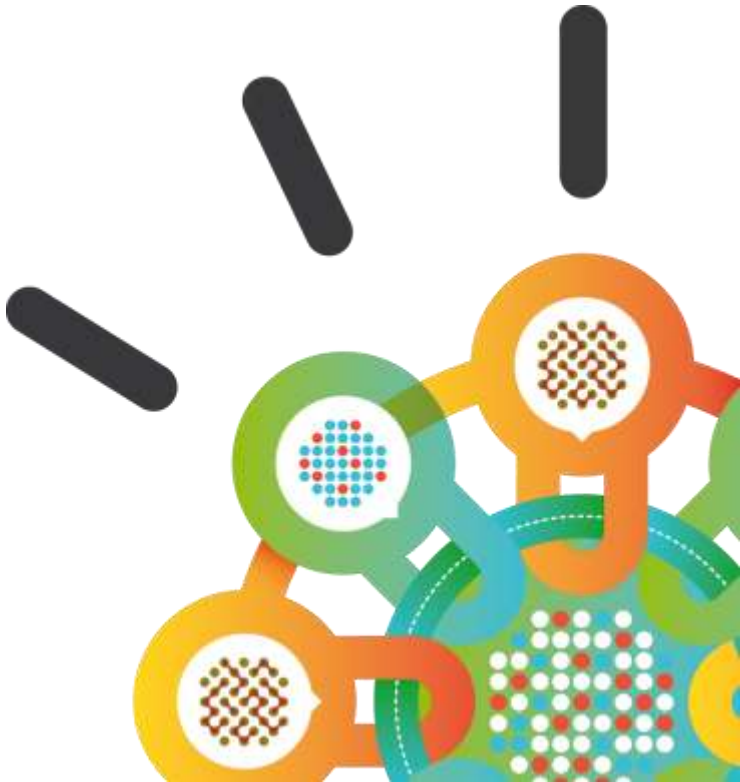
Security Intelligence.
Think Integrated.

Bezpečnostní témata spojená se Zákonem o kybernetické bezpečnosti

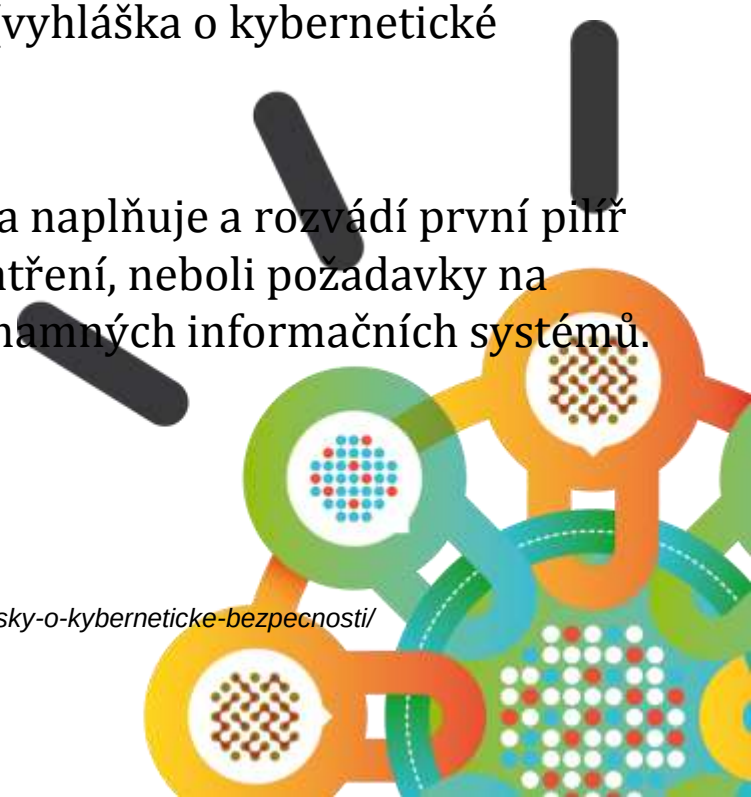
Ing. Jiří Slabý, Ph.D.
Business Solution Architect
IBM



Zákon je zákon

Národní bezpečnostní úřad vypracoval k návrhu zákona o kybernetické bezpečnosti, který byl předložen k dalšímu legislativnímu procesu do Parlamentu Českére publiky, **návrh prováděcího předpisu**, kterým je vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti).

Návrh **vyhlášky o kybernetické bezpečnosti** zejména naplňuje a rozvádí první pilíř zákona o kybernetické bezpečnosti – bezpečnostní opatření, neboli požadavky na standardizaci kritické informační infrastruktury a významných informačních systémů.



Zdroj: http://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/nbu-vypracoval-navrh-vyhlasky-o-kyberneticke-bezpecnosti/

