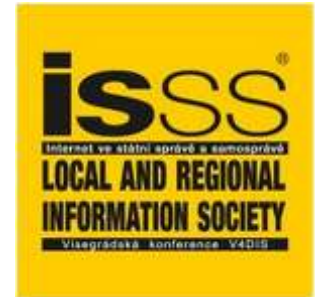
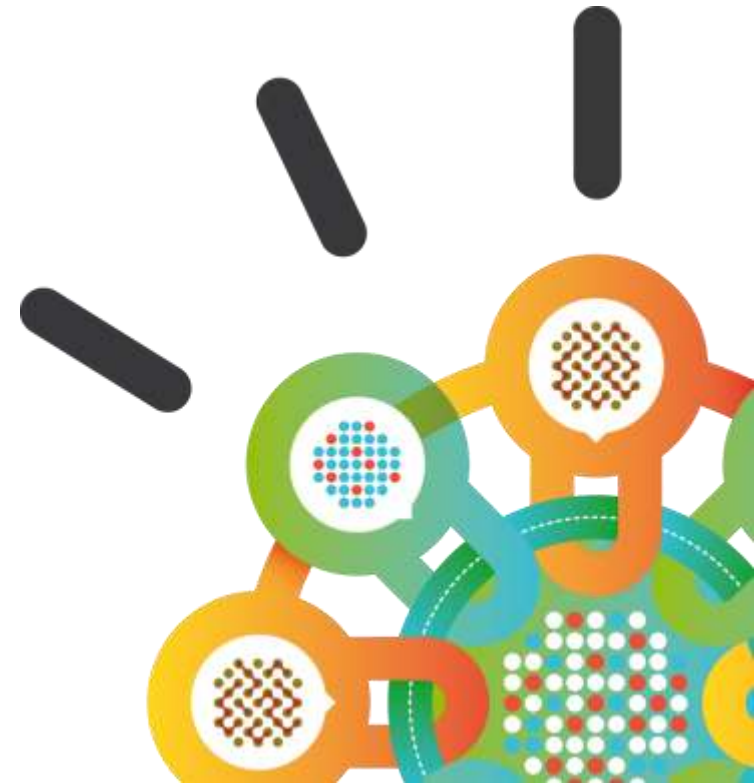


Security Intelligence.  
Think Integrated.



## Bezpečnostní témata spojená se Zákonem o kybernetické bezpečnosti

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

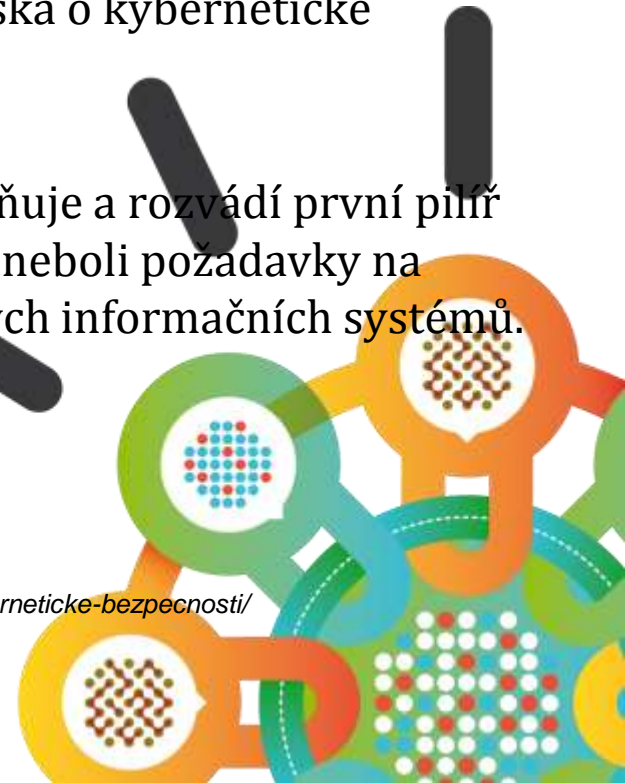


## Zákon je zákon

Národní bezpečnostní úřad vypracoval k návrhu zákona o kybernetické bezpečnosti, který byl předložen k dalšímu legislativnímu procesu do Parlamentu České republiky, **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-vyhlasiky-o-kyberneticke-bezpecnosti/>



