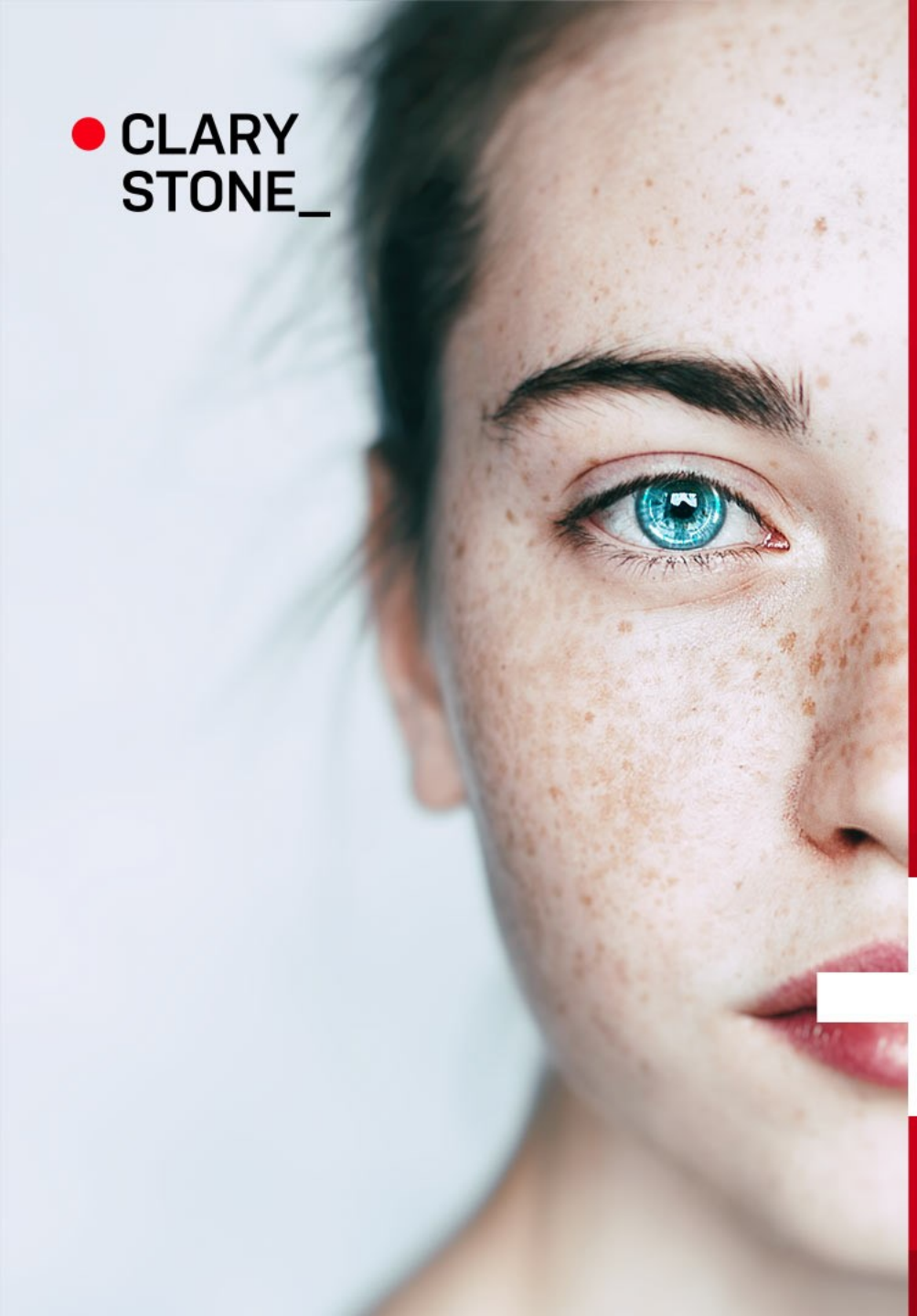
CLARY STONE_



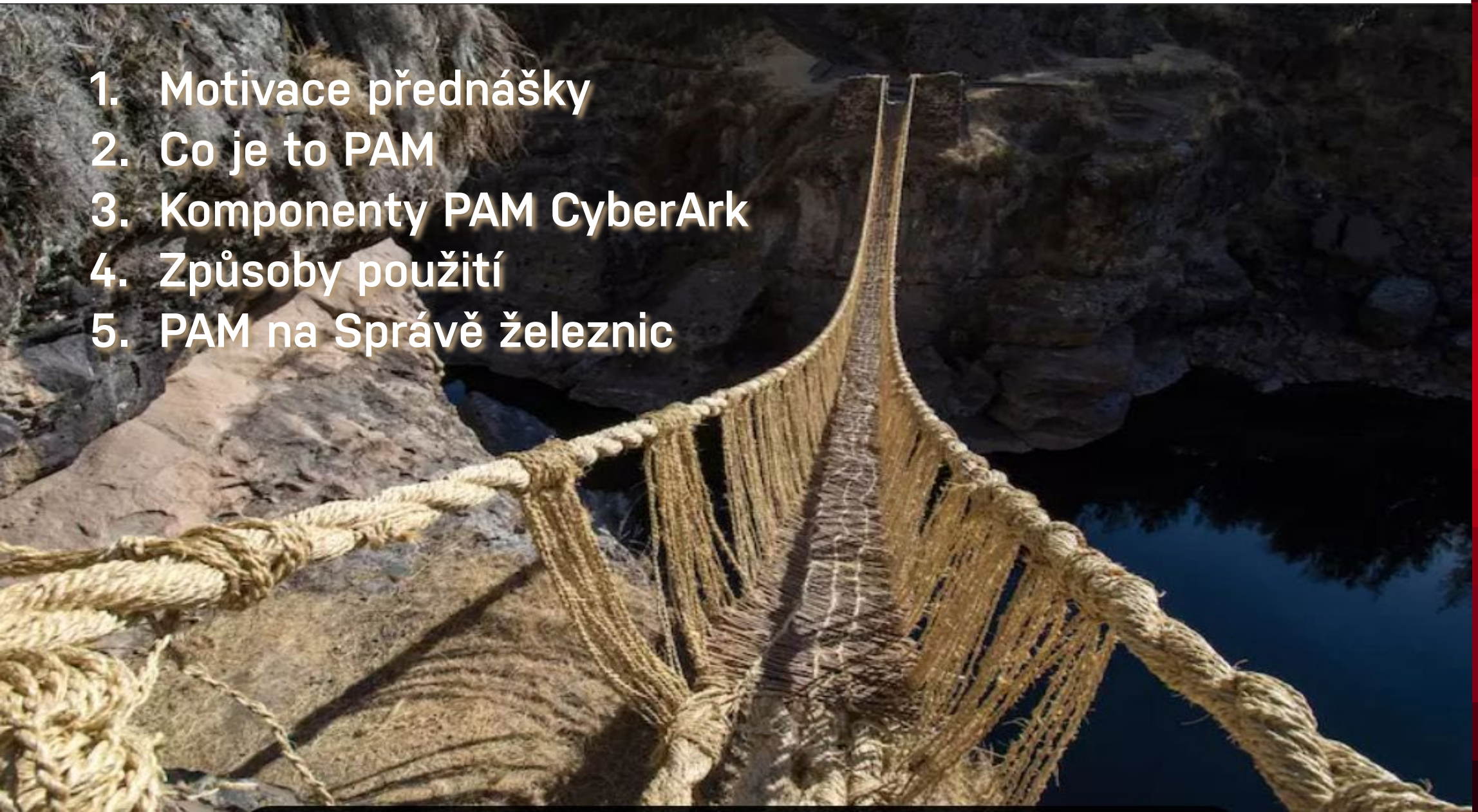
BEZPEČNÝ PŘÍSTUP KE SPRÁVĚ APLIKACÍ A SYSTÉMŮ_

Konference sdělovací a zabezpečovací techniky na železnici_

Mgr. Petr Koch

Olomouc, 6. 10. 2021

DNEŠNÍ AGENDA_



1. Motivace přednášky
2. Co je to PAM
3. Komponenty PAM CyberArk
4. Způsoby použití
5. PAM na Správě železnic

01 MOTIVACE_

MOTIVACE_

iDNES.cz / ZPRAVODAJSTVÍ
Domácí Zahraničí Krimi Kraje Ekonomika Kultura
Praha a střední Čechy
Zprávy Sport Tipy na výlet Jízdní řády MHD Firmy Práce Metro
Hacker způsobil benešovské nemocnici škodu 59 milionů, policie ho nedopadla

