THE PERFECT STORM

The influence of the Open Source Industry on IT-investments in the Public domain and beyond

SUSE

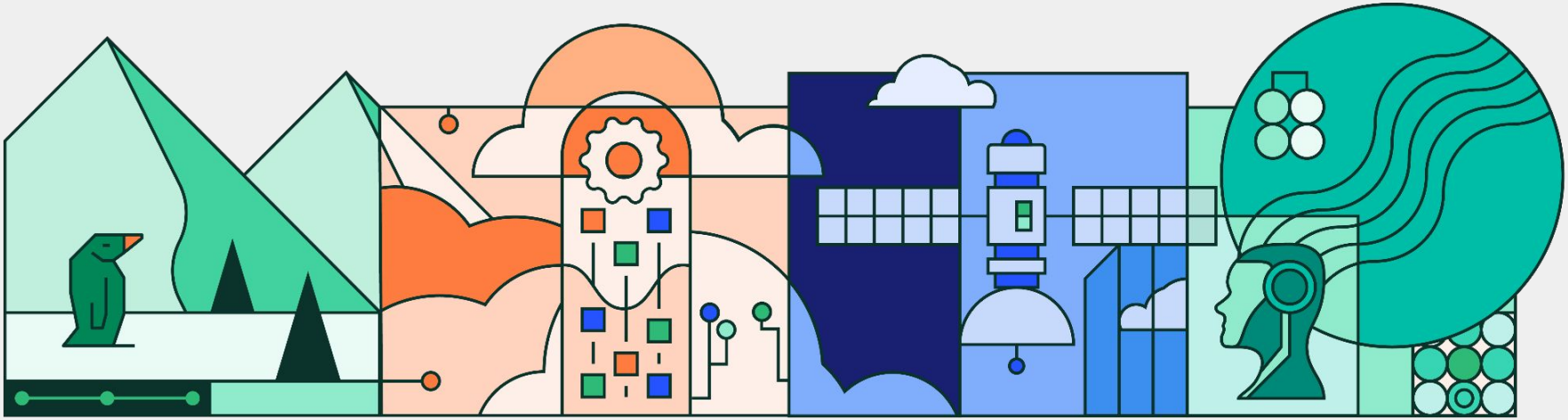
Emiel Brok

Open Source Ambassador at SUSE
Co-Founder & Board Member DOSBA


OpenInfra
USER GROUP
SWEDEN
SAVE THE DATE
22 MAY 2025
Open Infra Forum
0:33 / 4:23

Bringing the infinite potential of open source to the enterprise

The open infrastructure platform



Linux

Cloud native

Edge

AI

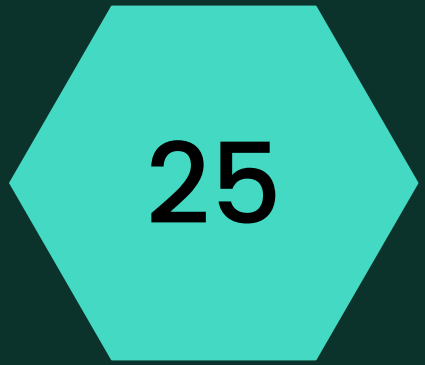
Perfect Storm

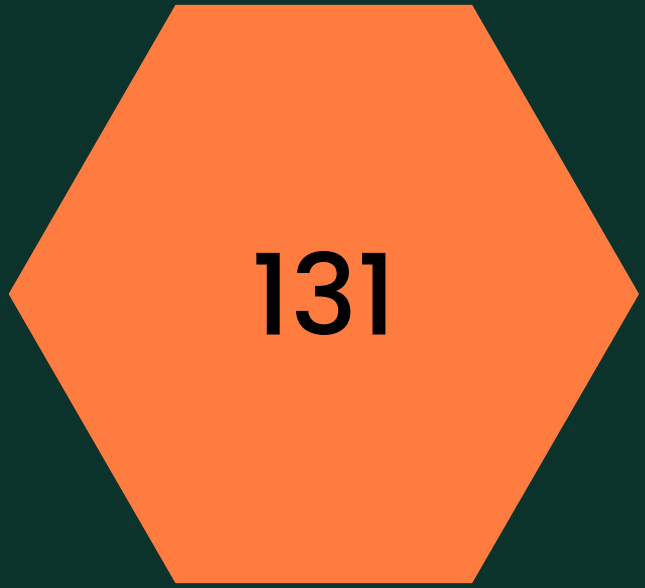
Perfect Storm:
An extreme situation in which many things happen at the same time.

