Title

Detecting Malicious Activities and Behavioral Analysis of Runtime Containers

Conference

HPE Parasparam 2024

Peer reviewed

Authors

Rohan C

Sana Behl

Publication Status

Submitted

Writing Sample Type

Technical White Paper

Detecting Malicious Activities and Behavioral Analysis of Runtime Containers

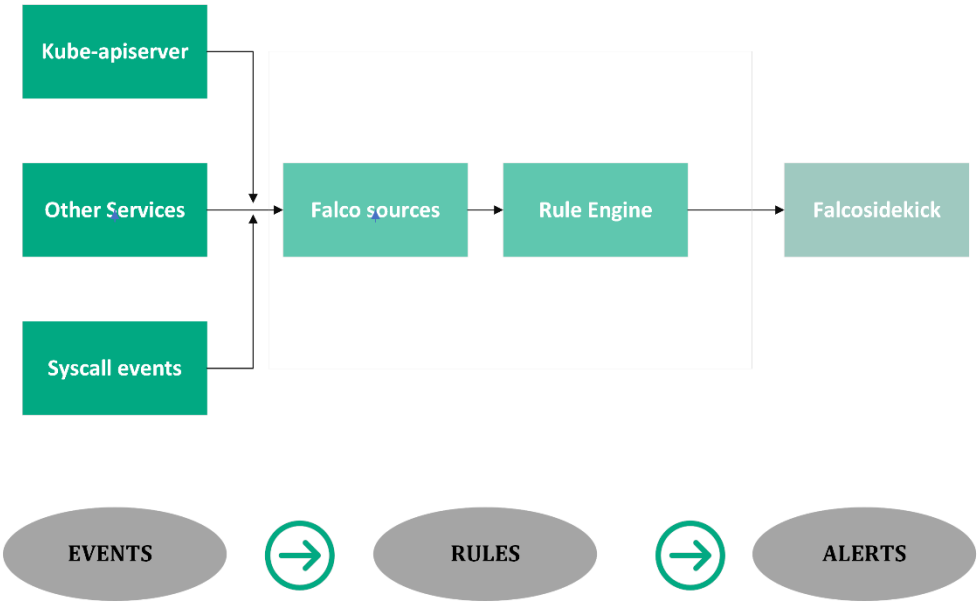
Rohan Chandrashekar, Sana Behl
Professional Services – Global Competency Center – CPAE and Cybersecurity
chandrashekar@hpe.com, sbehl@hpe.com

Abstract

This paper introduces an innovative solution for detecting malicious activities and performing behavioral analysis of runtime containers using Falco Sidekick. Falco, an open-source runtime security tool, monitors containerized environments for suspicious activities. Our unique integration of Falco Sidekick enhances this by forwarding security events to a custom-developed web UI and a Slack plugin for real-time alerts. This solution offers comprehensive visibility and immediate response capabilities, providing a novel approach to container security. It significantly improves the security posture of containerized environments by ensuring real-time alerting and easy monitoring, crucial for maintaining operational integrity and preventing security breaches.

Problem statement

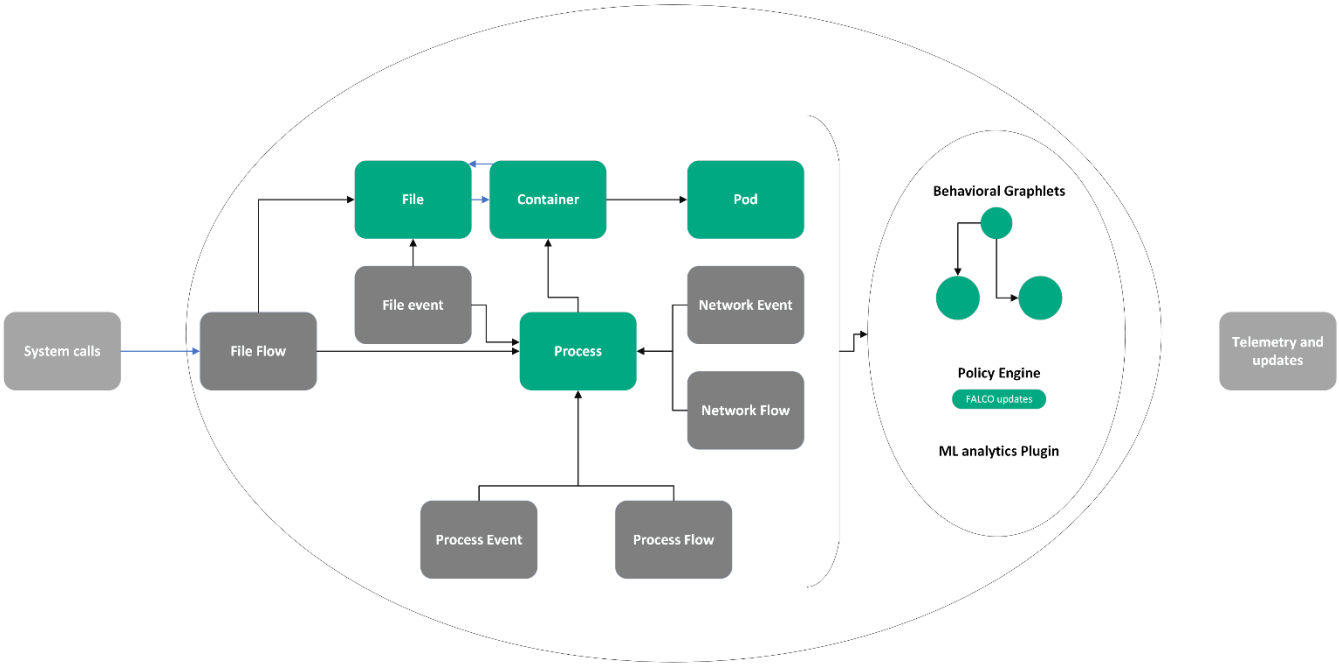
The widespread adoption of containerization has introduced significant security challenges, particularly in detecting and responding to malicious activities within containers. Traditional security solutions often fall short in dynamic, ephemeral container environments, making it essential to develop specialized security measures. Ensuring the security of runtime containers is critical from both technological and business perspectives to prevent breaches, data loss, and operational disruptions. For HPE, addressing these challenges is vital for safeguarding infrastructure and maintaining customer trust. Innovating in this area demonstrates HPE's commitment to providing advanced, secure solutions that protect customer data and applications.