Bloomberg Subscribe
Cybersecurity
Uber Hack Shows

Forbes
Grasping The Problem With Privileged Accounts

CNBC
The Capital One breach is unlike any other major hack, with allegations of a single engineer wreaking havoc

CNN BUSINESS
Every single Yahoo account was hacked - 3 billion in all

Privileged Account: The Master

FINANCIAL TIMES
Retail sector
England's NHS hit by large scale cyber attack

4. ŘÍJNA 2021 | FRANTIŠEK | 19°C, OBLAČNO
iROZHLAS
DOMOV SVĚT EKONOMIKA SPORT KULTURA VĚDA KOMENTÁŘE ŽIVOTNÍ STYL VOLBY POČASÍ VINOHRADSKÁ 12
VĚDA VESMÍR PŘÍRODA TECHNOLOGIE HISTORIE TÝDEN VODY
Kde se nacházíte: iROZHLAS.cz / Věda a technologie / Technologie | Související témata: hacker hackeři hackerský útok NAKIT Vladimír Rohel Microsoft ministerstvo práce práce a sociálních věcí
Útok hackerů na státní správu byl sofistikovaný a složitý, říká Rohel ze státní IT agentury

heft Attack
8/30/2019 02:10 PM
DARK Reading
sends stolen data out of the network
A new credential-theft attack campaign is using DNS to exfiltrate data. The

cyberscoop
TECHNOLOGY
Russian government hackers used office technology to try to breach privileged accounts

Montreal Gazette
Desjardins: Rogue employee caused data breach for 2.9 million members

Help Net Security
October 10, 2019
Impact and prevalence of cyberattacks that use stolen hashed administrator credentials

InformationWeek DARKReading
Watch the Watchers: 'Trusted' Employees Can Do Damage

BizTech
NIST Creates New Guidelines for Managing Privileged Accounts

HOSPODÁŘSKÉ NOVINY
TECH TESTY MOBILY & TABLETY POČÍTAČE INTERNET AV MÉDIA GEEKOSFÉRA HRY EKONOM EVENTS
Za třetinou všech útoků na české počítače stál jeden špionský program. Jeho terčem jsou uživatelská hesla
DOPORUČUJEME

The New York Times
Attack Gave Chinese Hackers Privileged Access to U.S. Systems

THE WALL STREET JOURNAL
Malware Targets Vulnerable Admin Accounts

CSO
Privileged Comes with Peril in World of Cybersecurity
Security experts have been warning enterprises for some time that the greatest security...

Privileged Account Details Are Often Shared and Can Be a Weak Entry Point for Attackers

Annual Data Breach Investigations Report
The use of stolen credentials still leads the way from a hacking variety standpoint...

CLARY STONE_

MOTIVACE_
Bezpečný přístup ke správě aplikací a systémů_

01

ZAČÍNÁ TO NA KONCOVÝCH ZAŘÍZENÍCH_

ANATOMIE ÚTOKU_

Počáteční vniknutí, většinou phishing

Pracovní stanice

Ukradené admin heslo

Pracovní stanice

Ukradené admin heslo **k serveru**

Získání přístupu ke VŠEM systémů

Kritické pracovní stanice

Kritické servery

Bezpečnostní systémy

Infrastruktura v Cloudu

Server

Použití hesla. Nezajímavý server. Jdeme na další.

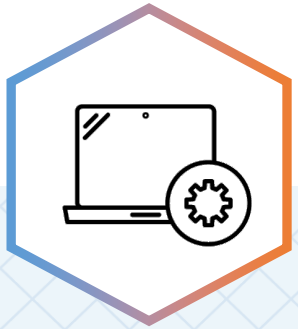
Server

Krádež admin hesla s vysokým oprávněním

Doménový kontrolér

Vygenerování tiketů pro všechny aktiva v doméně

UŽIVATEL S OPRÁVNĚNÍM „ADMIN" MŮŽE_



Měnit konfiguraci systému

Instalovat malware

Přistupovat k účtům a měnit je

87 % organizací nechává uživatelům lokální admin účty

Source: CyberArk Threat Landscape Survey, February 2018

DILEMA NEJEN NA SŽ: BEZPEČNOST x JEDNODUCHOST?