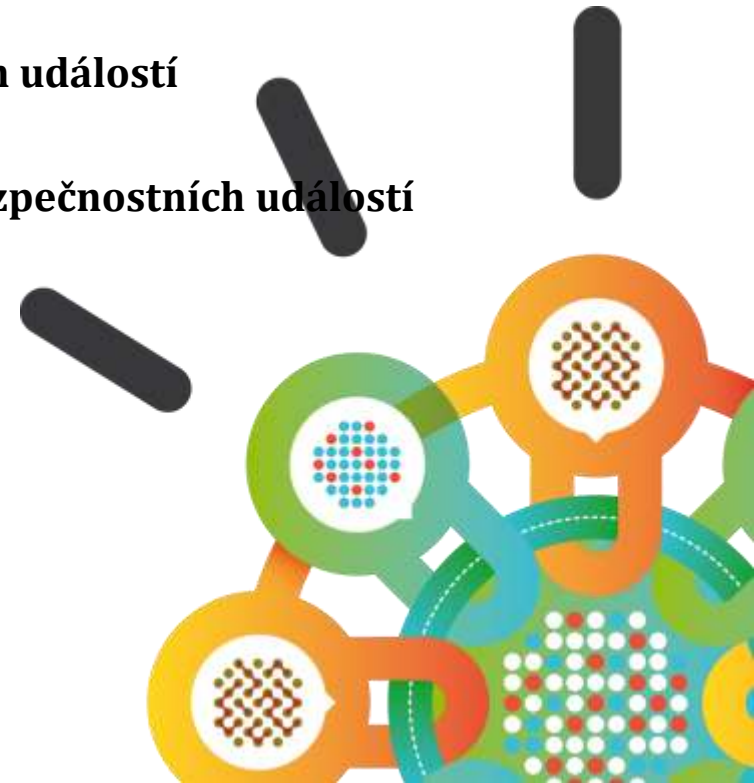
## Řada technických opatření

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

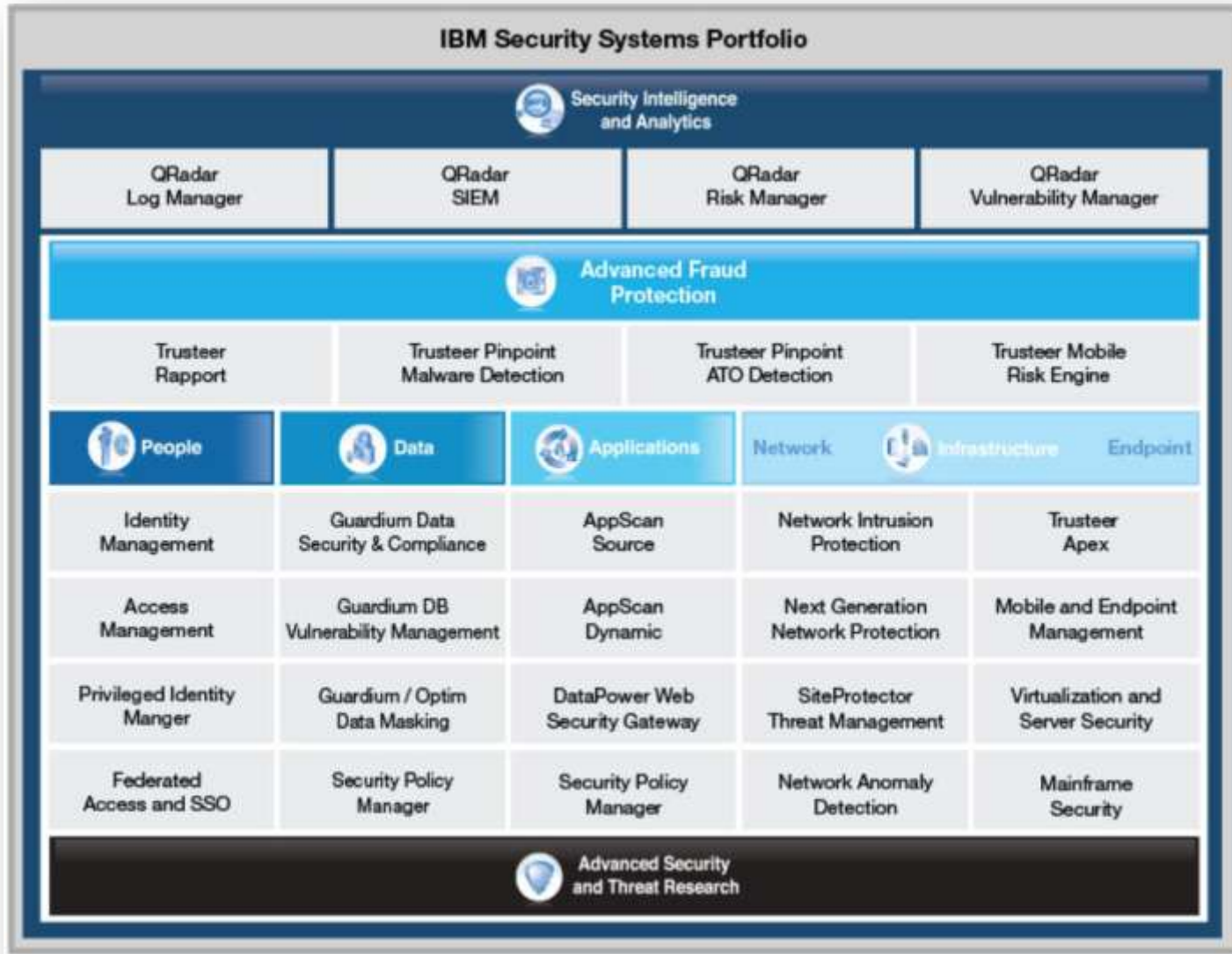
**§ 21 - Nástroj pro zaznamenávání činností kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů**

