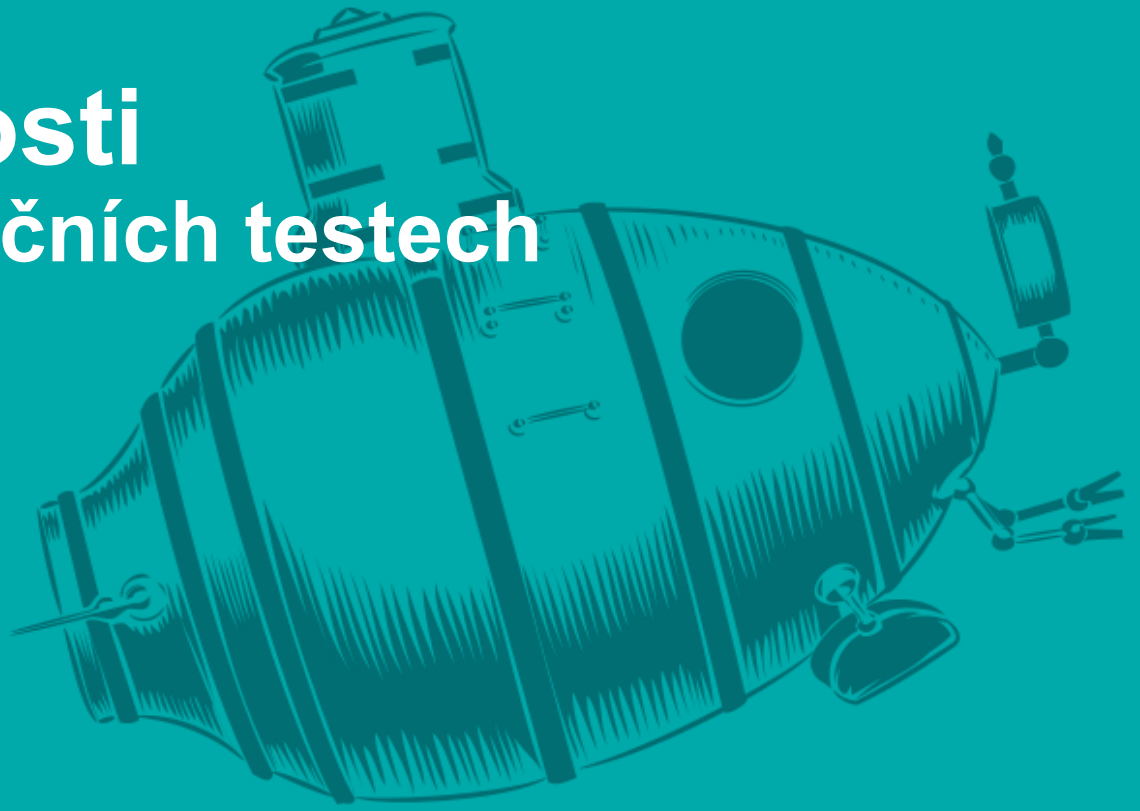
ALEF

Překvapující zranitelnosti
odhalené (nejen) při penetračních testech



Jan Kopřiva

jan.kopriva@alef.com @jk0pr

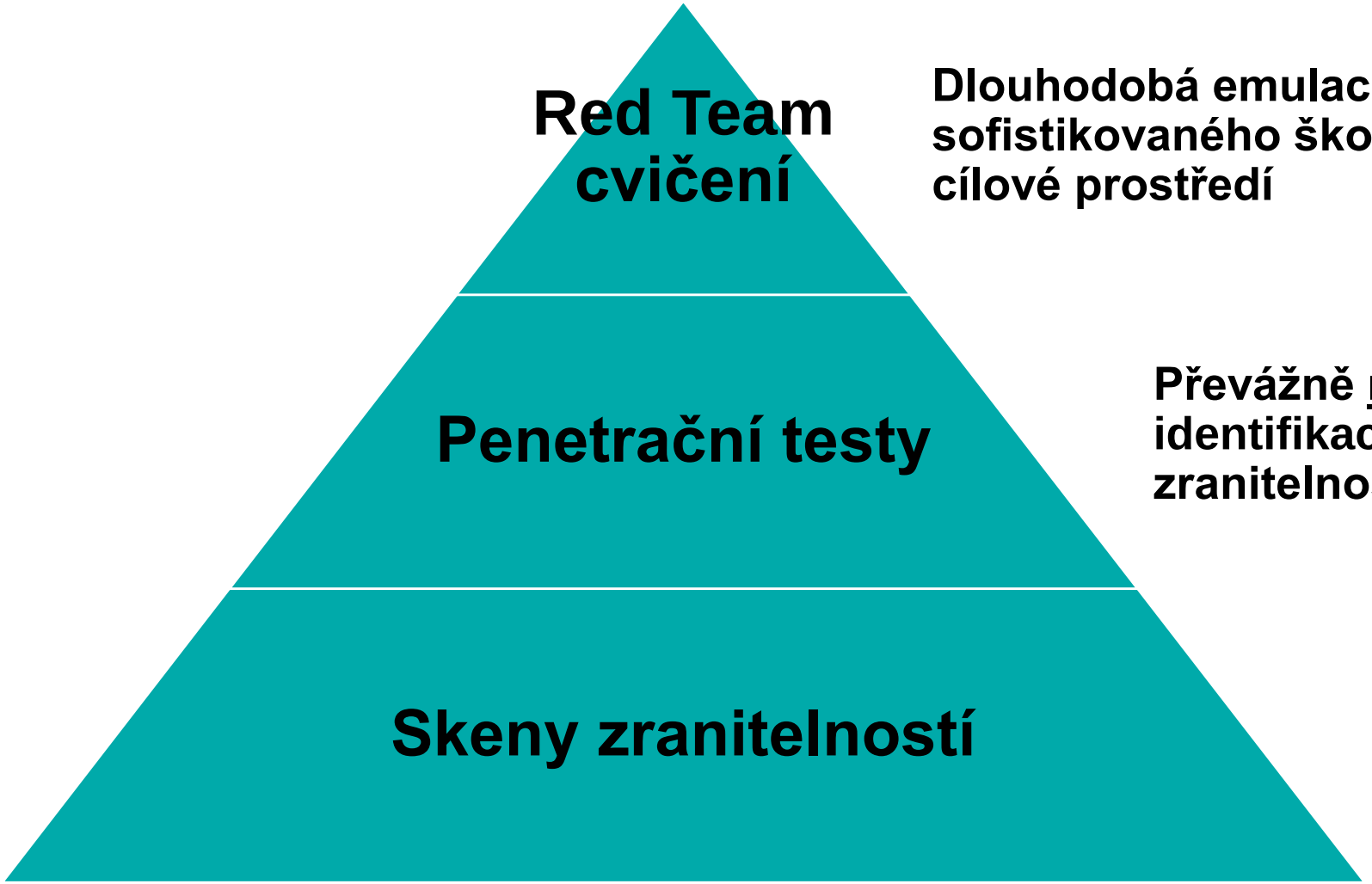
ALEF CSIRT

TLP: WHITE

Co je to vlastně zranitelnost?

- Chyba v SW s potenciálně negativními bezpečnostními dopady?
- Nezměněné defaultní heslo u rozhraní pro vzdálený přístup k systému?
- Místo ve fyzické bariéře, které umožňuje její snadné překonání?
- Bezhlavé klikání na odkazy v e-mailech ze strany koncových uživatelů?