	Uživatelé MAJÍ lokální ADMIN práva	Lokální ADMIN práva jsou odebrány
Provoz	Šťastní a produktivní uživatelé 	Zvýšená zátěž pro tým podpory. Zvýšený počet hovorů a nákladů. 
Bezpečnost	Zvýšené množství bezpečnostních incidentů 	Omezení útoku na koncové stanice 

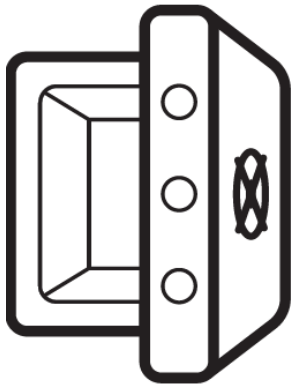
02 CO JE TO PAM_

CO JE TO PAM_

- **PAM** = Privileged Account Management
  - je systém pro zajištění bezpečnosti informační infrastruktury
  - zjednodušeně lze říct že je to „správce hesel"

- **PAM** řeší následující požadavky v oblasti kybernetické bezpečnosti:
  - provozování bezpečného úložiště hesel a klíčů k privilegovaným účtům
  - zajištění kontroly nad přístupem k privilegovaným účtům
  - možnost automatické změny hesel dle definované politiky bez zásahu člověka
  - zajištění izolace uživatelského prostředí (ke kterému se hlásíme) od cílového systému (na kterém pracujeme)
  - získání kompletní auditní stopy o činnostech prováděný z privilegovaných účtů
  - zajišťuje soulad s 181/2014 Sb. tzv. „Zákonem o kybernetické bezpečnosti"

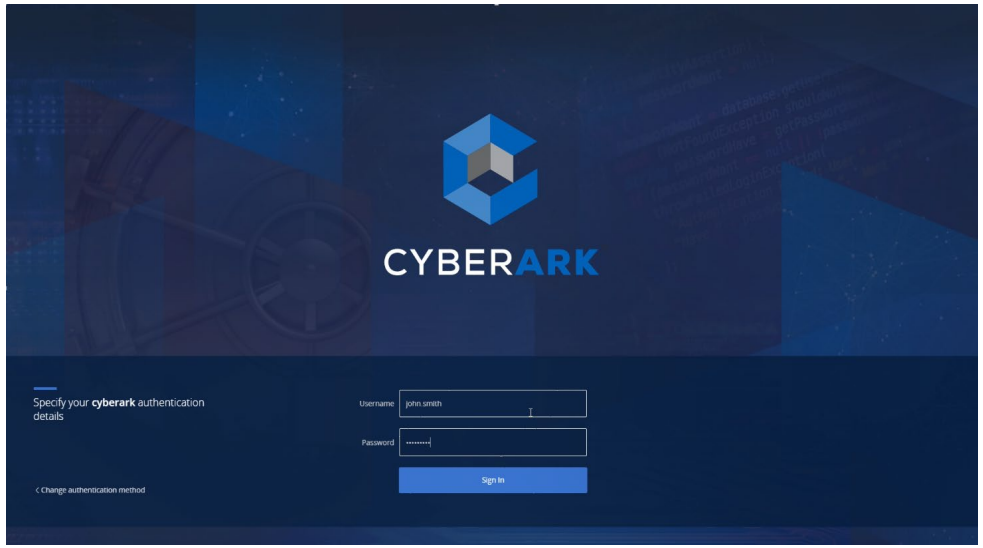
- **PAM** není všelék - nutná vazba na další systémy:
  - MFA - více faktorová autentifikace
  - Active Directory - autentizace/autorizace uživatelů
  - cílové systémy na kterých řídíme privilegované účty