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

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



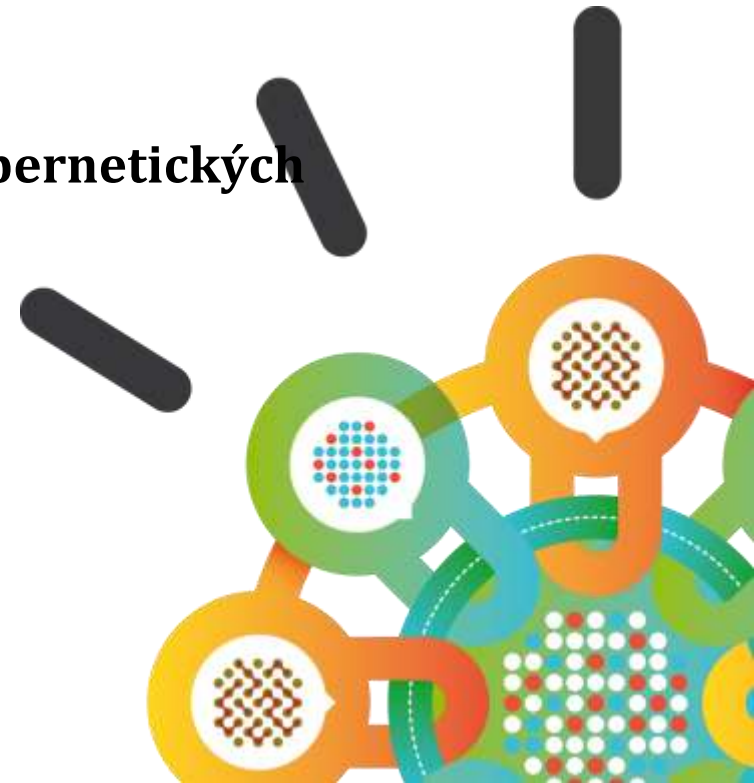
# IBM Security Framework



Security Intelligence.  
**Think Integrated.**

§ 23 - Nástroj pro sběr a vyhodnocení kybernetických  
bezpečnostních událostí

**IBM QRADAR SIEM**



# Security Information and Event Management = SIEM

## Zdroje



## Zabudovaná inteligence

- Automatická korelace, detekce zařízení
- Real-time analytika
- Masivní snížení množství
- Detekce anomálií
- Zabudovaná pravidla

**Automatický výběr**

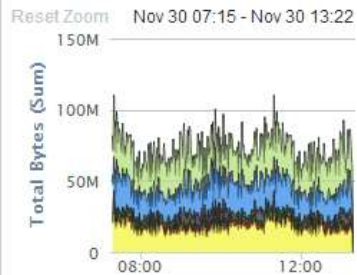
*Skutečný problém*

Show Dashboard: Application Overview

New Dashboard Rename Dashboard Delete Dashboard Add Item...

Next Refresh: 00:00:45

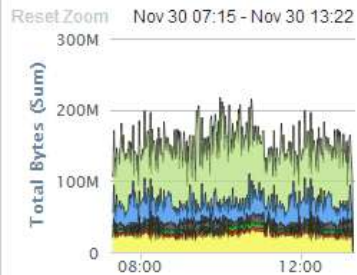
### Inbound Traffic by Country (Total Bytes)



- Legend
- NorthAmerica.UnitedStates
  - NorthAmerica.Canada
  - Europe.UnitedKingdom
  - Europe.Belgium
  - Remainder
  - Asia.China

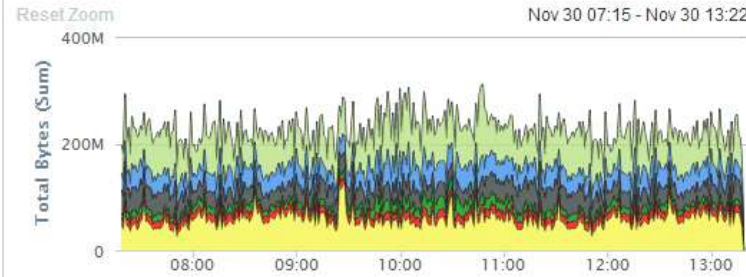
[View in Network Activity](#)

### Outbound Traffic by Country (Total Bytes)



- Legend
- NorthAmerica.UnitedStates
  - NorthAmerica.Canada
  - Asia.China

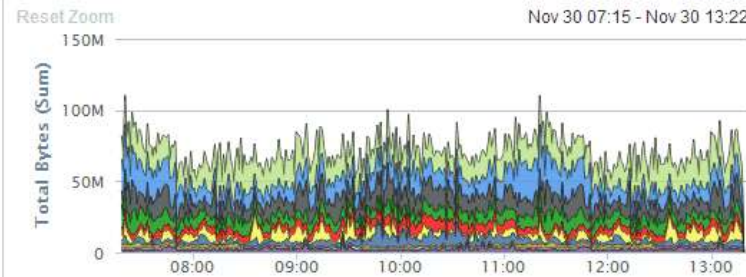
### Top Applications (Total Bytes)



- Legend
- Web.Web.Misc
  - other
  - P2P.BitTorrent
  - P2P.Kazaa
  - P2P.eDonkey
  - Remainder

[View in Network Activity](#)

### Top Applications Inbound from Internet (Total Bytes)

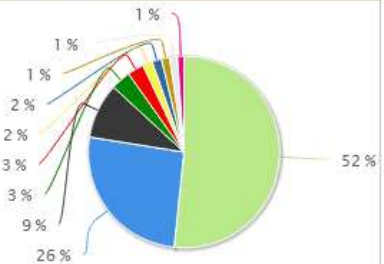


- Legend
- other
  - P2P.BitTorrent
  - Web.Web.Misc
  - Web.SecureWeb
  - P2P.eDonkey
  - Mail.SMTP
  - P2P.Kazaa
  - P2P.Gnutella
  - RemoteAccess.SSH
  - P2P.OpenNap
  - Remainder

[View in Network Activity](#)

### Top Countries (real-time)

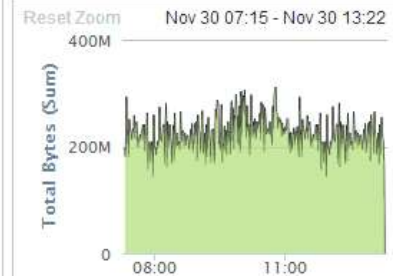
Value to Graph: Total Bytes (Sum)  
Chart Type: Pie Chart  
Display Top: 10



- Legend
- NorthAmerica.UnitedStates
  - NorthAmerica.Canada
  - Europe.France
  - Europe.Sweden
  - Asia.Japan
  - Asia.China
  - Europe.UnitedKingdom

[View in Network Activity](#)

