ALEF

Bug Bounty program a možnosti jeho využití

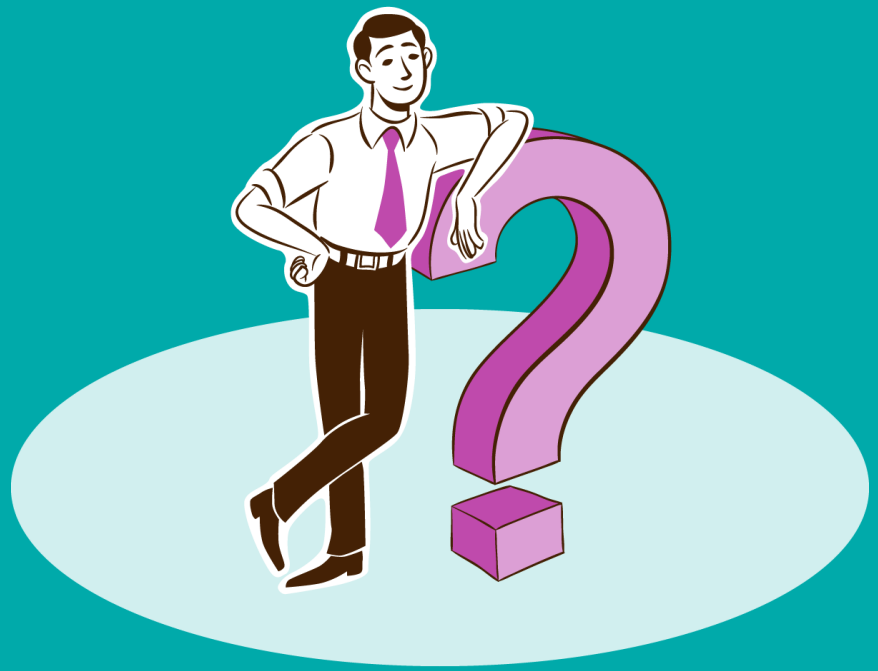
Milan Habrcetl

milan.habrcetl@alef.com

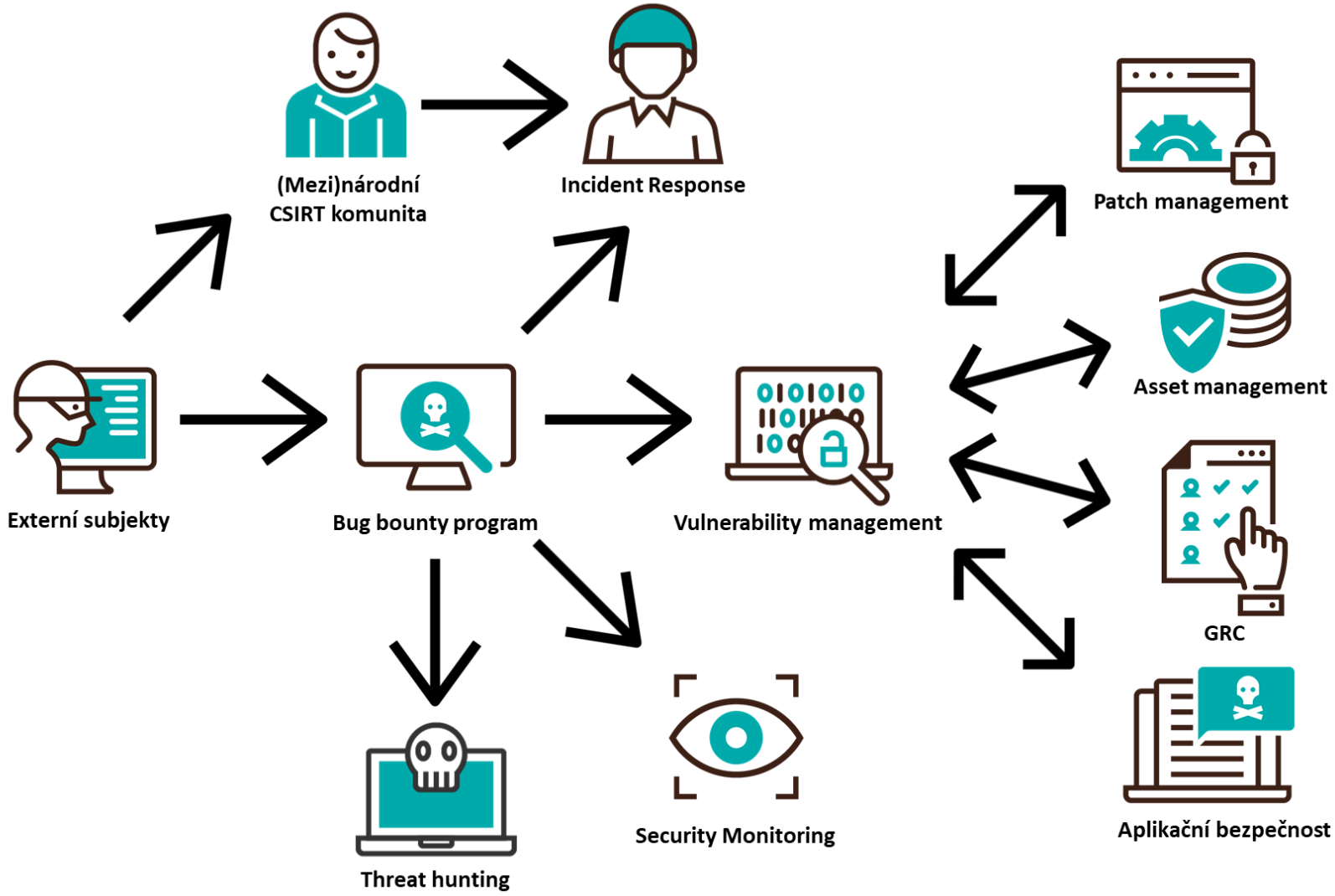
ALEF CSIRT

Co to je?

Program založený na principu crowdsourcingu pro identifikaci zranitelností v systémech organizace.



