application code, dependencies, and runtime environment are the structural units of containerized applications. Such images are generally drawn from open or closed repositories, which can actually uncover applications to security flaws. Non-detected vulnerabilities in container images can result in extremely bad outcomes like data theft, system failure and service loss.

Introduction

Containerization completely changed the ways applications are being deployed and managed into an approach that is efficient and based on consistent delivery across various environments. It is true that as more containers are used, so do the requirements for strong security solutions. One of the crucial components of container Image security is identifying vulnerabilities in the images through automation.

Container images with all the required elements, including application code, dependencies, and runtime environment are the structural units of containerized applications. Such images are generally drawn from open or closed repositories, which can actually uncover applications to security flaws. Non-detected vulnerabilities in container images can result in extremely bad outcomes like data theft, system failure and service loss.

Enacting an automated vulnerability scanning of container images is a preventive approach that allows to view and neutralize possible security threats prior to making the application go live in production environments. As a result of integrating the container build and deployment pipeline with vulnerability scanning utilities, the organizations are enabled to carry out the continuous assessment of the images security posture.

Regulatory Landscape

Forming an automatic vulnerability scanner in the process of container image creation is emerging faster than ever as governments and corporations realize that the container ecosystem has to be kept secure. A number of authorities have established guidelines and standards for containerized application development and release to secure environments.

The National Institute of Standards and Technology (NIST) has developed the NIST Special Publication 800-190, which offers guidelines for container technology application security [1]. This document describes measures for container image security that are based on your vulnerability assessment and remediation processes.

The Center for Internet Security (CIS) came up with the CIS Kubernetes Benchmark which is a document that describes a secure Kubernetes environment and also covers guidelines for container image vulnerability management [2].

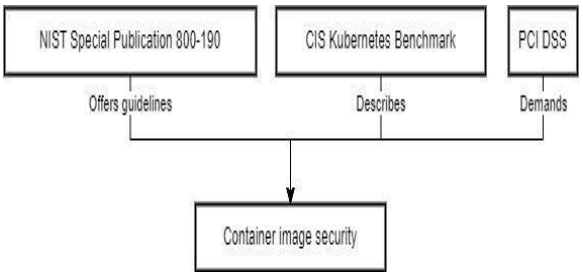

Figure 1: Container Image Creation

(Source: Self-created)

PCI DSS demands from the organizations that use payment card data to apply hardened security measures, including vulnerability remediation for container images that are used in their environments.

Compliance Measures

The adherence to regulatory rules and industry-leading practices are very necessary and should be taken into consideration while implementing the automated detection of vulnerabilities in container images. The organizations have to develop a comprehensive approach that would address different types of vulnerabilities, dis-function, policies, process, and technical mechanisms [3]. In this part this will concentrate on the main compliance measures that enterprises should undertake to create a useful and compliant vulnerability management program for their containerized environments.

First, an organization should establish and implement a comprehensive Vulnerability Management Policy which describes precisely the processes, roles, and responsibilities for the discovery, assessment, and removal of vulnerabilities in container images. The policy should encompass the criteria for risk assessment and risk ranking, as well as acceptable risk levels. It should also have clear deadlines for vulnerabilities elimination and classification in accordance with the assigned risk levels. With having a clear security policy, organizations will be certain of applying a continued and regular approach to vulnerability management within their containerized environment.

A key critical requirement here is the application of automated vulnerability scanning tools during the container build and deployment pipeline [4]. These tools should have been integrated into a system where the containers monitor and assess images for known vulnerabilities. Organizations should use industry-standard vulnerability databases and sources, like NVD (National Vulnerability Database) and seller-specific alerts, to have full coverage of possible holes. It is imperative to set these scanning tools up to auto scan newly or updated container images thus updating the security posture.

Then once the vulnerabilities are identified the organizations should develop a solid vulnerability removal process. This operation must include specific procedures that will remediate discovered weaknesses, including patching, updating, or rebuilding images with known vulnerabilities. Maintaining version control and change management is mandatory for following and documenting remediation steps taken to ensure traceability and auditability [5]. Besides, it is advisable to enact a checkpoint process for retesting and revalidating remediated container images before deployment to make sure that remediation efforts are effective and there are no new vulnerabilities or problems caused.