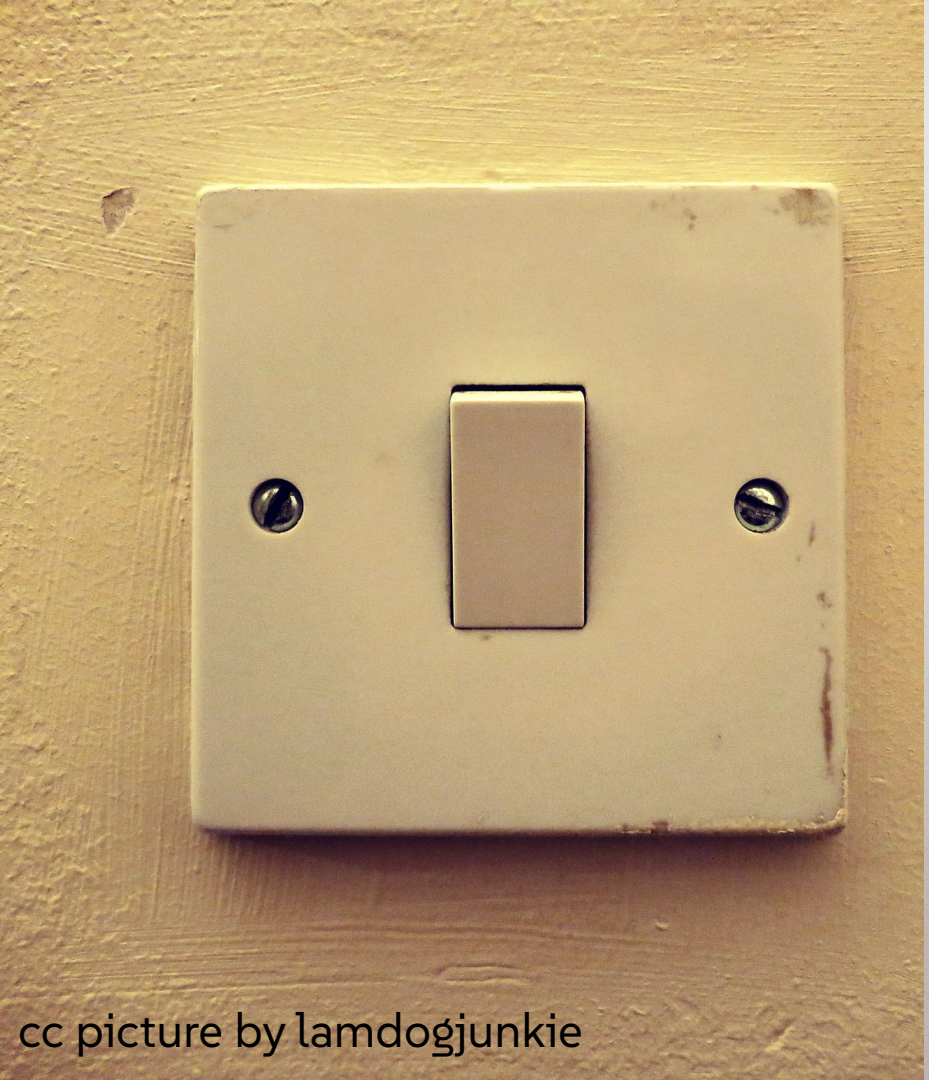
Disclaimer: I am not a lawyer

Disclaimer: I am not a technician


CAMEL


25

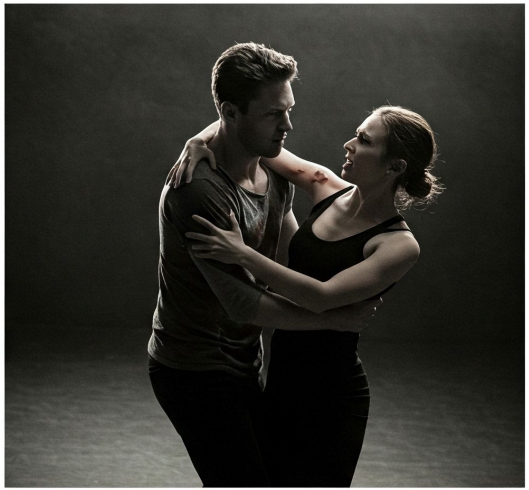

131



cc picture by lamdogjunkie


cc picture by taxaus

cc picture by so me




90
100
80
70
60

Most Pressing Regulatories

NIS-2

Network and Information Security Directive

- Okt. 18 2024
- Target Group Critical Infrastructure
- CEO liable
- Risk based security approach
- Responsibility for the cybersecurity of the supply chain

CRA

Cyber Resilience Act

- 2027
- Products with digital elements
- SBOM
- Vulnerability reporting
- Vendor Declaration

DORA

Digital Operational Resilience Act

- 2025
- Financial Sector
- Extensive Risk Management
- ITK for financial sector also affected

PCI-DSS

Payment Card Industry Data Security Standard

- V 4.0.1 Spring 2024
- Credit Card Information
- Detailed Security measures

Article 21 NIS-2 ad Supply Chain

Management **personally liable** (Art. 20), fines up to **10 Mio. EUR**

Article 21

Cybersecurity risk-management measures

1. Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services.

Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subparagraph shall ensure a level of security of network and information systems appropriate to the risks posed. When assessing the proportionality of those measures, due account shall be taken of the degree of the entity's exposure to risks, the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.

2. The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

(a) policies on risk analysis and information system security;

(b) incident handling;

(c) business continuity, such as backup management and disaster recovery, and crisis management;

(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

(f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;

(g) basic cyber hygiene practices and cybersecurity training;

(h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;

(i) human resources security, access control policies and asset management;

(j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

Sending 200 pages questionnaire is not enough!

In Germany entire Software Supply Chain is evaluated by:

Federal Office for Information Security

Deutsches IT-Sicherheitszertifikat

BSI-DSZ-CC-1151-2021

EAL 4 augmented

Valid until: 07.07.2026

Common Criteria

Sweden

Who me?