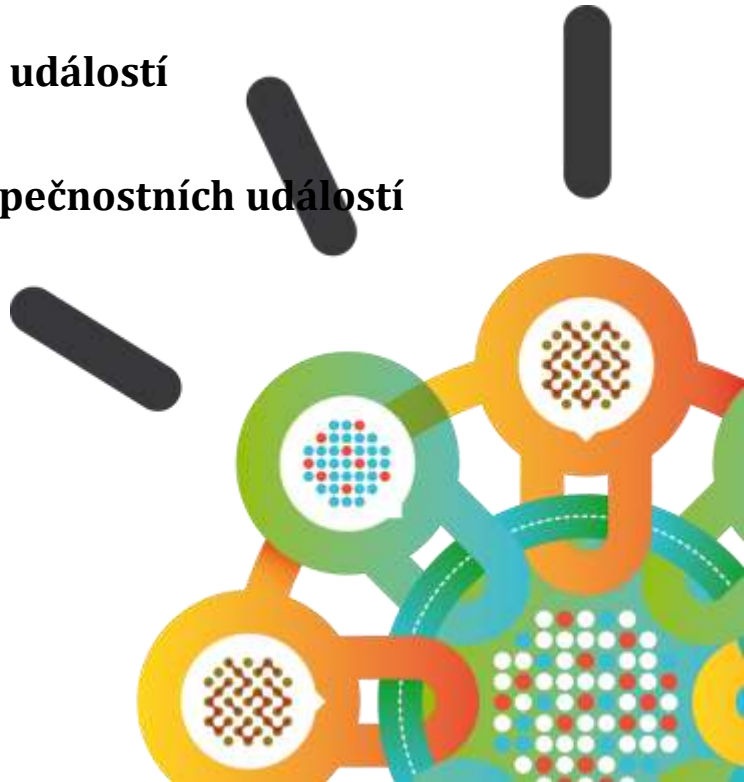
Řada technických opatření

§ 11 - **Řízení přístupu a bezpečné chování uživatelů**

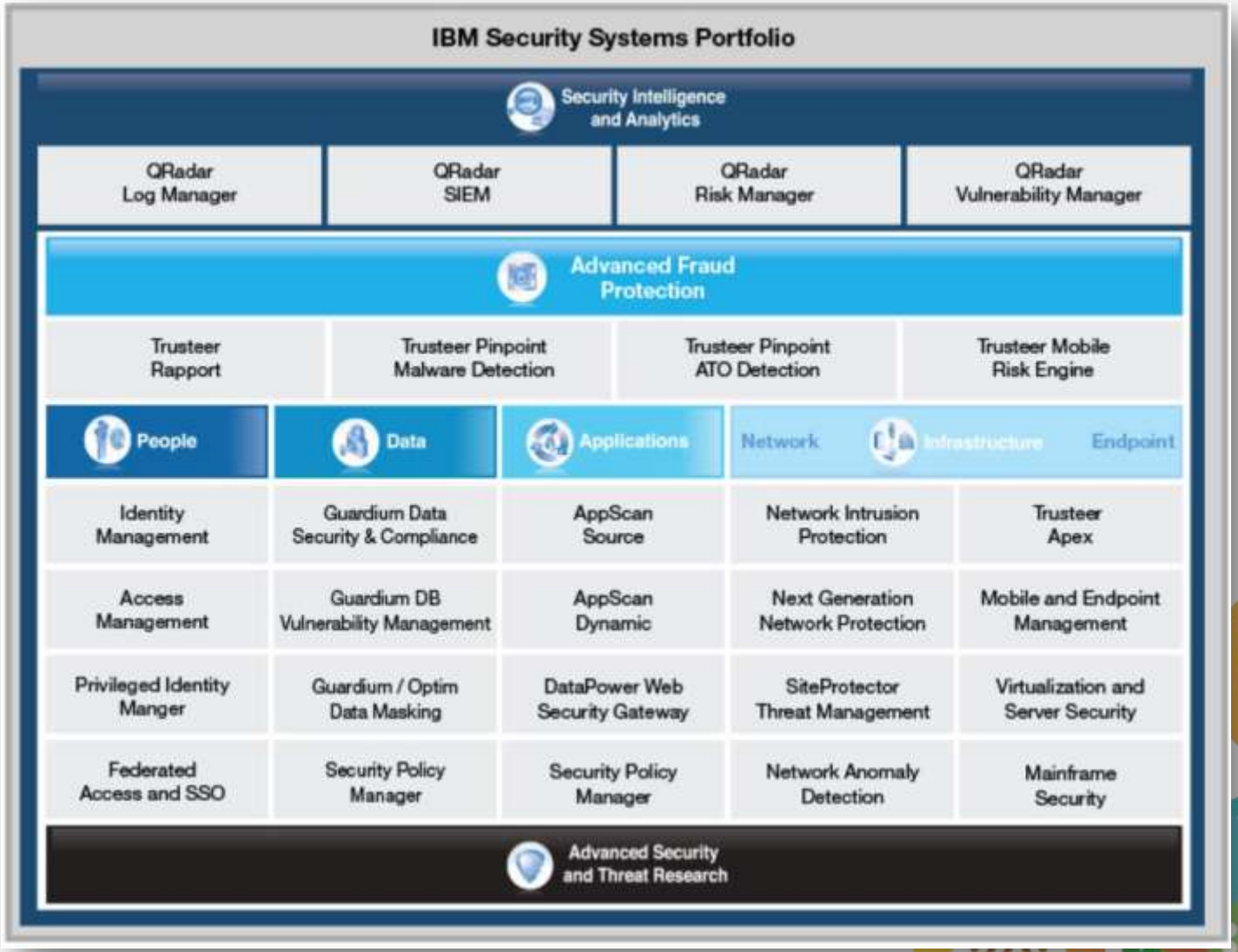
§ 21 - **Nástroj pro zaznamenávání činností kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů**

