



SFSCON 2023

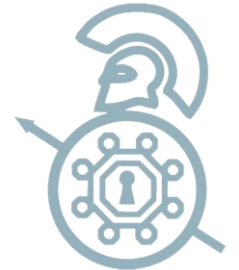
Containerization, micro-services in real life and Cybersecurity

Carlo Falciola

X: @CarloFalciola

carlo.falciola@exprivia.com

Bozen/Bolzano, 8 November 2024





Carlo Falciola

I manage Cybersecurity Delivery Services for Exprivia S.p.A..

More than 30 years of experience in Information Technologies, 20 of them helping organizations to increase their protection.

Some, little experience in the past within OOSS, with some years of collaboration with the OLPC Sugarlabs initiative back in the past.

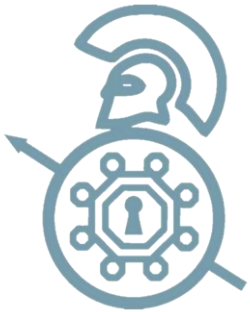
The team I'm managing is focused mostly into delivery of projects and consultancy in Cybersecurity (Technical) Governance, Identify and Prevention domains

We design and implement solutions that range from Security Assessments, Cybersecurity Compliance & Risk Management, Identity Security, Attack Surface management & Data Protection.



Summary

We'll try to briefly discuss how microservices architectures and containerization impact cybersecurity practises, which are the needed changes in approach, strategies and tooling



Cybersecurity: to be on the same page(s)

Nowadays Cybersecurity is wide and articulated, none of his several aspects can be ignored basically by anyone.

NIST v2.0 Cybersecurity Framework (CSF)



6 Main Functions
23 Categories
108 Subcategories

OOSS & Cybersecurity

Cybersecurity is a compulsory, tough and expensive task for all organizations of any size

Every organization must learn to make the best use of available resources in order to maximize their effectiveness and reduce risk

Cybersecurity is highly dynamic, continuously changing environment

The OOSS community made of developer, maintainer & adopter is not immune of this...



What are microservices: and what they mean for cybersecurity?

From the standpoint of Cybersecurity
Microservices are significant:

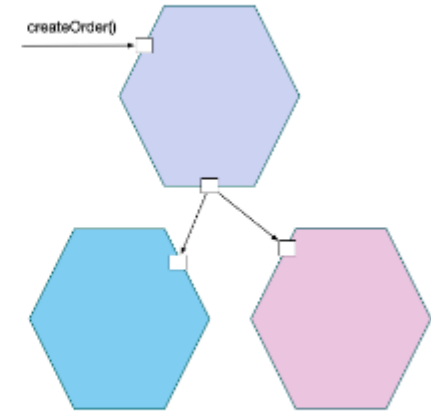
- Not-Human Identity
- Volatility - efimeral
- Inter-process and inter-machine communication
- Data exchange communication

What are microservices?

Microservices - also known as the **microservice architecture** - is an architectural style that structures an application as a collection of two or more services that are:

- Independently deployable
- Loosely coupled

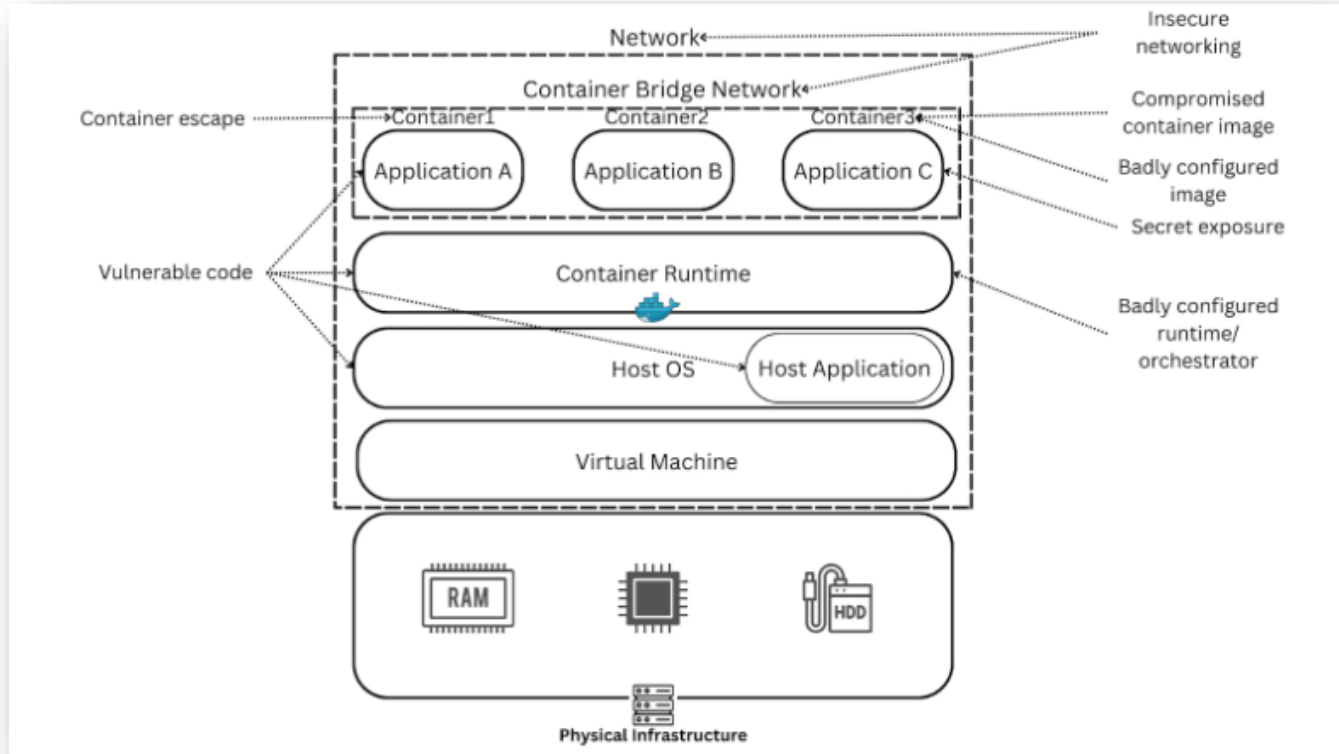
Services are typically organized around business capabilities. Each service is often owned by a single, small team.