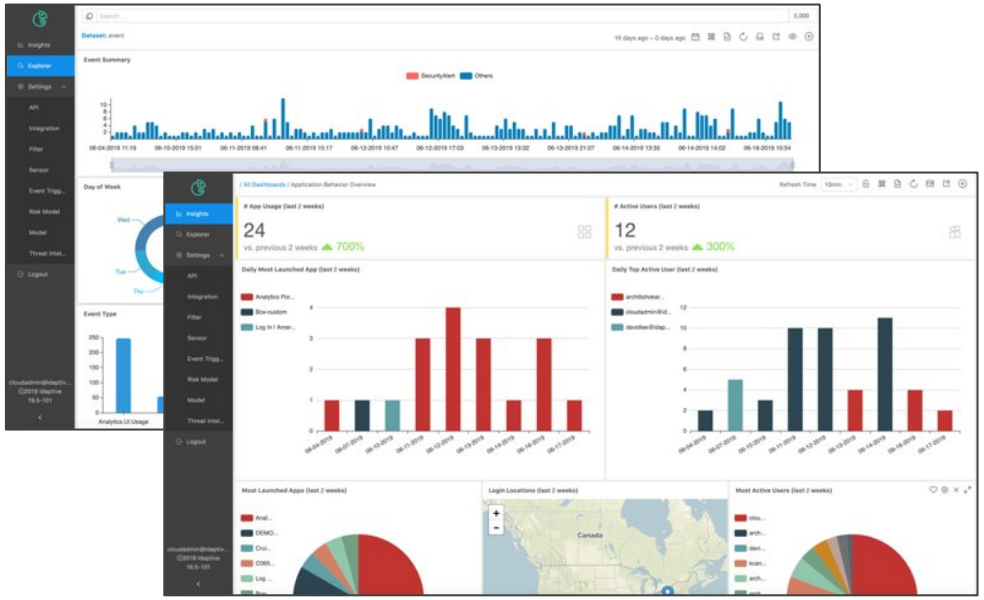


03 KOMPONENTY PAM CYBERARK_

KOMPONENTY PAM CYBERARK_

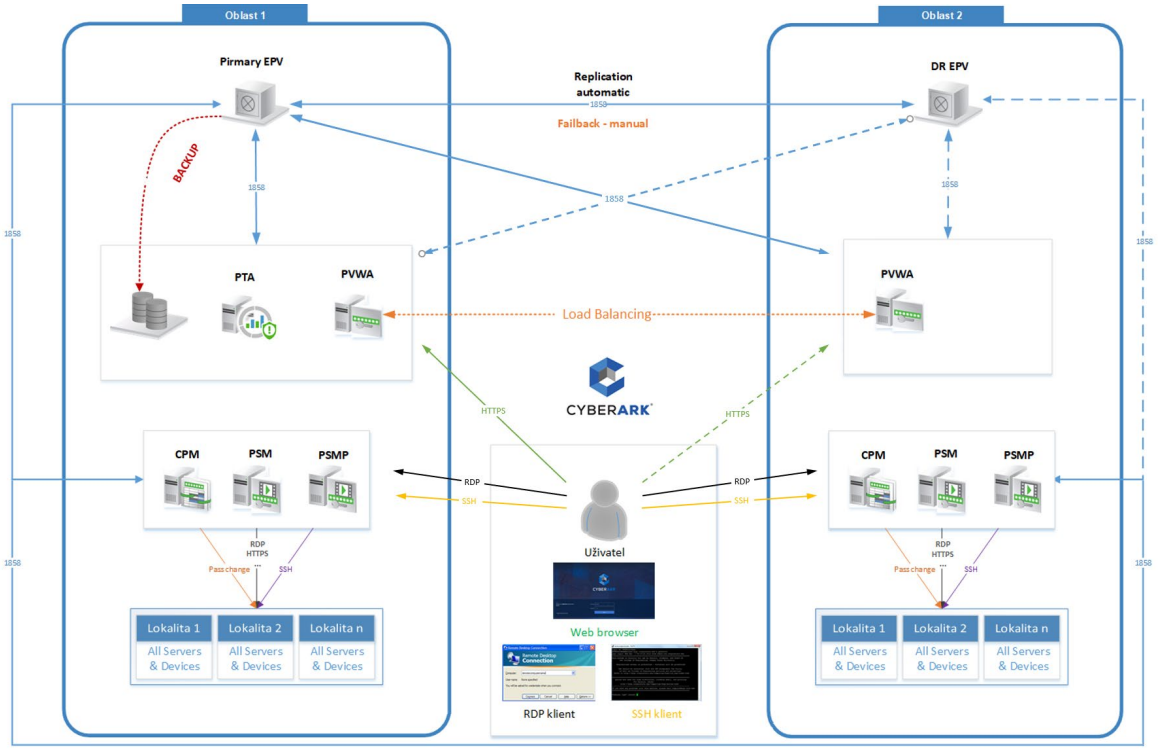
- Enterprise Password Vault (**EPV**)
  - vysoce zabezpečené úložiště hesel
  - v šifrované podobě uchovává hesla, konfigurační/auditní informace i záznamy aktivit
  - většinou zdvojená a data se replikují pro případ havárie
- Password Vault Web Access (**PVWA**)
  - webový portál pro uživatele a administrátory
  - Automatické připojení k cílovému systému dle přidělených přístupových práv
- Privileged Threat Analytics (**PTA**)
  - analýza chování a hrozeb v reálném čase





