MUNI

Asset (IT Inventory) Management

Seminář o bezpečnosti sítí a služeb 2023, CESNET

Daniel Tovarňák et al.

Masarykova univerzita, CSIRT-MU STR

Brno, Česká republika

07.02.2023

Dnešní téma – řízení aktiv a IT inventarizace

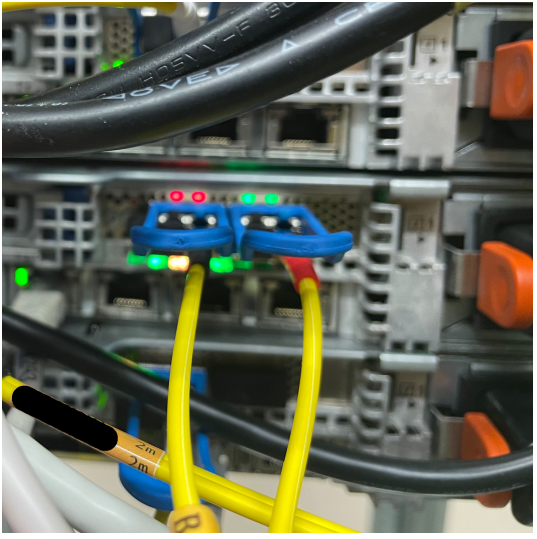
Dobře zvládnutý asset management je jeden ze základních atributů pro zvládnutí bezpečnosti. Probereme, jak by tato oblast mohla a měla vypadat v prostředí vysoké školy.

...aneb od kabelů k balíčkům.

Proč by bylo dobré chovat se k IT inventáři stejně (dobře), jako se teď chováme k fyzickému majetku. A co by to znamenalo?

Co a proč.

Vím co chráním a provozuji (?)



ITILv4 ITAM (IT Asset Management)

Řízení aktiv je zavedený a doporučený postup pro akvizici, provoz, údržbu a vyřazování aktiv organizace.

Cíle

- maximalizace hodnoty
- optimalizace nákladů
- řízení rizik
- podpora rozhodování
- regulace a závazky
  - nákup
  - znovupoužití
  - vyřazení
  - likvidace

Terminologie (ISO 27k, ISO 31k) – verze v1

- **Riziko** je účinek nejistoty na dosažení cílů organizace.
- **Událost** je něco co se stalo, nebo se předpokládá, že se to stalo.
- **Důsledek** je vliv **události** na cíle organizace.
- **Eventualita** je hypotetická událost. Představuje zdroj nejistoty.
- **Hrozba** je eventualita, u které lze očekávat negativní důsledky.
- **Slabina** je chyba, opomenutí, nebo nedostatek v procesech, postupech, pravidlech, politikách, opatřeních, organizaci, systémech, síti, SW, či HW.
- **Zranitelnost** je **slabina** která dovoluje realizaci hrozby.
- **Opatření** je prostředek, který zachovává, nebo modifikuje riziko.
- **Aktivum** je cokoliv hodnotného, co přispívá k cílům organizace.

Aktiva a IT inventář

Dělení aktiv

- Primární aktiva – procesy a činnosti, informace
- Podpůrná aktiva – HW, SW, sítě, lidé, lokality, org. rámec