- Chybějící proces pro skartaci dat?

Co je to vlastně penetrační test?



Dlouhodobá emulace aktivit technicky sofistikovaného škodlivého aktéra zaměřeného na cílové prostředí

Převážně manuální testy zaměřené na identifikaci známých i neznámých zranitelností v cílovém prostředí

Automatizované testy zaměřené na identifikaci známých zranitelností a konfiguračních nedostatků v SW

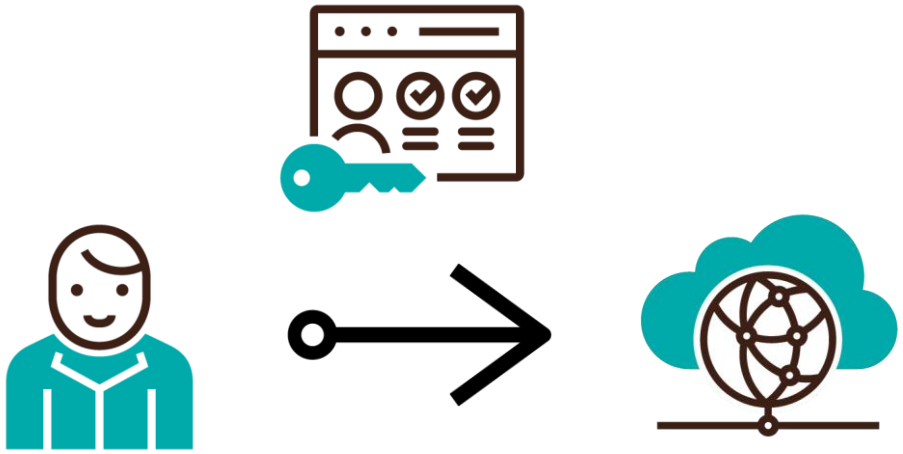
ALEF

S jakými typy penetračních testů se lze setkat?

