CYBERARK

Prečo chrániť privilegované účty?

Daniel.Hetenyi@cyberark.com

Riziká nechránených privilegovaných účtov

Bezpečený prístup k citlivým dátam	> Neautorizovaný prístup k citlivým dátam > Nemonitorovaný prístup k citlivým dátam > Nevhodný prístup k citlivým dátam
Bezpečnosť privilegovaných účtov	> Neautorizovaný prístup k privilegovaným účtom
Management oprávnení	> Prístup nie je odobratý, keď sa zmení rola (e.g. Accounts and/or SSH keys) > Prístup nie je odobratý, keď užívateľ odíde (i.e. Contractor, tretia strany) > Prístup nie je odobratý, keď služba sa prestane používať (e.g. Service Accounts)
Riadenie privilegovaných účtov	> Udelené nevhodné oprávnenia > Kontrola udelovania prístupov k privilegovaným účtom
Monitoring privilegovaných účtov	> Chýba reporting v reálnom čase o zneužití privilegovaného účtu > Nevedú sa záznamy o využití prívilegovaných účtov > Veľmi časovo náročná forenzná analýza s chýbajúcou indexáciou

CYBERARK®

OPM Breach – Stručný přehled

Organization Overview	
Industry	Federal Government
Employees	4.1 million (federal employees)[1]
Headquarters	Washington, DC

Co se vlastně stalo?

- **Duben 2015:** OPM zjišťuje, že jim bylo odcizeno přibližně 4.2 milionu citlivých údajů státních zaměstnanců
- **Červen 2015:** Bylo odhaleno, že rozsah celého případu je pravděpodobně mnohem větší, než se předpokládalo
- **Počet postižených osob:** 21.5 milionů stávajících i bývalých státních zaměstnanců a dodavatelů
- **Co bylo ukradeno:** osobní, zdravotní a rodinné údaje, informace o prověrkách, atp…
- **Odkud hrozba pochází:** Čína
- **Motivace: Špionáž**


The Washington Post

New OPM data breach numbers leave federal employees anguished, outraged

By Joe Davidson July 9 Follow @JoeDavidsonWP

If misery loves company, the Office of Personnel Management had a of good days. Then, its cyber sinkhole got much, much deeper.

News about computer problems grounding United Airlines, shutti New York Stock Exchange and taking the Wall Street Journal's h offline momentarily overshadowed OPM's problems and de vulnerable the digital world is, even in the private sector.


The New York Times

Attack Gave Chinese Hackers Privileged Access to U.S. Systems

By DAVID E. SANGER, NICOLE PERLROTH and MICHAEL D. SHEAR JUNE 20, 2015

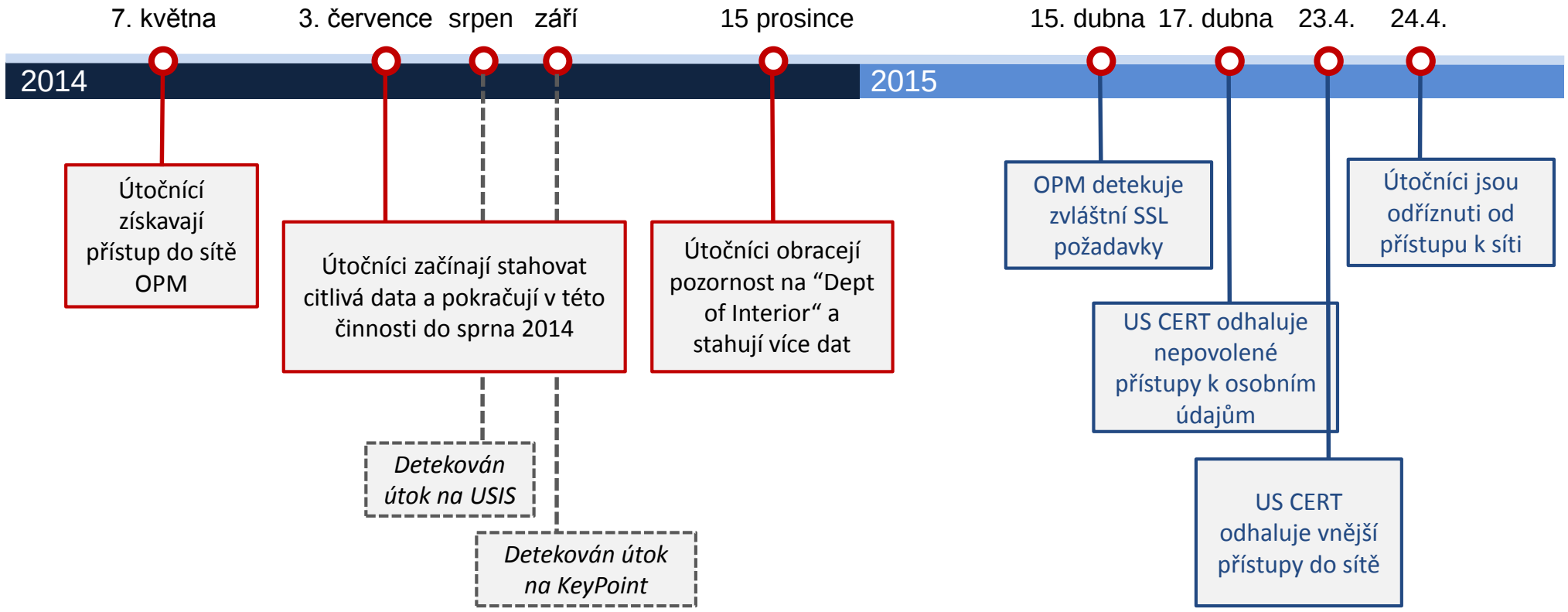
Katherine Archuleta, director of the Office of Personnel Management, in Congress on Tuesday. Cliff Owen/Associated Press

WASHINGTON — For more than five years, American intelligence agencies followed several groups of Chinese hackers who were systematically draining information from

