INTISARI

MONITORING KEAMANAN *RUNTIME* PADA KUBERNETES MENGGUNAKAN FALCO

Ryan Fadhillah
20/457221/SV/17668

Penggunaan Kubernetes sebagai platform manajemen kontainer telah semakin meluas dalam beberapa tahun terakhir. Seiring dengan pertumbuhan penggunaan Kubernetes, keamanan menjadi isu krusial yang perlu diperhatikan secara serius. Deteksi ancaman pada fase *runtime* merupakan kapabilitas keamanan Kubernetes paling penting untuk dimiliki. Hal ini dikarenakan keamanan pada fase *runtime* merupakan garis pertahanan terakhir dalam sebuah sistem keamanan. Untuk mengatasi masalah tersebut, penelitian tugas akhir ini berfokus pada pengembangan alat *monitoring* keamanan *runtime* menggunakan Falco. Selain itu, Tugas Akhir ini juga mengembangkan metode untuk melakukan *tuning rules* untuk meningkatkan kapabilitas deteksi dari *rule default* Falco. Proses pengujian kapabilitas deteksi dilakukan terhadap 3 skenario serangan yang termasuk kedalam daftar resiko yang ada pada OWASP Top 10 *Cloud-Native Application Security*, di antaranya yaitu *Remote Code Execution* (RCE), *Exfiltration using common linux binaries* dan *privileged container*. Melalui proses *tuning* terhadap beberapa *rule* sesuai dengan skenario pengujian, Tugas Akhir ini berhasil meningkatkan efektivitas deteksi terhadap *malicious activity* pada lingkungan Kubernetes. Hal ini memberikan kontribusi signifikan bagi organisasi yang ingin mengimplementasikan Falco dalam mengamankan fase *runtime* pada infrastruktur Kubernetes.

Kata Kunci: Kubernetes, *Runtime Security*, Falco, *Tuning rule*, OWASP Top 10 *Cloud-Native Application Security*

ABSTRACT

RUNTIME SECURITY MONITORING IN KUBERNETES USING FALCO

Ryan Fadhillah
20/457221/SV/17668

The use of Kubernetes as a container management platform has significantly increased in recent years. With the growth of Kubernetes usage, security has become a crucial issue that must be taken seriously. Threat detection during the runtime phase is the most important security capability that Kubernetes should possess. This is because runtime security serves as the last line of defense in a security system. To address this issue, this final project focuses on developing a runtime security monitoring tool using Falco. Additionally, this project develops methods for tuning rules to enhance the detection capabilities of Falco's default rules. The detection capability testing process is conducted against three attack scenarios included in the OWASP Top 10 Cloud-Native Application Security risks, including Remote Code Execution (RCE), exfiltration using common linux binaries, and privileged container. By tuning several rules according to the testing scenarios, this project successfully improves the detection effectiveness of malicious activities in a Kubernetes environment. This significantly contributes to organizations that aim to implement Falco for securing the runtime phase in their Kubernetes infrastructure.

Keywords: Kubernetes, Runtime Security, Falco, Rule Tuning, OWASP Top 10 Cloud-Native Application Security