Testy

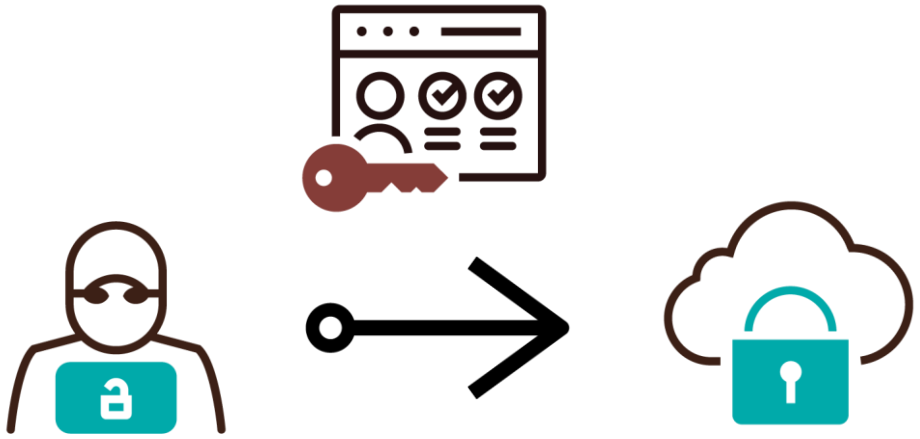
- webových a mobilních aplikací,
- IT infrastruktury,
- fyzických bezpečnostních opatření,
- lidského faktoru (sociální inženýrství),
- ICS, IoT, Wi-Fi, SIP,…

Co bychom čekali u webových aplikací?



ALEF

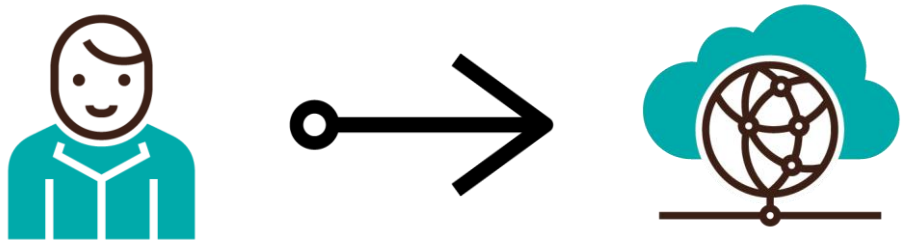
Co bychom čekali u webových aplikací?



ALEF

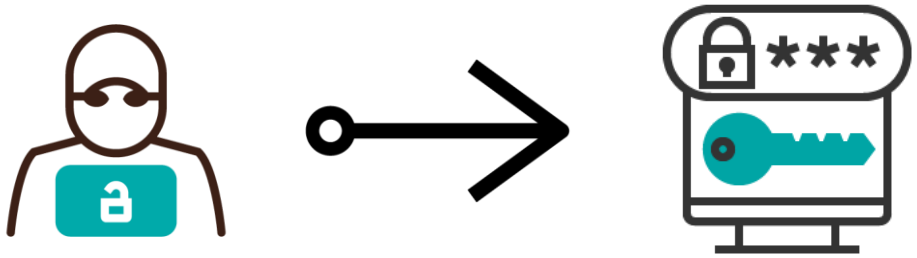
Co bychom u webových aplikací čekali méně?

jan.kopriva@alef.com



Co bychom u webových aplikací čekali méně?

admin@alef.com



Nebezpečné logy v bezpečnostních systémech

- Webové GUI ve FW, IPS, SIEM nebo log managementu není nic než webová aplikace
- Na ní ale přeci nikdo nemůže zaútočit...nebo ano?
- Většina bezpečnostních systémů umí logovat neúspěšné přihlášení i zobrazovat logy o této aktivitě
- Co když místo jména účtu vložíme do přihlašovacího pole škodlivý JavaScript?