microservices.io

Container Security

The Container threat model



Container Security Tools

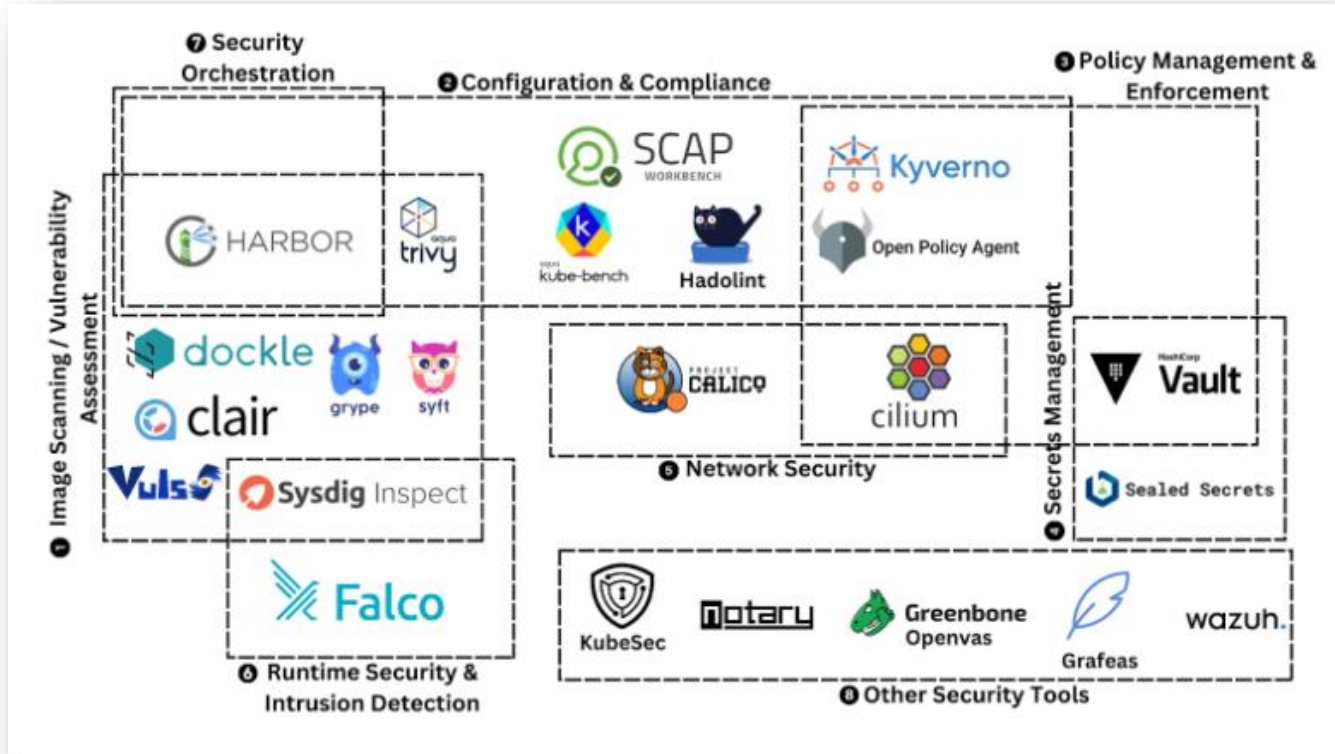
Container Security Tools belongs to different interleaved categories:

- Image Scanning/Vulnerability Assessment
- Runtime Security & Intrusion detection
- Configuration & Compliance
- Policy Management & Enforcement
- Network Security
- Other



Container Security & OOSS

Some Available Tools



Microservices «logical» security

A microservices based architecture is made of many components that interact each other exchanging relevant and sometimes sensitive data. Any component need to manage the question “*may x do y?*”

The OWASP organization (<https://owasp.org/>) has a very interesting “*Microservices Security Cheat Sheet*” (https://cheatsheetseries.owasp.org/cheatsheets/Microservices_Security_Cheat_Sheet.html) that address, describe and compare approaches and pattern related to authentication and authorization in microservices architectures:

- Edge Level Authorization
- Service-level Authorization



The OWASP guide also give recommendations on how to implement authorization strategies based on the concept of “defense in depth” and introduce the concept of “Authorization Policy”



Some conclusions

- Cybersecurity in microservices based Architectures has different needs
- Containers need continuous monitoring and vulnerability scanning both at configuration and operational level.
- Networking is more pervasive and abstracts from the physical/appliance layer
- Identity management assumes a key role and fine granularity



Grazie per l'attenzione

Segui @CarloFalciola
[linkedin.com/in/carlo-falciola-6aa18a](https://www.linkedin.com/in/carlo-falciola-6aa18a)



www.exprivia.it

Diritti di autore e copyright

Questo documento è proprietà esclusiva della società Exprivia S.p.A e non può essere riprodotto, anche in forma parziale, senza un'autorizzazione scritta della società stessa.