CYBERARK

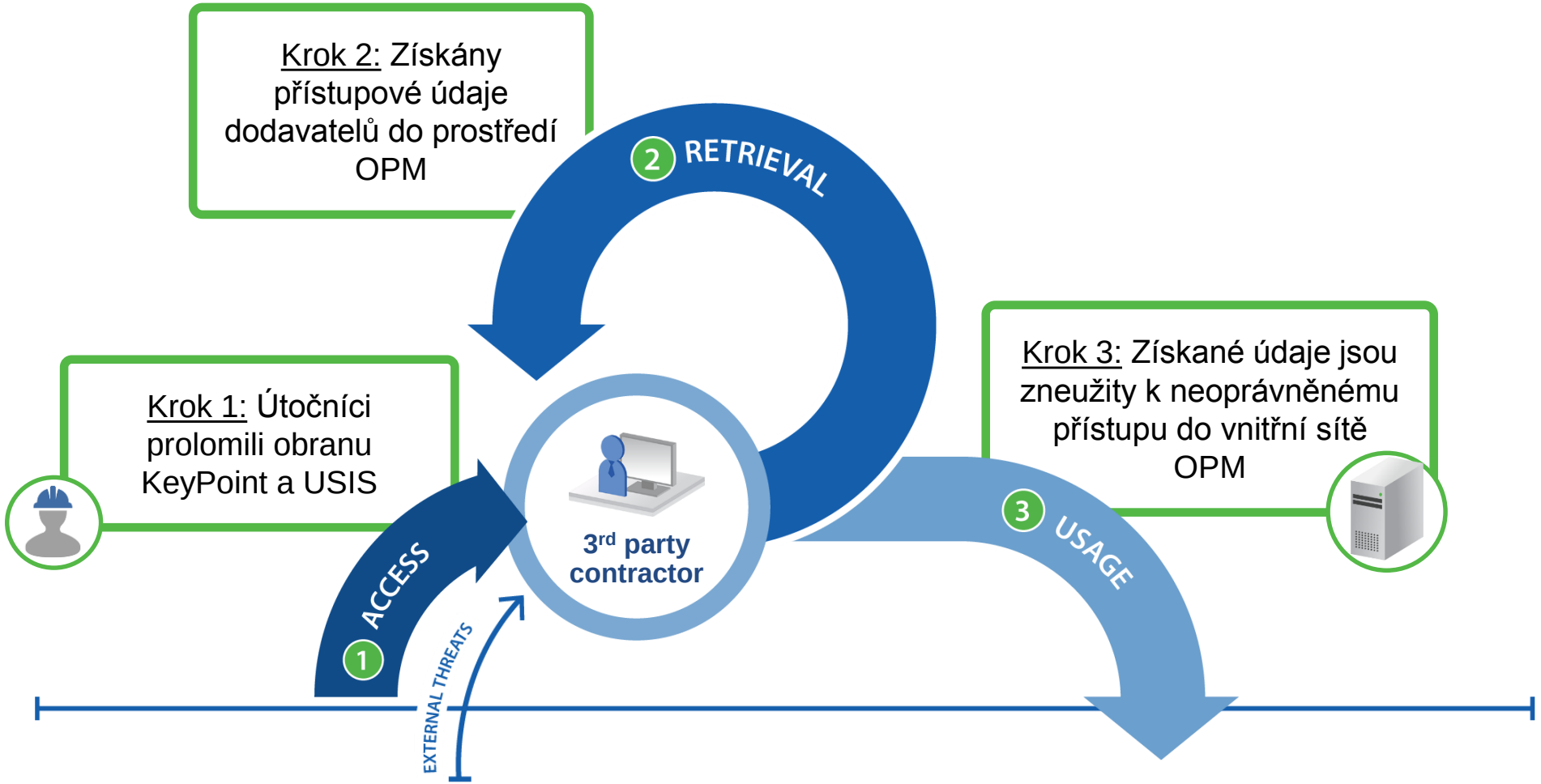
Časová osa útoku

Útočníci uvnitř korporátní síte po dobu **11 měsíců,** než byl útoku odhalen a zastaven.



CYBERARK

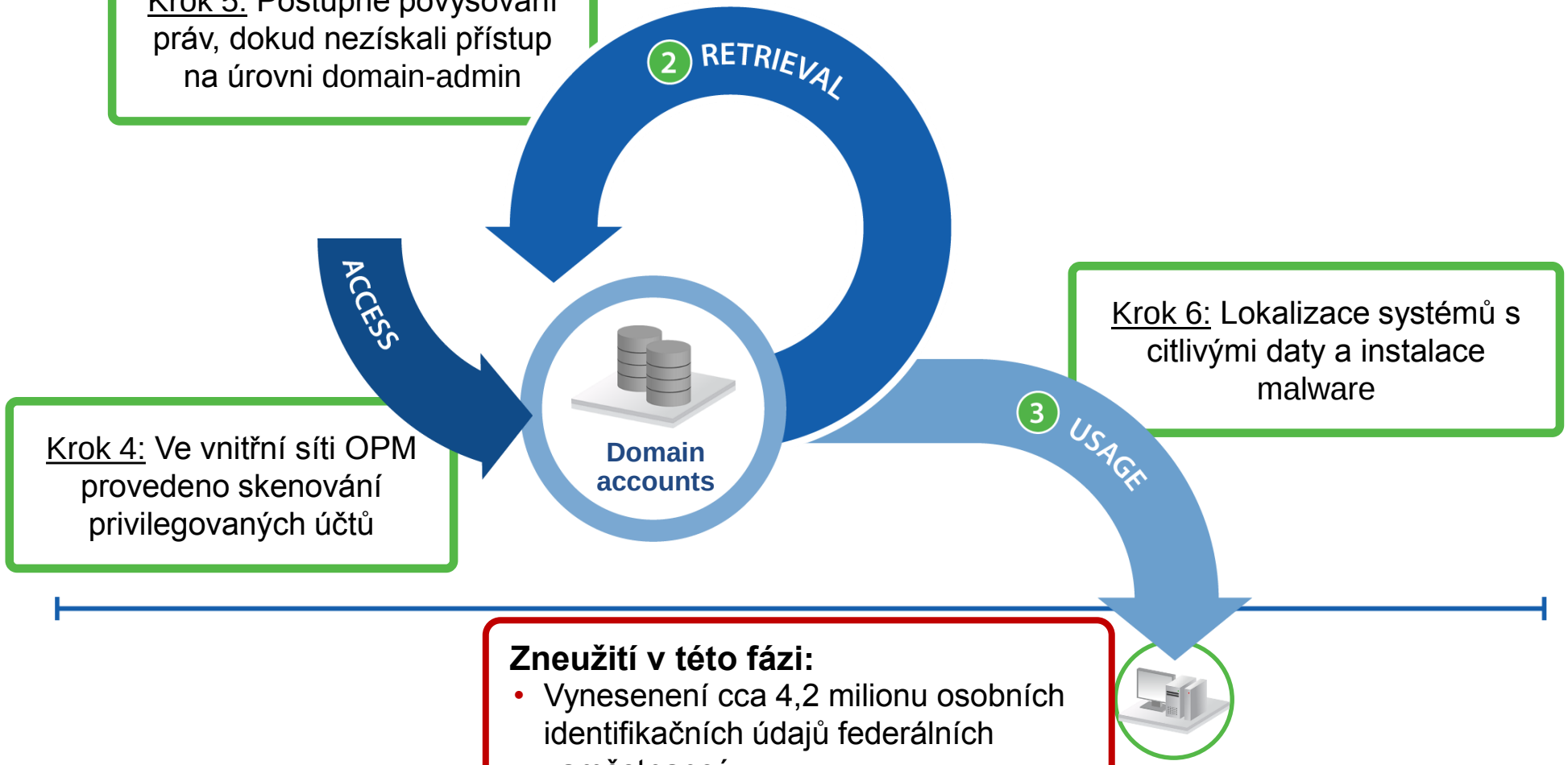
Jak útok začal?



CYBERARK

Co následovalo?

