VATES

Open Infrastructure made simple

VATES

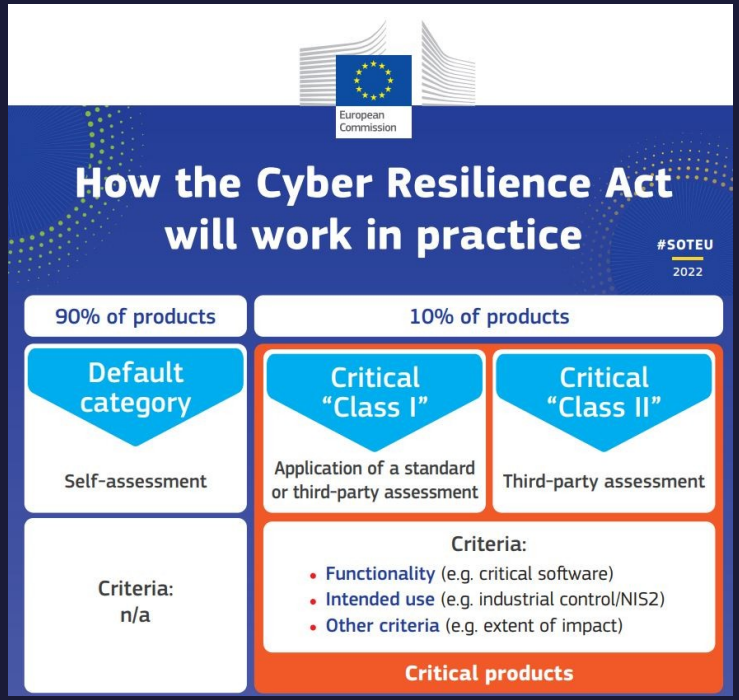
Open Infrastructure made simple

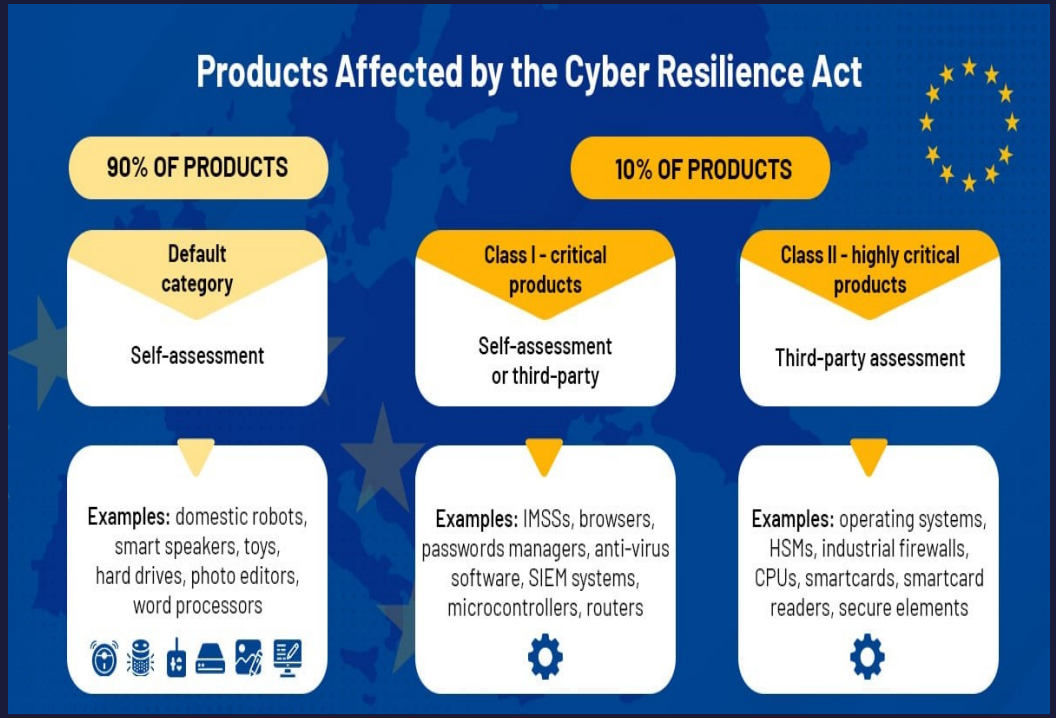
Let's all get over the CRA!

Charles-H. Schulz

08/11/2024

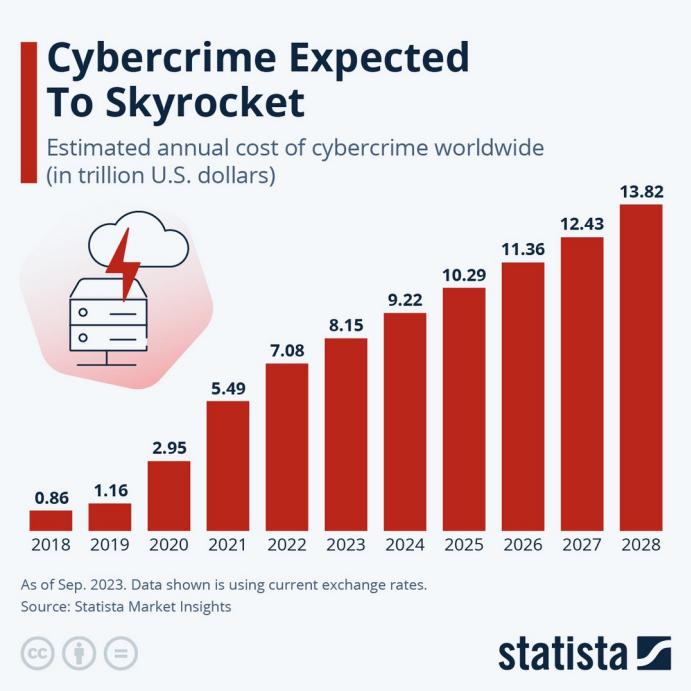
What's the CRA all about ?

