SFSCON 2023

Opensource to help increase organizations Cybersecurity posture

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

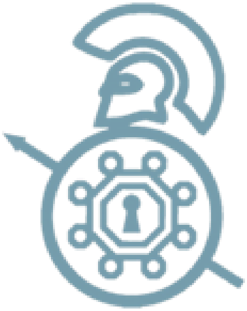
Carlo Falciola

X: @CarloFalciola

carlo.falciola@exprivia.com

Bozen/Bolzano, 10 November 2023

Agenda



1. whoami
2. Cybersecurity for Opensource
3. Secure Development & Maintenance for OOSS
4. Opensource for Cybersecurity
5. A Thought Task
6. An Opportunity
7. Conclusions

whoami

Carlo Falciola

I’m Cybersecurity Delivery Services Manager 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.

OOSS & Cybersecurity

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

.

La Cybersecurity is highly dynamic, continuously changing enviroment

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

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

Secure Development for Opensource

But there aren’t any virus for Linux!

And so what?

There are some many other ways Linux and OOSS can be compromised and weaponized against organizations….

Only one name to remember: Log4J

Reputation of OOSS can be heavily impacted by cybersecurity incident carried on leverage even a single critical vulnerability….

Cybersecurity and OOSS Development

Any OOSS project must be developed with security in mind, otherwise it will remain unused or counterproductive

What's is needed to start produce and deliver code that is reasonably secure by design? A very good starting point is the OWASP (https://owasp.org/) site and in particular the page that lists several available tool that help analyze code for OOSS (https://owasp.org/www-community/Free_for_Open_Source_Application_Security_Tools).

There are different groups of tools to be leveraged in development and maintenance, here is a take from the OWASP page:

- Static Application Security Testing (SAST) Tools
- Dynamic Application Security Testing (DAST) Tools
- (Primarily for web apps)
- Interactive Application Security Testing (IAST) Tools - (Primarily for web apps and web APIs)
- Keeping OpenSource libraries up-to-date (to avoid Using Components with Known Vulnerabilities (OWASP Top 10-2017 A9))
- Static Code Quality Tools

So let's use them and declare it!

Cybersecurity and his complexity

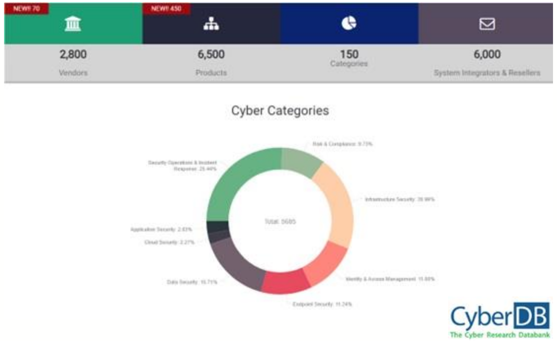
Cybersecurity has many dimensions of complexity that must be considered and continuously monitored and this drives a considerable economic impact on organization of any size

- Extremely high technological dynamism.
- Numerous technologies available on the market:
  - Difficulty of choice and selection.
  - Rapid functional and technological obsolescence.
  - Costs to bear.
  - Skillsets needed.
- Potential catastrophic impacts, sometimes even lethal for the organization.
- Need for involvement of the entire workforce.
- Management of risk arising from third parties

A Thought Task

There are so many security technologies that are constantly and rapidly evolving, and it is very difficult to keep up in all sectors, however continuous evolution normally benefits in terms of effectiveness, costs and times. Here are 2 useful indicators:

Wideness of the Market

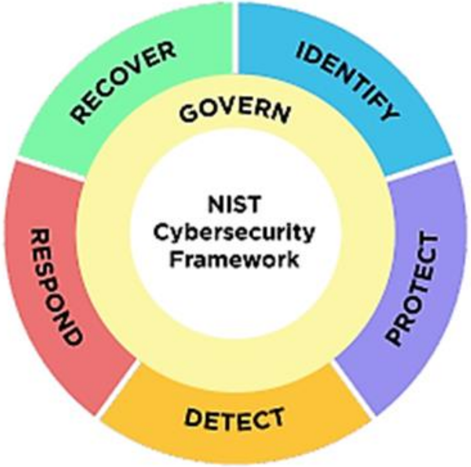

NEW! 70
NEW! 450
2,800
Vendors
6,500
Products
150
Categories
6,000
System Integrators & Resellers
Cyber Categories
Risk & Compliance: 9.73%
Security Operations & Incident Response: 25.44%
Infrastructure Security: 20.99%
Application Security: 2.83%
Cloud Security: 2.27%
Total: 5685
Data Security: 15.71%
Identity & Access Management: 11.80%
Endpoint Security: 11.24%
CyberDB
The Cyber Research Databank

2.800 Vendors

6.500 Tecnologies

CyberDB is an U.S. site that try to list all available cybersecurity technologies& vendors available in that market and that gives us a valuable indicator…

NIST v2.0 Cybersecurity Framework (CSF)



6 Main Functions

23 Categories

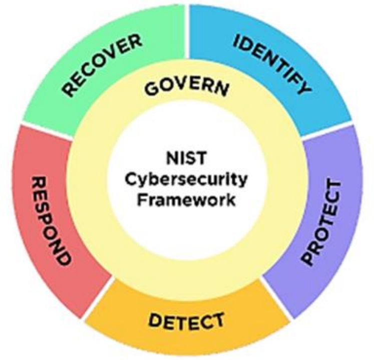
108 Subcategories

Is/has Cybersecurity an opportunity for Opensource Software?

Yes, definitely….

Yes, definitely….

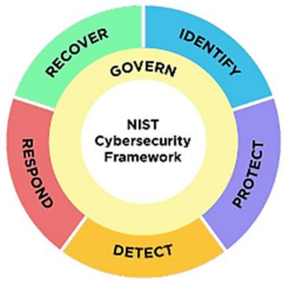
Actually many of them...



6 Main Functions
23 Categories
108 Subcategories

And maybe one in particular….

Cybersecurity Governance



6 Main Functions
23 Categories
108 Subcategories

Gover of Cyber: How to

Know the infrastructure

- Asset Management
- SW e HW Inventory & correlations between them

Figure out his own Security Posture

- Cybersecurity Assessment
- Internal & External Vulnerability Assessment

Cyberrisk management

- Qualify and quantify Cyber Risks
- Implement a continous Risk Management Platform

Cyber Risk Management

- This is a valuable tool for "gathering together" the many indicators associated with safety activities and quantifying their effects.
- Every security measure adopted, be it organizational, technological, infrastructural or policy, must be measured.
- The measures can be related to quality, completeness of adoption and coverage, installation and management costs, impacts on the organization and technologies

Conclusions

- Cybersecurity is difficult but high potential for the OOSS ecosistem.

- Secure development and maintenance is a must and existential theme for any opensource project

- There are many options to develop and have success in the domain, maybe some are closer than others.

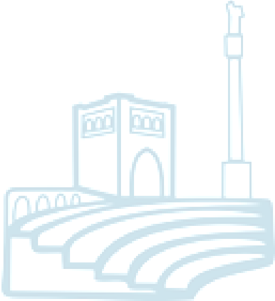
- **Cybersecurity Govern «is here to stay»**

exprivia CyberSecurity

The art of optimizing Investments reducing risks

Grazie per l’attenzione

Segui @CarloFalciola
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.