### DSCP - Precedence (Total Bytes)



**Offense 3063** Summary Attacks Targets Categories Annotations Networks Events Flows Rules Actions Print

Magnitude		Relevance	0	Severity	8	Credibility	3
Description	Target Vulnerable to Detected Exploit preceded by Exploit Attempt Preceded by Recon preceded by Exploit/Malware Events Across Multiple Targets preceded by Recon - External - Potential Network Scan	Event count	1428 events in 3 categories				
Attacker/Src	202.153.48.66	Start	2009-09-29 16:05:01				
Target(s)/Dest	Local (717)	Duration	1m 32s				
Network(s)	Multiple (3)	Assigned to	Not assigned				
Notes	Vulnerability Correlation Use Case Conficker worm exploit (CVE 2008-...	Correlation of vulnerability data with IDS alerts An attacker originating from China is using the...					

**Attacker Summary** Details

Magnitude		User	Karen
Description	202.153.48.66	Asset Name	Unknown
Vulnerabilities	0	MAC	Unknown
Location	China	Asset Weight	0

**Top 5 Categories** Categories

Name	Magnitude	Local Target Count	Events
Buffer Overflow		8	8
Misc Exploit		3	3
Network Sweep		716	1417

**Top 5 Local Targets** Targets

IP:DNS Name	Mag...	Vulnerable	Chained	User	MAC	Location	Weight
Windows AD Server		Unknown	No	Unknown	Unknown	main	8
10.101.3.3		Unknown	No	Unknown	Unknown	main	0
10.101.3.4		Unknown	No	Unknown	Unknown	main	0
DC106		Yes	No	Unknown	Unknown	main	10
10.101.3.11		Unknown	No	Unknown	Unknown	main	0

**Top 10 Events** Events

Event Name	Magnitude	Log Source	Category	Destination	Dst Port	Time
Misc Exploit - Event CRE		Custom Rule Engine-8 : grad...		10.101.3.15	445	09-29 16:06:33
NETBIOS-DG SMB v4 srvsvc NetrpPathCo...		Snort @ 10.1.1.5		10.101.3.10	445	09-29 16:06:28
NETBIOS-DG SMB v4 srvsvc NetrpPathCo...		Snort @ 10.1.1.5		10.101.3.15	445	09-29 16:06:33
Misc Exploit - Event CRE		Custom Rule Engine-8 : grad...		10.101.3.13	445	09-29 16:06:31
Network Sweep - QRadar Classify Flow		Flow Classification Engine-5 : ...		10.101.3.10	445	09-29 16:05:01
Network Sweep - QRadar Classify Flow		Flow Classification Engine-5 : ...		10.101.3.15	445	09-29 16:05:01
Network Sweep - QRadar Classify Flow		Flow Classification Engine-5 : ...		10.101.3.10	445	09-29 16:05:01
Network Sweep - QRadar Classify Flow		Flow Classification Engine-5 : gradar-vm	Network Sweep	10.101.3.15	445	09-29 16:05:01

Jaký útok?

Nakolik byl úspěšný?

Kdo je zodpovědný?

Kolik cílů zasaženo?

Nakolik jsou systémy kritické pro můj bussiness

Některé z nich zranitelné?

Kde jsou všechny důkazy?

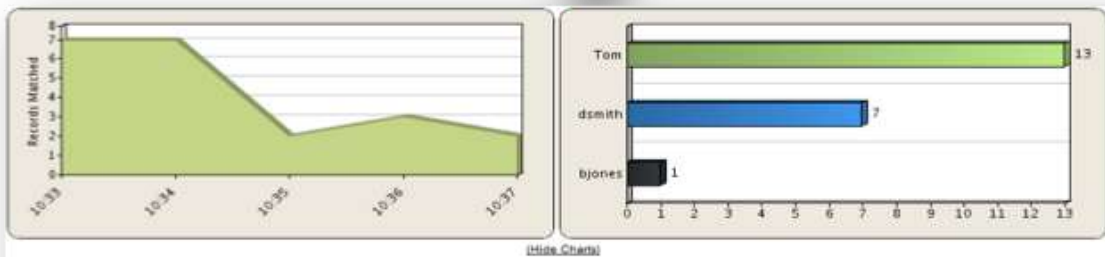




Offense 2834 Summary Attackers Targets Categories Annotations Networks **Events** Flows Rules Actions Print

Magnitude				Relevance	3	Severity	5	Credibility	3
Description	Single Host preceded by Login Failures Followed By Success preceded by Login failure to a disabled account preceded by Authentication: Repeated Login Failures			Event count	36 events in 6 categories				
Attacker/Src	10.103.7.88 (dhcp-workstation-103-7-88.acme.org)			Start	2009-09-29 10:33:34				
Target(s)/Dest	10.101.3.10 (Windows AD Server)			Duration	4m 51s				
Network(s)	IT_Server.main			Assigned to	Not assigned				
Notes	Windows Authentication Use Case Demo data to demonstrate event-only Windows Authentication use case, including login failures, login attempt to disabled account, etc. This attack is comprised of :- Event(s): Multiple authentication attempts from ...								

Opakované neúspěšné přihlášení (Že by uživatel zapomněl heslo?)