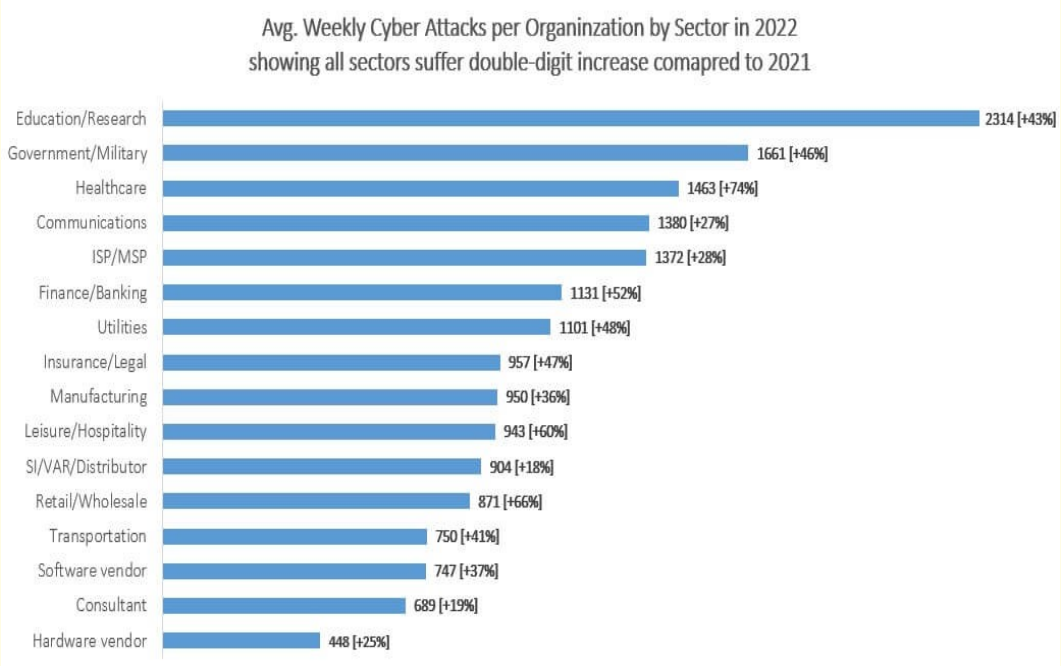




VATES

But why ?





VATES

How’s FOSS fitting in ?

- CRA applies to FOSS as soon as there’s a commercial activity around it in the EU
- Major distinctions :
  - FOSS foundations and projects themselves are not subject to CRA
  - The author of any FOSS is not directly responsible for audits & evaluations

VATES

Audits ? Evaluations ?

- Still to be decided for a large part
- Critial level III : Common Criteria based evaluation by a *trusted third party*
- Critical level II : Evaluation through a third party (very likely), but NO standardized methodology
- Everything else : self-assessment

VATES

Disclosures ?

- Known vulnerabilities must be disclosed to the ENISA and/or your national cybersecurity agencies
- Make sure you label your stable/final releases properly as they are the ones audited and targeted by the CRA (ENISA must be theoretically alerted)
- This induces complexity, but also BETTER security processes

VATES

In practical terms...

- 90 % of software falls in the non critical categories
- What about the rest ?
  - Chances are if you are selling services on an operating system or a cryptographic component securing data centers you know it has to be audited anyway
  - Category 2 is likely to have some lightweight 3rd party evaluation with cheap or diminishing prices

VATES

I develop FOSS - HELP !

- Make sure you label your releases properly
- The « Open Source Stewards » :
  - Large FOSS Foundations (but likely established foundations in general : The Document Foundation?) can finance the security audits / facilitate self assessments
  - A commercial activity MUST exist in order to comply with the CRA requirements

VATES

Adverse effects

- Obvious complexity, especially for SMBs
- Increased centralization around a few large FOSS Foundations : LF, Eclipse, etc.
- Fear and Uncertainty on digital innovation across Europe
- Can the ENISA even deal with all the incoming security data ? … ????

VATES

Future perspectives

- Uncertainty is still going to remain for a while
- **Will it really improve the general level of security ?**
- Automation, pooled audits and AI tools will help a lot :
  - Tools for self assessment, web tools for better releases tagging
  - Pooled audits (less work, cheaper prices)
  - Automated platforms for security framework evaluations (bug bounties) will facilitate audits
  - Prices will fall down significantly

VATES

Thank you !

Charles.schulz@vates.tech