I Sverige och Europa finns ett stort beroende av de amerikanska it-jättarnas tjänster. Det behöver brytas, skriver debattskribenten. Lise Åserud NTB/TT

”Sverige stannar utan it-tjänster från USA – vi måste göra oss redo”

DEBATT. Sverige måste göra sig redo för en värld där tillgången till amerikanska it-tjänster begränsas, skriver Daniel Byström.

Publicerad 6 maj 2025 kl 09.00 Senast uppdaterad 6 maj 2025 kl 09.07

Det här är en debattartikel. Åsikterna som framförs är skribentens egna.

Världen går just nu igenom en turbulent handelstid och många länder arbetar febrilt för att förhålla sig till nya förutsättningar och tullar. Strålkastarljuset har bland annat riktats mot handelsbalansen mellan Europa och USA.

Det inledande fokuset har hamnat på handeln med varor, vilket fått Europas

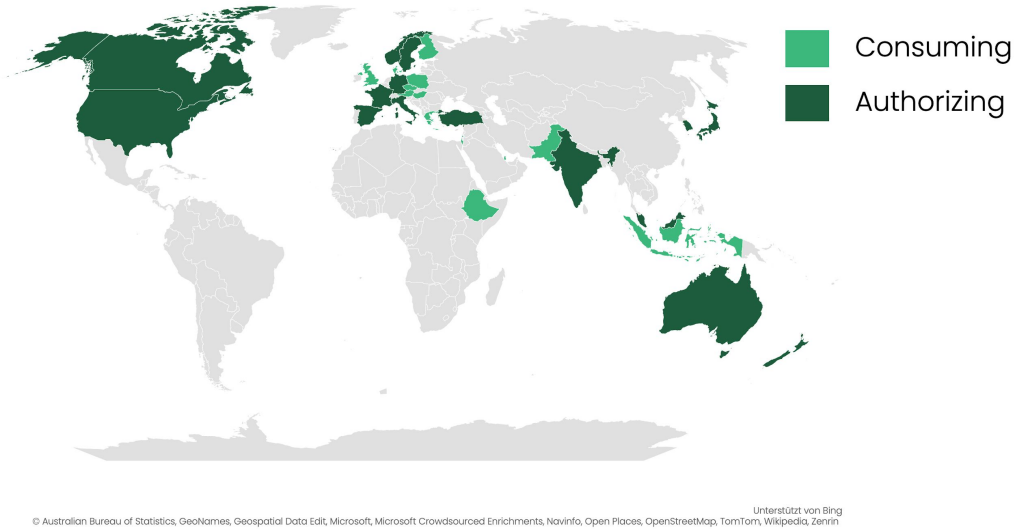
POPULÄRT

1 Forskarlarm: Ozempic kan trigga depression och självmordstankar

Source: https://www.nyteknik.se/debatt/sverige-stannar-utan-it-tjanster-fran-usa-vi-maste-gora-oss-redo/4358003

Common Criteria Recognition

CCRA



SOGIS-MRA

EAL 4 +

Sectors of high criticality

1. Energy
   a) Electricity
   b) Distinct heating and cooling
   c) Oil
   d) Gas
   e) Hydrogen
2. Transport
   a) Air
   b) Rail
   c) Water
   d) Road
3. Banking
4. Financial market infrastructures
5. Health
6. Drinking water
7. Waste water
8. Digital infrastructure
9. ICT service management (business to business)
10. Public Administration
11. Space

≥ 50 Employees & ≥ 10 Mio Annual Turnover
Who
is not on these lists?

Sectors of high criticality

1. Energy
   a) Electricity
   b) Distinct heating and cooling
   c) Oil
   d) Gas
   e) Hydrogen
2. Transport
   a) Air
   b) Rail
   c) Water
   d) Road
3. Banking
4. Financial market infrastructures
5. Health
6. Drinking water
7. Waste water
8. Digital infrastructure
9. ICT service management (business to business)
10. Public Administration
11. Space

Other critical Sectors

1. Postal courier services
2. Waste Management
3. Manufacture, production and distribution of chemicals
4. Production, processing and distribution of food
5. Manufacturing
6. Digital Providers
7. Research

≥ 50 Employees & ≥ 10 Mio Annual Turnover
Who
is not on these lists?

Public domain picture by GT#3

Is ISO 27001 sufficient?

RAIN OF STARS
18 pralines by 9 chefs

NIS-2 Article 21(2) minimal Security Requirements

All-hazards approach on network, information systems and physical environment

a) Risk analysis and IT System security Policies
b) Incident handling
c) Business Continuity
d) Supply Chain Security
e) Network and information systems security
f) Effectiveness assessment policy
g) Cyber hygiene and cybersecurity training
h) Cryptography policies
i) Access Control HR policies
j) Multi-factor authentication, continuous authentication, secured voice video and text communication, secured emergency communication systems

Covered by:

ISO 27000 Series

Common Criteria EAL 4+

- Sending 200 pages questionnaire is not enough!
- ISO 27001 Certification of the supplier does not guaranty coverage of customers security requirements