Člověk není vždy tím nejslabším článkem

... občas k tomu má ale velmi blízko

- Na profesionálně vytvořený spear phishing s vizuálně identickou doménou a přihlašovacím portálem se téměř vždy někdo „chytí“
- Zajímavý flash disk se soubory jako „seznam odměn vedení.xls“ nebo „platové_výměry_2020.xls“ mívají velkou úspěšnost

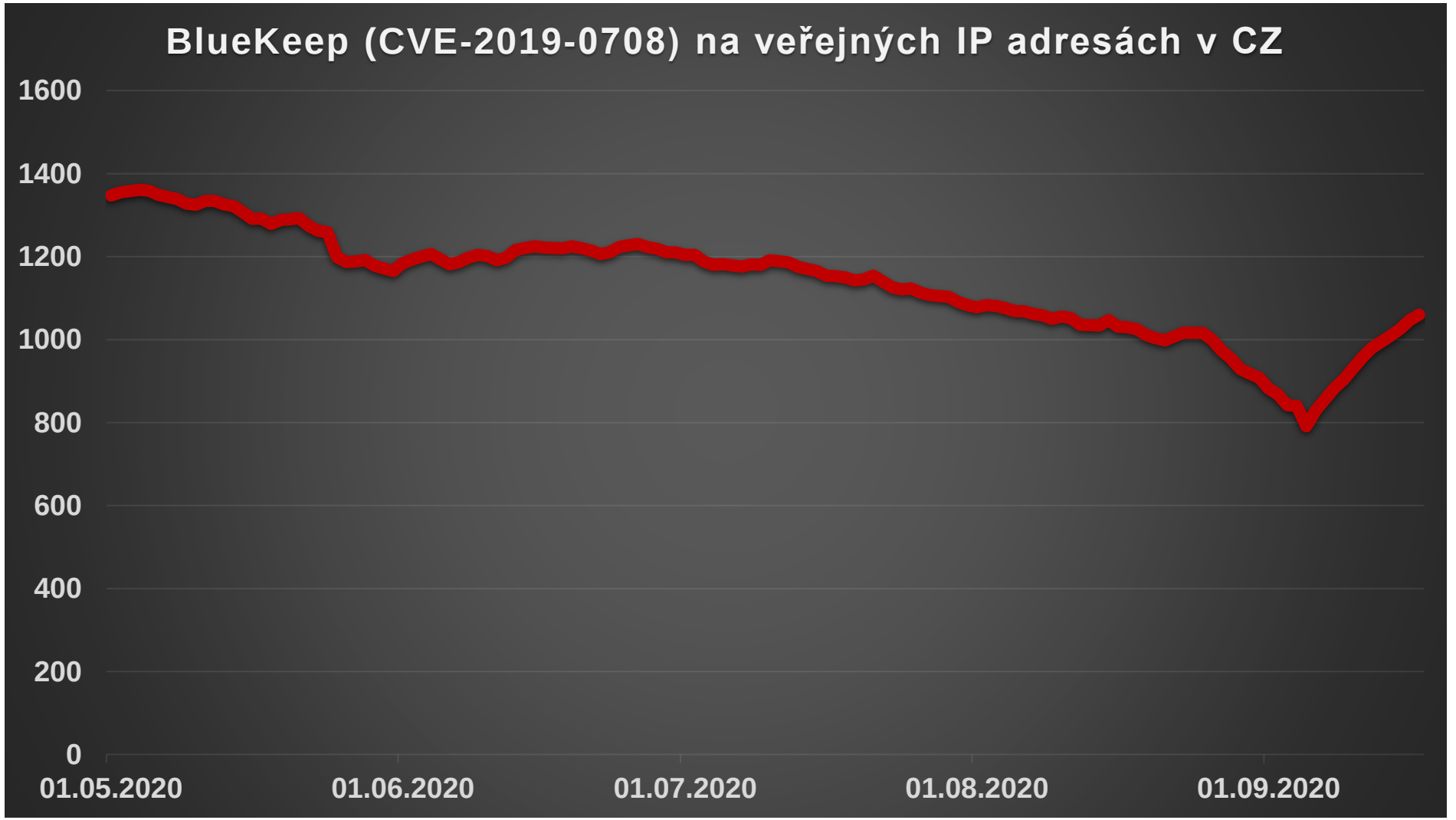
Ostraha ani ostnatý drát nemusí stačit...