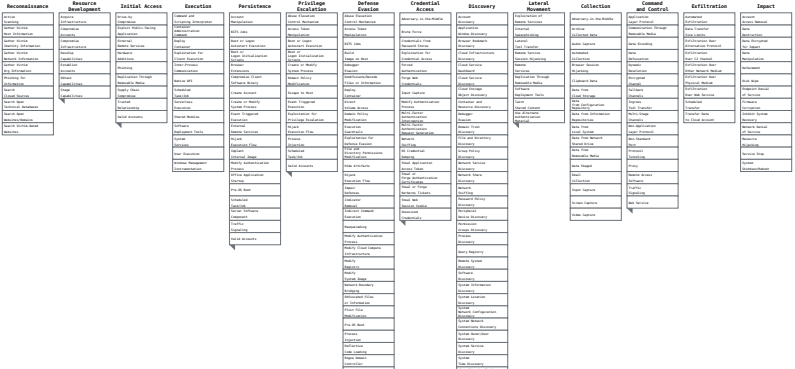
Hodnocení aktiv

- Cena kabelu vs. cena služby, kterou připojuje

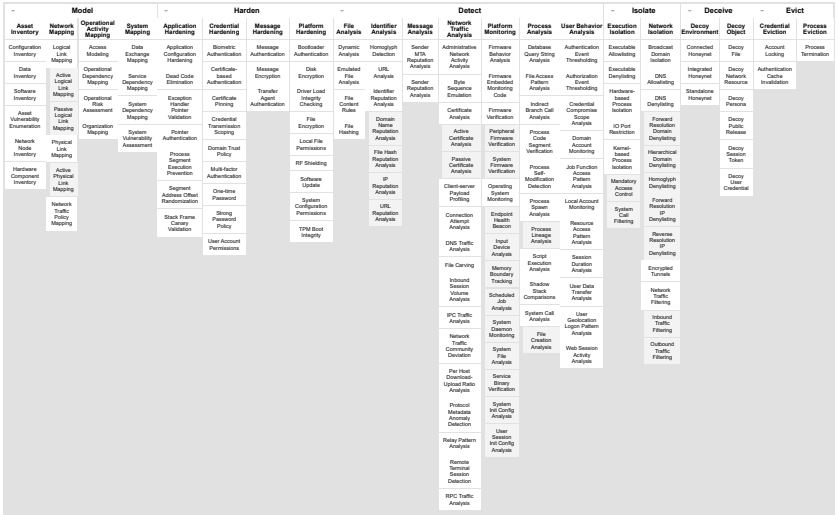
IT inventář

- Fyzické lokality, místnosti, napájení
- Kabely, patch panely, transceivery
- Rozvaděče (racky) a jejich jednotlivé pozice
- Zařízení a jejich komponenty
- VLANy, IP adresy, prefixy, FW pravidla, směrovací pravidla
- Operační systémy, balíky, aplikace, knihovny
- Krizové a provozní kontakty
- Uživatelé a koncové prvky (laptopy, mobily, desktopy, servery)

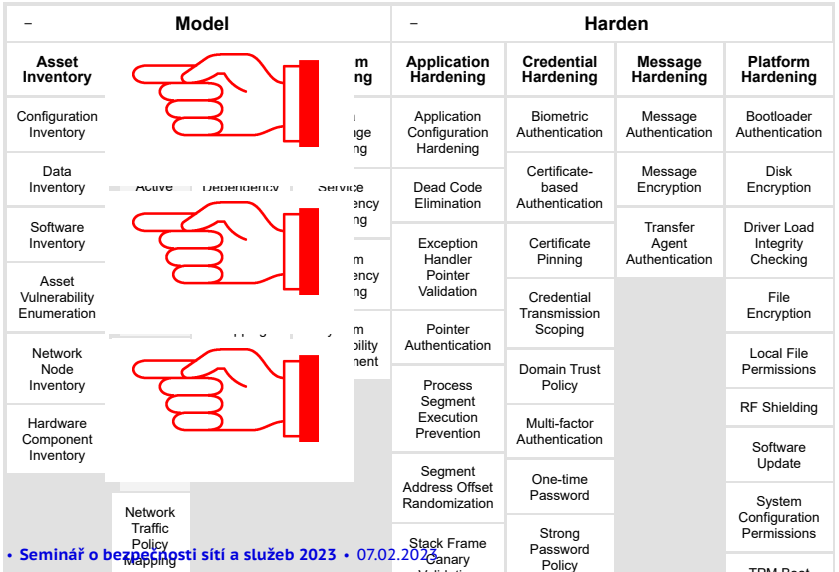
MITRE ATT&CK® Enterprise TTPs



MITRE D3FEND™ Knowledge Graph



MITRE D3FEND™ Knowledge Graph



Jak.

Geografická data

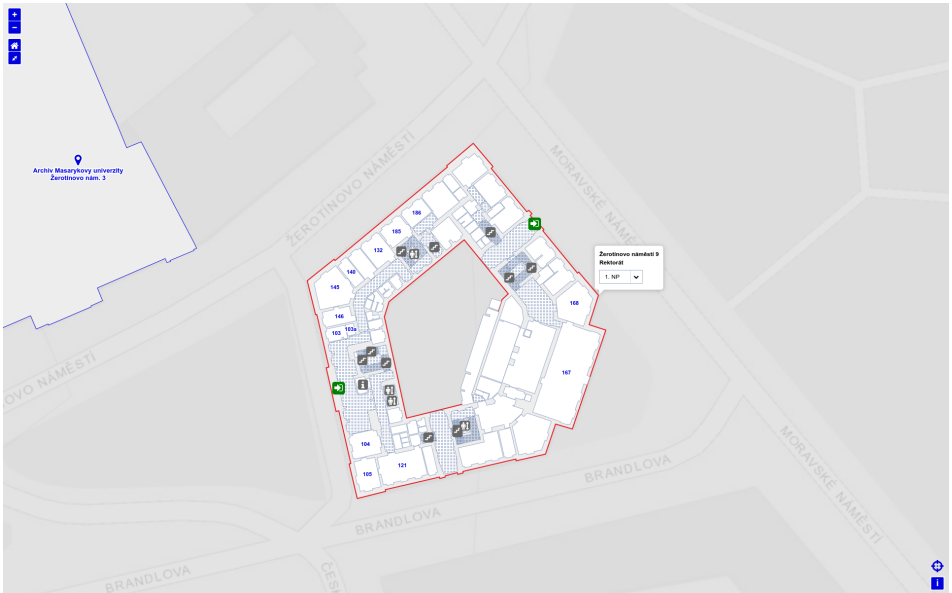
Příklady

- Stavební pasport
  - Budovy, místnosti
  - Okna, dveře, schodiště
- Technologický pasport
  - Zařízení všeho druhu
  - Topení, elektroinstalace (silnoproud i slaboproud)
  - Vzduchotechnika a klimatizace
- Komunikační sítě
  - Optické sítě
  - Metalické sítě
  - Bezdrátové sítě