Krok 5: Postupné povyšování práv, dokud nezískali přístup na úrovni domain-admin



Krok 6: Lokalizace systémů s citlivými daty a instalace malware

Krok 4: Ve vnitřní síti OPM provedeno skenování privilegovaných účtů

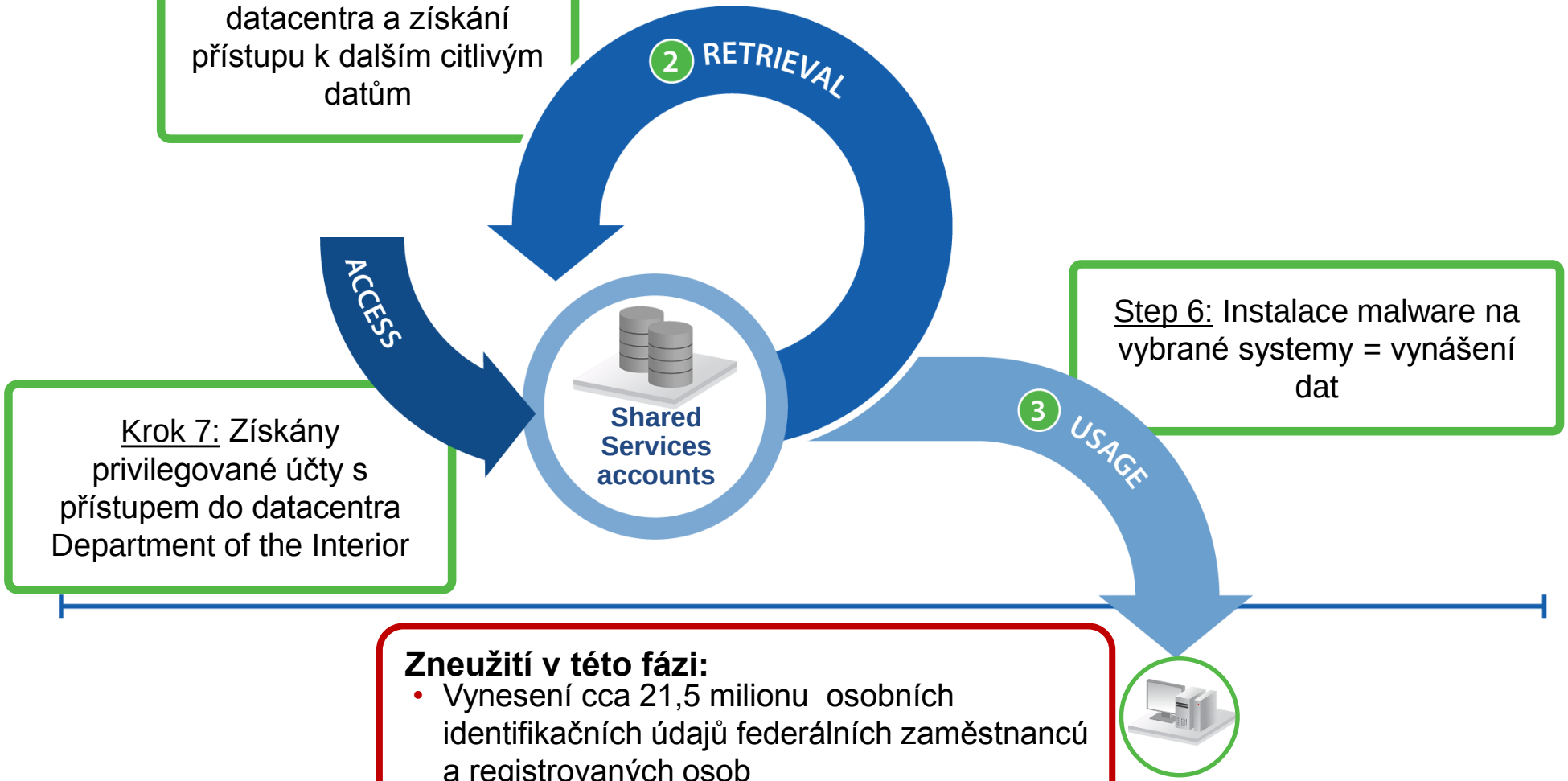
Zneužití v této fázi:

- Vynesenení cca 4,2 milionu osobních identifikačních údajů federálních zaměstnancú
- Lokalizace privilegovaných účtů Dept. of the Interior

CYBERARK

Jaký by konečný výsledek aktivit útočníků?

Krok 8: Proskenování datacentra a získání přístupu k dalším citlivým datům



Step 6: Instalace malware na vybrané systemy = vynášení dat

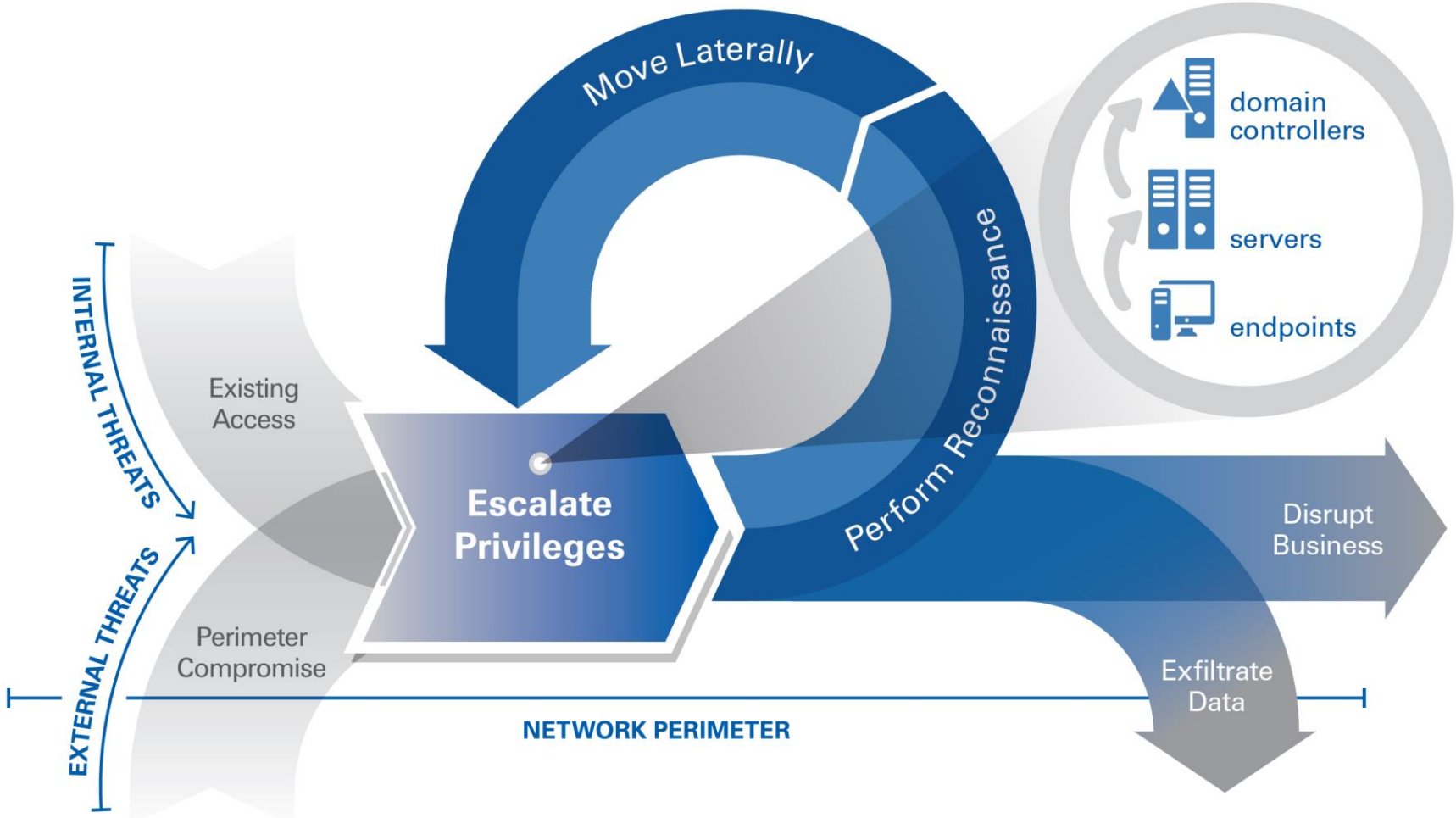
Krok 7: Získány privilegované účty s přístupem do datacentra Department of the Interior