Common Criteria EAL 4+ vs ISO 27001

Some highlights

Common Criteria EAL 4 + Flaw Remediation

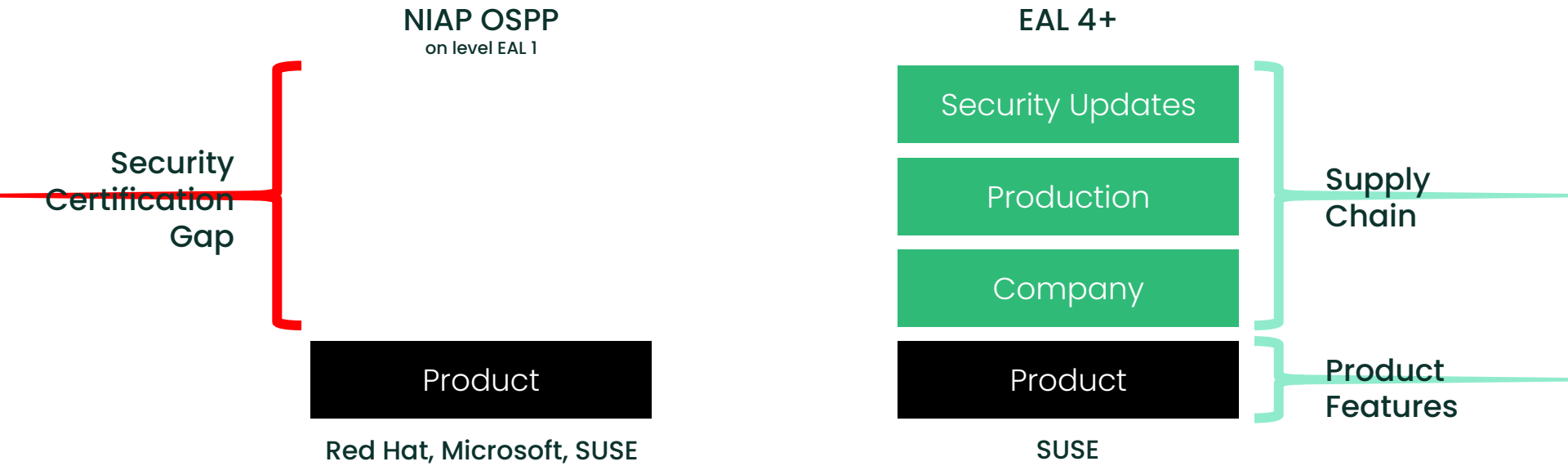
- Product specific including organization
- Demanding **full control** and description over all security aspects
- No compromise approach **transparent to the customer**
- Suitable to **highest security standards**
- **Fully comparable**

ISO 27001

- Organizational, **excluding product features**
- Delegation possible so delegated areas are **blind spots**
- Balancing risk with investment **unknown to customer**
- **Good enough security** for unknown level
- **Not comparable** depending on risk analysis

SUSE

EAL 4+ Certification Scope



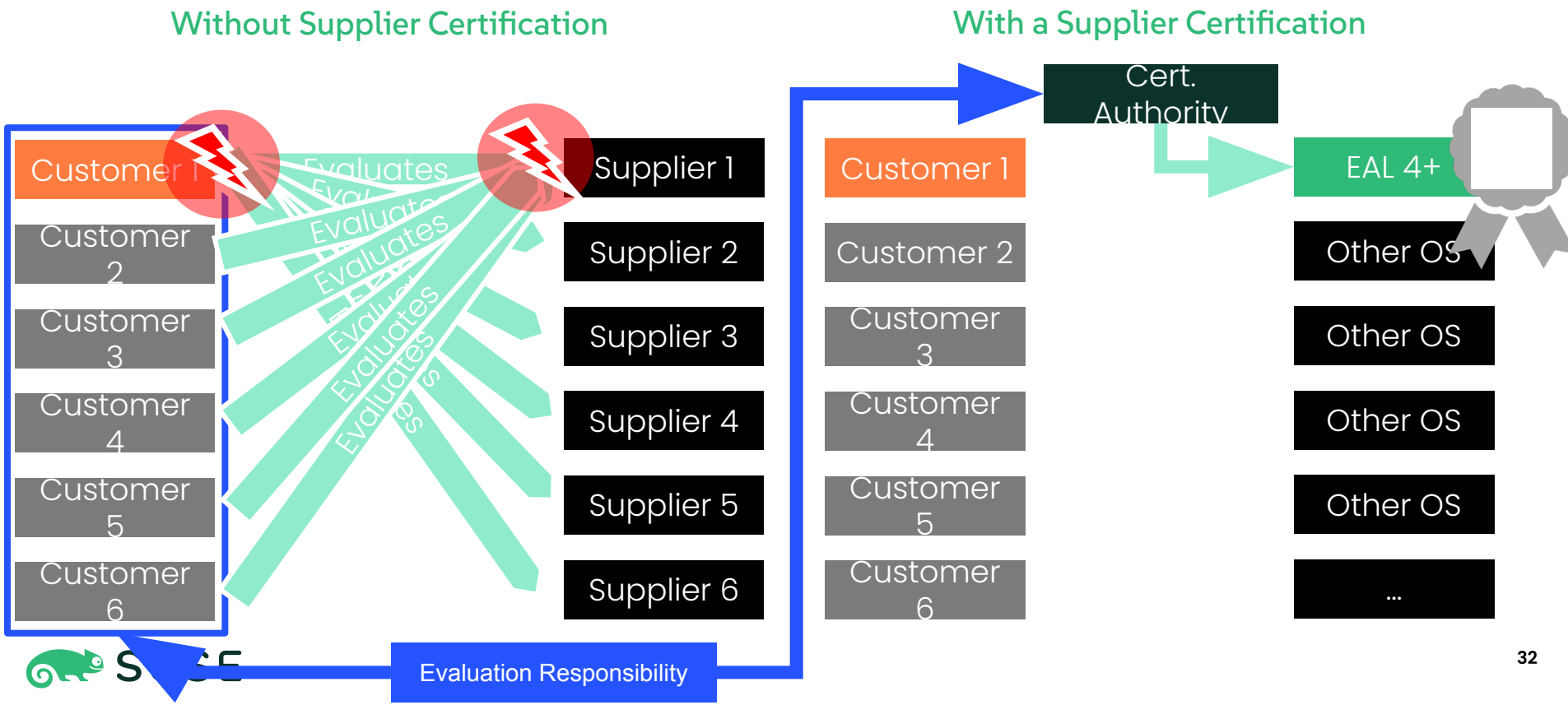
SUSE is the Only General Purpose OS that did both