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

Username	Source IP (Unique Count)	Destination IP (Unique Count)	Event Name (Unique Count)	Log Source (Unique Count)	Category (Unique Count)	Event Count (Sum)	Count
Tom	10.103.7.88	10.101.3.10	Multiple (4)	WindowsAuthSe	Multiple (4)	19	13
dsmith	10.103.7.88	10.101.3.10	Multiple (4)	WindowsAuthSe	Multiple (3)	7	7
bjones	10.103.7.88	10.101.3.10	Logon Failure - ...	WindowsAuthSe	Host Login Failed	1	1

Event Name	Log Source	Source IP	Destination IP
Host Login Succeeded - Event CRE	Custom Rule Engine-8 :: qradar-vm	10.103.7.88	10.101.3.10
Host Login Failed - Event CRE	Custom Rule Engine-8 :: qradar-vm	10.103.7.88	10.101.3.10
Host Login Failed - Event CRE	Custom Rule Engine-8 :: qradar-vm	10.103.7.88	10.101.3.10
Remote Access Login Failed - Event CRE	Custom Rule Engine-8 :: qradar-vm	10.103.7.88	10.101.3.10
Remote Access Login Failed - Event CRE	Custom Rule Engine-8 :: qradar-vm	10.103.7.88	10.101.3.10
Suspicious Pattern Detected - Event CRE	Custom Rule Engine-8 :: qradar-vm	10.103.7.88	10.101.3.10
Suspicious Pattern Detected - Event CRE	Custom Rule Engine-8 :: qradar-vm	10.103.7.88	10.101.3.10

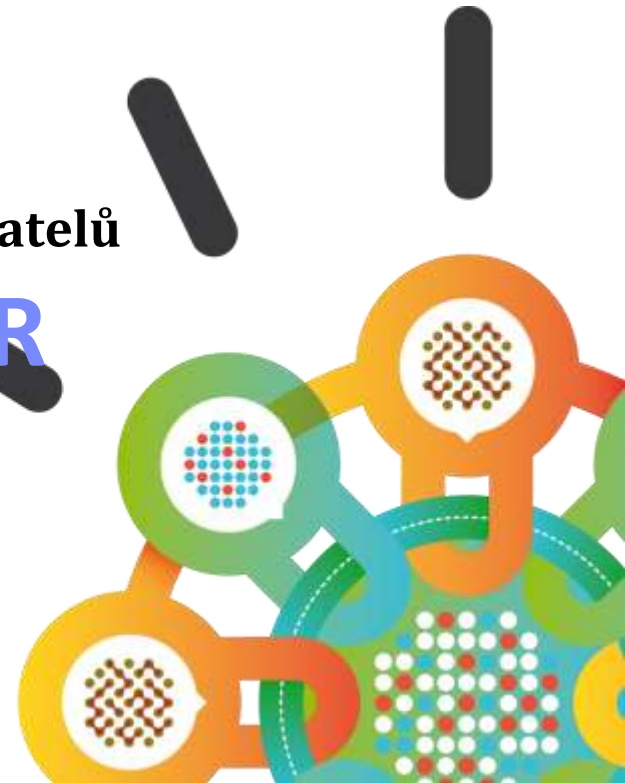
Po čase se login podařil = host byl kompromitován

Security Intelligence.  
Think Integrated.



§ 11 - Řízení přístupu a bezpečné chování uživatelů

**IBM ENDPOINT MANAGER**  
**IBM MAAS360**



# IBM Endpoint Manager

## Koncová zařízení



Desktopy / laptopy / servery



Mobilní zařízení



Specializovaná zařízení



Patch Management



Lifecycle Management



Software Use Analysis



Mobile Devices / MaaS360



Power Management



Core Protection



Server Automation



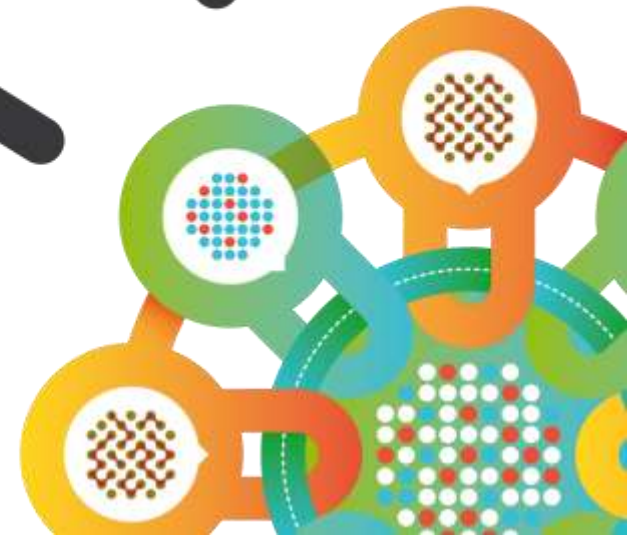
Security and Compliance

- 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:

