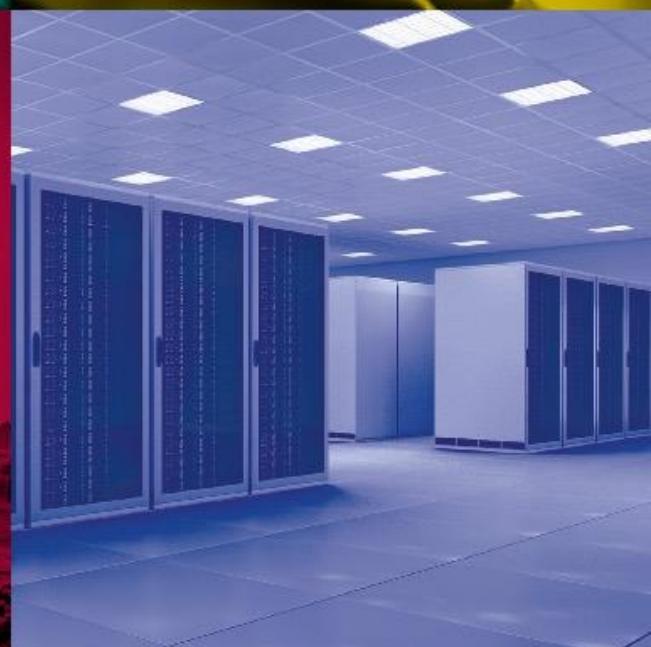
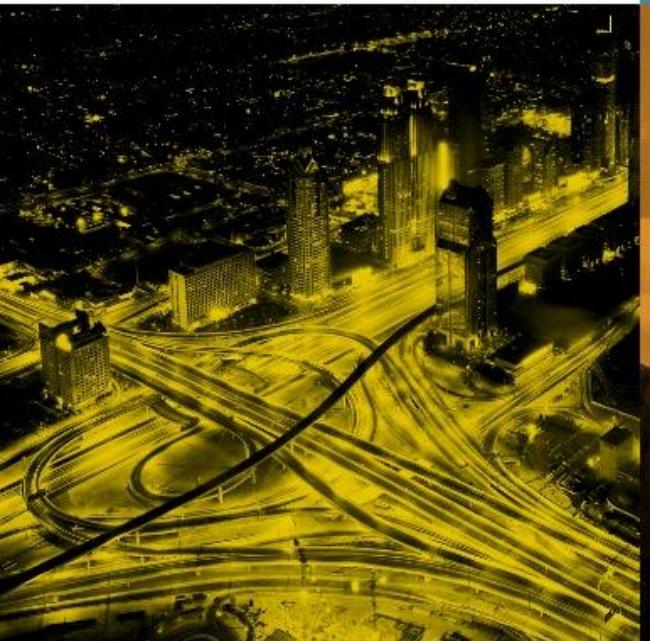


NIL





Robert Turnšek, NIL

INFORMACIJSKA VARNOST OBLAČNIH STORITEV



- V kompleksnih sistemih je varnost pametno razumeti kot **varnostno zanesljivost** (assurance), ne pa kot **količino** varnostnih kontrol
- **Varen sistem** je tisti, ki dela točno tisto, kar bi moral in nič manj
- Predvsem pa nič več!
- Sisteme privzeto postavljamo po **načelih najboljših praks** (ki jih je še kako mogoče izboljšati)