- Bezpečnostní oplocení, kontrola všech přijíždějících vozidel do areálu před závorou a dvojité vstupní dveře do budovy vyžadující použití RFID karty zní velmi dobře...ale:
  - V době příjezdu ranní směny (6:00) je tma a s ohledem na vysokou frekvenci příjezdů je závora u vjezdu ponechána otevřená
  - Ranní příchozí se ne vždy osobně znají, ale dveře si vzájemně podrží
  - Kanceláře uvnitř budovy jsou opatřeny jmenovkami a nejsou zamčené

Zastaralé a nepatchované systémy jsou časté

ALEF

...ale neměli bychom je zpřístupňovat online



ALEF

O to podstatné ale nemusíme přijít jen online...

- Provádíte v rámci organizace bezpečnou skartaci již nepotřebných pevných disků?
- Máte správně nakonfigurované všechny webové servery?
- Nenahrávají zaměstnanci vaší organizace citlivá data na veřejná úložiště?

ALEF

Tohle se týká jen těch, co neřídí bezpečnost...

...nebo ne?

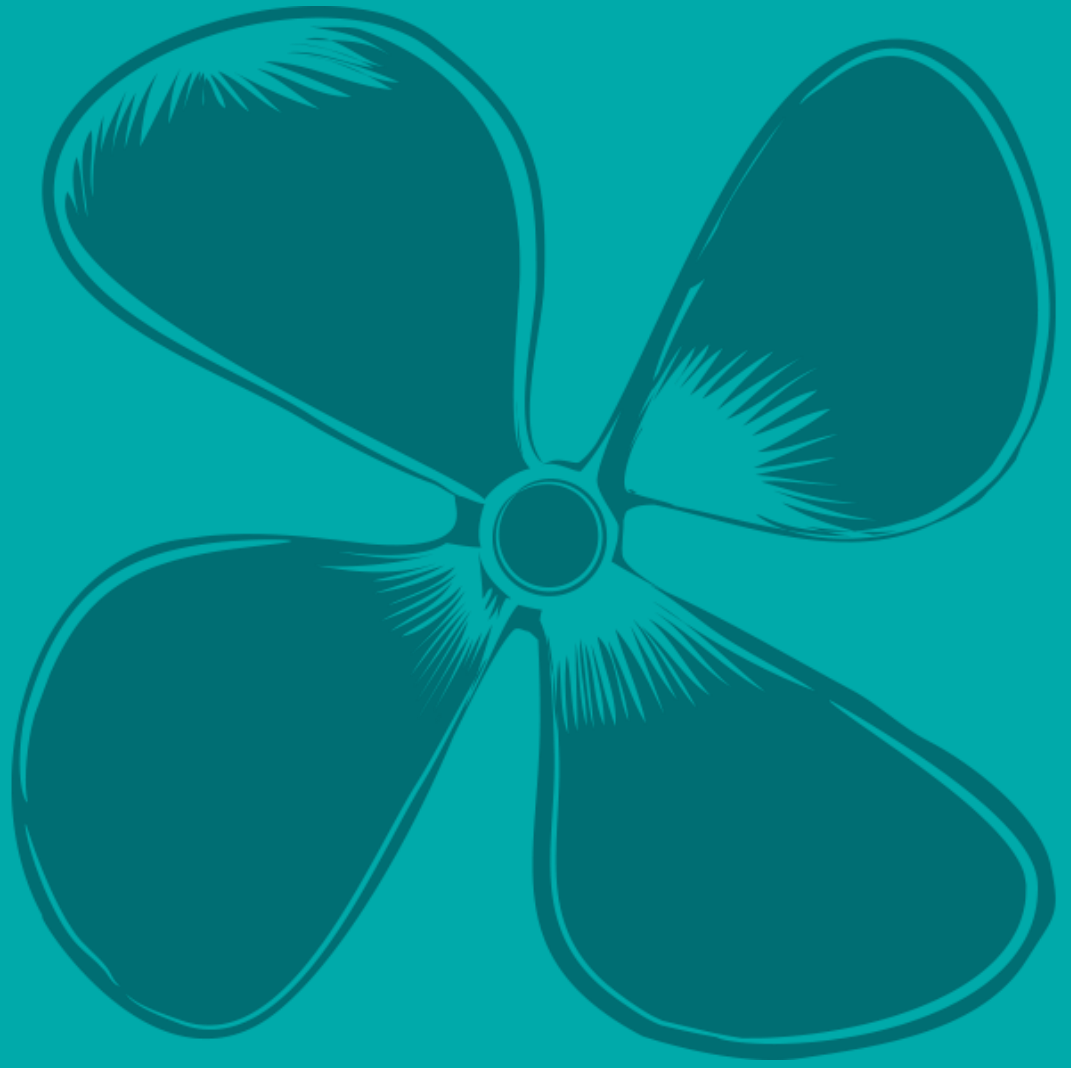
Compliance ≠ Security

Zranitelnosti jsou v každém prostředí

- Bez jejich aktivního vyhledávání je neobjevíme
- Pravidelné patchování a vulnerability skeny jsou dobrý základ, ale nestačí
- Praktické testování pomáhá
  - Pozor na omezený rozsah testů
  - Pozor na volbu testerů