Our solution

Our solution enhances security monitoring and incident response for runtime containers by integrating Falco with Falco Sidekick. The unique aspect of our innovation is the development of a custom web UI and a Slack plugin for real-time alerts. The web UI provides an intuitive interface for visualizing security events detected by Falco, while the Slack integration ensures immediate notification of critical incidents to relevant personnel. This dual integration

offers a seamless monitoring experience, enabling swift incident response and proactive security measures. Our contribution includes designing and implementing the web UI, configuring Slack integration, and streamlining the deployment process. This innovative approach ensures comprehensive security coverage, real-time alerting, and efficient monitoring, significantly improving the security posture of containerized environments.



Evidence the solution works

We validated our solution by deploying it in a controlled test environment with multiple containerized applications. Falco successfully detected various suspicious activities, including unauthorized file access and abnormal network connections. These events were promptly forwarded by Falco Sidekick to the custom web UI and Slack channel, providing real-time alerts and detailed insights. Screenshots of the working prototype illustrate the web UI displaying live security events and Slack notifications of critical incidents. This demonstrates the solution's operational effectiveness, real-time monitoring capabilities, and responsiveness, confirming its ability to enhance security in containerized environments.

Competitive approaches

Several solutions, such as Aqua Security and Sysdig Secure, offer comprehensive container security features. However, our solution's unique integration of Falco Sidekick with a custom-developed web UI and real-time Slack notifications provides distinct advantages in usability and immediacy of response. While other solutions may offer similar detection capabilities, our approach emphasizes real-time alerting and seamless integration, ensuring faster incident response and easier monitoring. These features are critical for maintaining robust security in dynamic container environments, giving HPE a competitive edge by offering an advanced, integrated security monitoring solution that is both effective and user-friendly.

Current Status

The solution is currently in the prototype stage, with successful implementation in a controlled test environment. The custom web UI and Slack integration have been developed and tested, providing real-time security event monitoring and alerting. We are now refining the solution for scalability and reliability, preparing it for deployment in more extensive, production-level environments. Initial feedback indicates strong potential for enhancing container security and operational efficiency. Continued development efforts are focused on optimizing performance and ensuring robustness in varied real-world scenarios, positioning the solution for broader adoption

within HPE's infrastructure and services.

Next steps

Future developments will focus on scaling the solution for large-scale deployments and integrating additional alerting endpoints to cater to diverse operational needs. Enhancing the analytical capabilities of the custom web UI will provide deeper insights into security events and trends, enabling more proactive security measures. Further work will involve rigorous testing in varied real-world environments to ensure robustness and reliability. Ultimately, this solution aims to become an integral part of HPE's security offerings, providing customers with cutting-edge tools for safeguarding their containerized applications and ensuring the highest levels of security and operational integrity.

Acknowledgements

We would like to express our sincere gratitude to Anand Chettri for his invaluable guidance, insightful suggestions, and continuous encouragement throughout the process. We are deeply thankful to Sudip Mondal and Ashutosh Pattanayak for their expertise and critical feedback, which greatly enhanced the quality of this work. We extend our appreciation to Nishith Kattupunathil for his invaluable mentorship, which was crucial to the development of this paper. Lastly, we are grateful to Anil NV for his support and guidance. Their contributions were indispensable to the development of this paper, and we are deeply appreciative of their support and collaboration.

References

[1] Salamero, Jorge. "Kubernetes runtime security with falco and sysdig." (2019).

[2] Gantikow, Holger, Christoph Reich, Martin Knahl, and Nathan Clarke. "Rule-based security monitoring of containerized workloads." SCITEPRESS-Science and Technology Publications, 2019.