§ 22 - **Nástroj pro detekci kybernetických bezpečnostních událostí**

§ 23 - **Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí**



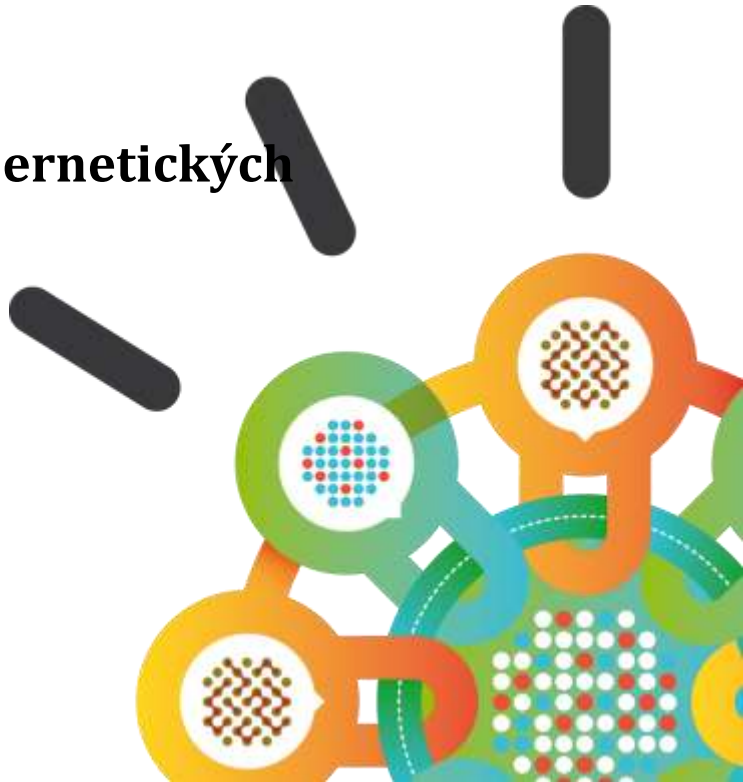
IBM Security Framework



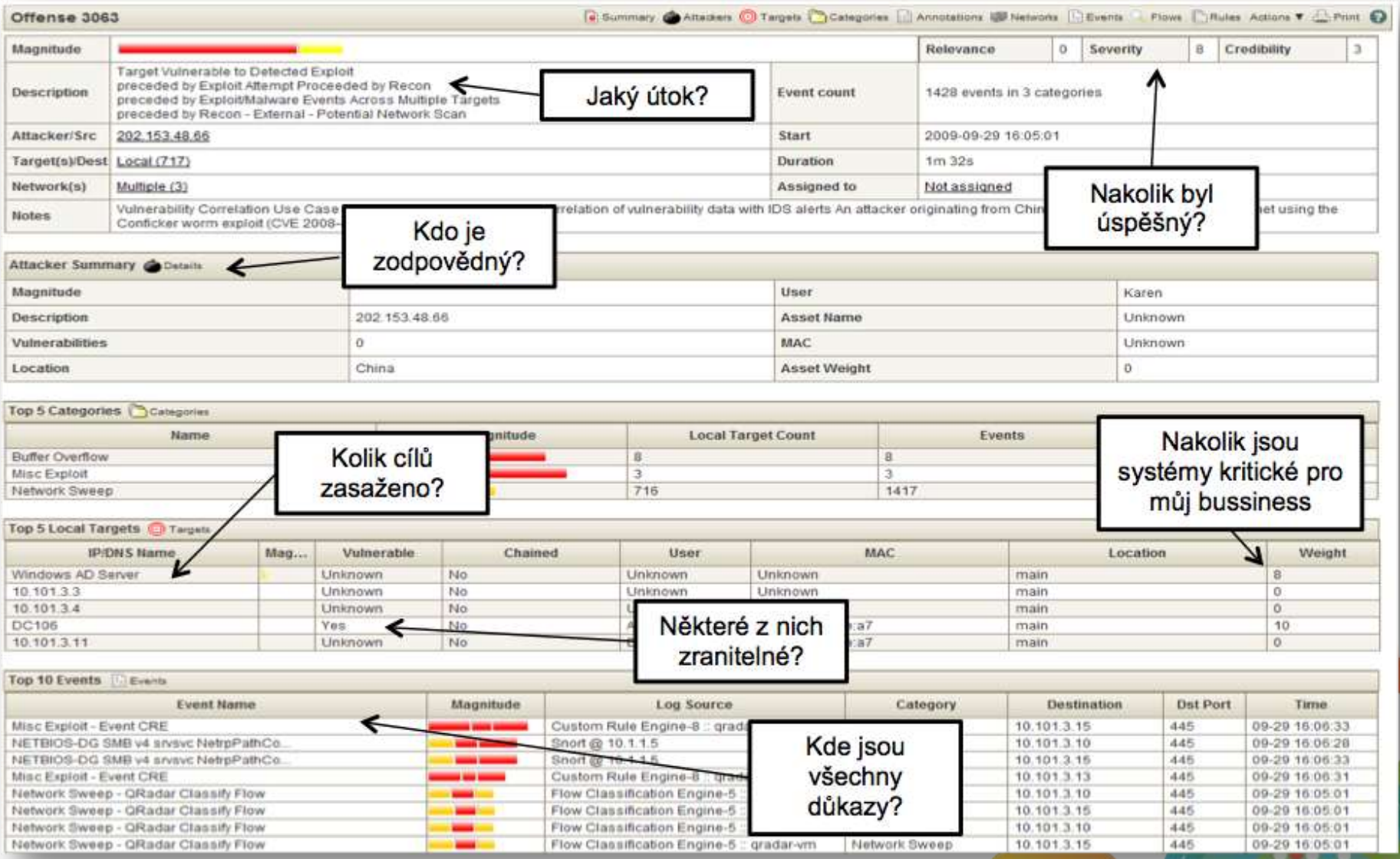
Security Intelligence.
Think Integrated.