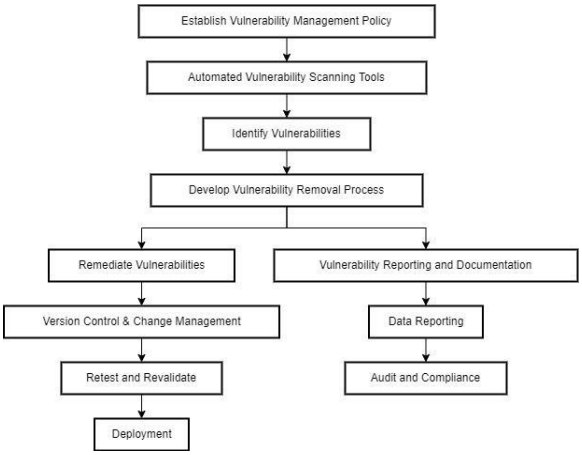

Figure 2: Compliance Measures Steps

(Source: Self-created)

Making this a significant part of compliance, along with complete vulnerability reporting and documentation, also plays an important role. Organizations need to have mechanisms for reporting data that will help identify the level of the vulnerabilities, risk level and actions taken to resolve the issues identified. Such reports must be subject to and conducted by competent bodies such as security

teams, application owners, and compliance officers [6]. Routine reporting and accounting not only ensures the right judgment but also creates a backup text that can be used for audits and compliance.

To strengthen compliance, organizations therefore should consider implementing solid access controls and separate duties of the workforce. This entails limiting access to container image as well as linked resources to only authorized personnel, using proper role-based access controls, and imposing safe authentication and authorization mechanisms. In addition, organizations can adopt the process of providing secure practices of software supply chain such as the validation and verifying container images from trusted sources to reduce risk of introducing vulnerability through third-party dependency or component.

Regular information security auditing and reviewing are some indispensable compliance measures. Organizations should run periodic evaluations of their working environments with containerization that include vulnerability scanning, penetration testing, and compliance audits [7]. These assessments should value the actual results of discussed vulnerability management procedures, highlight the problems and suggest the ways of their improvement.

Additionally, organizations must be involved in the training and awareness campaigns to guarantee that the employees concerned with the construction, deployment, and maintenance of containerized applications are informed about vulnerability management best practices, compliance regulations, and their roles and responsibilities within the general security framework.

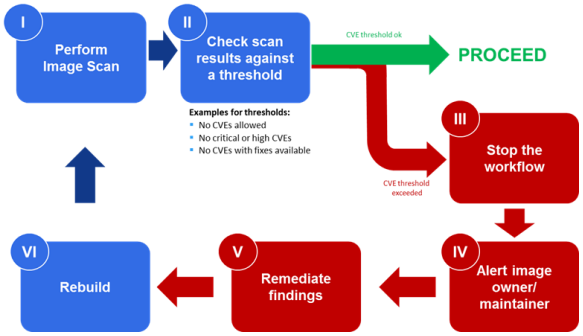

Figure 3: Container Vulnerability Management

(Source: https://www.medium.com)

Finally, it's advisable that the organizations keep up to date with the regular changes in regulatory compliance, industry standards, and best practices that govern vulnerability in the containerized environment [8]. This needs keeping track of regulatory bodies, industry groups, and security forums on a daily basis, for any updates, advisories or potential new threats. This ensures the closeness of industry peers and the experts as well which can provide better ideas and also facilitate sharing of best practices for improving vulnerable management regulatory compliance.

Through the proper implementation of these compliance measures, companies will be able to develop and enforce a robust and compliant vulnerability management process for their containerized environments. This approach not only improves the overall security stance but also shows the dedication to utilizing the compliance standards and industry best practices, which aim to persecute the sensitive data individual trust and reduce the risks associated with the security vulnerabilities which exist in the container images.

Building up a strong vulnerability remediation program involves more than just installing technical controls and processes. One should take into consideration a comprehensive strategy encompassing organizational policies, governance structures, continuing observation and improvement [9]. With the aim of adhering to the regulatory standards and the industry best practices, organizations will have to concentrate on the creation and action of thorough vulnerability management policies.