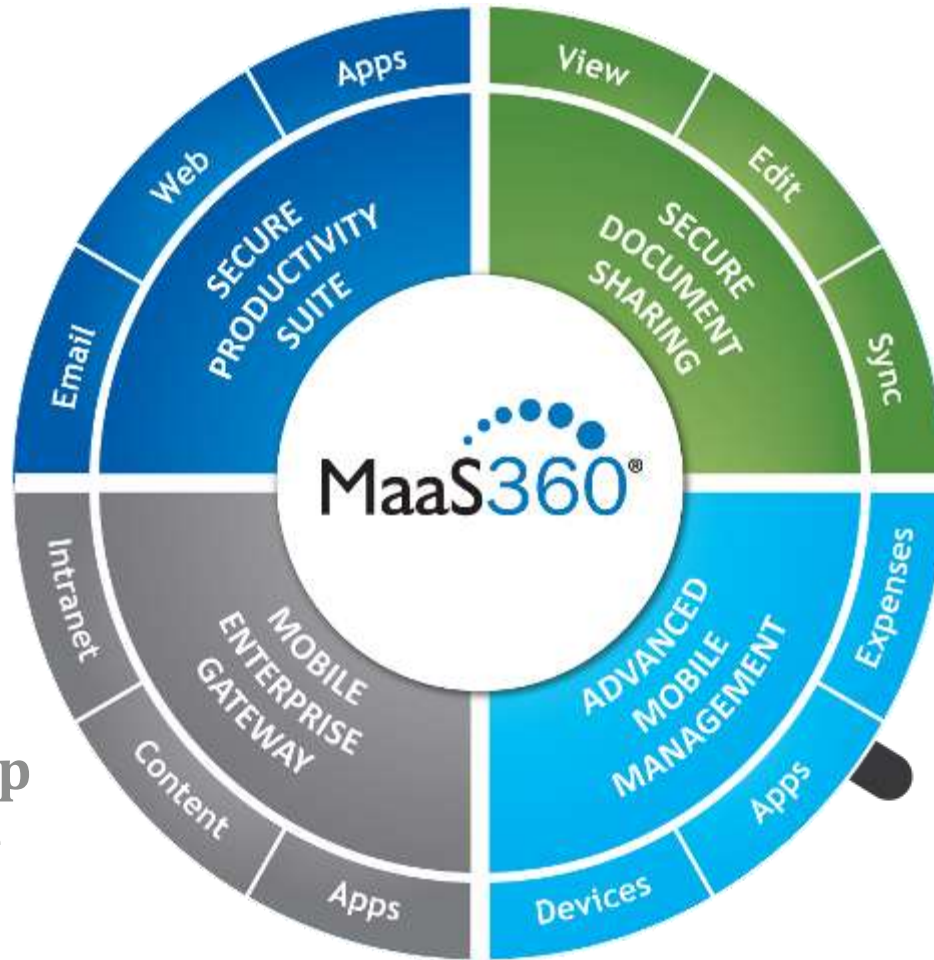
- Automatické odhalení zařízení
- Patch Management
- Inventorizace HW a SW
- Distribuce SW
- OS instalace
- Vzdálený přístup