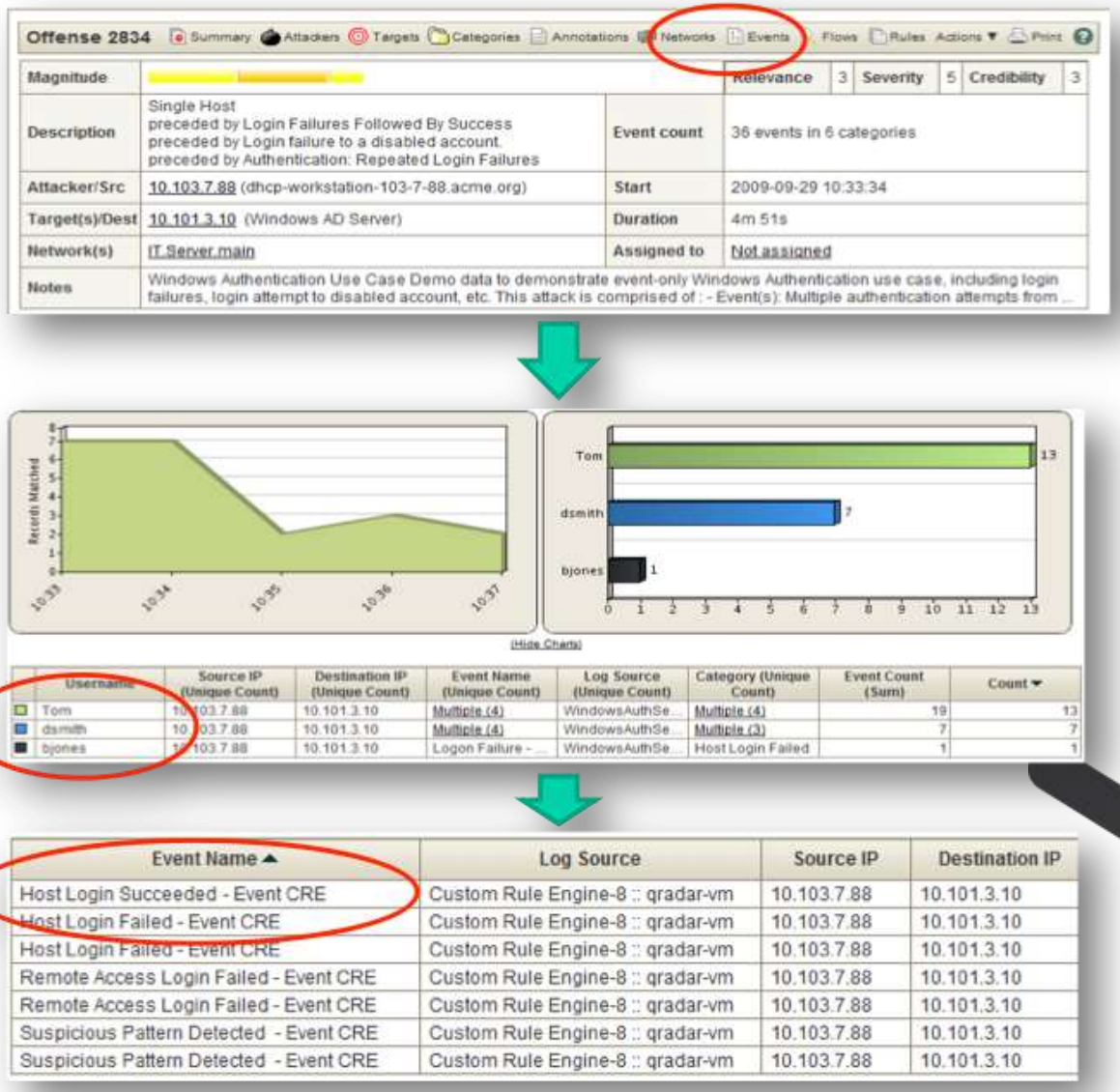
§ 23 - **Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí**

IBM QRADAR SIEM



Security Information and Event Management = SIEM





Opakované neúspěšné přihlášení (Že by uživatel zapomněl heslo?

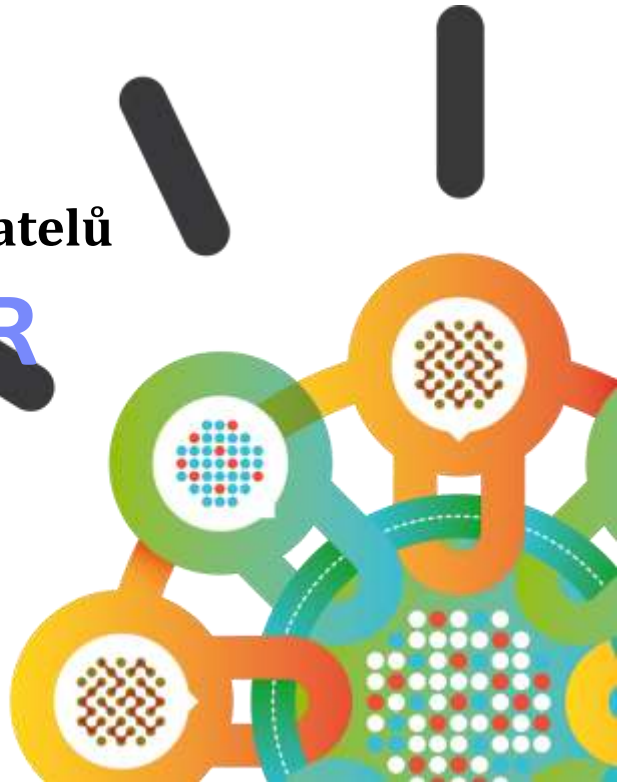
Opakované neúspěšné přihlášení na více účtů (Brutal force útok?)