KOMPONENTY PAM CYBERARK_

- Privileged Session Manager (**PSM**)
  - bezpečný JUMP Server
  - sem se připojují uživatelé (místo přímo k cílovým systémům
  - zajišťuje izolaci a chrání tak cílové systémy při kompromitaci
  - zaznamenává aktivity ve formě videonahrávky
  - poskytuje tak kompletní auditní stopu
  - pro přímý SSH (Secure Shell) přístup Privileged Session Manager Proxy (PSMP)
- Central Policy Manager (**CPM**)
  - pravidelná kontrola přihlašování
  - automatické změny hesel (komplexnosti a stáří)

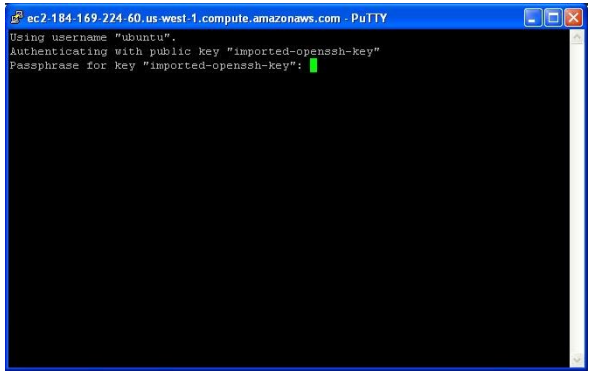


04 ZPŮSOBY POUŽITÍ_

ZPŮSOBY POUŽITÍ_

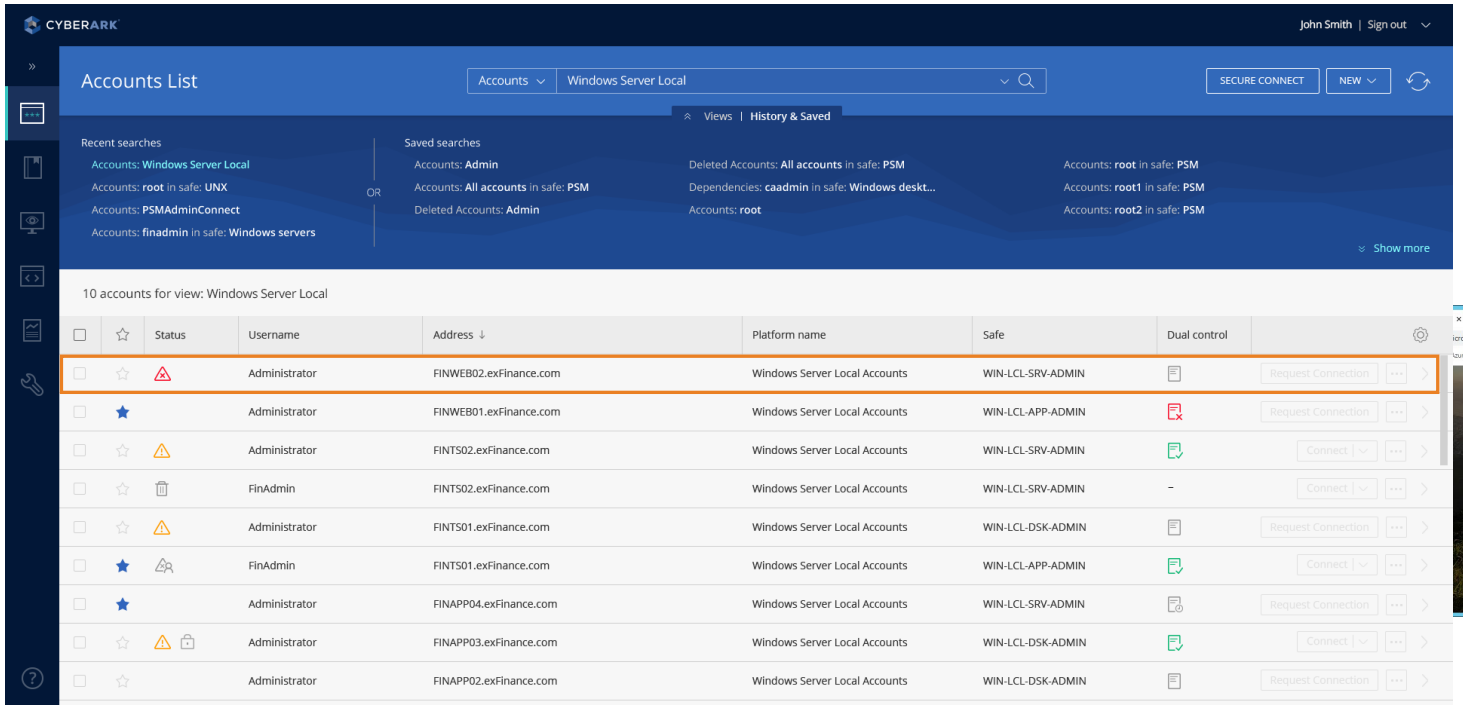
- Bezpečné uložení autentizačních údajů (heslo či SSH klíč) v trezoru a následně:
  - připojení k zařízení vybraným účtem bez zobrazení hesla
  - zobrazení nebo zkopírování hesla
  - změna hodnoty hesla v trezoru
  - změna hesla na cílovém zařízení
  - zpřístupnění hesla až na základě schválené žádosti