The policies should serve as the basis for the entire container vulnerability management program which define the roles, responsibilities, processes, and procedures that are followed for identifying, assessing, mitigating and reporting of vulnerabilities residing in the container images. The policies should state the criteria for risk assessment, risk classification, and risk tolerance, and should specify deadlines for vulnerability remediation based on the

risk level. Organizations will be able to carry out an aligned and standardized approach to risk management across their containerized environment if their policies are well-defined. This ensures fulfilling legislation and industry standards.

Figure 4: Vulnerability Management Process

(Source: www.g2.com)

Moreover, organizations should develop a formally established governance structure to supervise the introduction and enforcement of vulnerability management processes. This can be accomplished by establishing the cross-functional vulnerability management committee or a task force whose membership will be represented by different stakeholder groups namely security, operations, development, legal, and compliance teams [10]. A committee should be accountable for determining and analyzing vulnerability management policies, allocating roles and responsibilities, defining risk tolerance levels and prioritization criteria, ensuring resource adequacy, assessing the program's effectiveness, fostering interdisciplinary collaboration, and conducting formal escalation and reporting.

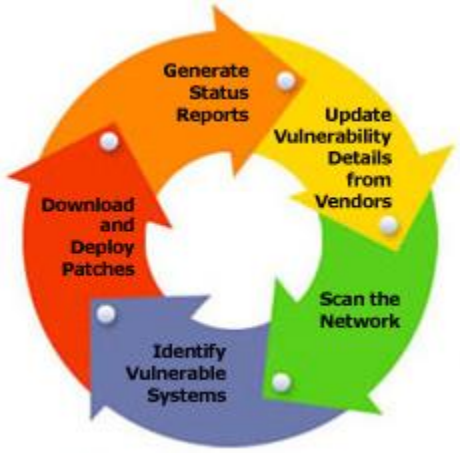

Figure 5: Vulnerability Patch Management Process

(Source: www.manageengine.com)

Moreover, it is essential for organizations to establish complete and detailed guidelines which will be utilized as procedures for vulnerability patch management activities. These techniques are expected to be inclusive of all vulnerability management processes such as vulnerability identification along with the assessment, risk assessment and prioritization methodology, vulnerability remediation procedures, vulnerability reporting and documentation, access control and segregation of duties, secure software supply chain, security training and awareness programs, and incident response and recovery practices.

Comprehensive monitoring and constant enhancement are fundamental steps in the process of complying with regulatory standards and industry best practices. Organizations need to establish the review process of their vulnerability management program periodically in order to improve its effectiveness and point the weakness. Vulnerability management can be accomplished via constant security audits, running through various industry forums and regulatory bodies, collaborating in peer-sharing forums, analyzing and reviewing vulnerability data and metrics, getting to the root cause of security incidents, and continuously reviewing and updating vulnerability management tools, processes, and procedures.

The organizations that are looking for assurance from third parties can show that they have strict security measures and that they do observe standards [11]. This includes the certification or endorsement by recognized bodies such as NIST Cybersecurity Framework, ISO 27001, or the Center for Internet Security (CIS) Benchmarks. Besides using third-party security firms or independent auditors to conduct complete assessments of vulnerability management programs and give objective appraisals, recommendations and advice for improvement is another approach an organization can choose.

Effective vulnerability management is not about events anymore but is a continuous process that follows recommendations and adapts them to changing threats and the regulatory environment. Organizations must maintain a security and compliance culture by conducting awareness and training programs for employees working with containerized apps, which include those involved in development, deployment, and maintenance. These systems must inform workers about the significance of the vulnerability management, the role of the employee and failures to comply. In addition, employees must be made aware of possible consequences.

Collaboration and information sharing also include protection of privacy and data handling. It is a must for organizations to be active members of industry forums that gather to discuss newest threats, best practices when it comes to vulnerability management for containerized systems and lessons learned elsewhere. This teamwork can help the experts gauge the effectiveness of applied remedies and share them with each other so as to strengthen the compliance.

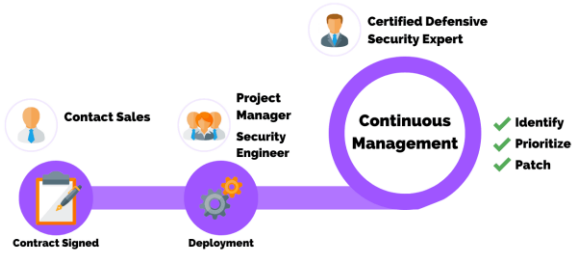

Figure 6: Effective Vulnerability Management

(Source: www.purplesec.us)

Additionally, organizations have to develop efficient documentation and record keeping practices to ensure that the audit trails are impeccable and they can store the evidence of compliance. This covers noting vulnerability management policies, procedures, risk assessments, remediation steps, and variations or reprieves granted to any party [12]. The consistent reporting and documentation would not only make informed decision-making easier but also enable historical retrospect useful for auditing and compliance.