## Přínosy:

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



**Bezpečný  
kontejner**



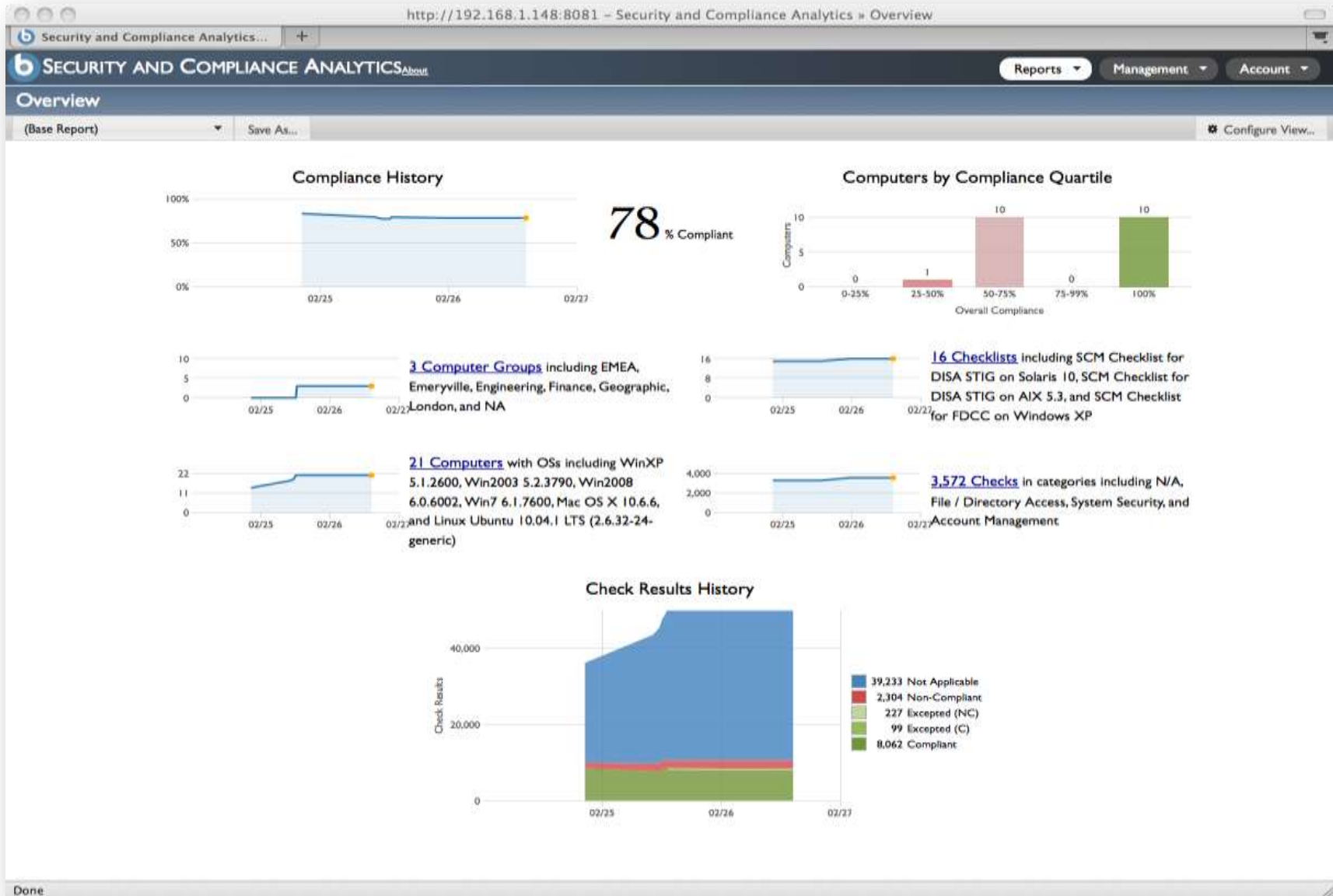
**Bezpečné sdílení  
dokumentů**

**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

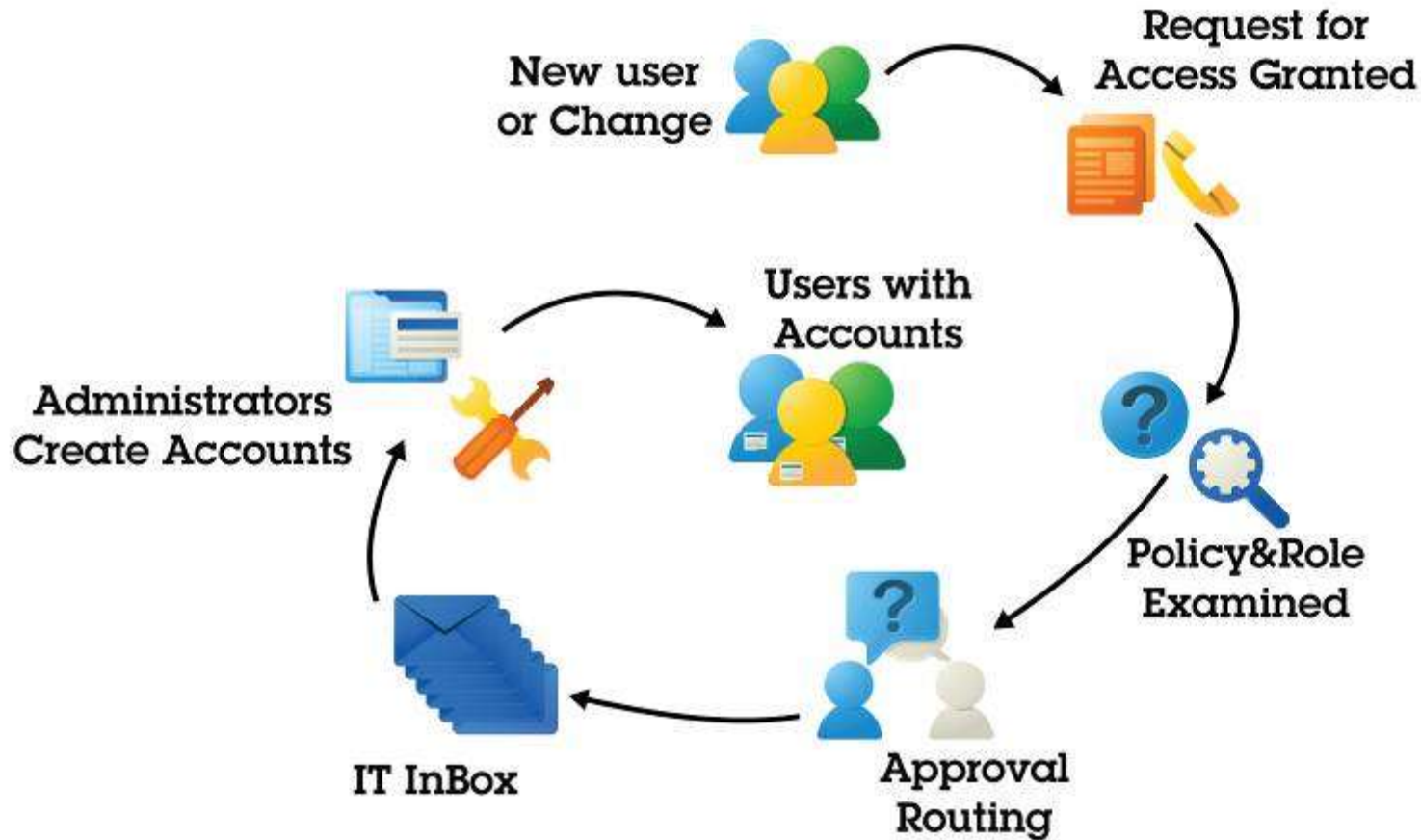
§ 21 - Nástroj pro zaznamenávání činností kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů