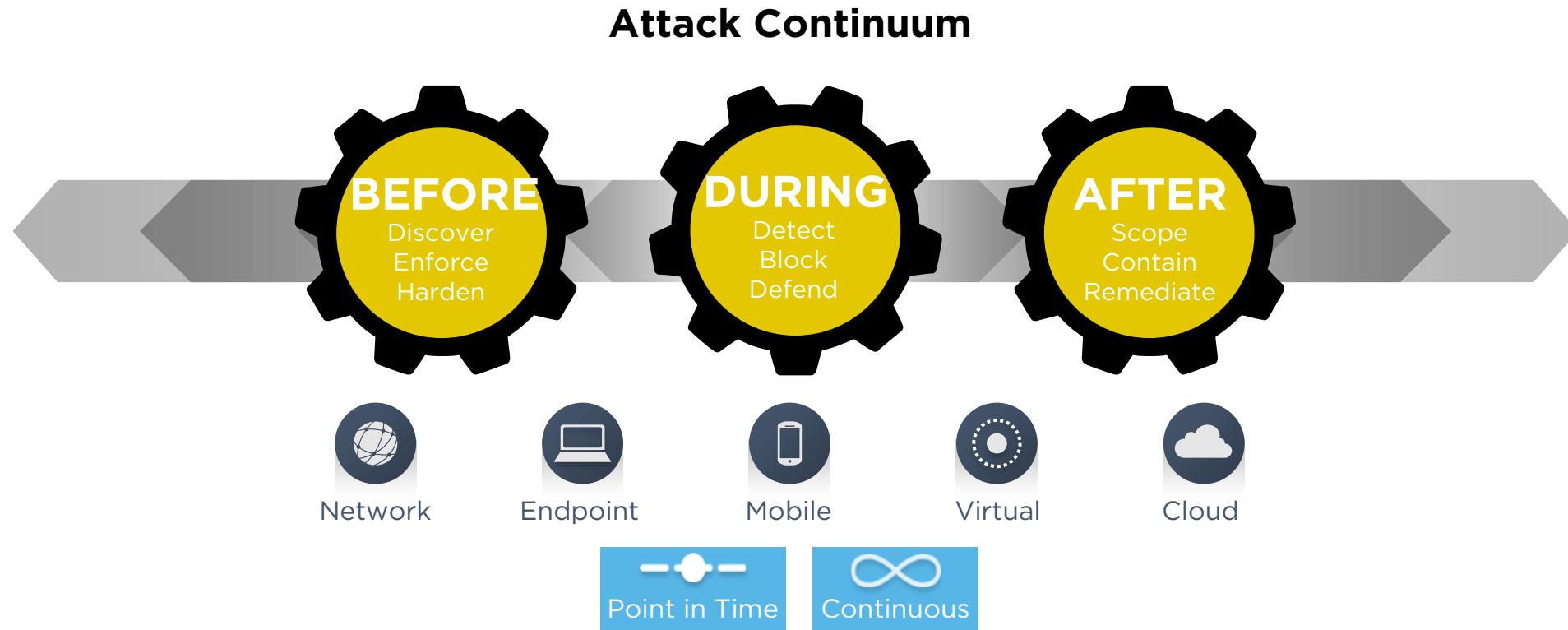


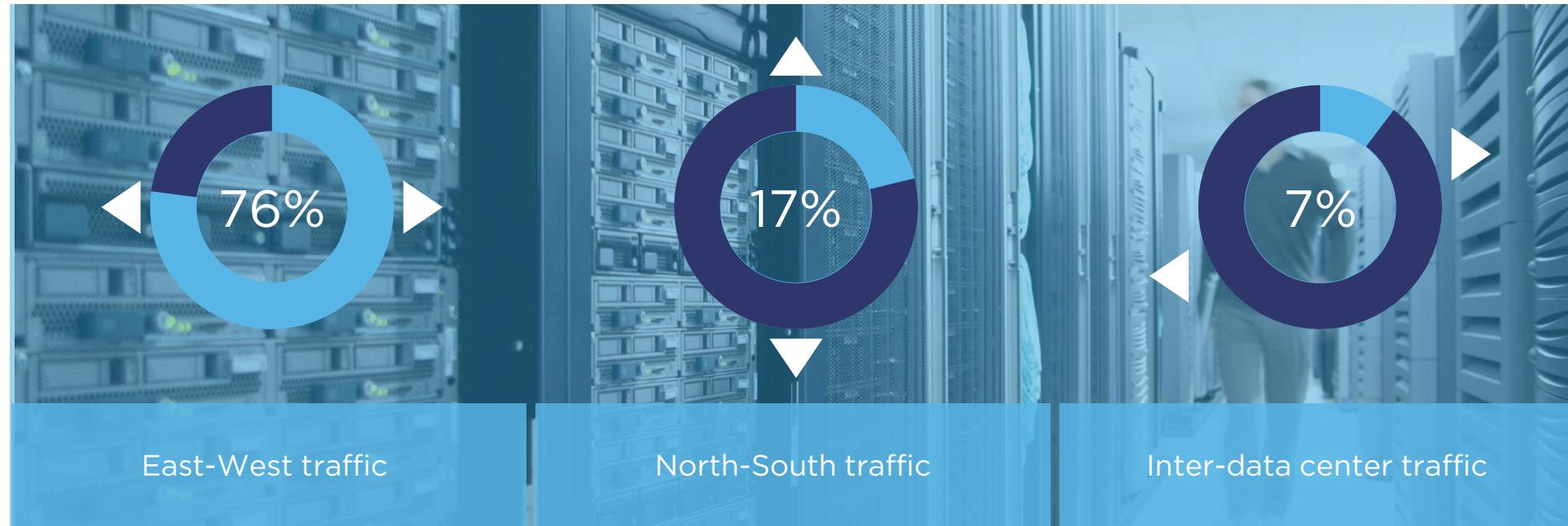


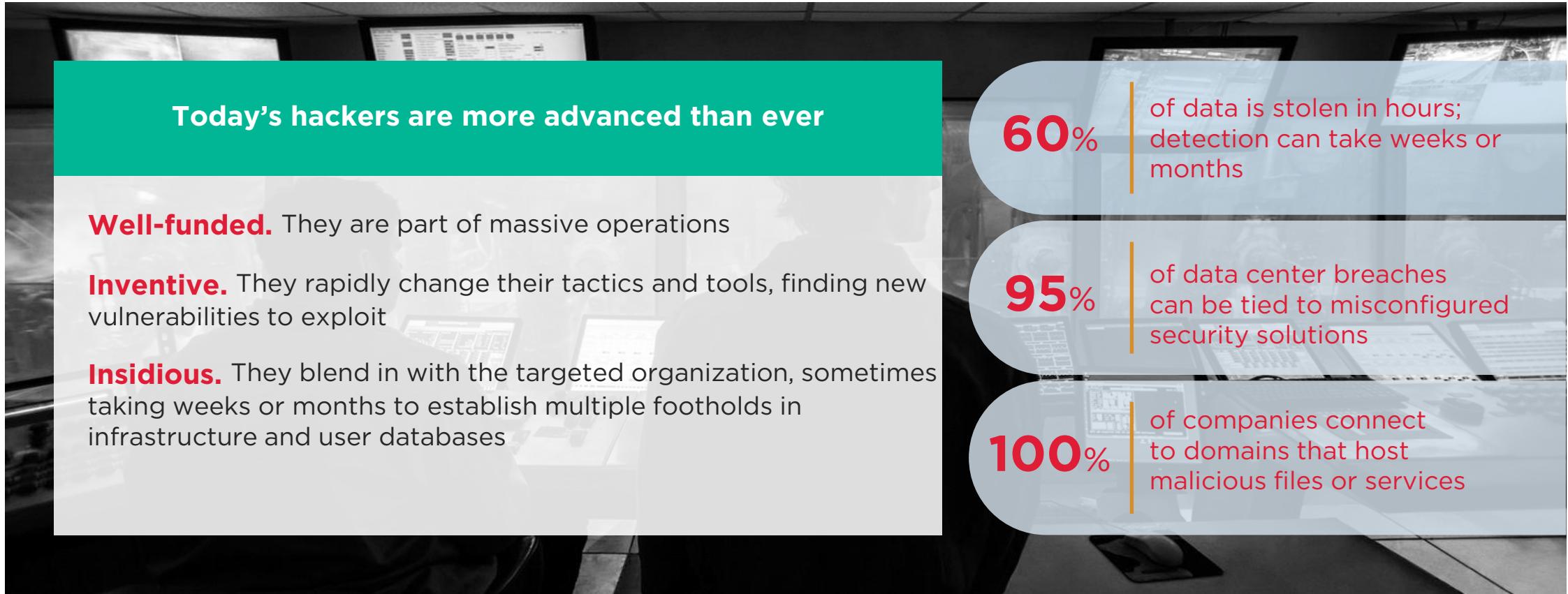
- V čem je varnost oblačnih infrastruktur drugačna od klasične informacijske varnosti?
 - Nove plasti programske opreme
 - Še bolj deljeni viri
 - Horizontalnost, velik doseg tveganj
 - Večstanovalskost in samopostrežba
 - Novi načini stika z Internetom



Varnost in časovna komponenta









1. Razumevanje in upravljanje tveganj „brez“ oblaka (fizična, infosec, itd.)
2. Horizontalno upravljanje tveganj oblačne infrastrukture (brez silosov)
3. Varnostna transparentnost proti stanovalcem in obojestransko razumevanje razmejitve varnostne odgovornosti med stanovalcem in upravljalcem (varnostni SLA/PLA ter obravnavo incidentov)
4. Varovanje upravljalnih vmesnikov oblaka, API in avtomatizacije
5. Varna logična ločitev stanovalcev na vseh nivojih ter obramba virov pred stanovalci samimi
6. Varnost osebja in upravljalnih procesov
7. Odpornost kritičnih funkcij oblaka na „eno varnostno napako“ (upravljalsko ali programsко/monokultурно)
8. DDoS (Internet / „shared“ naprave in povezave)
9. Varnostno krušenje, ponovno rojstvo in omejitve „testiranja“
10. Varno brisanje (ali šifriranje) medijev in nastavitev
11. SDL (varen razvoj programske opreme za oblačno infrastrukturo)





HVALA! / Q & A / rturnsek@nil.com