TOVEK

Každý má svá tajemství

Prověřování privilegovaných uživatelů pomocí OSINT

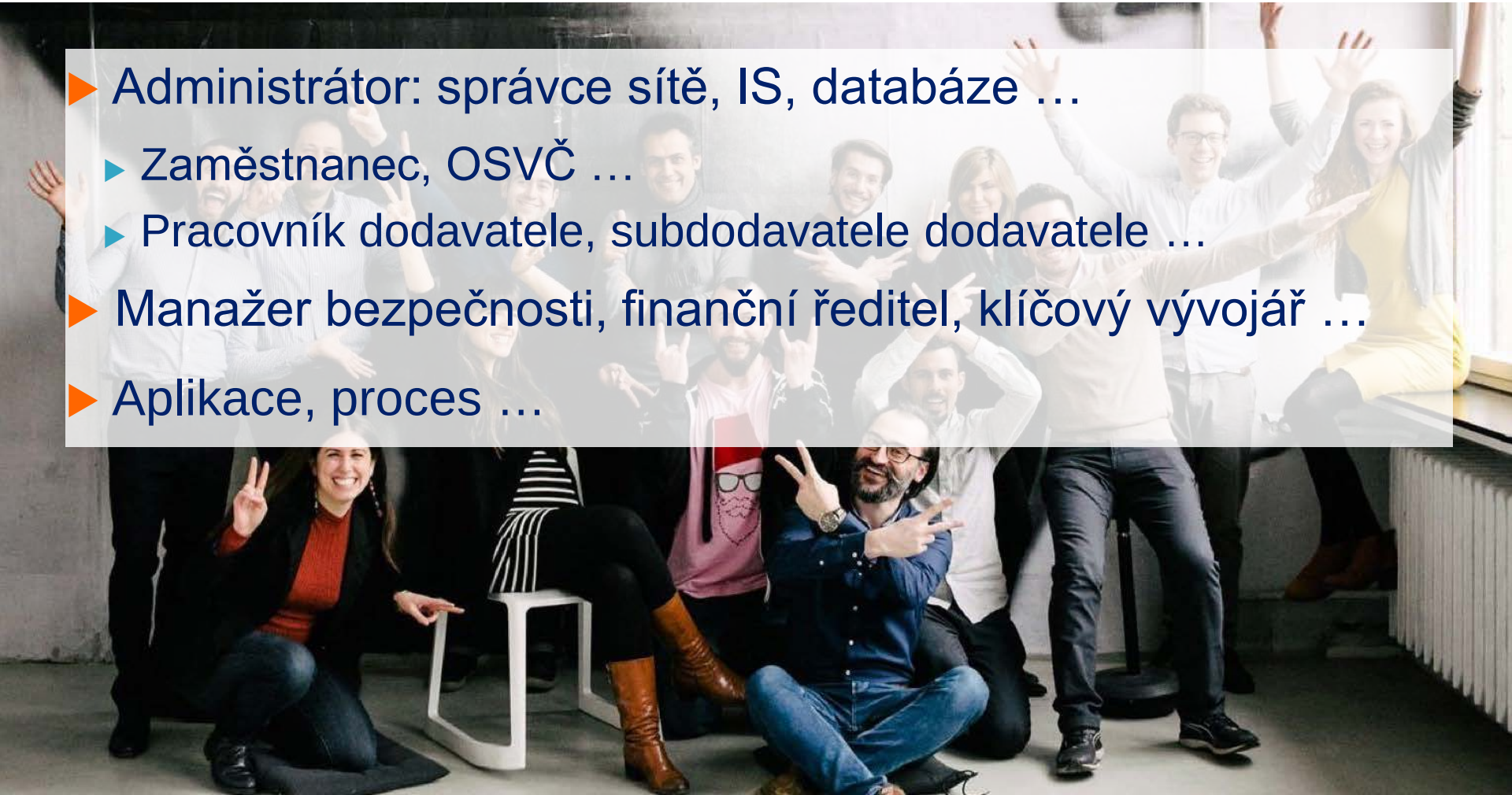
najít ▸
pochopit ▸
využít ▸

Miroslav Nečas

Osnova prezentace

- Celostní pohled na (kybernetickou) bezpečnost
  - Privilegovaní uživatelé
  - Bezpečnostní rizika
  - Vektory útoku na privilegované uživatele
- Každý má svá tajemství
  - Rizikový profil osoby, firmy
  - Prověřování založené na OSINT
  - SW kGate Finder
  - Ukázka výstupní zprávy

Privilegovaný uživatel



- Administrátor: správce sítě, IS, databáze …
  - Zaměstnanec, OSVČ …
  - Pracovník dodavatele, subdodavatele dodavatele …
- Manažer bezpečnosti, finanční ředitel, klíčový vývojář …
- Aplikace, proces …

Rizika spojená s privilegovanými uživateli

- **Narušení činnosti organizace**
  - Výroba produktů, poskytování služeb, výzkum a vývoj, řízení…
- **Újma na majetku organizace**
  - Finance, nemovitosti, výrobní zařízení, materiál, IP…
- **Ohrožení života, zdraví a práva**
  - Zaměstnanců, zákazníků i třetích stran
- **Reputační rizika**
  - Únik citlivých informací, ohrožení dobrého jména organizace

Vektory útoku na privilegované uživatele

- **Tradiční metody**
  - (Spear) Phishing, Mallware, Memory Crawling, Lateral Movement
- **Ještě tradičnější metody**
  - Zneužití důvěry a vztahů
  - Nátlak, vydírání, uplácení…
  - Různé formy sociálního inženýrství
- **Hybridní vektory útoku**

Privilegovaný uživatel nutně nemusí být oběť

Zhenhua Data Technology

Soukromou firmu založil a pravděpodobně spoluvlastní čínský občan Wang Xuefeng, bývalý inženýr IBM.

