Mestrado em Engenharia de Tecnologias e Sistemas Web

Sistema de Monitorização de Segurança de Containers

Vladimir Kaznacheev

Domingos Martinho

RESUMO

Este trabalho teve como objetivo final monitorizar os parâmetros de segurança e o seu estado em ambientes de container construídos em diversas tecnologias conhecidas. Para mostrar que comprar equipamentos de proteção caros não é a única maneira de atender às necessidades de segurança, é mais importante desenvolver as competências da equipe.

PALAVRAS-CHAVE

Cíbersegurança, containers, docker, monitorização, frameworks.

OBJETIVOS

A segurança cibernética pode ser alcançada por meio do desenvolvimento sistemático, mas os desenvolvedores precisam estar cientes desses riscos e problemas de segurança. Se a segurança cibernética for fornecida após a conclusão do desenvolvimento, os sistemas serão construídos de forma insegura com bugs difíceis de corrigir. As organizações estão contratando uma infinidade de especialistas em cibersegurança que foram treinados e certificados nas áreas de segurança de computadores e redes.

METODOLOGIA

Para registrar os resultados do estudo, bem como demonstrar claramente os objetivos e diretrizes deste trabalho, criarei um protótipo de sistema de monitorização de segurança de containers Docker. Este parágrafo descreve os métodos usados para desenvolver o protótipo. Como base metodológica foi escolhido o Scrum. Os principais motivos da escolha Scrum foram. O backlog do protótipo contém uma lista dos seguintes itens, que também foram priorizadas.

M Must have	Desenvolvimento de modelo de ameaça Instalação e configuração baseado do Photon OS Definir sensores e APIs para coletar uma coleção de dados de segurança Criação um ambiente de teste de microsserviço baseado no Docker Desenvolvimento o code de master-container Montagem de todos os elementos na versão alfa Teste funcional e teste de produtividade Fixes de bugs
S Should have	Programação de algoritmos para encontrar anomalias de segurança em contauners Desenvolvimento do frontend React
C Could have	Estudar a documentação do Python SDK for Docker Processamento e análise profunda dos dados coletados
W Won't have	Suporte Alibaba, AWS, Azure

RESULTADOS

A investigação mostra que a monitorização de segurança em tempo real é mais eficaz para trazer a segurança dos sistemas de informação a um nível aceitável do que a monitorização periódica e o uso das configurações fornecidas pelas plataformas/sistemas standard. Os resultados qualitativos mostraram que alguns profissionais de segurança cibernética tinham dúvidas, confiando apenas nas propriedades do gráfico visual. No meu estudo, também confirmei a presença de um grande número de vetores de ataque e os benefícios da visualização.

CONCLUSÃO E DISCUSSÃO

Novos desafios e problemas de cibersegurança nos obrigam a pesquisar as novas formas de proteger os dados. Entre eles está a compra de novas ferramentas de desenvolvedores conhecidos neste campo. No entanto, também pode considerar desenvolver seu próprio sistema de monitoramento, que posteriormente pode ser integrado ao CI/CD e servir como um contador de ameaças para o DevSecOps. Como resultado da pesquisa, respondemos de forma inequívoca à questão principal sobre a automatização da recolha de dados relacionadas à segurança cibernética de containers.Com a ajuda do uso de ferramentas próprias desenvolvidas e ferramentas open source comprovadas, uma resposta positiva também foi dada à visualização dos dados coletados.

ESTADO DA ARTE

À medida que mais processos de desenvolvimento migram para a nuvem, é fundamental validar a segurança das imagens extraídas de vários repositórios. Brady et. al, (2020) descrevem um sistema contínuo de alto produtividade e implantação contínua (CI/CD) que pressupõe que a segurança do Docker ocorre durante todo o ciclo de desenvolvimento de software. Os autores apresentam imagens com vulnerabilidades e medem a eficácia de sua abordagem para detetar e identificar vulnerabilidades e ameaças à segurança. Além disso, eles usam a análise dinâmica para avaliar a segurança dos containers do Docker de acordo com seu comportamento.

Sultan et. al (2019), detalham os princípios básicos da virtualização baseada em containers e fornecem vários exemplos de tecnologias de container. Em seguida, os autores fornecem uma análise detalhada da literatura sobre segurança e soluções de containers. Como resultado do desenvolvimento e especificação de um modelo de ameaça, eles identificaram os vetores de ataque mais prováveis para containers e criaram quatro casos de uso genéricos que devem cobrir os requisitos de segurança em um ambiente de ameaças de container-host. Esta é uma investigação muito poderosa e profunda, que tomei como base teórica para minha dissertação.

Outro estudo importante para o meu trabalho foi publicado por Tunde-Onadele et. al, (2020) que fornece um estudo da eficácia de vários esquemas para detetar vulnerabilidades para containers. Especificamente, eles implementam e avaliam um conjunto de esquemas de deteção de vulnerabilidades estáticos e dinâmicos usando 28 explorações de vulnerabilidades do mundo real que são amplamente distribuídas em imagens Docker.

O estudo de Sadique e Cassell (2021) é o que mais se aproxima do meu estudo, especialmente em relação ao problema declarado e ao método de solução semelhante que o pesquisador deveria resolver. E os ataques cibernéticos se tornaram um problema. Para se proteger contra eles, a troca de informações sobre segurança cibernética e a visualização de ameaças cibernéticas foram identificadas como importantes tópicos de pesquisa. Sadique e Cassell (2021) desenvolveram a plataforma CYBersecurity information Exchange with Privacy (CYBEX-P), que implementa desenvolvimentos em ambas as áreas como uma ferramenta de segurança colaborativa acessível.

BIBLIOGRAFIA

Ahmad Imtiaz, S. S. (2019). Container Security: Issues, Challenges, and the Road Ahead. IEEE Access.

Kelly Brady, S. M. (2020). 10th Annual Computing and Communication Workshop and Conference (CCWC). Docker Container Security in Cloud Computing. Las Vegas: IEEE.

Olufogorehan Tunde-Onadele, J. H. (2020). IEEE International Conference on Cloud Engineering (IC2E). A Study on Container Vulnerability Exploit Detection. Prague: IEEE .

Farhan Sadique, A. C. (2021). 2021 IEEE 20th International Symposium on Network Computing. Sharing is Caring: Optimized Threat Visualization for a Cybersecurity Data Sharing Platform . Boston: IEEE.

CONTACTOS

vnkazna@gmail.com