Zneužití v této fázi:

- Vynesení cca 21,5 milionu osobních identifikačních údajů federálních zaměstnancú a registrovaných osob
- Ukradena osobní, rodinné, zdravotní informace a další údaje

CYBERARK

Cílem útočníka je povýšení oprávnění na co nejvyšší úroveň



CYBERARK

Hlavní Hacker NSA – jak mě udržíte mimo vaši síť?

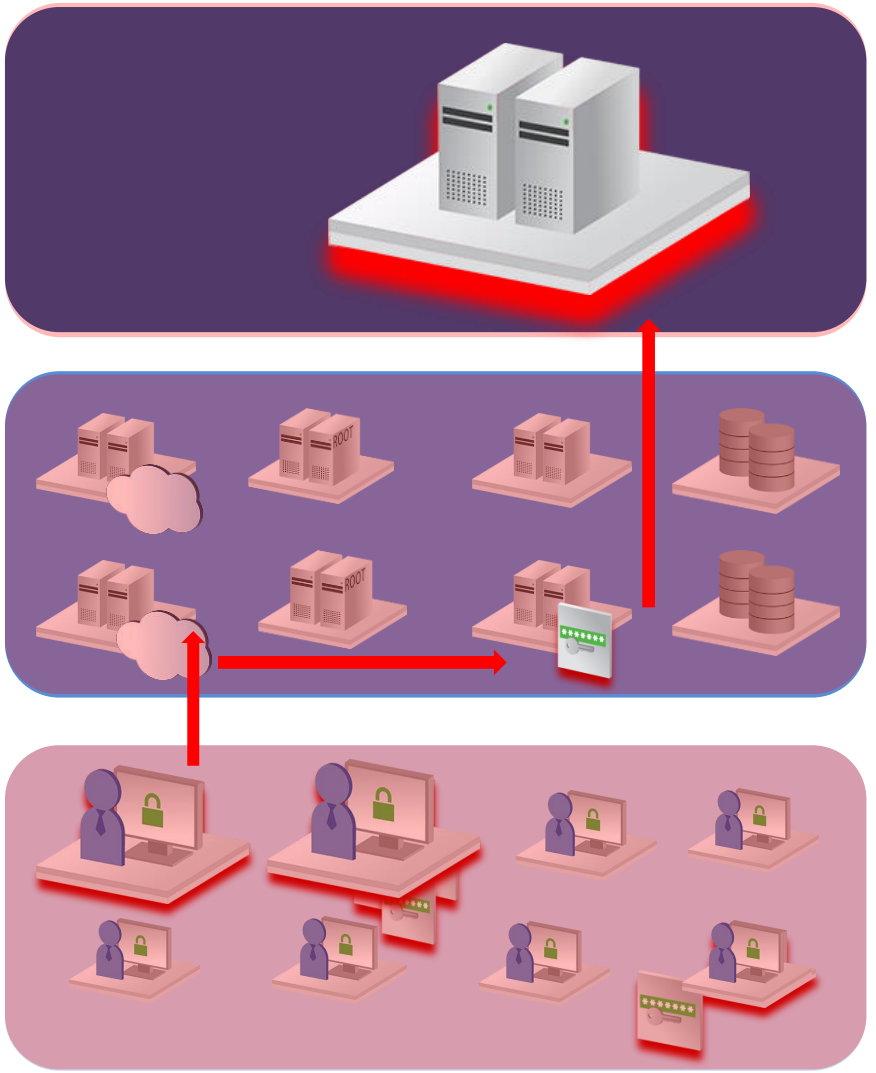
Rob Joyce - šéf NSA Tailored Access Operations:

- “V dnešním světě APT hráčů (jako je třeba NSA), jsou privilegované účty králem v možnostech získání přístupu k systémům.”
- “Nikoliv účty VIP zaměstnanců, ale účty síťových/doménových/systémových administrátorů mohou útočníkům otevřít cestu.”
- “NSA také často potěší hard-coded hesla v aplikacích, nebo hesla, která jsou přenášena v čitelné podobě – např. použitím starších protokolů – a tím snadno dostupná.”

CYBERARK

Ako získa útočník najvyššie práva?

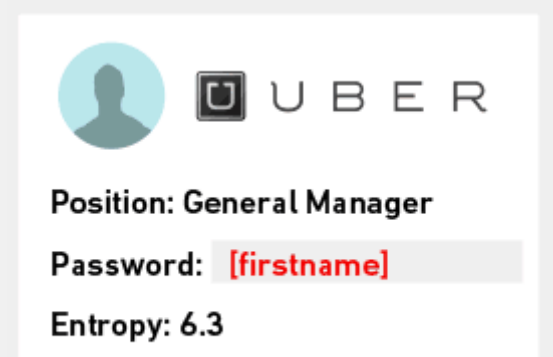
- Ukradnutie prihlasovacích údajov
- Laterálne pohyby – povyšovanie práv

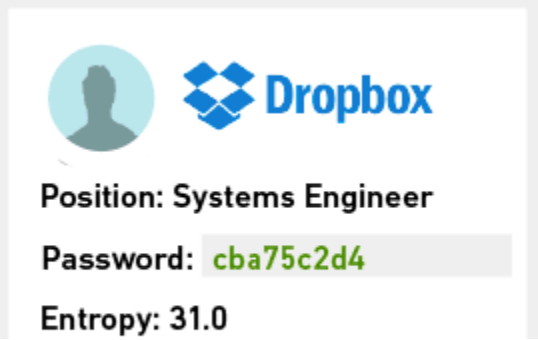


CYBERARK

Problémy s heslami k privilegovaným účtom

- Zistenie - hack užívateľa s domain admin právami odomyká prístup k 80% infraštruktúry na 1 krok
- Privilegovaných účtov je 3-5x viac ako zamestnancov
- Žiadne heslo napísané v plain texte ***nikdy*** nebude dosť komplexné