Posláním společnosti je: „Pomoci sběrem zámořských otevřených dat velkolepé obrodě čínského národa„

Zhenhua Data se na svém blogu na sociální síti nazývá Odbor 99, což může odkazovat na číslování divizí čínské armády.

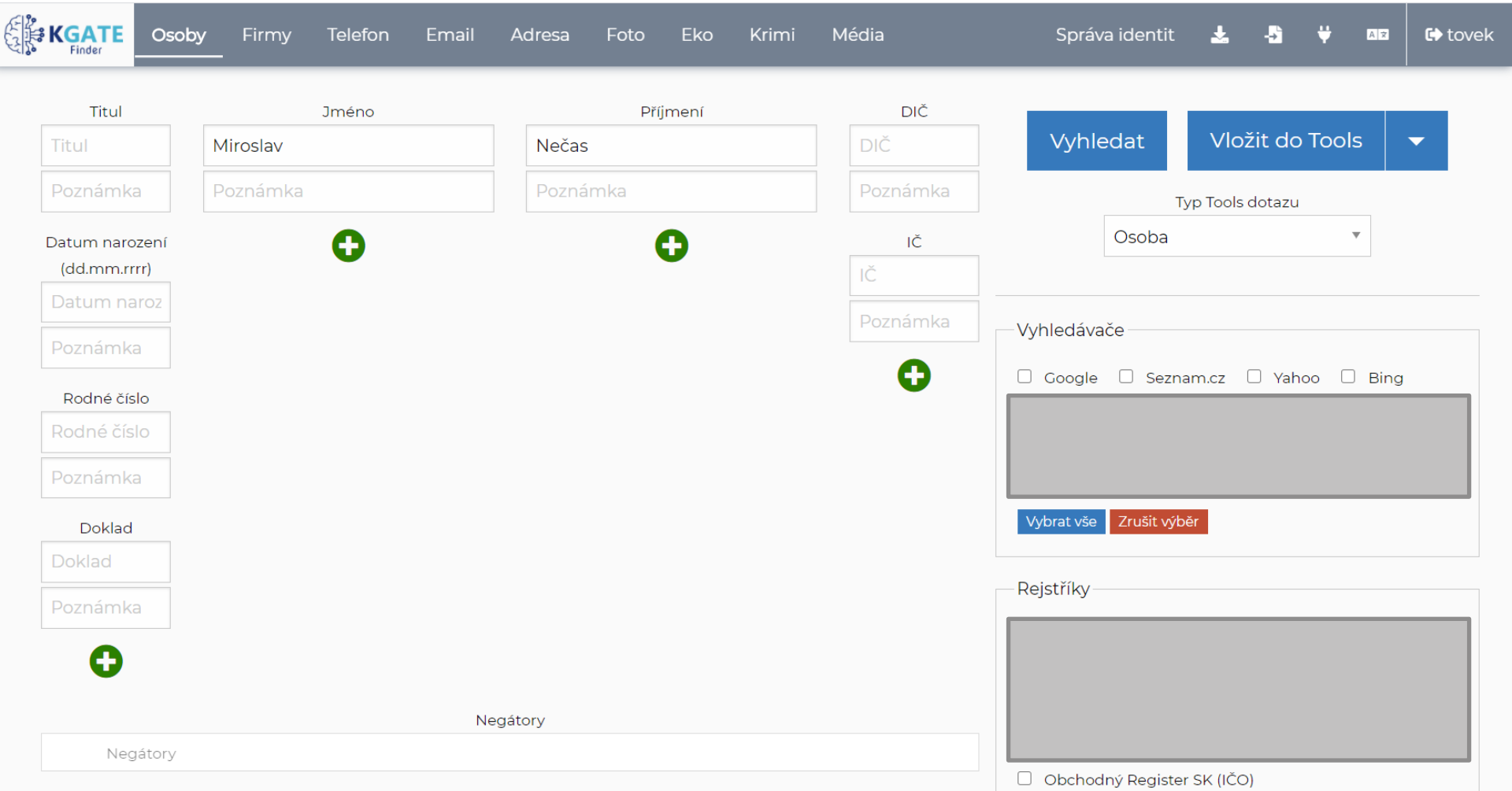
Jak dopředu zjistím, co se stane?