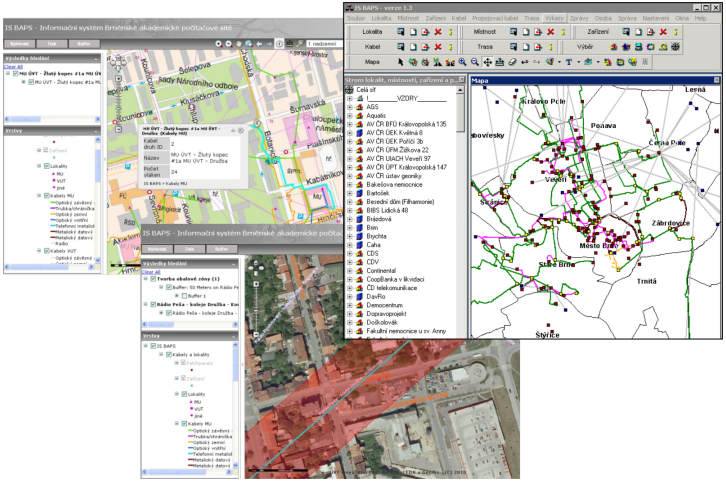
Přínosy

- Plánování a projektování výstavby
- Správa (poruchy a opravy)
- Fyzická bezpečnost, napájení a konektivita

Munimap + data stavebního pasportu MUNI

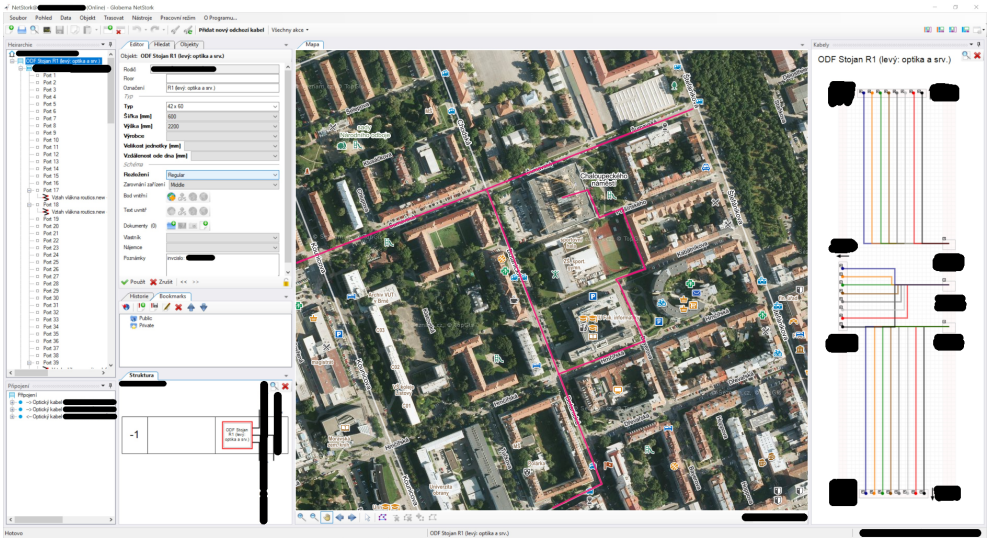


IS BAPS (Brněnská Akademická Počítačová Síť)



- Zdroj: `https://muni.cz/go/pribeh-gisu`

Globema NetStork



Síťová a výpočetní infrastruktura, datová centra

Příklady

- Data Center Infrastructure Management (DCIM)
  - Lokality, místnosti, napájení, konektivita, rozvaděče, rack pozice, PDUs
  - Kabeláž, patch panely, rozhraní, transceivery
  - Zařízení všeho druhu (servery, switche, routery, FW)
- IP Address Management (IPAM)
  - VLANy, IP adresy, prefixy, rezervace prefixů, VRF
- Bezdrátové sítě
- Virtualizace
  - Virtuální stroje a virtualizační clustery
- Technické, nouzové a bezpečnostní kontakty

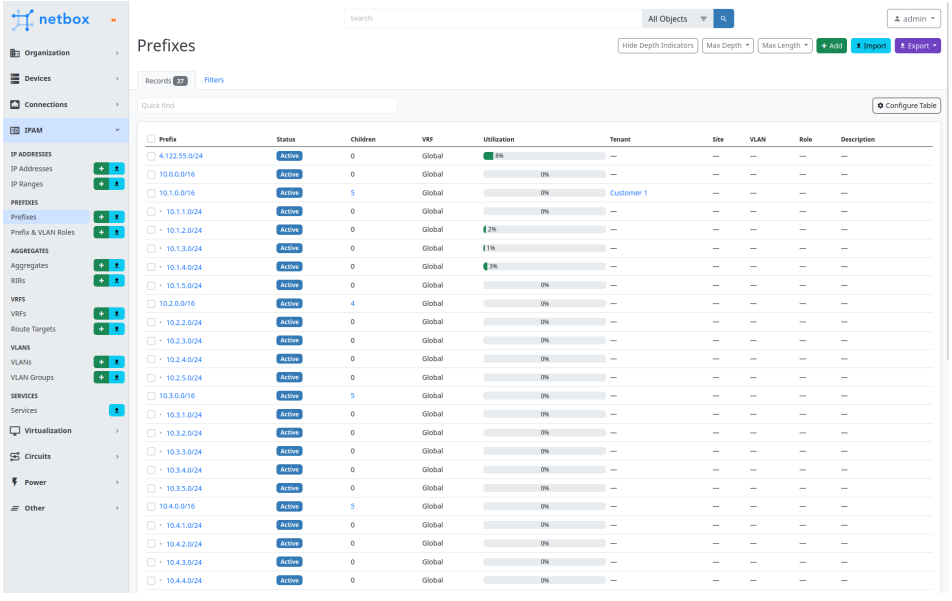
Přínosy

- Plánování a architektura, správa (poruchy a opravy)
- Fyzická bezpečnost, síťová bezpečnost, **situační povědomí**
- Řízení zranitelností systémů (HW/SW)