Předpoklady a návaznosti na BBP

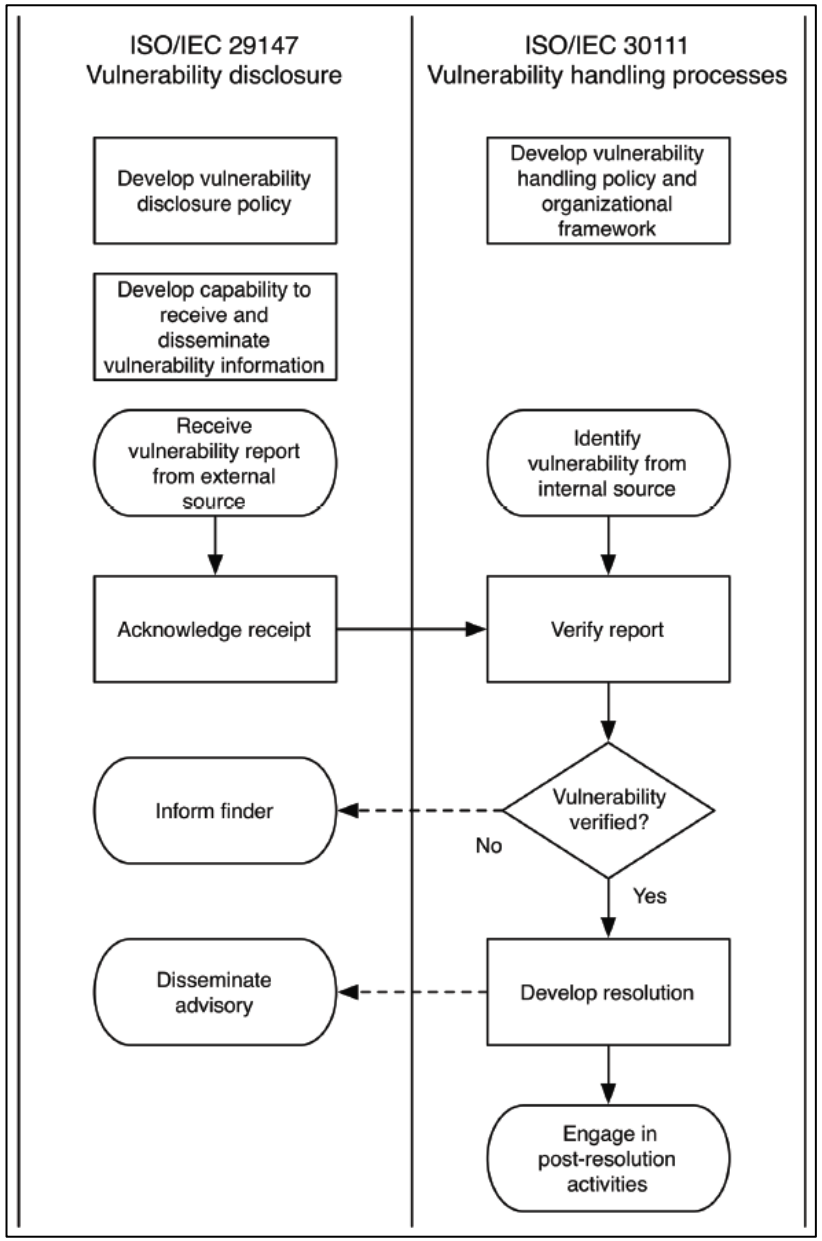


ALEF

Zavádění BBP v organizaci

Zavádění BBP v organizaci

- ISO/IEC 29147 – Vulnerability Disclosure
- ISO/IEC 30111 – Vulnerability Handling