EAL = Evaluation Assurance Level (how much has been checked)

Common Criteria EAL 4 + Certification

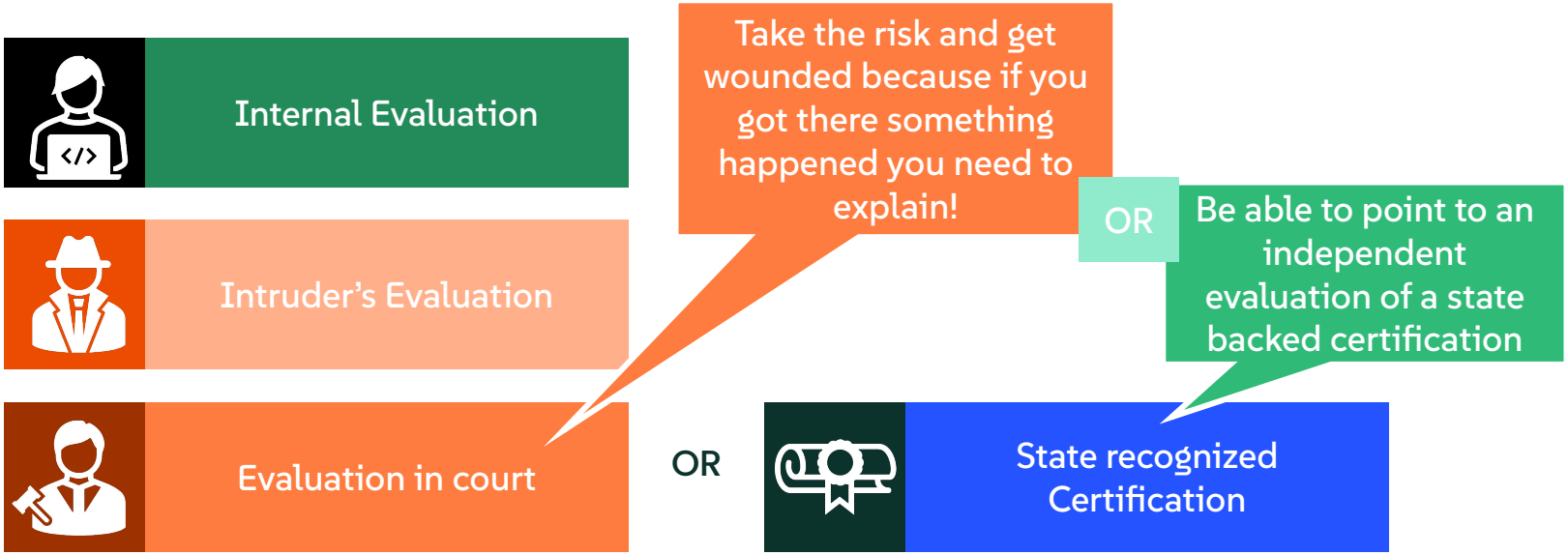
Certified Secure Software Supply Chain

Supply Chain Evaluation Effort



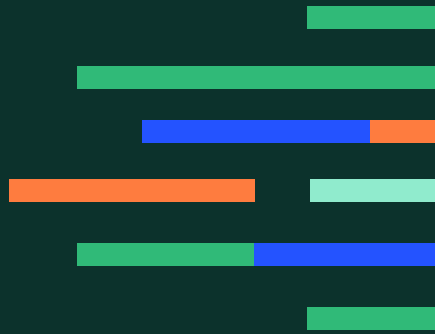
Triathlon of evaluation

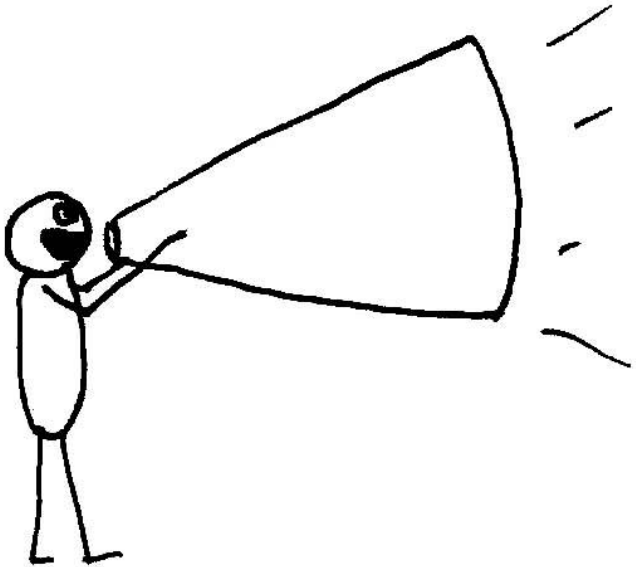
Every Organization might face at least 3 Evaluations



SUSE

How does Open Source Industry influence this storm?





