Mitigating OWASP Top 10 Risks for Kubernetes with a Cloud-Native Response Engine

This research dissertation focuses on extending the principles of the OWASP Top 10 framework to address security challenges specific to Kubernetes, a leading container orchestration platform, by leveraging an open-source, cloud-native response engine – **Falco Talon**.

Author

Nigel Douglas | C00292053@setu.ie | (+353) 083 474 3639

Supervisor

Michael Gleeson.

Course / Institution

MSc Cybersecurity, Privacy and Trust – South-East Technological University [SETU]

01 Introduction

The OWASP foundation is fundamentally open source, which means the security community can contribute findings to the project where they see fit.

When adopting Kubernetes, we introduce new risks to our containerized apps and infrastructure, that wouldn't always be relevant to traditional monolithic application architectures. ***[1]***

The OWASP Kubernetes Top 10 is aimed at helping security practitioners prioritize the top 10 categorized risks specific to Kubernetes clusters

02 Literature Review

There are little to no references to OWASP Top 10 specific to Kubernetes in peer-reviewed indexes (eg: IEE Xplore, ACM)

Kernel introspection alone cannot ensure compliance with Kubernetes T10 controls. ***[2]*** Kubernetes Audit logs are required to compliment system calls from the Linux kernel.

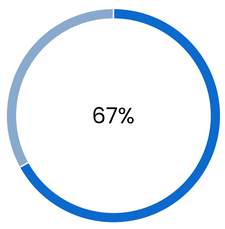
Closed-source technologies cannot aptly keep up with evolving risk frameworks such as OWASP Top 10 for Kubernetes. ***[3]***

03 Research Questions

1. How do the existing OWASP Top 10 controls perform with the unique security challenges presented by Kubernetes clusters?
2. What specific vulnerabilities in Kubernetes security do the existing OWASP Top 10 controls fail to adequately address?
3. How can we show that these vulnerabilities can be mitigated through a cloud-native response engine (in experiments) ?
4. How effective is the cloud-native response engine in improving overall Kubernetes security posture?

04 Methodology

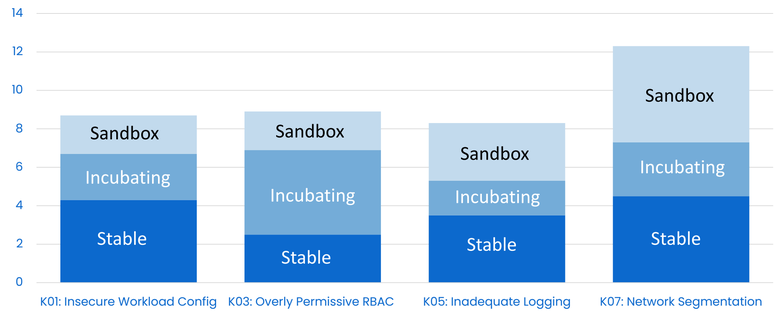
This research adopts a **mixed-methods approach**, combining both qualitative and quantitative techniques to address the research questions comprehensively.
The rationale behind this approach lies in the multifaceted nature of the research objectives, which require a nuanced understanding of existing security frameworks, practical experimentation, and empirical analysis.



By synthesizing key findings from the latest threat reports (beyond scope of available academic literature), we can identify gaps in the OWASP Top 10 project.

Propose new controls to the open-source OWASP Top 10 project based on those qualitative findings.

.



Author new Falco rules that address the proposed T10 controls while striving to minimize any potential False/Positive detections.
Rules are categorized into Stable (working with low False/Positives).
Incubating (working but still have false/positive detections).
Sandbox (not yet in a stable state and cannot be proposed to the project).

05 Results/Findings

1. The OWASP Top 10 framework for Kubernetes is still a long way from maturity. **[4]**
2. This research paper has already led to several accepted contributions to the OWASP Top 10 project for Kubernetes.
3. Falco Talon (the response engine for open-source Falco) provides a novel approach to enforcing the Top 10 controls in Kubernetes.
4. Since YAML is the language of Kubernetes, it makes sense that Falco and Talon should allow detections and response rules be written in the YAML – improving operational efficiency for DevOps engineers. ***[5]***

06 Next Steps

Overall, this dissertation serves as a call to action for greater collaboration, innovation, and community engagement in addressing cybersecurity challenges in Kubernetes environments.

By fostering a culture of continuous improvement and open collaboration, security researchers can collectively work towards a more secure and resilient cloud-native ecosystem.

By highlighting the Kubernetes Audit Plugin for Falco, we can demonstrate why Falco is the de facto standard for cloud-native intrusion detection while providing public rules to improve security coverage in Kubernetes.

Related Literature

1. Theodoropoulos, T.., (2023). Security in Cloud-Native Services: A Survey. Journal of Cybersecurity and Privacy. [online] 3(4), pp.758–793.: doi:https://doi.org/10.3390/jcp3040034.
2. Agarwal, S., (2022). Threat Detection and Response in Linux Endpoints. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9668567: IEEE [10.1109/COMSNETS53615.2022.9668567].
3. Salih, N.K. and Zang, T. (2012). Survey and comparison for Open and closed sources in cloud computing. [online] arXiv.org. doi:https://doi.org/10.48550/arXiv.1207.5480.
4. Grossman, J., (2017). The OWASP Top 10 — Response to the controversy from Jeff Williams. Medium.com: https://medium.com/@JoshCGrossman/the-owasp-top-10-response-to-the-controversy-from-jeffwilliams-d080f33ae1f.
5. Schmeling, B. and Dargatz, M. (2022). The Impact of Kubernetes on Development. Apress eBooks, pp.1–57. doi:https://doi.org/10.1007/978-1-4842-7942-7_1.