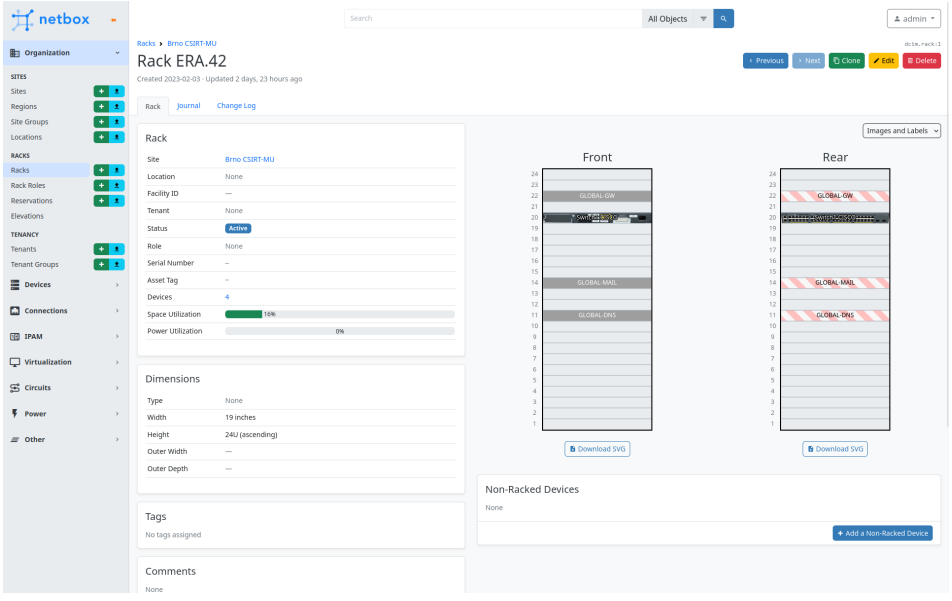
NetBox

- `https://netbox.dev/about/`
- Ucelené open-source řešení
  - DCIM, IPAM
  - Virtualizace, bezdrátové sítě
  - Organizace infrastruktry
  - Kontakty různého druhu
- Zachování jisté volnosti
  - Vlastní atributy
  - Některé koncepty lze ohnout požadovaným směrem
- Infrastrukturní agent (o agentech dále)
- Globální vyhledávání
- Řízení přístupu na úrovní objektů
- Zdroj pravdy, velmi omezeně pak příjemce pravdy
- Rozšiřitelnost
  - Python + Django, Python knihovna
  - GraphQL API pro čtení, REST API (OpenAPI)