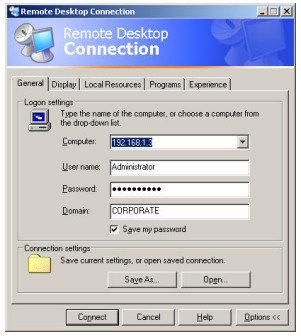
- Připojení k cílovému systému přímo z SSH klienta
  - uživatel se připojí přímo ze svého počítače k SSH Jump Serveru
  - Jump Server uživatele ověří a zkontroluje oprávnění k vybranému účtu ve Vaultu
  - uživateli je předána již přihlášená relace (+záznam aktivity)

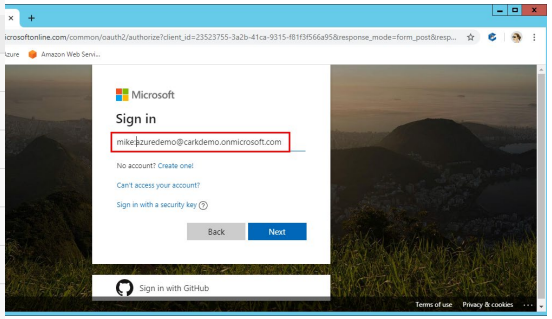


ZPŮSOBY POUŽITÍ_

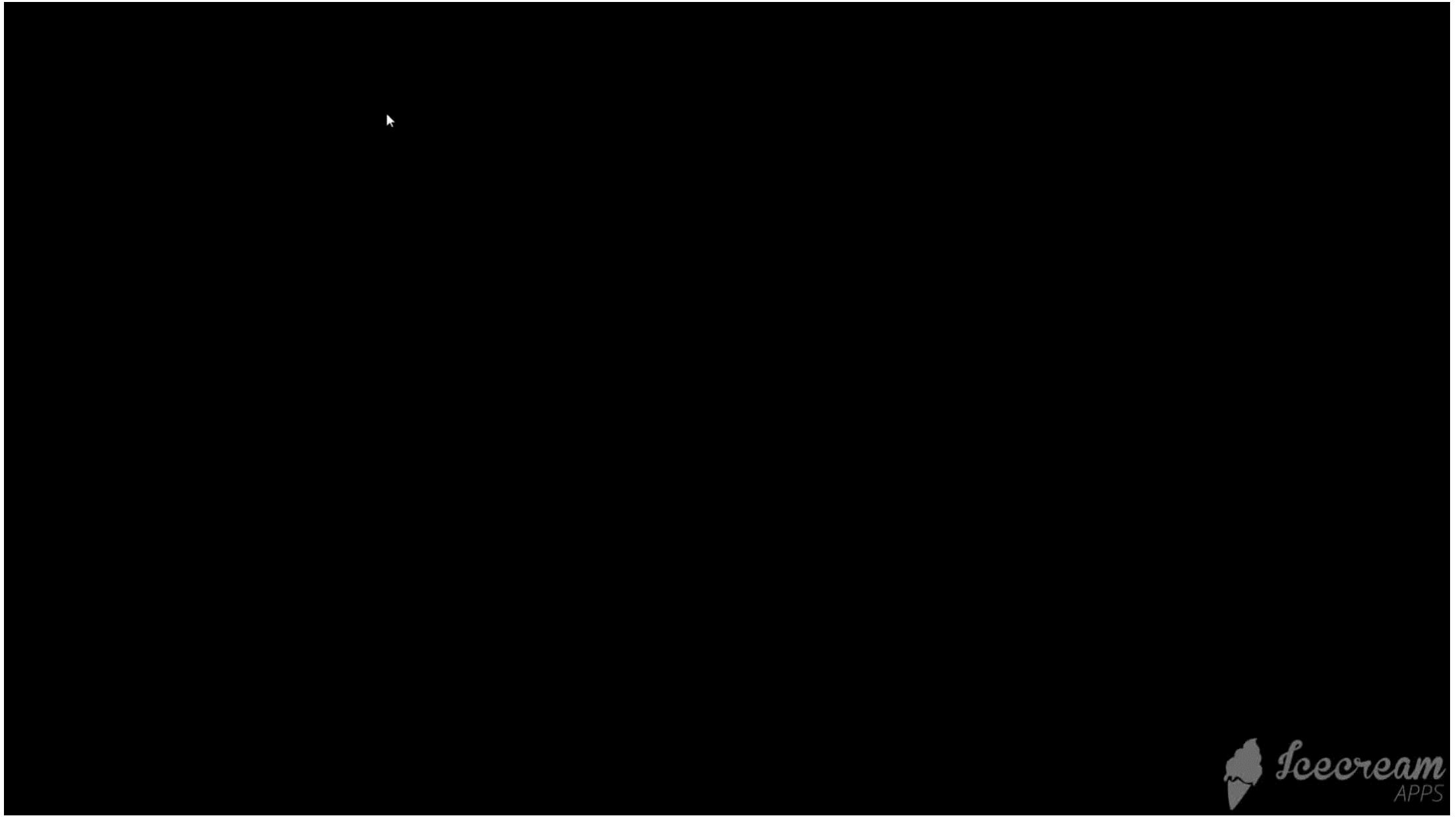
- Připojení k cílovému systému přes webové rozhraní
  - po přihlášení do webového PVWA uživatel vidí jen svoje účty
  - CONNECT generuje jednorázový RDP soubor pro připojení k Jump serveru
  - na Jump serveru je spuštěna příslušná klientská aplikace
  - uživateli je předána již přihlášená relace (+záznam aktivity)
  - uživatel se ověřuje pouze jednou při přístupu do PVWA a ke koncovým systémům je již přihlašován automaticky







ZPŮSOBY POUŽITÍ - VIDEO UKÁZKA_



05 PAM NA SPRÁVĚ ŽELEZNIC_

PAM NA SPRÁVĚ ŽELEZNIC_

- systém PAM CyberArk je v prostředí Správy železnic od ledna 2021
- v rámci implementace nasazení na:
  - správu operačních systémů na bázi Windows a Linuxových serverů
  - SQL a Oracle databází
  - systému SAP atd.
- stále je kapacita pro integraci dalších cílových systémů
- k dispozici dostatek licencí pro další privilegované uživatele
- systém má ve správě Odbor Informatiky O22
- projekt realizovala společnost DimensionData a Clarystone

CYBERARK

CLARY STONE_

DĚKUJI ZA POZORNOST_

Mgr. Petr Koch
Clarystone s.r.o.
Na Větrově 889/13, 142 00 Praha 4

www.clarystone.com