OSBA - COSS - DOSBA - ... - ...

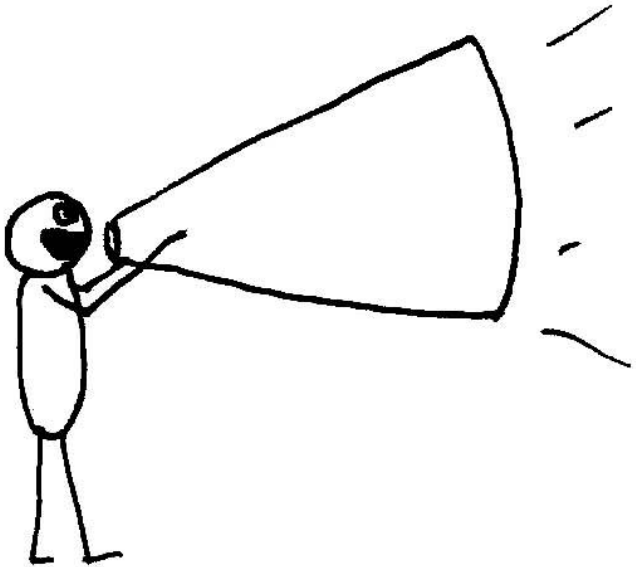
APELL - OFE - ... - ...

OpenInfra Forum

Many many more

PUBLIC MONEY

PUBLIC CODE




Everyone
is a policymaker!

Thank you

Agenda

- Slide 1 (Title slide)
- Slide 2 (Intro of me (3 minutes)
  - History OSS & Emiel (Storytelling)
  - My role at SUSE as OSS Ambassador
  - (Slide 3) Friday Ketchup
  - Slide 4 Disclaimer: I am not a lawyer, please also talk to them!
  - Public money, Public Code
- Slide 3 (storm phase 1, More tools)
- Slide 4 (storm phase 2, more complex tools) (try to get IP address on your next divide (IP4)
- (connectify)
- Slide 5 (old school switch vs nowadays switch)
- Slide 6 (Storm phase 3, international turbulence, increasing pressure and importance)
- Slide 7 (storm phase 4, EU regulations)
  - Customer Situation (Finish Example, Storytelling)
  - Storm is coming! (GoT)
  - Which Storm? (EU Regulation)
  - Why? (We are at WAR)
    - Reaction = NIS-2
    - Perfect (Finnish) Storm: Changing society by digitalisation
      (Switch analogy: old switch to modern "switch"= computer, who is in? Bad guys? Maybe
      That is why EU comes with NIS-2 is for Critical infrastructure (Slide 3)
  - What do you need to do? (Slide 4)
    - Com criteria (Slide 7) International framework of Cyber Sec Certs, implemented by standard (ISO 15408 and the CCRA and SOGIS-MRA) (Pic
    - ISO 27001 is not enough (slide 8) you can exclude elements!
    - CRA Cyber Resillion Act
    - Not just you, also your supplier? Do you know?
- SUSE (Super strong coat, shorts all ways :))
  - **Vision: Bringing the infinite potential of open**
  - **Mission: ???**
  - **Enterprise Ready (New to deliver slide by Knut)**
  - **Example of Knut of Germany re make sure that OSS was not excluded**
  - **Investment in protection will save you money in the long run?**
  - **Because of these regulations (CRA) encourage (also) OSS companies to**
  - **Is a company also publishing upstream?**
  - **How we build is what is certified,**
  - **Certs are product based not process based**
- **Uitsmijter: Remember a good coat is not enough, you also need shoes, equipment and behave yourself.**
  What YOU need is OSS products, but only if they protect you for Finish Arctic Weather!

Storm is Coming!

Emiel would like to protect you for not just a Dutch Storm but even for the Arctic, Storm that is coming. He'll explain the NIS-2 so you are aware and should be prepared. But also how you can benefit from it.

Mindtrek Keynote

NIS-2: Article 21: Personal liable (slide 5 of Knut's deck).

Shopping list for any CIO that needs his/her sleep https://www.commoncriteriaportal.org/products/index.cfm
Compliace: >EAL 4+ including ALC_FLR.3

Why? Because this filters all products where the entire Supply Chain Security has been evaluated.

Reference for Recognition is the SOGIS-MRA

If they shop from this list

Slide 12 = which countries?

EAL = Evaluation Assurance Level = how deep is the evaluator looking into your supply chain.