These thorough conformity measures render a robust and conforming vulnerability management program available for a given containers' environment. Beyond everyday security, the approach shows the commitment to respect regulations and industry standards and which, in turn, safeguard sensitive data, keep the customer trust and decrease the likelihood of the vulnerabilities in container images to affect negatively.

Governance and Oversight

Governance structure is the key factor for succeeding with infrastructural elements related to vulnerability management and standards in the containerized ecosystem. The best plan is creation of a dedicated cross-functional vulnerability management committee or task force which supervises the implementation, application, and optimization of the vulnerability management policies and processes. The committee needs to consist of the members from diverse stakeholder groups, such as security, operations, development, legal, and compliance, and this will allow for promotion of collaboration and effective decision making.

Policy definitions and review on vulnerable management must be a priority for this committee and they should make sure that their policies are always aligned with evolving regulatory requirements and industry best practices. The committee shall therefore outline the features that each of the teams require for the identification, assessment, remediation and reporting on the different teams and

departments for effectiveness and accountability [13]. Another task of the committee will be to determine what tolerance of risk for the system is appropriate and its prioritization criteria for vulnerability remediation, based on the factors such as severity, exploitability and potential impact.

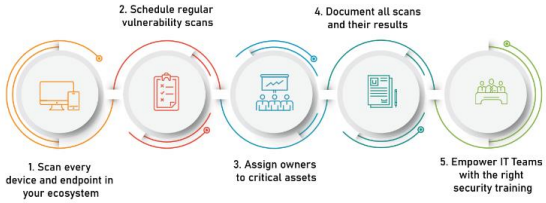

Figure 7: Vulnerability Management Governance

(Source: www.spiceworks.com)

In addition, the committee should make certain that sufficient resources, including experts, finances, and technical equipment, are assigned for these activities on vulnerability management. This will allow the organization to ensure that it has all the important capabilities needed to adequately identify, evaluate and remediate vulnerabilities in due time. Constantly assessing and reporting the overall program effectiveness, including metrics like time-to-detection, time-to-remediation and vulnerability backlog, should not be neglected, since it shows us what improvements can be made and what is considered to be compliant.

Setting up a well-defined escalation and reporting process as a further aspect of governance and oversight is important. The vulnerability management committee shall outline the clear thresholds of escalation of vital vulnerabilities with their remediation plans to senior management and relevant stakeholders. This process is a transparency-boosting force, and pressing issues can be dealt with in a timely manner, which is very important in the mitigation of high-risk vulnerabilities.

Optimal Methods and Suggestions

To improve vulnerability detection and ensure compliance with regulations, organizations are advised to implement a layered approach that involves use of automated scanning, threat intelligence, and manual reviews. Introducing state-of-the-art scanning solutions from the industry not only into the build and deployment pipelines, but also in real-time, helps ensure continuous monitoring and vulnerability discovery. These tools should be customized to get notifications from systems updated with latest vulnerability databases and advisories of vendors to make them fully comprehensive.

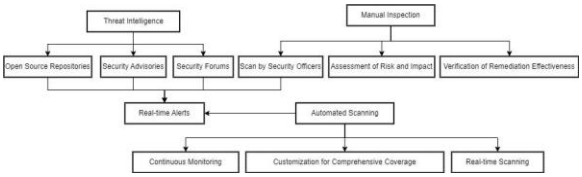

Figure 8: Suggestions

(Source: Self-created)

Alongside that, organizations can also make use of extra threat intelligence sources like open source vulnerability repositories, security advisories and security forums to remain informed about present vulnerabilities and respond to them proactively [14]. This enables real-time visibility into the security posture of container images and immediate alerts to involved parties once vulnerabilities or security gaps have been newly detected.