CYBERARK

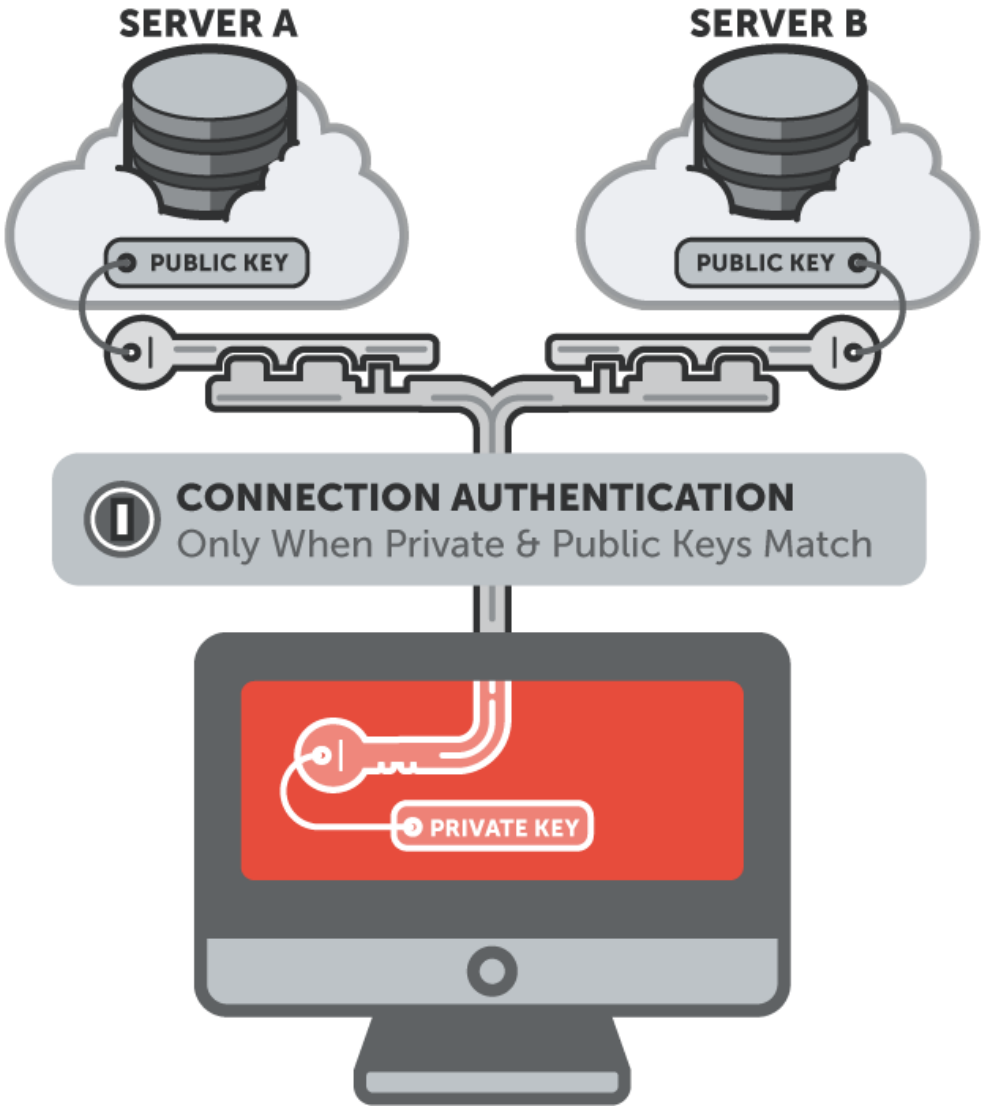
A čo SSH kľúče?

Výsledky našich scanov:

- 65% organizácii neriadi SSH kľúče
- 46% nikdy nerotovalo SSH kľúče
- 10% SSH kľúčov poskytuje ***root*** prístup

V organizácii s 500 servermi je viac ako 100.000 SSH párov.

- 51% utrpelo kompromitáciu kvôli SSH kľúčom

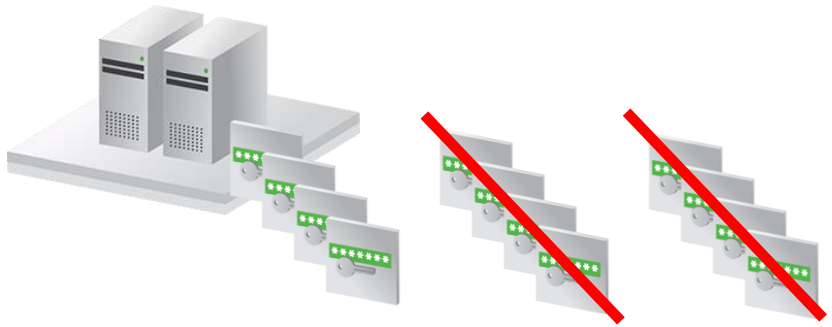


CYBERARK®

Princípy ochrany

Ako sa brániť ukradnutiu prihlasovacích údajov

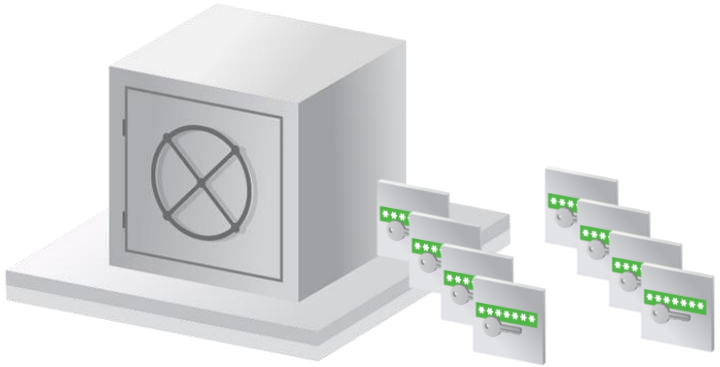
1. Zmenšite počet privilegovaných účtov



   - Vymažte nepoužívané účty
   - Využívajte built-in účty

2. Riaďte a zabezpečte prihlasovacie údaje

   - Bezpečne skladujte heslá a SSH kľúče pre všetky silné účty
   - Prístupy iba autorizovaným užívateľom
   - Používajte jednorázové heslá
   - Pravidelne rotujte heslá
   - Odstráňte hard coded heslá