Další předpoklady pro efektivní BBP

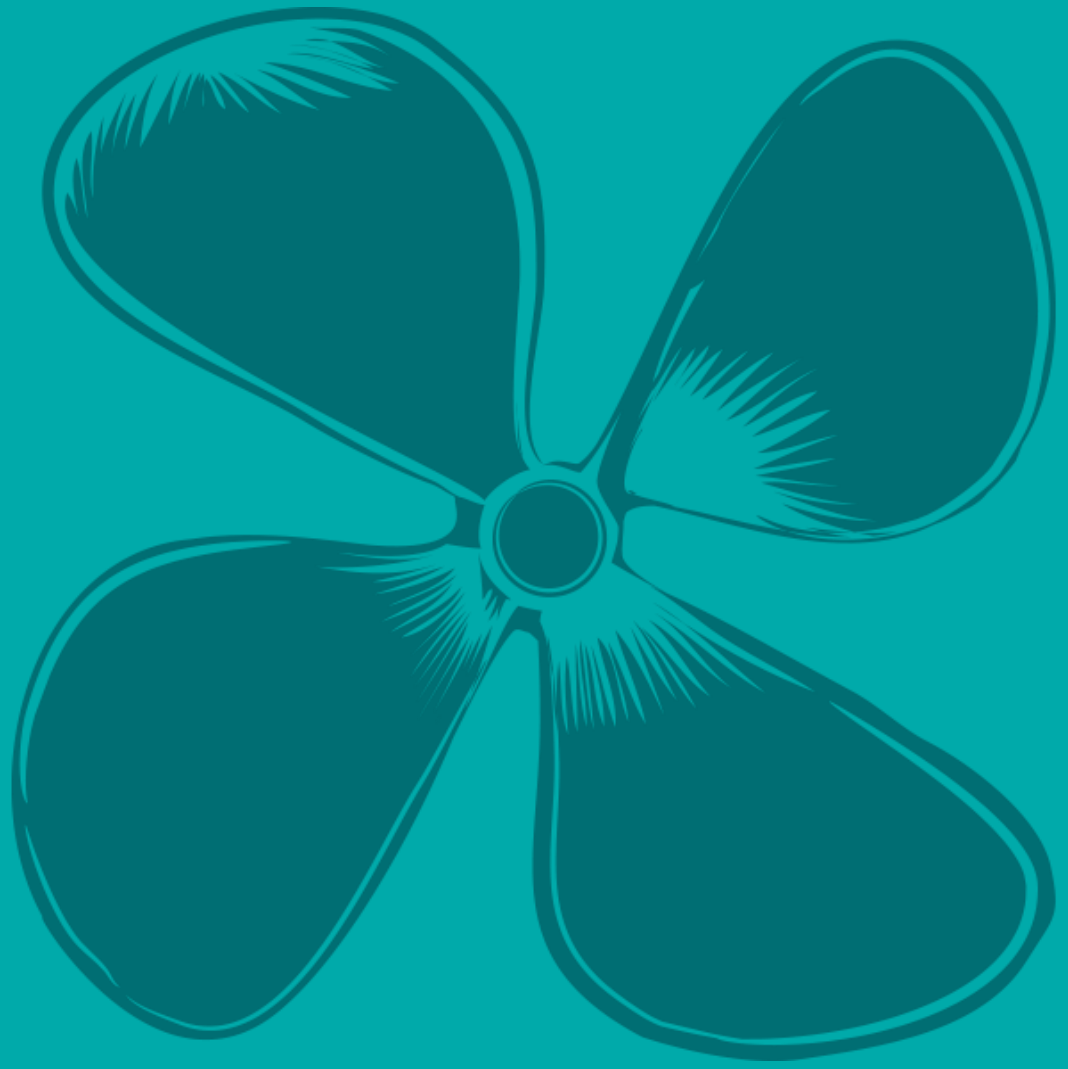
Další předpoklady pro efektivní BBP

- Stanovení a publikace podmínek BBP
  - Rozsah, zakázané aktivity, požadavky na report, klasifikace
- Efektivní komunikace s ohlašovateli
  - Security.txt (RFC 9116), PGP/GPG klíče
- Odměňovací schéma
- Nastavení a vyhodnocování souvisejících metrik
- Vyloučení střetu zájmů
- Evidence nálezů
  - Nalézt a vyloučit duplicitní hlášení

ALEF

ALEF

Závěr



Milan Habrcetl

milan.habrcetl@alef.com

ALEF CSIRT