Whilst automation is indispensable, the manual inspection as well as validation should not be ignored in the vulnerability management procedure. This entails enlisting educated security officers to run scans, assess potential risk as well as impact of detected vulnerabilities, and verify effectiveness of remediation efforts. The integration of automated and human ways can lead to more accuracy and efficiency at the stage of discovering vulnerabilities and remediating.

Conclusion

Adherence to the regulatory frameworks and industry good practices makes up the main part of the deployment of automated vulnerability scanning in container images. The establishment of strong governance models, comprehensive policies and procedures, continuous monitoring and improving mechanisms, and using third-party verification and accreditation would allow organizations to show their dedication to secure activities and adherence to the regulations.

An approach that encompasses the policy level, technical controls, and real-life tailoring is a necessity in building a top-notch and compliant vulnerability management program. Creating security's culture, promoting collaboration and mutual sharing of information, as well as maintaining detailed records should always be the focus.

At the end of the day, this approach not only strengthens the cybersecurity stance of the organization but also safeguards the integrity of information, maintains user confidence, and prevents exposure to the risks of vulnerabilities that exist in container-based frameworks. Compliance should be viewed as a continuous process of unfailing efforts and devotion that are to be used for tracking and outpacing the emerging risks and complex regulatory environment changes.

Reference List

Journals

[1] Gonzalez, D., Perez, P.P. and Mirakhorli, M., 2021, October. Barriers to shift-left security: The unique pain points of writing automated tests involving security controls. In Proceedings of the 15th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM) (pp. 1-12).

[2] Jaisinghani, G., 2022. VULNERABILITY MANAGEMENT IN THE AGE OF CONTAINERS–A REVIEW. International Journal of Information Security (IJIS), 1(01).

[3] Voruganti, K.K., 2021. Implementing Security by Design practice with DevSecOps Shift Left Approach. Journal of Technological Innovations, 2(1).

[4] Rajapakse, R.N., Zahedi, M., Babar, M.A. and Shen, H., 2022. Challenges and solutions when adopting DevSecOps: A systematic review. Information and software technology, 141, p.106700.

[5] Kadri, S., Sboner, A., Sigaras, A. and Roy, S., 2022. Containers in bioinformatics: applications, practical considerations, and best practices in molecular pathology. The Journal of molecular diagnostics, 24(5), pp.442-454.

[6] Pinconschi, E., Bui, Q.C., Abreu, R., Adão, P. and Scandariato, R., 2022, July. Maestro: A platform for benchmarking automatic program repair tools on software vulnerabilities. In Proceedings of the 31st ACM SIGSOFT international symposium on software testing and analysis (pp. 789-792).

[7] Viitasuo, E., 2020. Adding security testing in DevOps software development with continuous integration and continuous delivery practices.

[8] Vakhula, O., Opirskyy, I. and Mykhaylova, O., 2023. Research on Security Challenges in Cloud Environments and Solutions based on the "Security-as-Code" Approach.

[9] Paprzycki, M., Ganzha, M., Wasielewska, K. and Lewandowski, P., 2021. DEVSECOPS METHODOLOGY FOR NG-IOT ECOSYSTEM DEVELOPMENT LIFECYCLE–ASSIST-IOT PERSPECTIVE. Journal of Computer Science and Cybernetics, 37(3), pp.321-337.

[10] Pendyala, V., 2020. Evolution of integration, build, test, and release engineering into devops and to DevSecOps. In Tools and Techniques for Software Development in Large Organizations: Emerging Research and Opportunities (pp. 1-20). IGI Global.

[11] Colotti, M.E., 2023. Enhancing Multi-cloud Security with Policy as Code and a Cloud Native Application Protection Platform (Doctoral dissertation, Politecnico di Torino).

[12] Orazi, G., Vallittu, K., Sainio, P. and Virtanen, S., 2020. Enhancing and integration of security testing in the development of a microservices environment.

[13] Jha, A.V., Teri, R., Verma, S., Tarafder, S., Bhowmik, W., Kumar Mishra, S., Appasani, B., Srinivasulu, A. and Philibert, N., 2023. From theory to practice: Understanding DevOps culture and mindset. Cogent Engineering, 10(1), p.2251758.

[14] Sojan, A., Rajan, R. and Kuvaja, P., 2021, November. Monitoring solution for cloud-native

DevSecOps. In 2021 IEEE 6th International Conference on Smart Cloud (SmartCloud) (pp. 125-131). IEEE.