Rizikový profil osoby

Služba založená na OSINT

- **Prováděná eticky a legálně**
  - Souhlas prověřovaného
  - Otevřené zdroje informací
  - V souladu s GDPR
- **Prováděná expertem s podporou SW**
  - Automatizace manuálních úkonů
  - Lidská práce s vysokou přidanou hodnotou
  - Závěrečná zpráva a doporučení

Software kGate Finder



Více než 150 zdrojů

- Internetové vyhledavače a sociální sítě
- české i zahraniční rejstříky
- transparentní účty, dotace, smlouvy
- kriminální databáze a sankční seznamy
- internetová tržiště, sdílené prostory, DarkNet
- reverzní vyhledávání v obrázcích

Výstupní zpráva

- Prověřovaná osoba se na základě dostupných informací o vzdělání a praxi jeví jako kvalifikovaný specialista pro rozvojové projekty. V případě zájmu angažovat prověřovanou osobu, doporučujeme ověřit informace uvedené v profilu na LinkedIn, soustředit se zejména na úspěšnost realizovaných projektů.
  - Prověřovaný není evidovaný mezi hledanými, či pohřešovanými osobami. Ve veřejně dostupných zdrojích nejsou evidovány pohledávky po lhůtě splatnosti a ani exekuční tituly vztahující se k prověřovanému. Je vlastníkem, nebo spoluvlastníkem několika nemovitostí. Jedna z nich, která byla spoluvlastněna s paní xxxxxx, rodinný dům v obci xxxxxxx, byla aktuálně prodána.
  - Při analýze sociálních sítí a médií nebyly nalezeny negativní informace o činnosti prověřovaného vztahující se k aktivitám prověřovaného.
  - Prověřovaný je jednatelem ve společnosti xxxxxxxxxxxxxx Česká republika, IČ: xxxxxxxxxx.
  - Společnost vznikla xxxxxxx 100% vlastníkem společnosti je xxxxxxxxxx, a společnost sídlí na adrese bydliště. Bytovou jednotku vlastní xxxxxxxxx, vlastní mimo jiné, i lesní pozemek sousedící s pozemkem prověřovaného, na kterém je rekreační objekt. Majetky jsou v katastru obce xxxxxxxxx.
  - Společnost xxxxxxxxx se vysoce pravděpodobně angažuje v projektu xxxxxxxx. Tento projekt se zabývá vývojem a výrobou xxxxxxxx.
  - V roce xxxxxxxx prověřovaný kandidoval jako nezávislý do zastupitelstva obce. Získal xxxxxxxx hlasů.
  - Sportovní aktivity a koníčky nebyly prověřovány.

Pozvánka na workshop

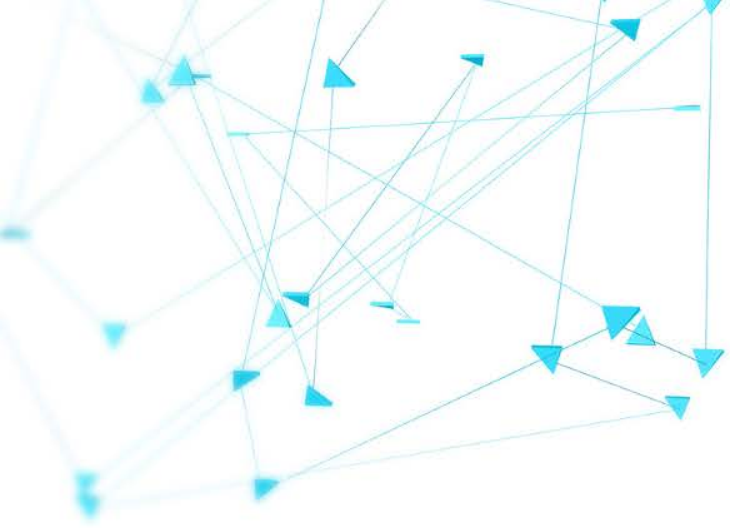
- **Analýza personálních rizik**
  - Workshop s Pavlem Hegerem, který má dlouholetou zkušenost ze státní i soukromé sféry. Připravoval podklady k hodnocení rizik při jednání s fyzickými a právnickými osobami pro politiky i manažery.
  - Ukáže vám jak, z množství dílčích informací propojených do souvislostí vyvodit stručné a jasné závěry či doporučení.
  - Dokáže vám, že chytré zpracování informací z čistě otevřených zdrojů je pro byznys mnohem důležitější a mnohem bezpečnější než snahy získávat informace nelegálně a neeticky.
- **Tovek Academy, Chrudimská 2, Praha 3, max. 12 osob**
  - 12. listopadu 2020
  - 26. listopadu 2020
  - 3. prosince 2020

kontakt: info@tovek.cz

Otázky a odpovědi

- Celostní pohled na (kybernetickou) bezpečnost
  - Bezpečnostní rizika spojená s privilegovanými uživateli
  - Hybridní vektory útoku

- Každý má svá tajemství: služba s přidanou hodnotou
  - Rizikový profil osoby / firmy
  - Prověřování založené na OSINT
  - Výstupní zpráva s doporučením dalších kroků



TOVEK

Děkuji vám za pozornost!

Miroslav Nečas
necas@tovek.cz