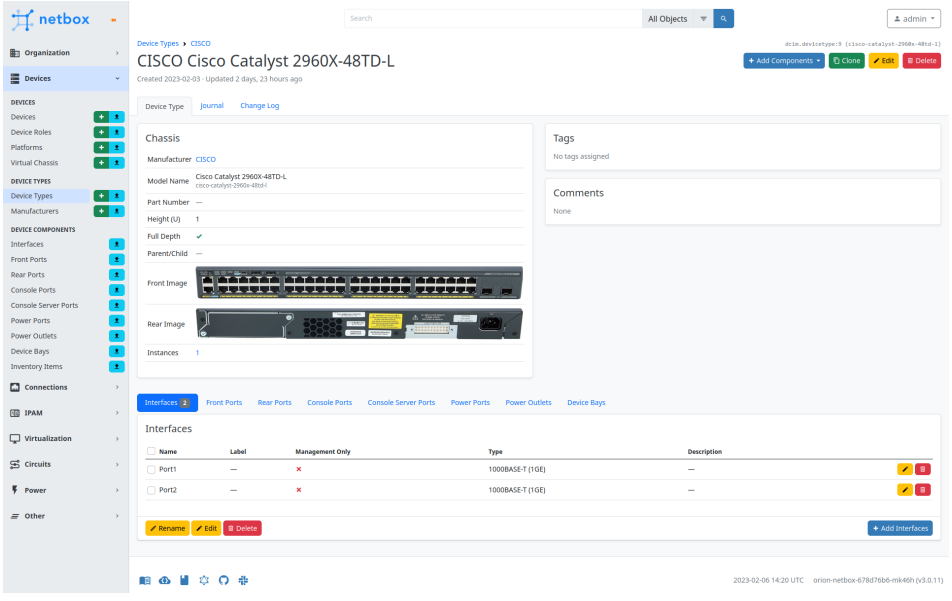
NetBox – IP prefixy



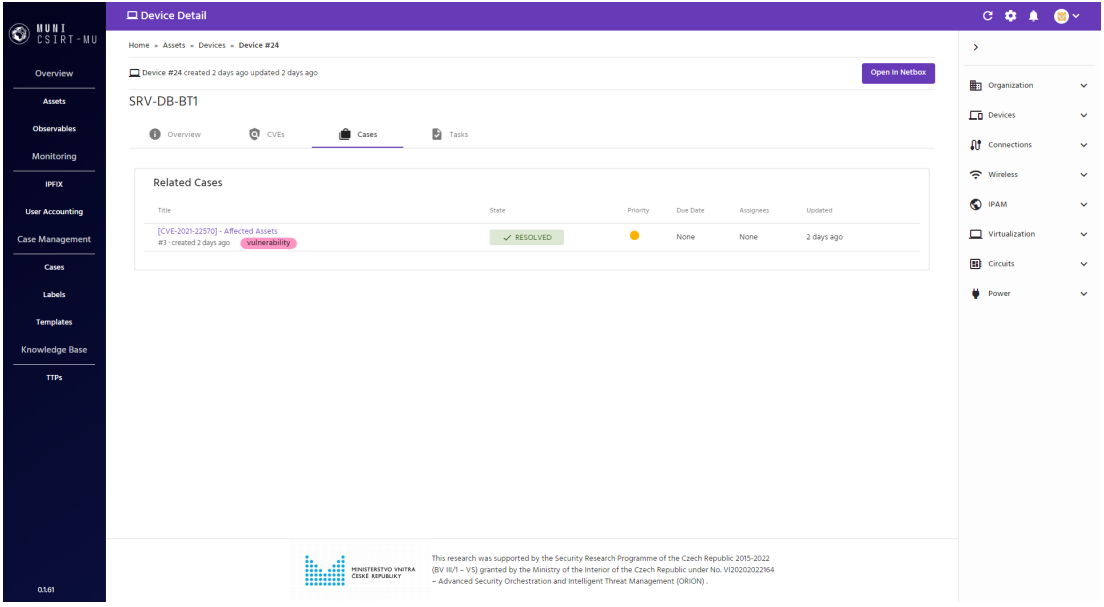
NetBox – pohled na rack



NetBox – detail typu zařízení



Netbox – integrace s ostatními nástroji



Uživatelé a koncové prvky, software

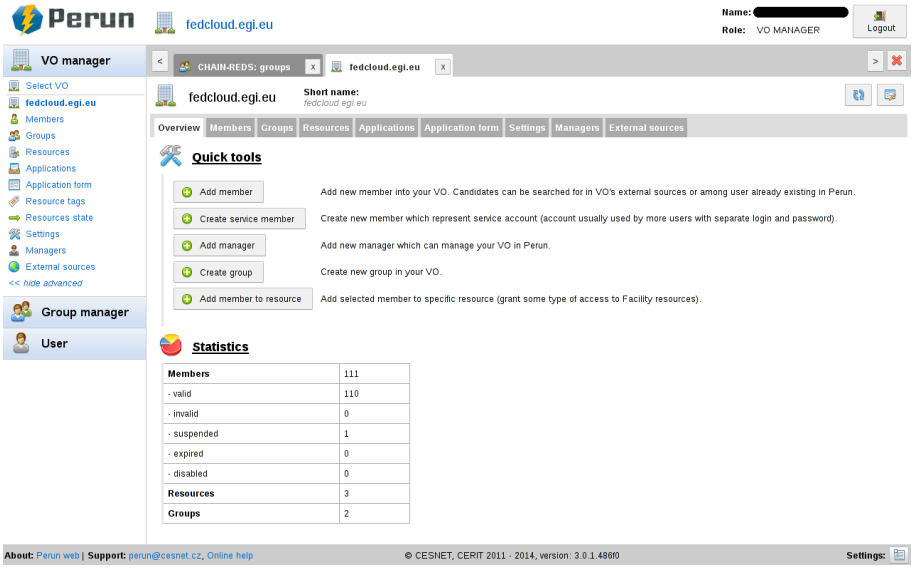
Příklady

- Uživatelské
  - Účty, skupiny
  - Přístupy, oprávnění
- Koncové prvky
  - Síťové prvky, (virtuální) servery
  - Laptopy, desktopy, mobily, BYOD, IoT
  - COKOLIV co jde strčit do sítě
- Software
  - Mikro-kód, firmware, BIOS
  - Operační systémy, middleware, hypervizory
  - Aplikace, balíky, systémové komponenty

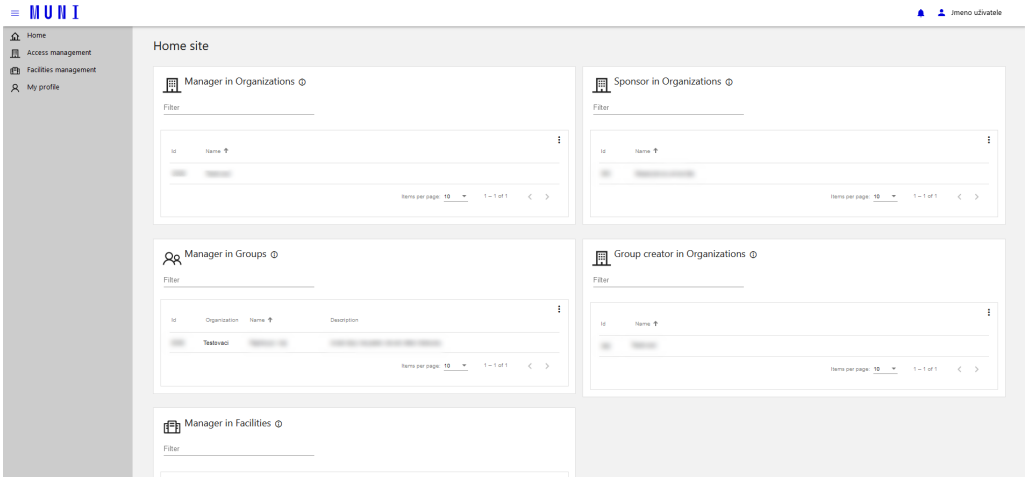
Přínosy

- Péče o uživatele
- Uživatelská bezpečnost, **situační povědomí**
- Řízení přístupu, **zranitelností** a bezpečnosti obecně

Perun (CESNET)



Perun (CESNET), MUNI instance



Řízení zranitelností pro počítačové systémy v 1 min.

