

Vládní bezpečnostní certifikace a open source

Aneb jak (ne)přijít o rozum :)

Jaroslav Řezník
Principal Program Manager
Product Security Compliance and Risk

O čem bude dnešní přednáška

Co jsou a jaké existují vládní certifikace?

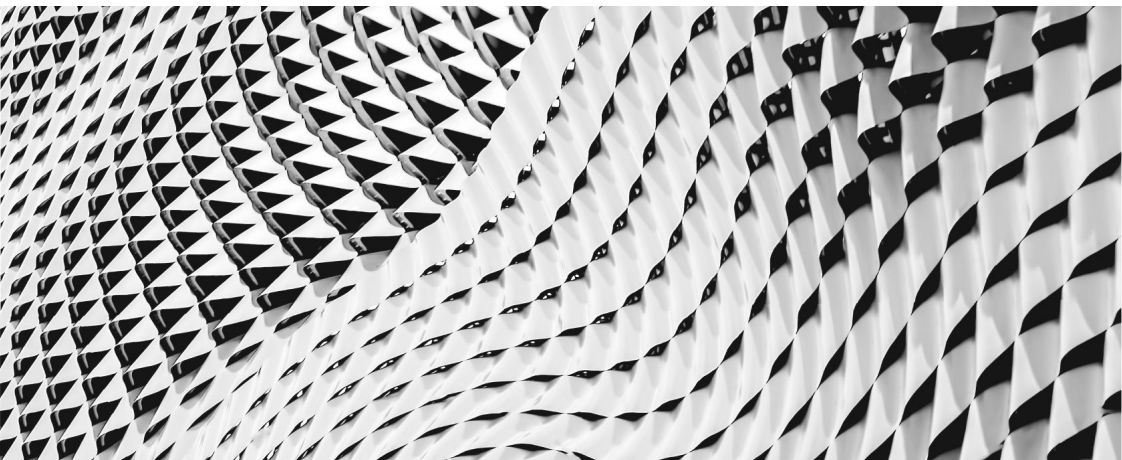
Proces.

Jak jdou vládní certifikace dohromady s open source?

Jaké nástrahy číhají u open source?

Závěr :)

Co jsou vládní certifikace?



1. přezkoušení kvality
produktů, služeb a
způsobilosti pracovníků
určenou zkušebnou dle
norem + vystavení
certifikátu/ oprávnění k
užívání/ provozu
2. úřední ničení
přebytečných zásob a
vyřazeného materiálu =
[z]certifikování,
certifikátor, c. komise
(Lidový slovník pro
chalupáře :D)



- **Zabezpečení vládních systémů a důvěrných dat je dnes prioritou**
 - **Aneb dobří versus zlí**
- **Certifikace jsou jednotná metodika jak dosáhnout**
 - **Jak vyšší bezpečnosti**
 - **Tak srovnání úrovně bezpečnosti**

Významné certifikace



COMMON CRITERIA

Common Criteria for Information Technology Security Evaluation je mezinárodní standard (ISO/IEC 15408) pro certifikaci počítačové bezpečnosti.

Produkty: RHEL, JBoss EAP, RHCS, RHV

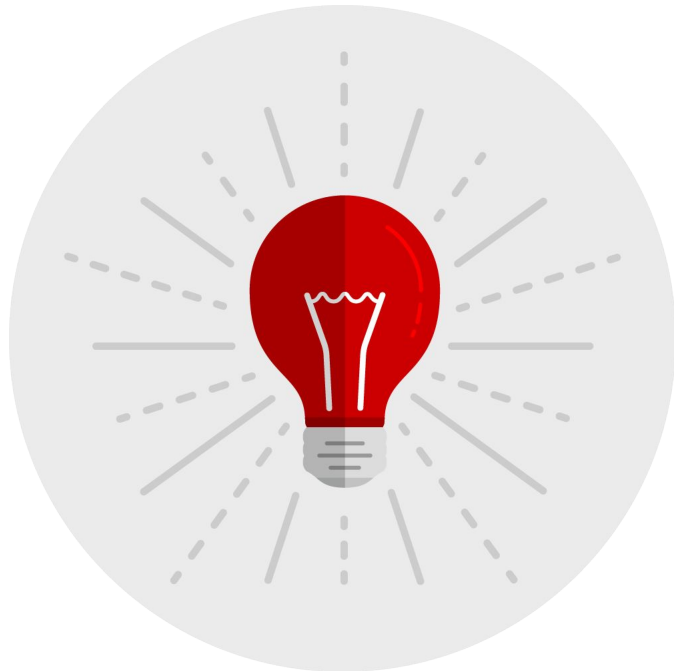


FIPS 140-2

Federal Information Processing Standard Publication 140-2 je americký vládní standard pro počítačovou bezpečnost používaný ke schvalování kryptografických modulů.