Evaluator = (internationally) accredited person AND an accredited "government" agency representative. (IN FINLAND **Finnish Transport and Communications Agency (Traficom)**

Risk: Hypervisors (VM-Ware does not)

Slide 7

APPELL - COSS - OSBA - DOSBA - ... - OSF

SUSE at a glance

Our vision is to bring the infinite potential of open source to the enterprise

90%+
Of the leading companies use SUSE*

30+
Years of open source expertise

2,500+
Passionate employees

We make Linux and manage many

We make Kubernetes and manage many

We make Zero-trust security the default

We make GenAI solutions for many models

We are pioneers in Edge technology

We offer world-class support

*Based on key Industries including Financial Services, Aerospace, Automotive, Pharma and Technology

SUSE

Benefits of Enterprise Open Source from SUSE

> Open Source is the backbone of digital innovation* Gartner®

Certified to the highest standards

Freedom of choice

Private by design

Zero-trust security

Control of costs at scale

Air gap friendly

SUSE

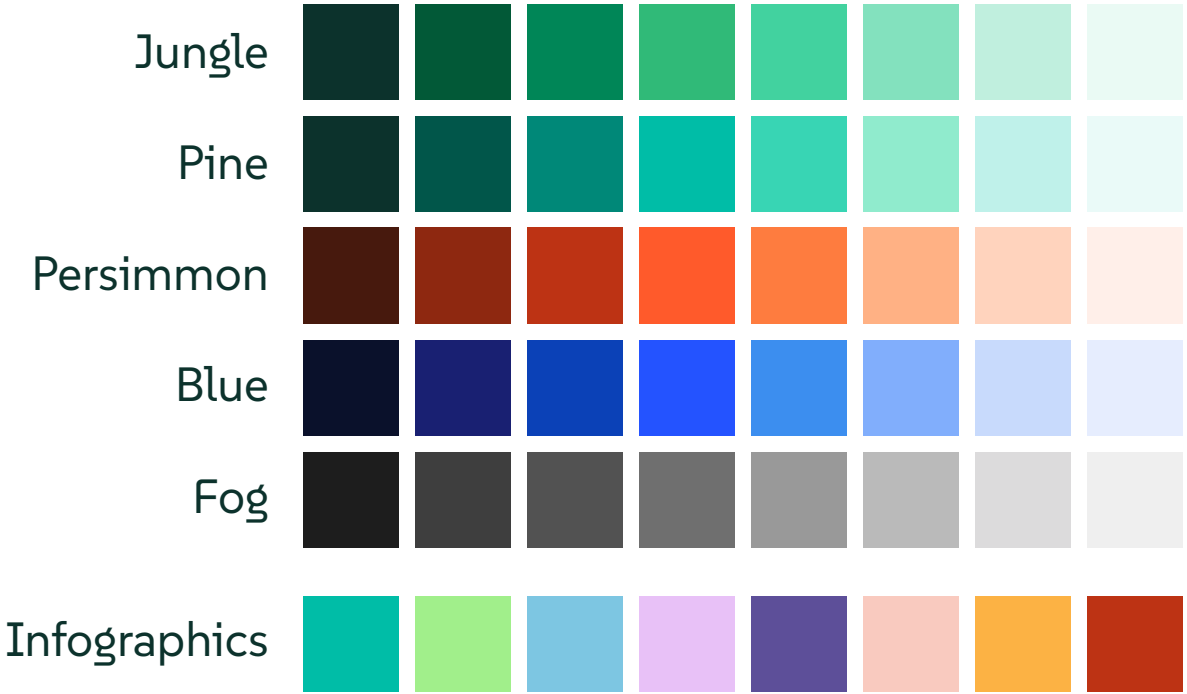
* Source: A CTO's Guide to Open-Source Software: Answering the Top 10 FAQs, 1 March 2024