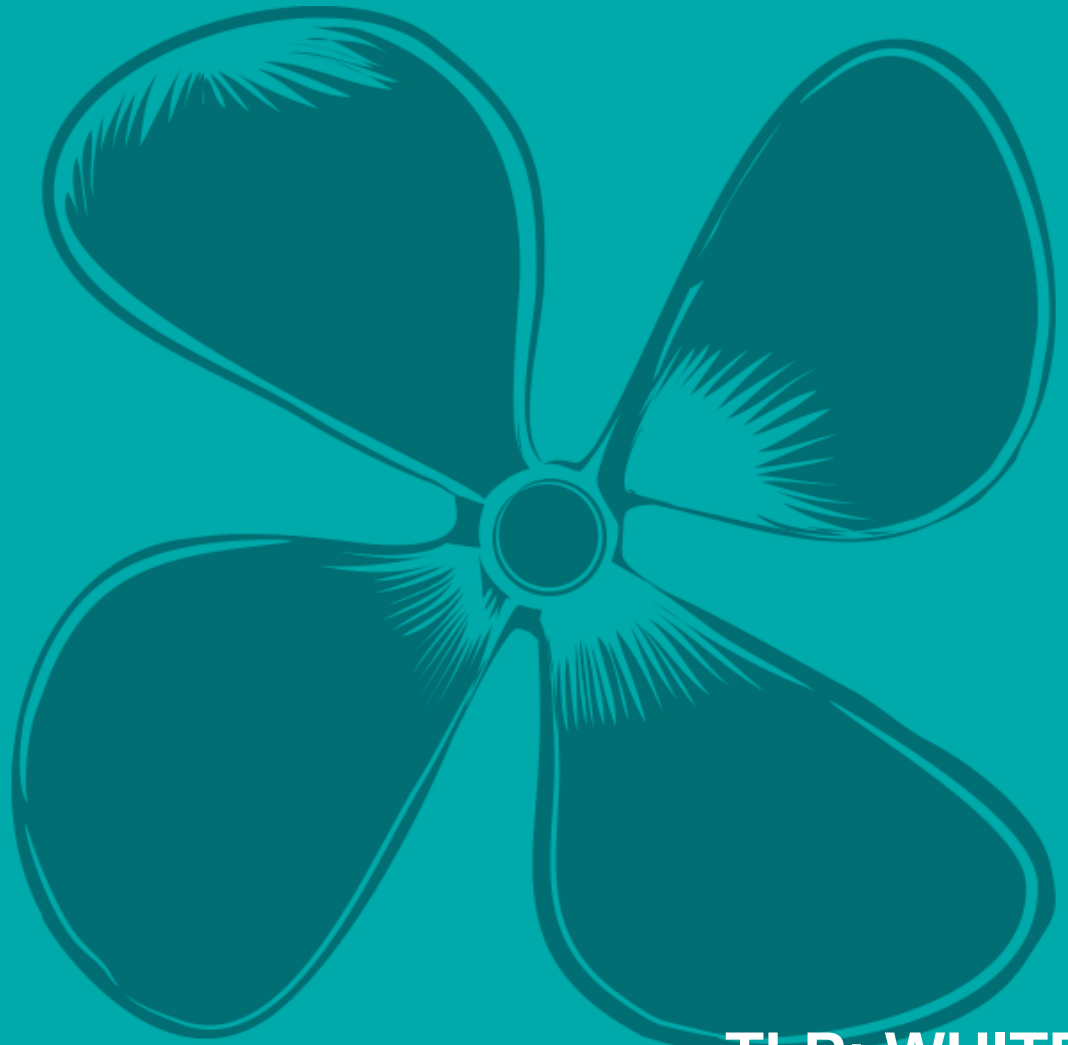
ALEF

Prostor pro Vaše dotazy



ALEF

Děkuji Vám za pozornost



TLP: WHITE