- Pokud znám název SW/HW, platformu a verzi, znám CVE zranitelnosti
- Pokud disponuji seznamem zařízení, umím otestovat jejich compliance s nějakým profilem

Security Content Aplication Protocol (SCAP)

- SCAP 1.0 – rok 2009
- Common Platform Enumeration (CPE)
- Common Vulnerabilities and Exposures (CVE)
- Open Vulnerability Assessment Language (OVAL)
- Software Identification (SWID)

```
wfn:[part="o", vendor="microsoft", product="windows_server_2008", version="r2",
↪  update="sp1", edition=ANY, language=ANY, sw_edition=ANY, target_sw=ANY,
↪  target_hw="itanium", other=ANY]
cpe:/o:microsoft:windows_server_2008:r2:sp1:~~~~itanium~
cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:*:*:*:*:itanium:*
```

Agentní a bez-agentní řešení pro koncové prvky

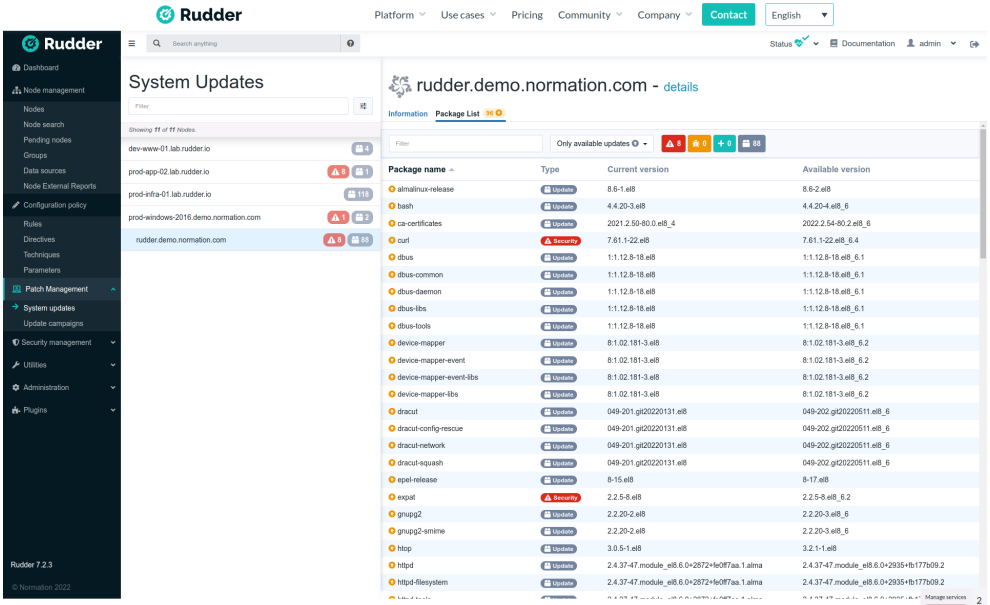
Bez-agentní řešení

- *Paradox – není agent, jako agent.*
- Nmap (`https://nmap.org/`)
- Nessus (`https://www.tenable.com/products/nessus/`)
- Sner4 (`https://github.com/bodik/sner4/`)
- OpenVAS (`https://www.openvas.org/`)

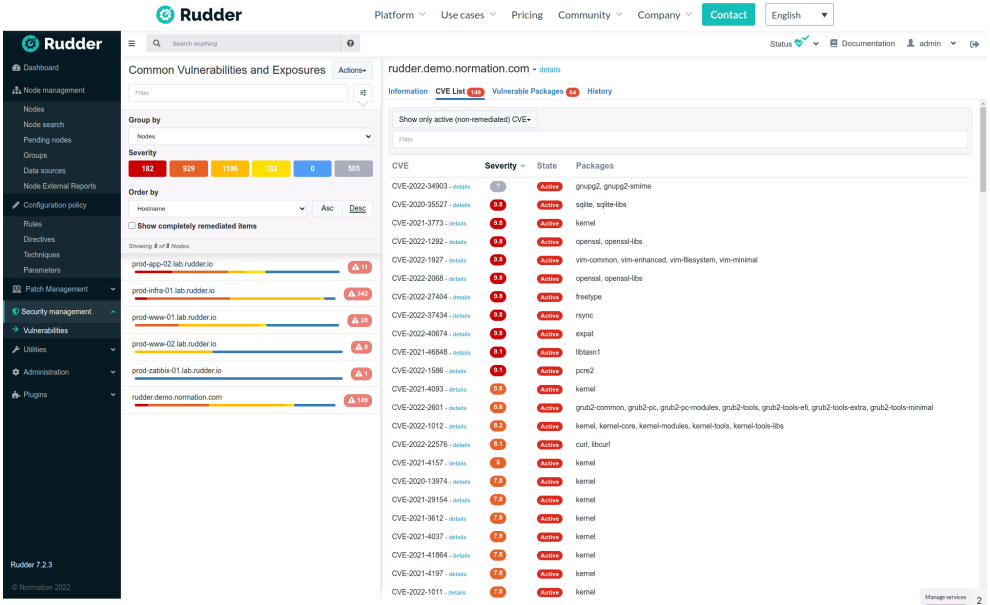
Agentní řešení

- *Paradox – kam všude nainstalovat agenty?*
- Rudder (`https://rudder.io/`)
- Lansweeper (`https://www.lansweeper.com/`)
- Snipe-IT (`https://snipeitapp.com/`)
- Pakiti (`https://github.com/CESNET/pakiti-server/`)

