ALEF

Audity bezpečnostních týmů podle metodiky SIM3

Jan Kopriva

jan.kopriva@alef.com

ALEF CSIRT

TLP: WHITE

Bezpečnostní tým CSIRT

- Computer Security Incident Response Team (CSIRT)
  - Specializovaný bezpečnostní tým
  - Zajišťuje implementaci proaktivních bezpečnostních opatření
  - Provádí reakci na bezpečnostní incidenty
  - Poskytuje další bezpečnostní služby

Kdy je CSIRT efektivní?

- Když má
  - Dobře navržené a dokumentované procesy
  - Vhodnou interní i vnější organizační strukturu
  - K dispozici kvalitní technické nástroje
  - Po všech stranách kompetentní personál

SIM3

- Security Incident Management Maturity Model
  - Metodika pro hodnocení zralosti/vyspělosti CSIRT týmů
  - Aktuálně ve verzi mkXVIIIb (9/2018)
  - 44 hodnocených parametrů ve 4 kategoriích
    - Organization
    - Human
    - Tools
    - Processes

Příklady parametrů

O-8 : KLASIFIKACE INCIDENTŮ (INCIDENT CLASSIFICATION)

Popis: Existence klasifikačního schématu a jeho užívání pro klasifikaci zaznamenaných incidentů. Klasifikační schémata většinou obsahují minimálně „typy“ nebo „kategorie“ incidentů, může v nich však být rovněž zohledněna i „závažnost“ incidentů.

Příklady parametrů

H-5 : EXTERNÍ TECHNICKÝ VÝCVIK (EXTERNAL TECHNICAL TRAINING)

Popis: Program umožňující členům CSIRT získat pro práci relevantní externí technický výcvik – např. TRANSITS, ENISA školení pro CSIRT týmy nebo relevantní komerční školení (CERT/CC, SANS, apod.).

Příklady parametrů

T-9: NÁSTROJE PRO DETEKCI INCIDENTŮ (INCIDENT DETECTION TOOLSET)

Popis: Soubor nástrojů zaměřených na detekci incidentů, nebo detekci stavů, při nichž je pravděpodobné, že k výskytu incidentů dojde. CSIRT tyto nástroje sám provozuje nebo užívá, nebo má přístup k jejich výstupům.

Upřesnění: Např. IDS, karantény, analýzy netflow.

Příklady parametrů

P-1 : ESKALACE NA VYŠŠÍ VEDENÍ (ESCALATION TO GOVERNANCE LEVEL)

Popis: Proces eskalace na vyšší management CSIRT, který je součástí stejné organizace jako CSIRT a jeho klientela. Pro externí klientelu: eskalace na vyšší vedení odpovídající klientské organizace.

Hodnocení parametrů

0 = neaplikovatelné / nedefinované / neznámé

1 = implicitní

2 = explicitní, interní

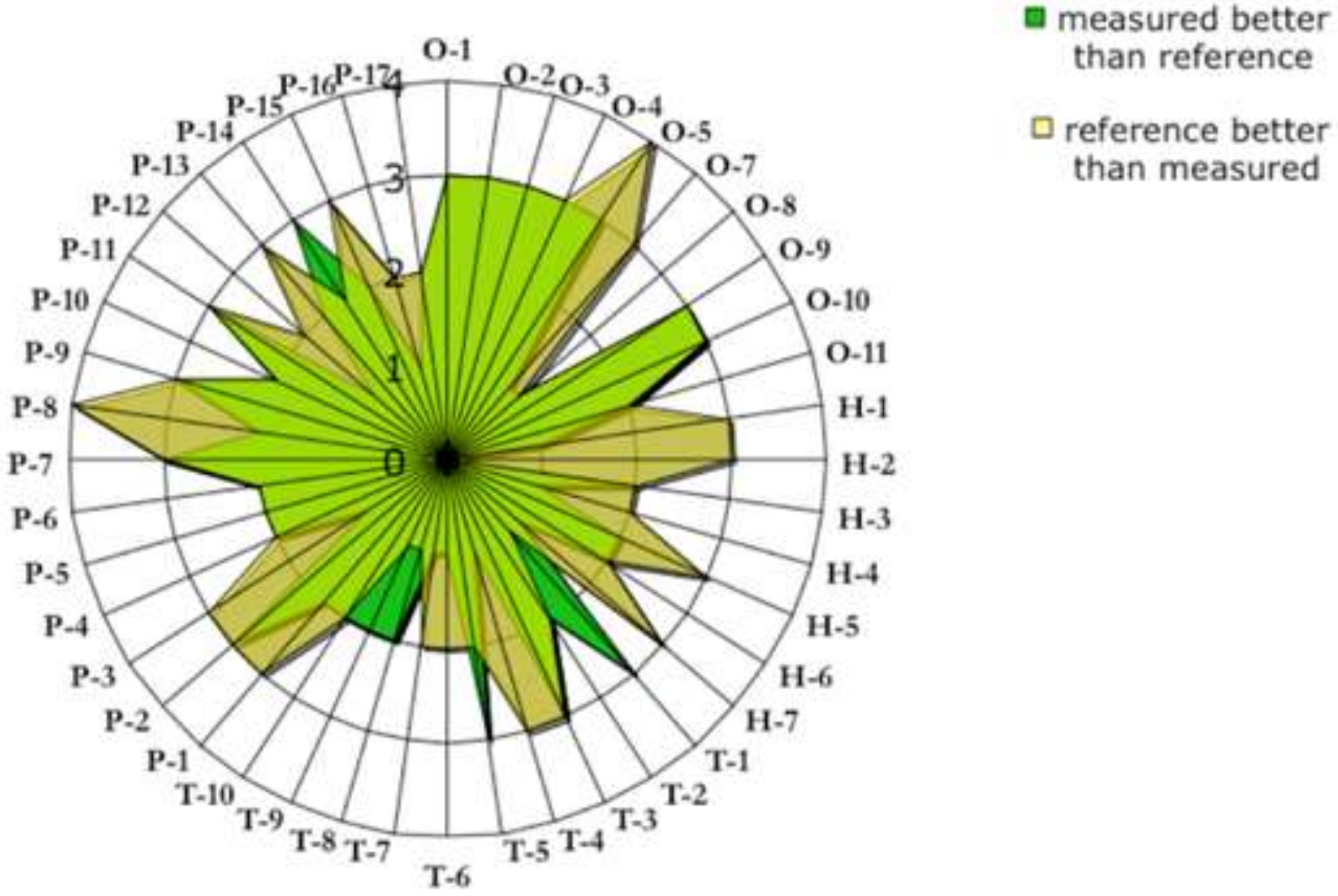
3 = explicitní, formalizované vedoucím CSIRT

