ABSTRACT

VULNERABILITY MANAGEMENT ANALYSIS ON CONTAINER DOCKER USING AQUASEC AND ANCHORE BASED ON *CYBER RESILIENCE REVIEW* (CRR) STANDARDS

By

MILENIA ARI OKTAVIANA

SID : 1202184238

One of the most widely used container technologies to provide IT services is Docker. The vulnerability in container technology, namely Docker, requires special management. Management of this vulnerability can be done technically with a software vulnerability scanner and standard Cyber Resilience Review (CRR) guidelines. Experiments were carried out with Aquasec and Anchore scanners that performed vulnerability scanning on two Docker Images systems. The two vulnerable systems have different versions, namely version – 1 and version – 2. The software elements in version – 2 have a higher versioning level than version – 1. Experimental data in the form of vulnerability reports are analyzed based on Cyber Resilience Review (CRR) which focuses on four stages namely Define a Strategy, Develop a Plan, Implement the Capability, Assess and Improve the Capability. So that the results of Category Vulnerability are obtained, namely 30 Closed Vulnerability, 10 Open Vulnerability, and 13 Newly Vulnerability. Continuation of this research can use aspects of Patch Management with more varied software tools.

Keywords: Docker, *Vulnerability*, *Scanner*, *Cyber Resilience Review* (CRR)