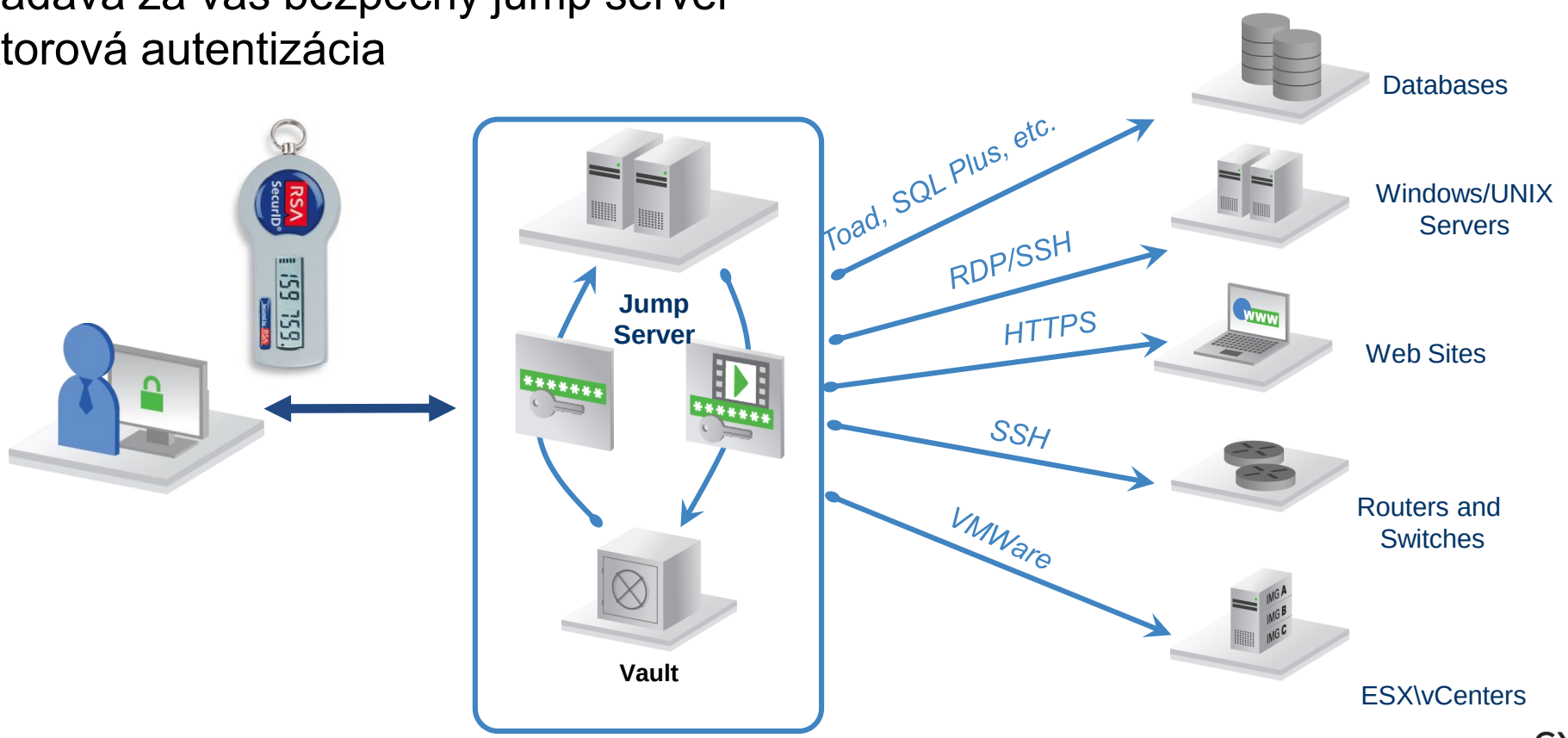


CYBERARK

Ako sa brániť ukradnutiu prihlasovacích údajov

3. Vytvorte bezpečné privilegované prístupy

- Izolácia session
- Heslá zadáva za vás bezpečný jump server
- Dvojfaktorová autentizácia



Laterálne pohyby - Ako sa brániť eskalácií práv v systémoch

1. Administrátori na svojej stanici majú len štandardného užívateľa

2. Hardening admin stanice

3. Services – nedávajte domain admin práva, ani rootovské oprávnenia

4. Kontrolujte práva na serveroch – segragation of duties

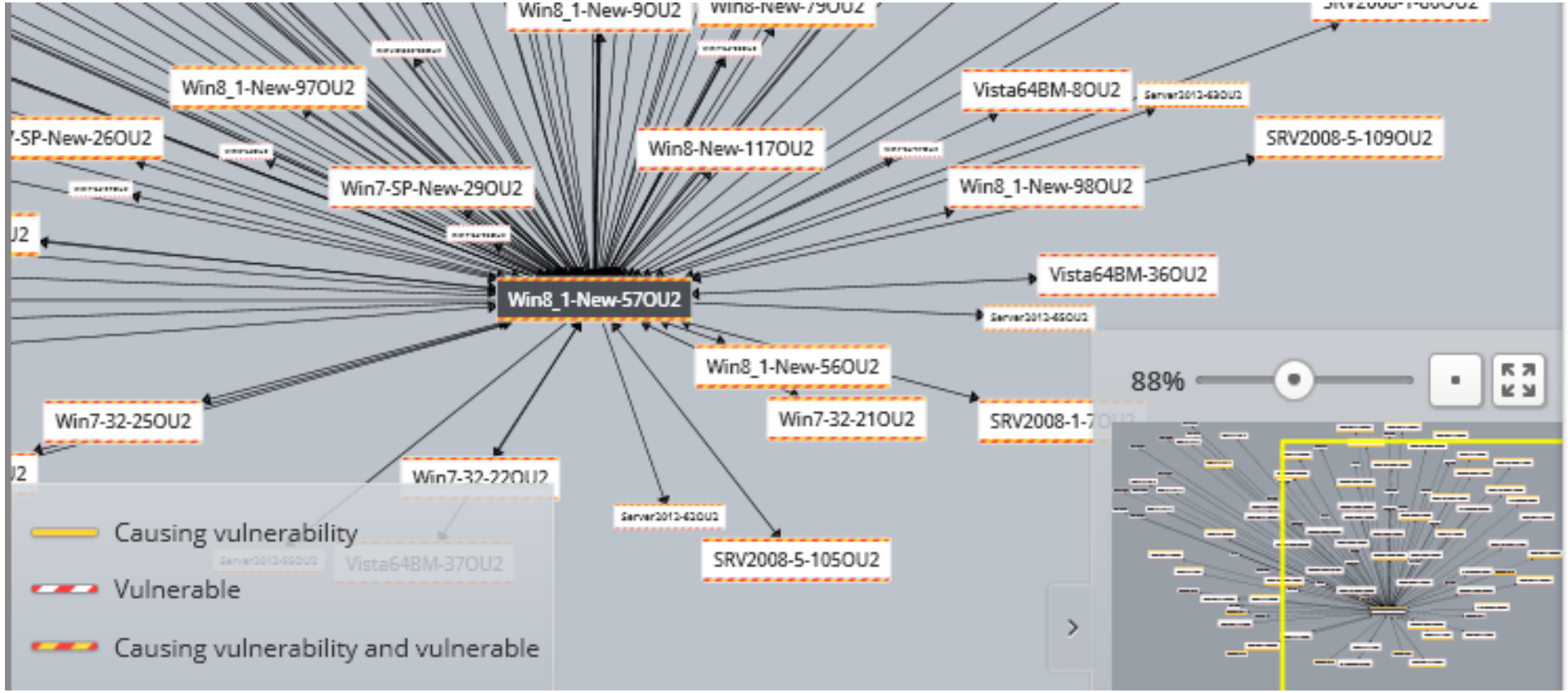
5. Strážte ukradnutie prihlasovacích údajov

CYBERARK

Ako sa brániť laterálnym pohybom

1. Zmapujte si potenciálne cesty – napr. CyberArk DNA

   - Pass the Hash, SSH Key Trust, Golden Ticket attacks
   - Staré účty, hard coded heslá