4 = explicitní, auditované z úrovně vedení nadřízené vedoucímu CSIRT

Jak je možné SIM3 využít

- SIM3 analýza/posouzení
  - Cílem zlepšování
  - Identifikace slabých míst
- SIM3 audit
  - Hodnocení všech parametrů
  - Možné porovnání naměřených hodnot s určitou baseline

SIM3 baseline



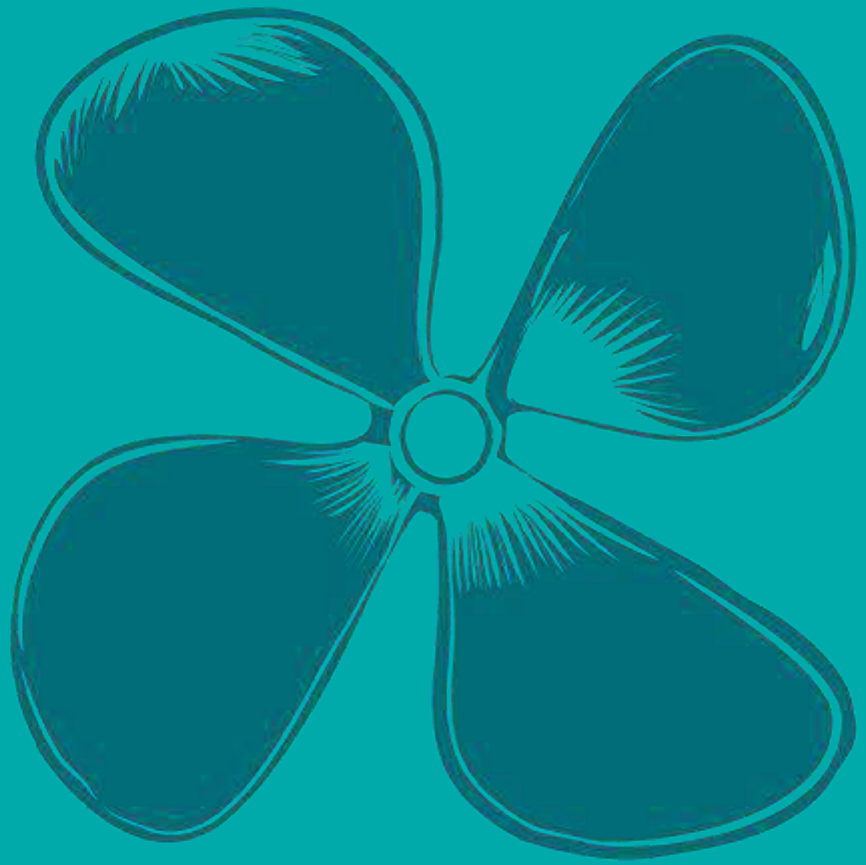
ALEF

Pro koho je SIM3 relevantní

- Národní CSIRT týmy v EU
- Týmy v Japonsku
- Týmy ve státní správě Slovenské Republiky
- Provozovatelé libovolného CSIRT

ALEF

Děkuji Vám za pozornost



TLP: WHITE