**IBM SECURITY IDENTITY MANAGER**



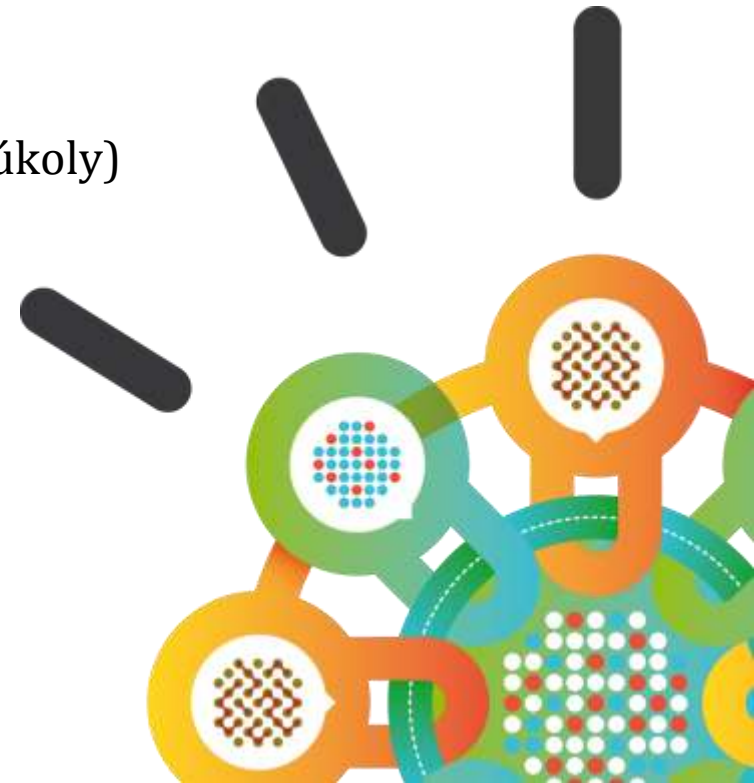


# Uživatelé, identity a životní cyklus



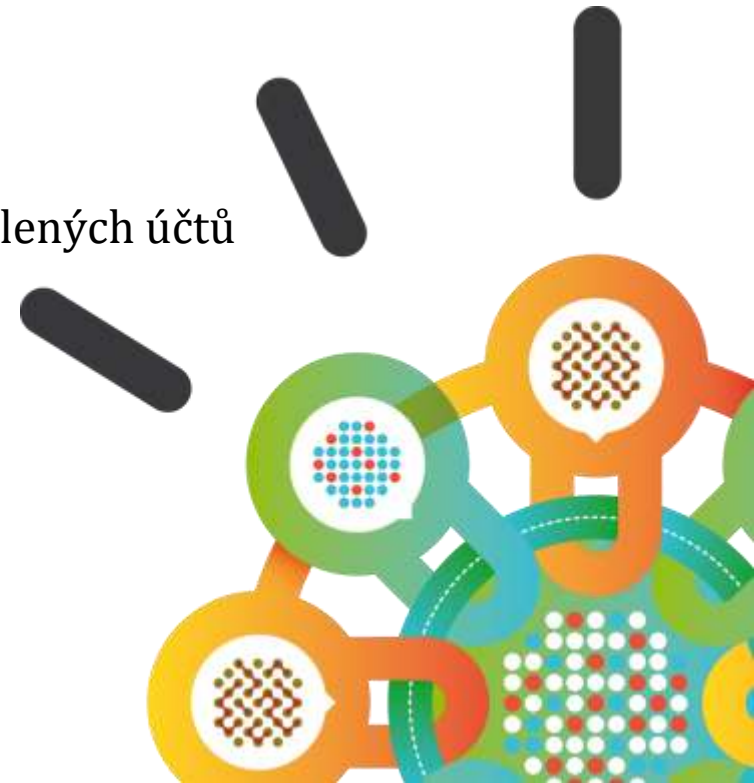
## Typické problémy

- 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
- Rozšiřitelnost o správu privilegovaných a sdílených účtů
- Možnost správy z mobilních zařízení
- Reportování, auditování



# Moderní rozhraní i pro mobilní zařízení

The image displays two overlapping screenshots of the IBM Security Identity Manager (ISIM) 'Request Access' web interface. The top screenshot shows the 'Select user' step, where users are listed in a grid. The bottom screenshot shows the 'Select access' step, where various application categories are presented in a grid.

**Top Screenshot: Select user**

- Page title: IBM Security Identity Manager
- User: Chuck Riegler | Log Out
- Navigation: Request Access | View Requests
- Progress: 1 Select user (active), 2 Select access, 3 Provide required information, 4 Done
- Search: Search for users
- Results: 1 - 27 of 27
- Sort By: Name (A-Z), Mail, Title
- User cards include:
  - Abe Austin (aaustin@krc.test) - Title: Accounts receivable
  - Akilah Orvis (aorvis@krc.test) - Title: Customer accounts specialist assist. region
  - Benton Magnani (bmagnani@krc.test) - Title: account receivable
  - Blythe Leak (bleak@krc.test) - Title: Customer support
  - Christal Delettre
  - Chuck Riegler
  - Deirdre Bourdon (dbourdon@krc.test) - Title: Customer support
  - Felicia Escobedo (fescobedo@krc.test) - Title: Account receivable

**Bottom Screenshot: Select access**

- Page title: IBM Security Identity Manager
- User: Chuck Riegler | Log Out
- Navigation: Request Access | View Requests
- Progress: 1 Select user, 2 Select access (active), 3 Provide required information, 4 Done
- Search: Search for access
- Search: All Categories
- Categories: All Categories (Collaboration, Remote access, Applications, Fileshares, Databases, Essentials, Teams)
- Results: 1 - 30 of 30
- Sort By: Name, Description, Availability
- Access cards include:
  - Accounting Plus (Accounts payable, receivable and more...)
  - Business Partner Connect (Allows business partners to access project manuals and support documentation)
  - Customer Contact Manager (Customer relationship and direct marketing management)
  - East Region File Share (File share containing region project files including confidential data)
  - Financial Reporting Application (Reporting of financial results)
  - North Region File Share (File share containing region project files including confidential data)
  - South Region File Share (File share containing region project files including confidential data)
  - Supply Order System (One stop shop for ordering departmental supplies etc...)
  - Support portal (L2, L3 portal)

Navigation at the bottom: < Back Select user | Request summary | Judith Hill | 4 | Next Provide information >

**Zákon  
o kybernetické  
bezpečnosti bez starostí**

Díky řešením a službám IBM v oblasti bezpečnosti budete moci klidně spát.

Mezinárodní systém  
včasného varování

Národní centrum  
kybernetické bezpečnosti

Povinnost hlásit  
incidenty

Moc děkuji

**Jiří Slabý**

+420 731 435 836

[jiri\\_slaby@cz.ibm.com](mailto:jiri_slaby@cz.ibm.com)

**Jiří Kucr**

+420 777 666 642

[jiri\\_kucr@cz.ibm.com](mailto:jiri_kucr@cz.ibm.com)