Po čase se login podařil = host byl kompromitován

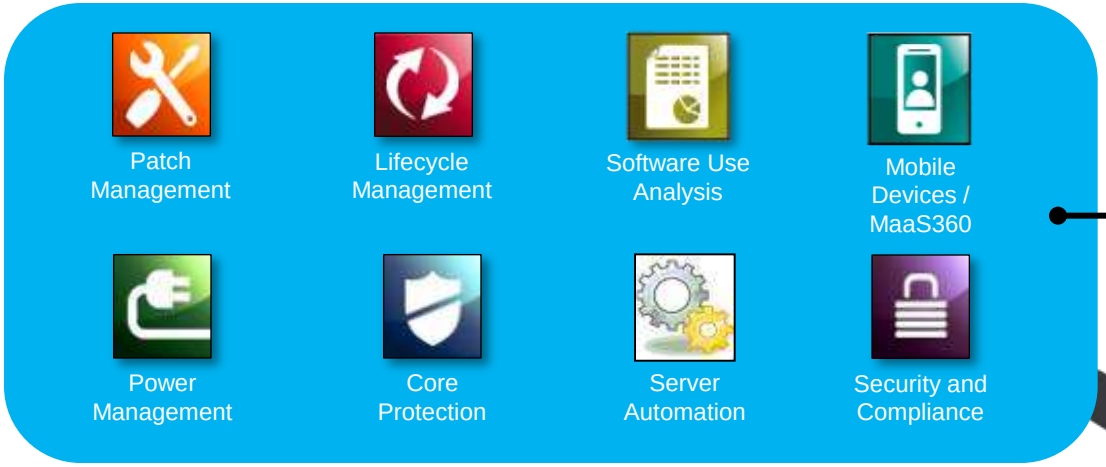
Security Intelligence.
Think Integrated.

§ 11 - **Řízení přístupu a bezpečné chování uživatelů**

IBM ENDPOINT MANAGER
IBM MAAS360



IBM Endpoint Manager



- Jeden agent
- Jedna konzole
- Jedna infrastruktura
- Jeden server

Správa zařízení

Zabezpečení zařízení

IBM Endpoint Manager

Patch Management

Vlastnosti:

- Správa aktualizací OS a aplikací
- Windows, Mac OS X, Linux a UNIX
- Aplikace:

- Adobe Acrobat, Reader
- Apple iTunes, QuickTime
- Adobe Flash Player, Shockwave
- Mozilla Firefox
- RealPlayer
- Skype
- Oracle Java Runtime
- WinAmp, WinZip

Přínosy:

- Bezchybná aktualizace pro všechny podporované systémy a aplikace
- Není nutno sledovat jednotlivé dodavatele, zda vydali nové aktualizace
- Kontinuální kontrola na úrovni agenta

Lifecycle Management

Vlastnosti:

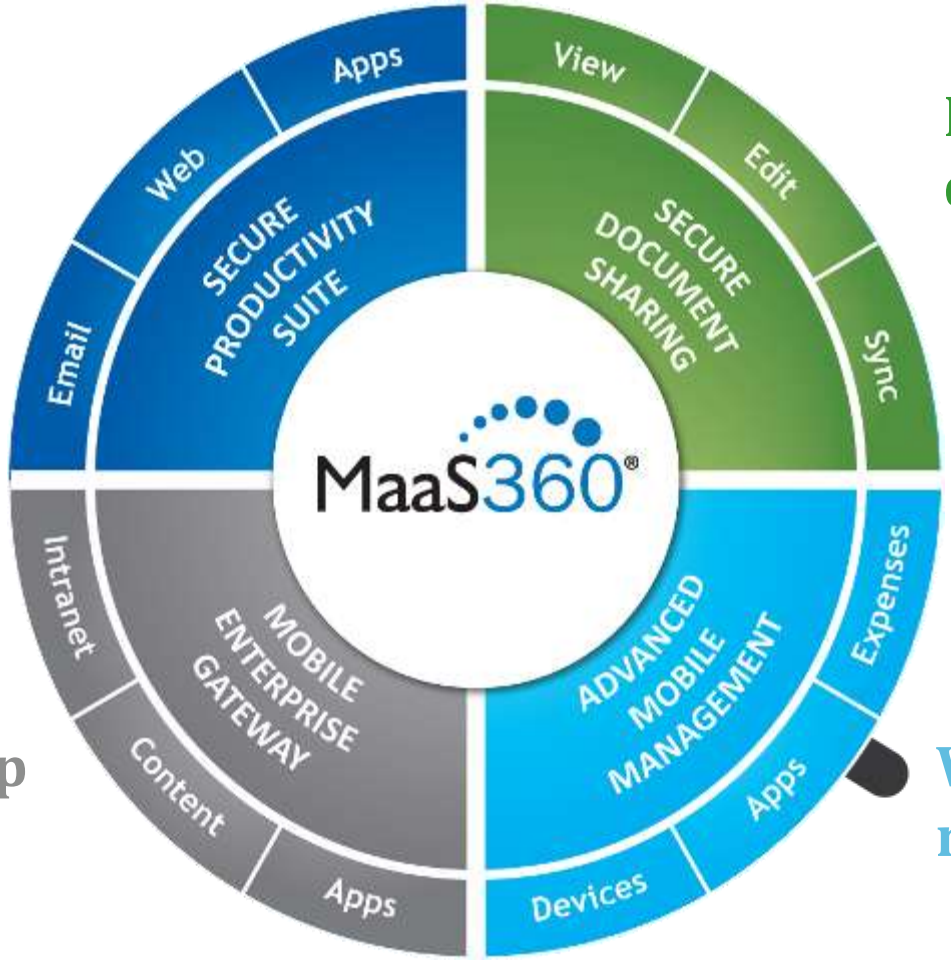
- Automatické odhalení zařízení
- Patch Management
- Inventorizace HW a SW
- Distrubuce SW
- OS instalace
- Vzdálený přístup

Přínosy:

- Jediná konzole pro správu kompletního životní cyklu stanic i serverů všech OS
- Od instalace OS, přes každodenní údržbu až po reinstalaci
- Katalog SW pro koncové uživatele