CYBERARK

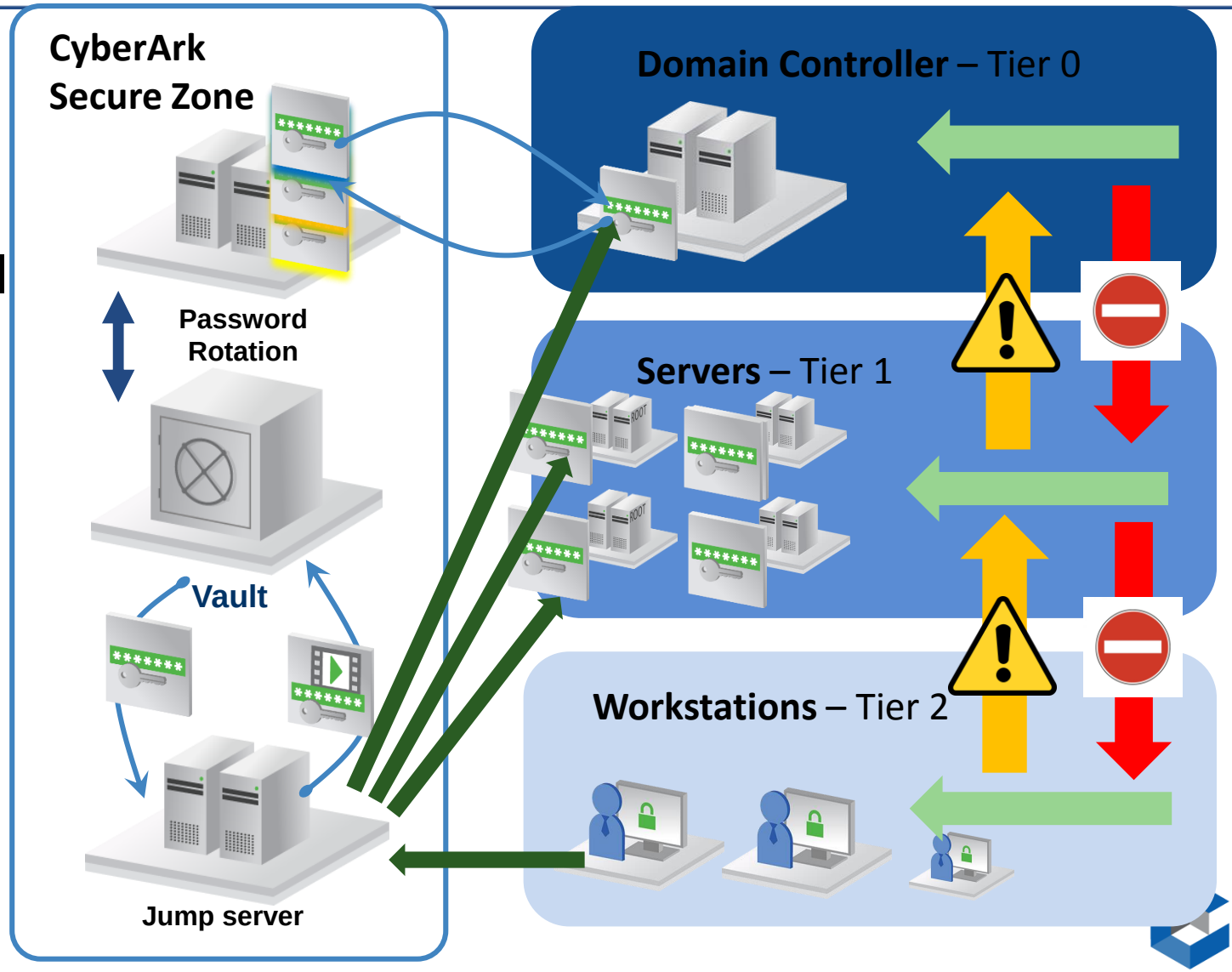
Ako sa brániť laterálnym pohybom

2. Jedinečné heslá pre lokálne účty

3. Znefunkčnite hashe hesiel a SSH kľúče po použití
   - Rotujte heslá / SSH kľúče

4. Tiering (zonácia) siete
   - Ohraničte škody

5. Využitie jump serveru
   - Zamedzte prenosu malware
   - Nezadávajte heslá



CYBERARK

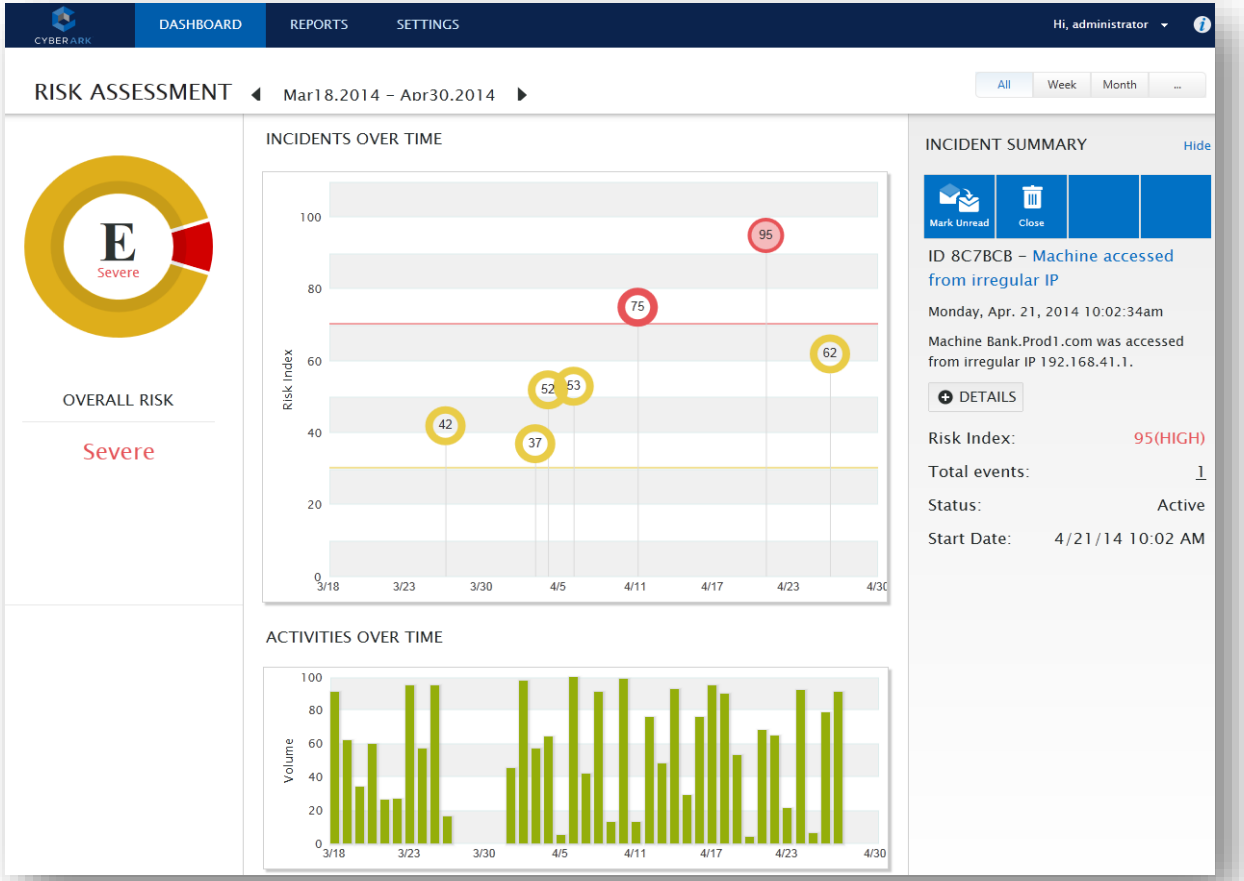
Ako sa brániť laterálnym pohybom – Detekcia a odpoveď