Produkty: RHEL 7/8/9

Další certifikace



USGv6

U.S. Government IPv6 compliance test program

SCAP

NIST's SCAP validační program

VPAT

Voluntary Product Accessibility Template (VPAT)

FedRamp

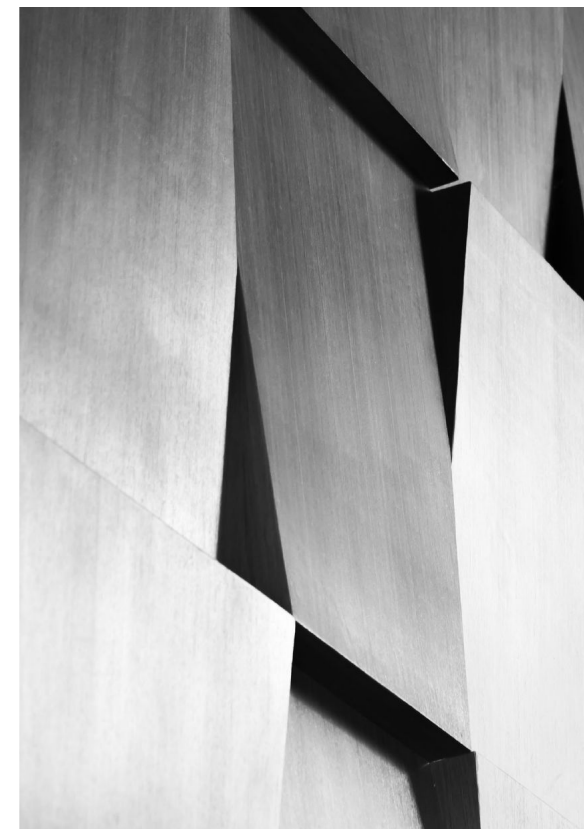
Govcerts hub:

<https://access.redhat.com/articles/2918071>



- **Vládní certifikace jsou velmi častou podmínkou pro vstup na vládní a regulované trhy (například zdravotnictví atd.)**
- **Poslední dobou je bezpečnost téma - výjimky přestávají existovat**

- **Konkurenční boj**
 - **Aneb sbírat razítka jako Pokemony**
 - **Víc certifikací znamená výhodu při výběrových řízeních, ale může vést až k neetickému jednání**





FIPS 140-2

- **Validace kryptografických modulů, certifikáty pro jednotlivé algoritmy a moduly**
- **Omezená sada povolených algoritmů (ala MD5)**



FIPS 140-2

- **NIST/CCCS CAVP a CMVP**
- **Americko-kanadský**
standard (ale FIPS 140-3 je
ISO)
- **Implementation Guidelines**
- **1SUB vs 3SUB vs 5SUB**

Common Criteria



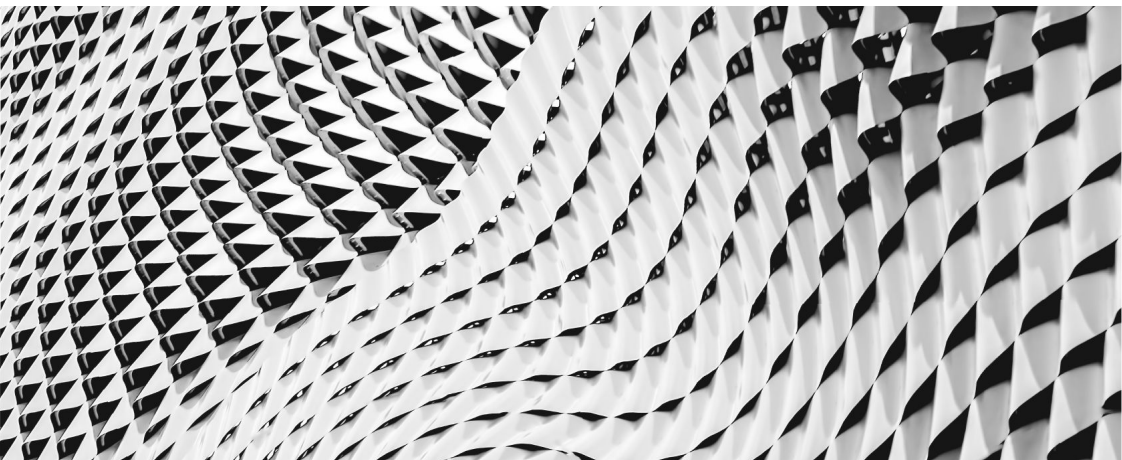
- **Mezinárodní ISO standard (ISO/IEC 15408)**
- **EAL, Protection Profiles**
- **Schémata (NIAP, BSI...)**
- **CCRA**

Common Criteria



- **SFRs, SARs**
- **Security Target**
- **Dokumentace**
- **Commercial Solutions for Classified (CSfC)**