Bezpečný kontejner

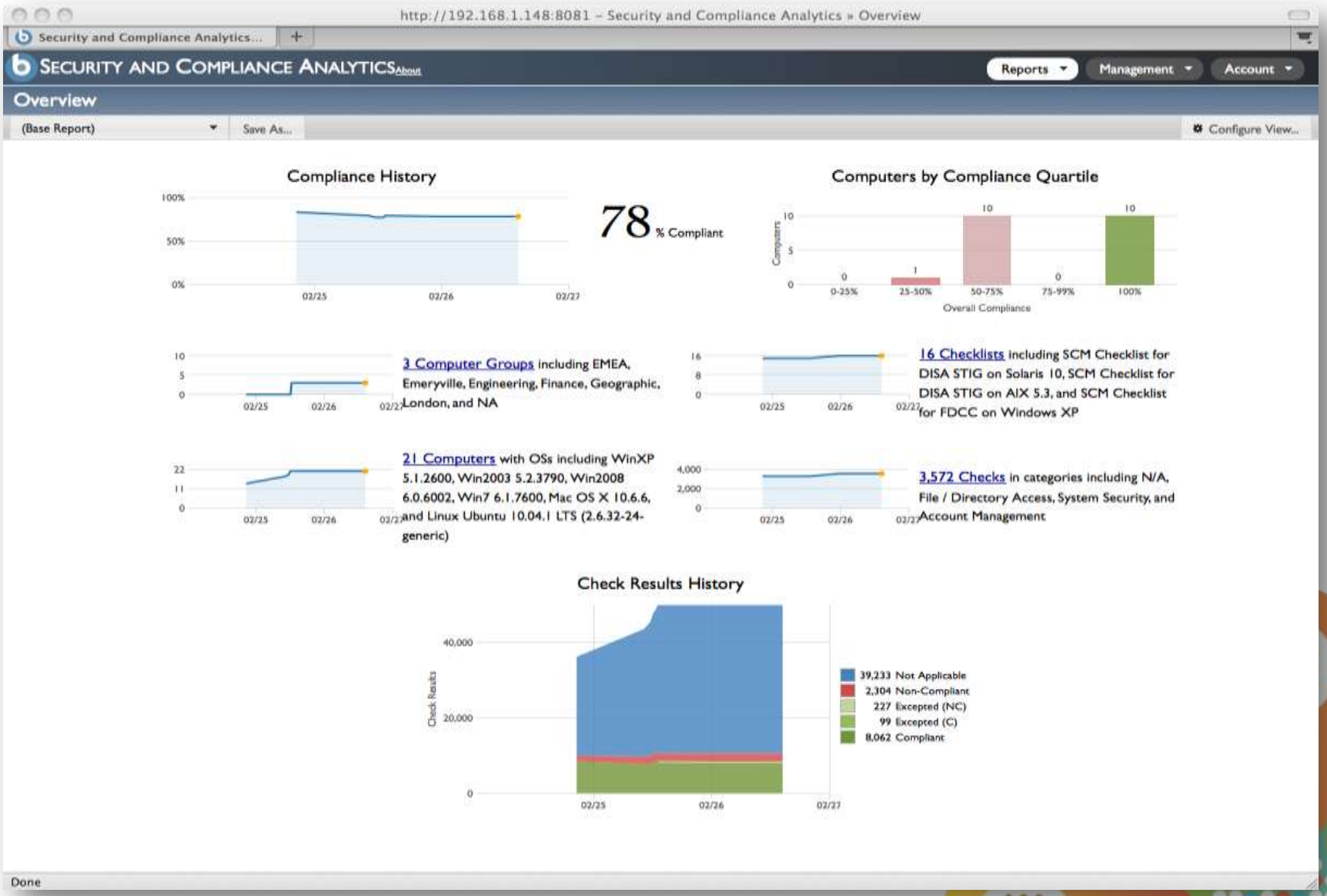
Bezpečné sdílení dokumentů



Snadný přístup do vnitřní sítě

Výkonná správa mobilních zařízení

Jediná platforma pro všechny mobilní potřeby



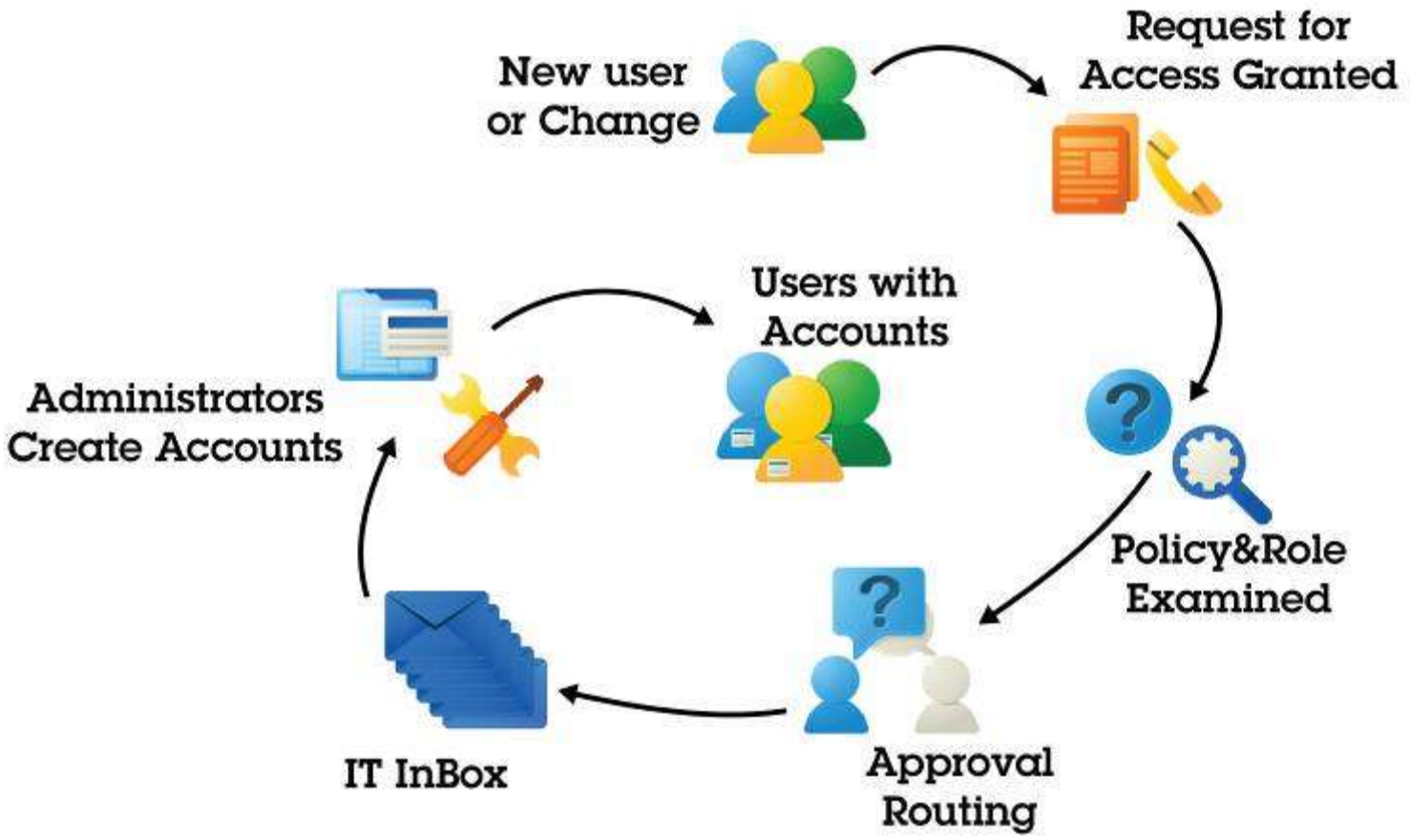
Security Intelligence.
Think Integrated.

§ 11 - **Řízení přístupu a bezpečné chování uživatelů**

§ 21 - **Nástroj pro zaznamenávání činností kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů**