6. Detekcia podozrivých aktivít na privilegovaných účtov

   - Nové neevidované účty
   - Nové SSH kľúče
   - Anomálie – časté prihlásenia
   - Podozrivé connecty mimo bezpečnú zónu
   - Kerberos/NTLM zraniteľnosti

7. Odpoveď v reálnom čase

   - Okamžitá výmena hesiel
   - Terminovanie pripojenia



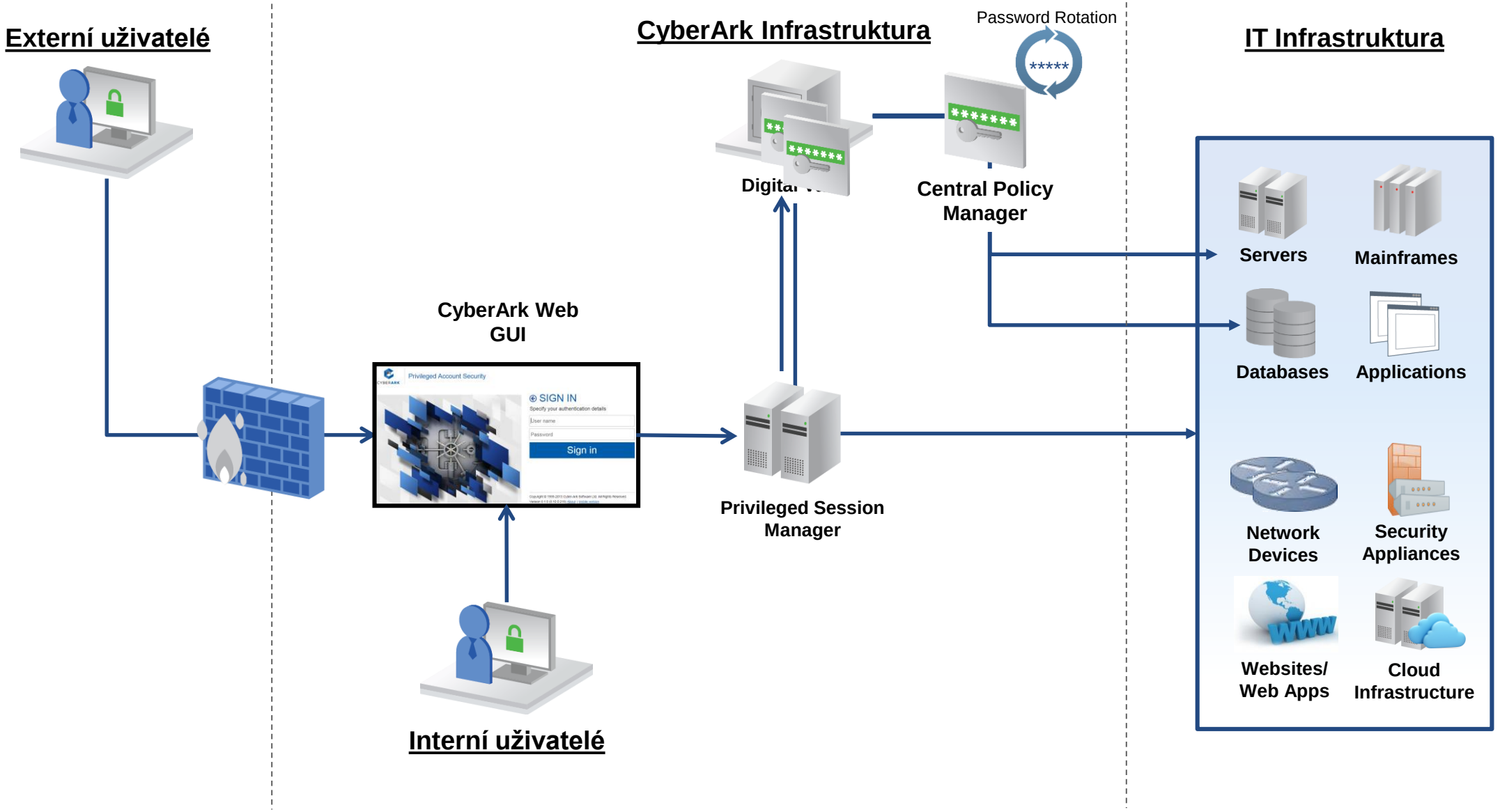
CYBERARK

Ako na to?

Fáza 1 – ŠPRINT – 1 mesiac – Hlavné ciele

Týždeň 1 Inštalácia	Inštalácia CyberArk a 2-faktorové overenie prístupov
Týždeň 2 Tier 0	Prístupy k Domain Controlleru (Tier 0) • **Domain admin** účty • Riadenie hesla s druhým faktorom, monitoring aktivít, izolácia session, kontrola anomálií
Týždeň 3 Local Admin	Znáhodnenie hesiel pre built-in účty • ***Local (Built-in) admin účty*** – administrator, root, oracle SYS/System, enable, iLO, ..
Týždeň 4 Servisné účty out-of-box	Vysoko rizikové servisné účty podporované out of box • ***Vulnerability Management*** – Qualys, Rapid7, Tenable, McAfee • ***Discovery*** – Service-Now Discovery, HP Universal Discovery, ForeScout,

CyberArk PAS – Architektúra



Fáza 2 - Privileged Account Security Program – 1-6 mesiacov

- Ochrana aplikačných účtov pre kritické databázy
  - Prístupy do databáz
  - Aplikačné účty a ich hesla v plain texte vo WebSphere, JBOSS, Tomcat, Weblogic
- Ochrana Tier 1 – Servre vo Windows Doméne
  - Vyhradené účty pre správu aktív s role based access
  - Monitoring, izolácia, detekcia podozrivých aktív a least privilege pre Tier 1
- Správa privilegovaných prístupov do Cloudu

CYBERARK

Fáza 3 - Privileged Account Security Program – 6-12 mesiacov

- Zaradenie novo vzniknutých účtov do CyberArk
  - Automatizácia, aplikácia bezpečnostných politík
- Prístupy dodávateľov cez PSM
  - Bezpečný, izolovaný a nahrávaný prístup cez PSM
- DevOps podpora
  - Automatické poskytovanie hesiel pre DevOps nástroje

CYBERARK

Fáza 3 - Privileged Account Security Program – 12+ mesiacov

- Ochrana Tier 2
  - Prístup k desktopom
  - Windows - Aplikačná kontrola, Riadenie oprávnení
  - Unix – Nastavenie oprávnení

- Ochrana servisných a aplikačných účtov
  - Popísanie usages pre servisné účty
  - Definícia práv servisných účtov a ich obmedzenie na nevyhnutné minimum (EPM)
  - Odstránenie hard-coded hesiel v aplikáciach, skriptoch

CYBERARK

Prečo CyberArk?

Integrácia out of box

Hĺbka riešenia

Zameranie iba na privilégia

Skúsenosti a referencie

CYBERARK

CYBERARK®

Ďakujeme.