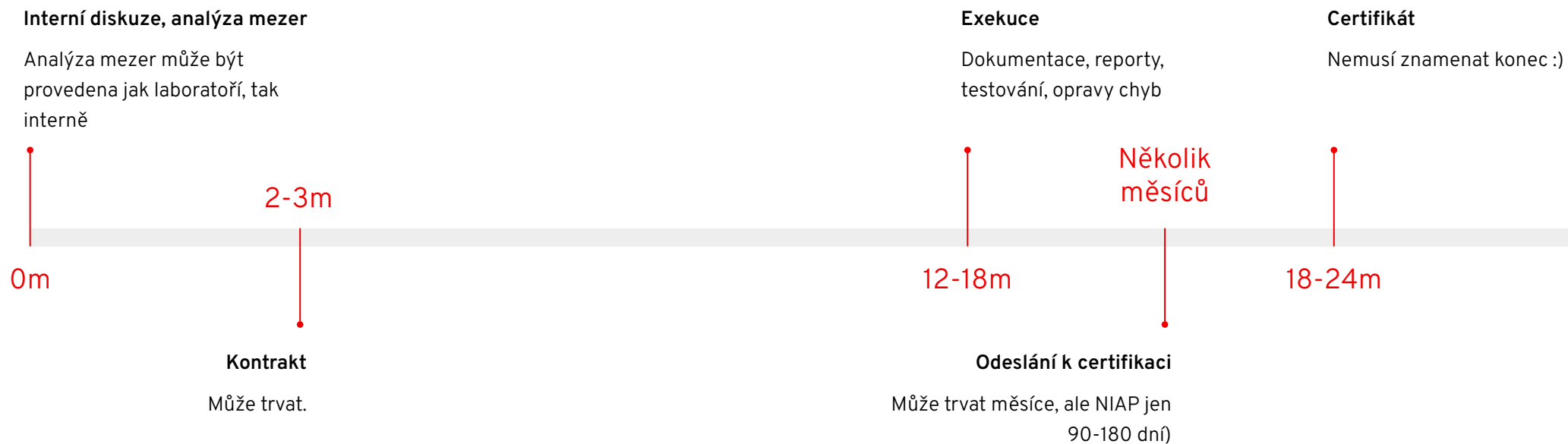
Proces



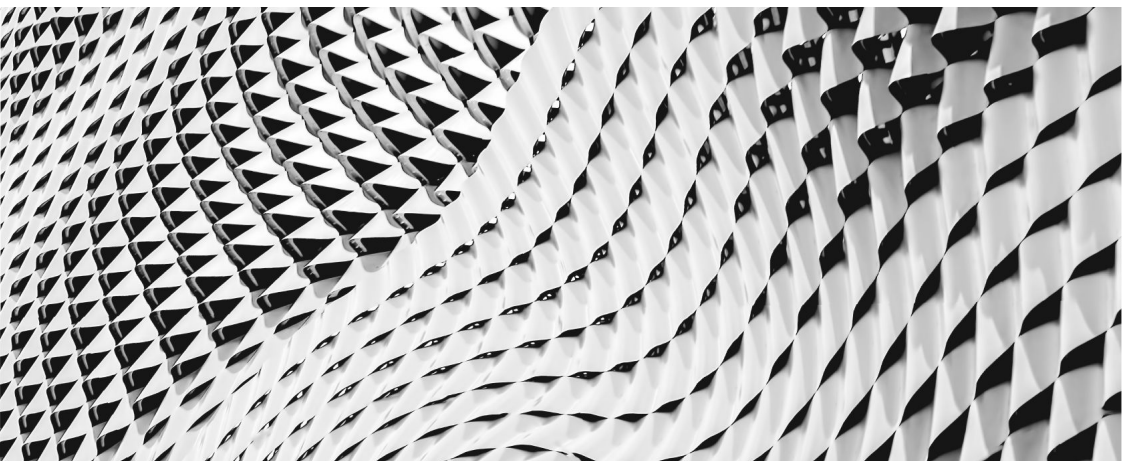


- **Dodavatel produktu (např. Red Hat)**
- **Akreditovaná laboratoř (např. Atsec, Acumen, Gossamer atd.)**
- **Vládní organizace (např. NIST, NIAP, BSI, OCSI atd.)**

Typická časová osa certifikace



Vládní certifikace a open source



Vládní certifikace a open source

Jak jdou dohromady navzájem?



- **Počáteční nedůvěra v open source jako takový**
- **Kontrola nad kódem a vývojem**
- **Náklady**

- **Site visits (EAL 4 a vyšší)**
 - **Fyzické zabezpečení, kontrola nad vývojem a vydáváním produktu**
 - **Dokumentace, spousta dokumentace**
- **Ale open source a vývojáři všude (s omezenou kontrolou)**
 - **Kdo jste něco přispěli?**





- **Náklady**
 - **Náklady na certifikaci mohou dosáhnout statisíců až milionů dolarů (zvláště CC EAL)**
 - **Open source projekty si je nemohou dovolit (ale třeba OpenSSL a FIPS)**



- **Změny vynucené certifikací**
 - Implementace změn jen pro certifikaci, často nepochopené open source komunitou
- **RNG, self tests atd.**



- **Nečekané změny ve standardech vs upstream first policy**
- **Časová náročnost vs release early, release often**
- **Skutečně větší bezpečnost???**
 - **Certifikované vs “děravé” verze**

CVE



- **Nepřítel!**
- **Nalezené CVE často
znamená měsíce práce
navíc**



Díky!

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.

 linkedin.com/company/red-hat

 youtube.com/user/RedHatVideos

 facebook.com/redhatinc

 twitter.com/RedHat