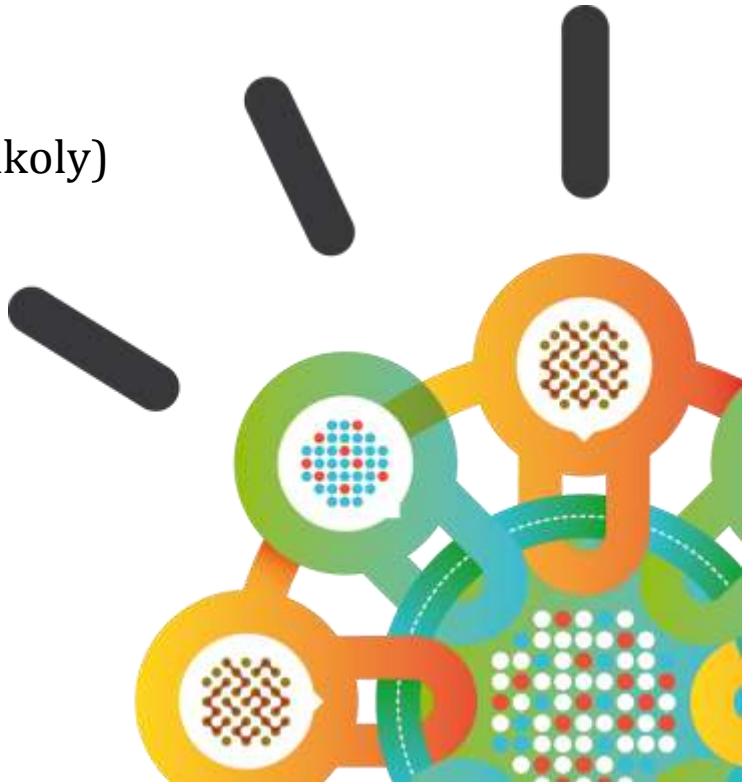
IBM SECURITY IDENTITY MANAGER

Uživatelé, identity a životní cyklus



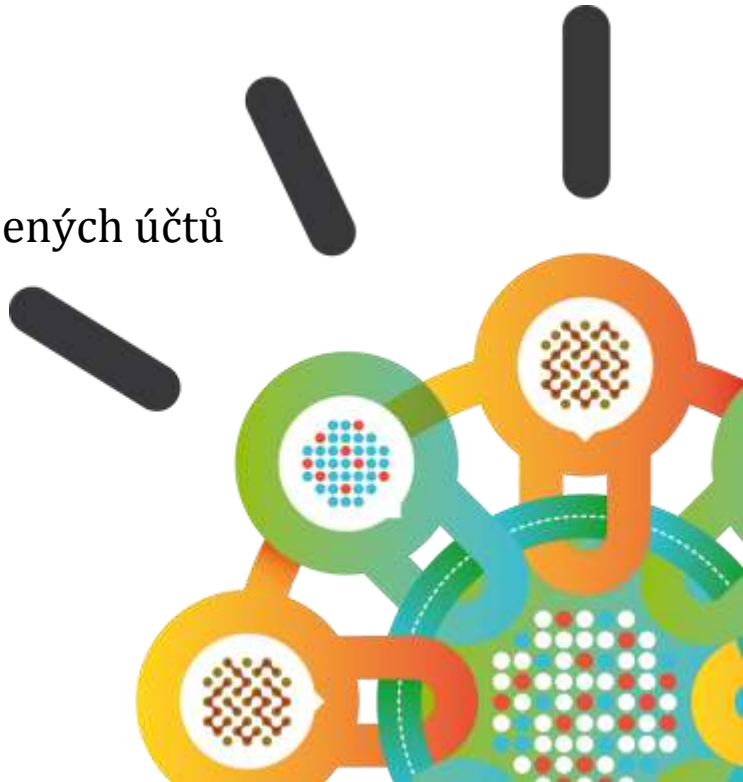
Typické problémy

- Neexistence politiky hesel a řízení přístupů
  - Přílišná komplexita a různorodost systémů
  - Nevyhovující nebo nepoužívané účty
- Neschopnost řídit celý cyklus uživatele
- Obtížné definovat a kontrolovat střet zájmů
- Soulad s předpisy (vnitřní, právní, ...)
- Nízká produktivita
- Náročnost na interní help-desk (repetitivní úkoly)

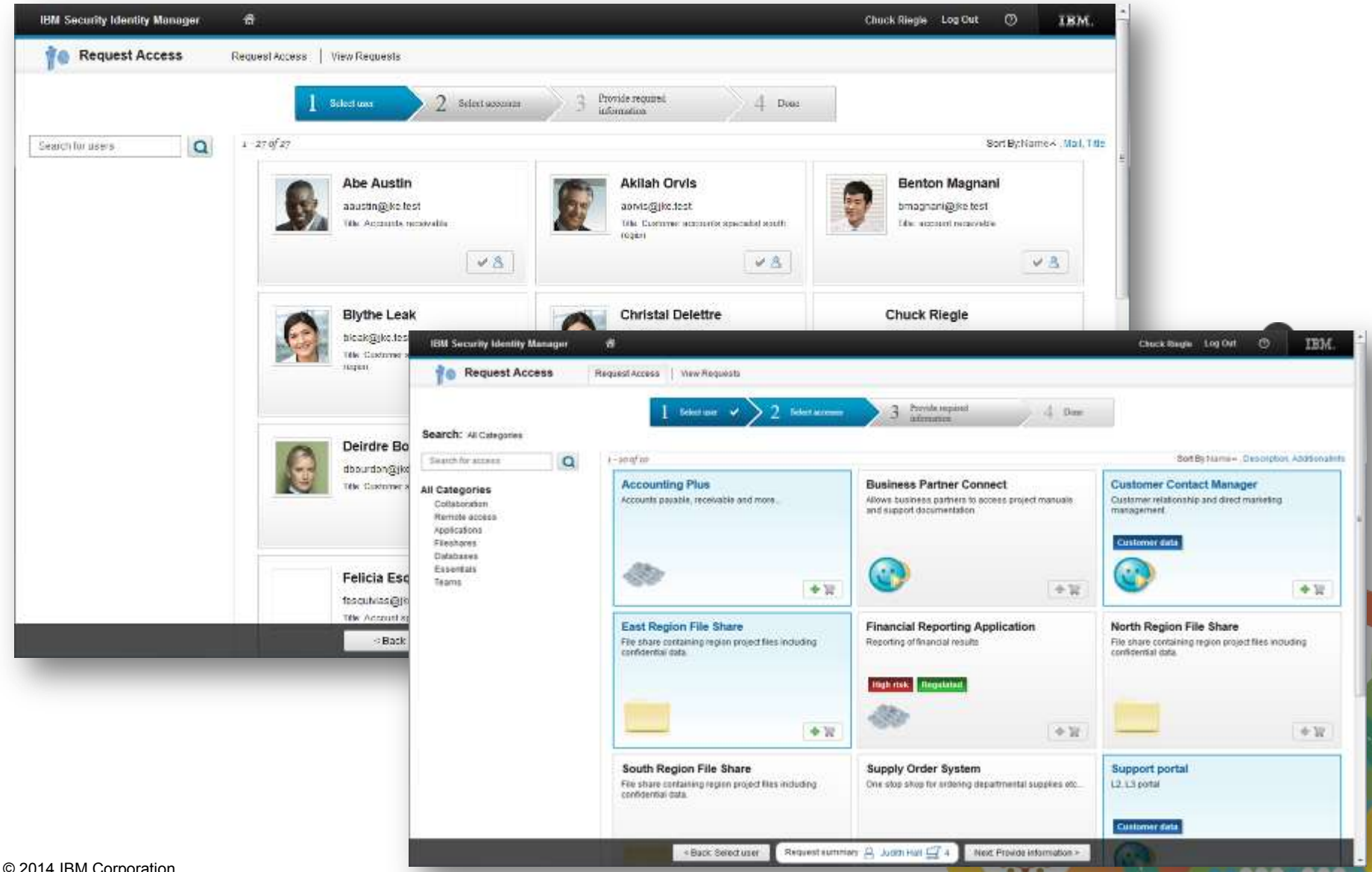


Co to přinese

- Umožňuje spravovat identity v rámci celého životního cyklu
  - Napříč všemi aplikacemi
- Je založen na rolích a politikách
- Pokročilá správa uživatelů rolí a jejich modelování
- Automatizace procesů a definice workflows
- Vynucování dodržování různých politik
- Self-service rozhraní pro uživatele
- Rozlišuje typy účtů – uživatelé a služby
- Rozšiřielnost o správu privilegovaných a sdílených účtů
- Možnost správy z mobilních zařízení
- Reportování, auditování



Moderní rozhraní i pro mobilní zařízení



Moc děkuji

Jiří Slabý
+420 731 435 836
jiri_slaby@cz.ibm.com

Jiří Kucr
+420 777 666 642
jiri_kucr@cz.ibm.com