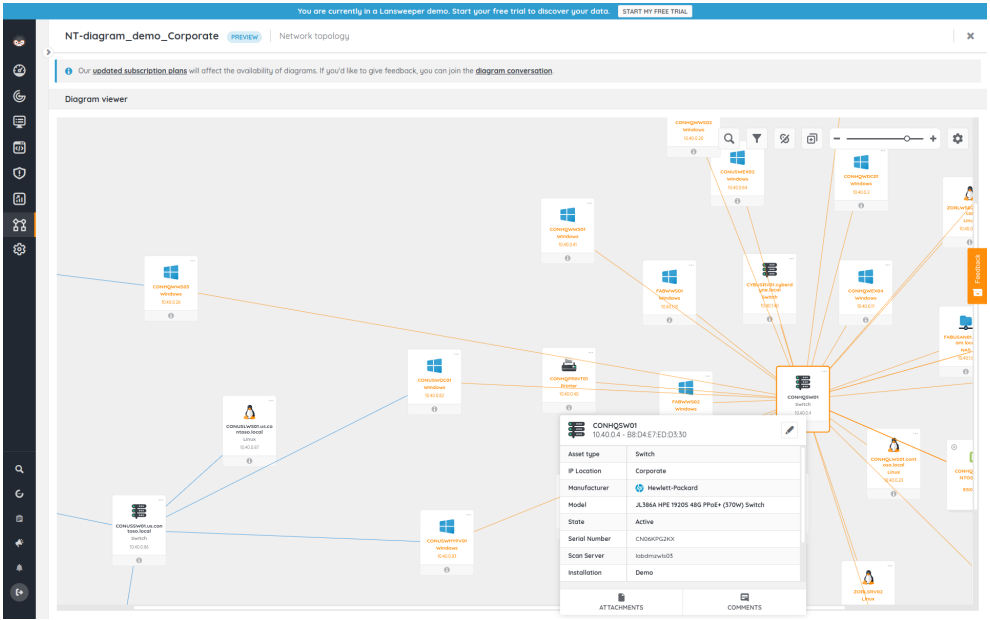
Rudder – přehled balíků



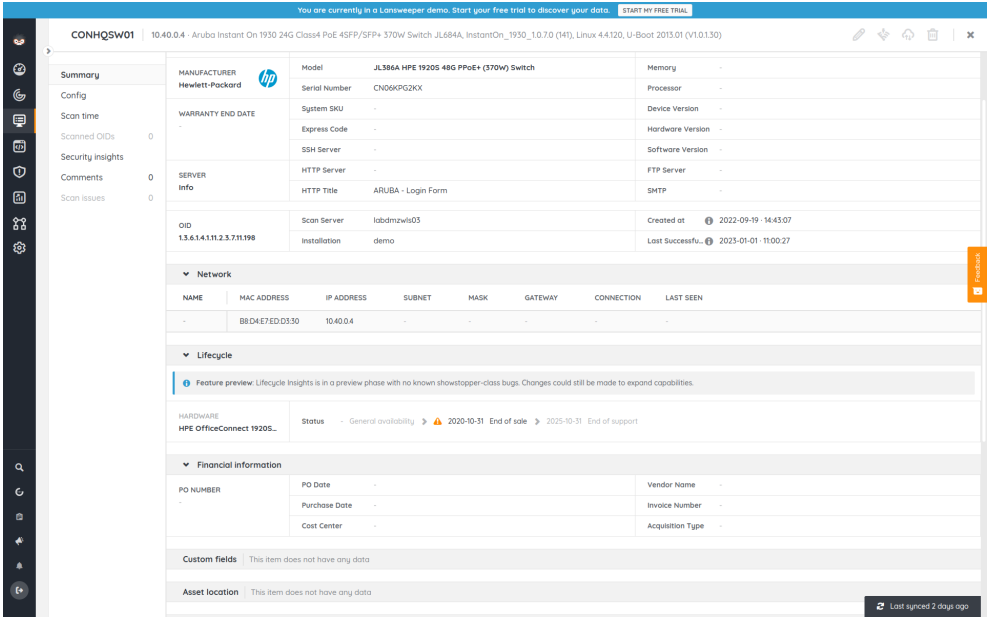
Rudder – přehled zranitelností



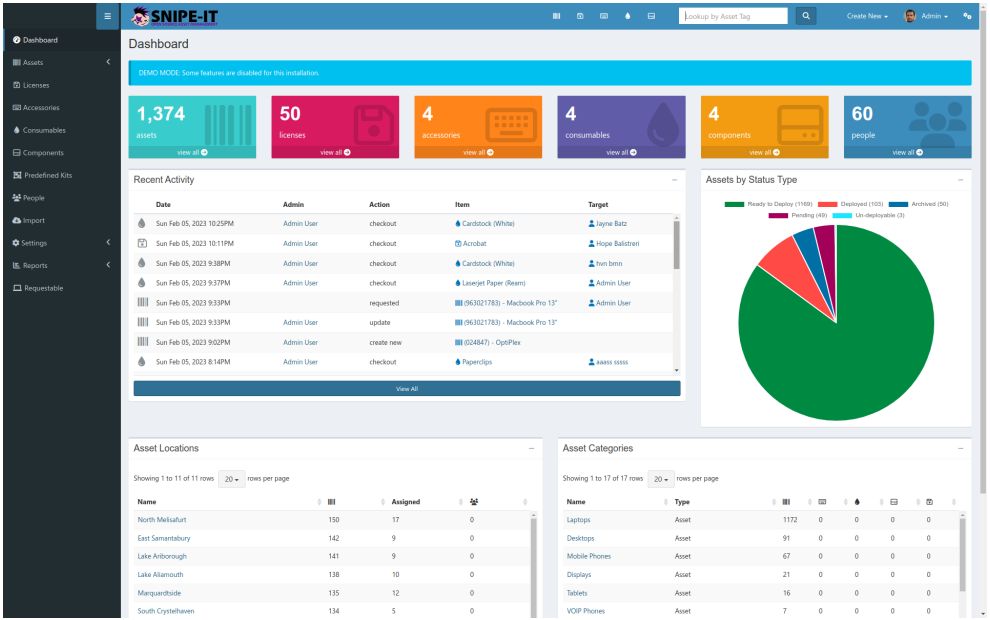
Lansweeper – diagram prvků



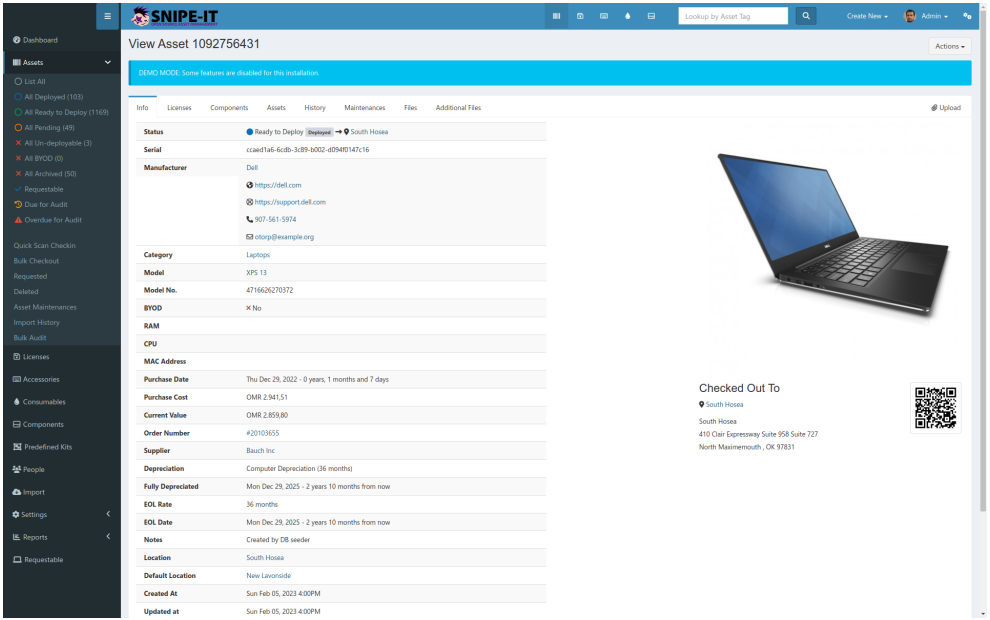
Lansweeper – detail prvku



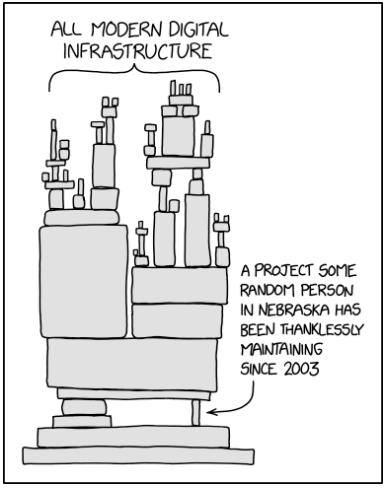
Snipe-IT – přehledová obrazovka



Snipe-IT – detail prvku



Software – knihovny a závislosti



- Zdroj: `https://xkcd.com/2347/`

Software – knihovny a závislosti

Příklady

- Závislosti všecho druhu
  - Maven (Java), PyPi (Python), NPM (Javascript)
- Závislosti na stabilním API (cloud služby)

Jak na to

- Software Bill of Materials (BOM)
- SaaS BOM

Přínosy

- Další úroveň řízení zranitelností
  - GitLab Dependency Scanning apod.
- Mitigace u zranitelností typu Log4shell

Proč to nejde?

- Rozmanitost IT inventáře
- Technický dluh
- Kognitivní zátěž jednotlivce
- Nízká úroveň automatizace
- Náklady vynaložené, ale ne ušetřené
- Absence politik, procesů a skutečného řízení

Co s tím?

- Automatizace, automatizace, automatizace
- Ale také dost manuální práce
- Podpora z vedoucích pozic
  - Čas na rozvoj
  - Lidské zdroje

Příklad s omezeným zdrojem pravdy

- Agentní systém
- Výše uvedené + hodnocení compliance
- Výše uvedené + IPAM/DCIM
- Výše uvedené + detekce rozdílů
- Výše uvedené + remediace rozdílů

MASARYK
UNIVERSITY