SUSE

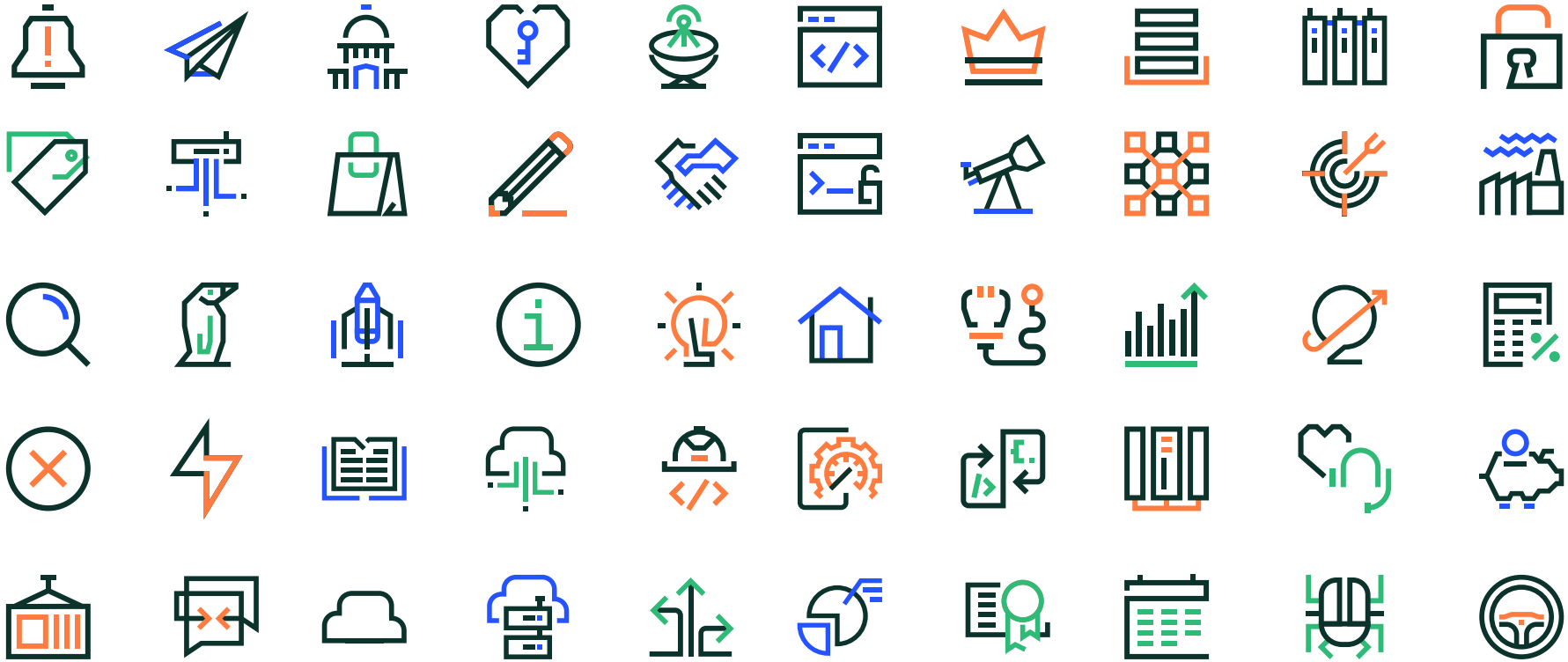
SUSE

Appendix

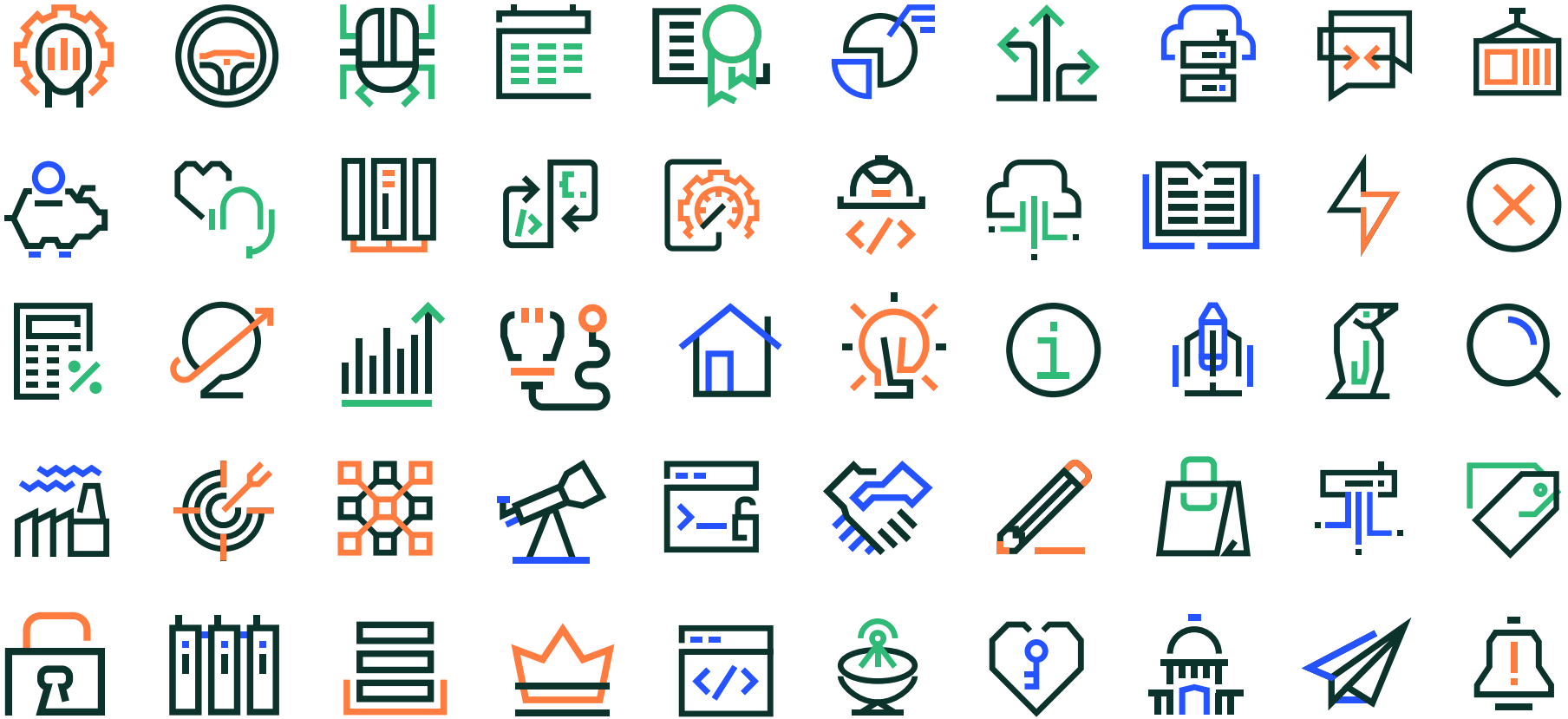
Palette, delete when deck complete



Icons, set custom fill and delete when deck is complete



SUSE



SUSE

SUSE

Choice happens

SUSE

Emiel Brok

Open Source Ambassador at SUSE

Bio: I'm living the open source philosophy for over 20 years. I trust the 'Power of Many' and 'Public Money Public Code' to continuously change the world into a better place. From different positions I lobby for ‘Open Source First’. I do this from my daytime job as Open Source Ambassador and also as co-founder of the DOSBA, The Dutch Open Source Business Alliance.I also host an online show called the ‘Friday Ketchup’.

Synopsis:

TBD