

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

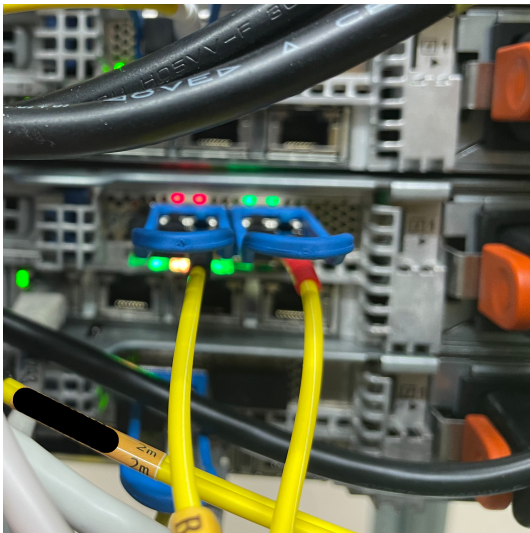
Dobře zvládnutý asset management je jeden ze základních atributů pro zvládnutí bezpečnosti. Probereme, jak by tato oblast mohla a měla vypadat v prostředí vysoké školy.

...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, síť, 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

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
<ul style="list-style-type: none"> ActiveX Collaboration External Remote Services Malware Remote Services Software Libraries Web Services 	<ul style="list-style-type: none"> ActiveX Collaboration External Remote Services Malware Remote Services Software Libraries Web Services 	<ul style="list-style-type: none"> Admin Brute Force Service Disruption Service Outage Software Libraries Web Services 	<ul style="list-style-type: none"> Command and Control Collaboration External Remote Services Malware Remote Services Software Libraries Web Services 	<ul style="list-style-type: none"> ActiveX Collaboration External Remote Services Malware Remote Services Software Libraries Web Services 	<ul style="list-style-type: none"> ActiveX Collaboration External Remote Services Malware Remote Services Software Libraries Web Services 	<ul style="list-style-type: none"> ActiveX Collaboration External Remote Services Malware Remote Services Software Libraries Web Services 	<ul style="list-style-type: none"> ActiveX Collaboration External Remote Services Malware Remote Services Software Libraries Web Services 	<ul style="list-style-type: none"> ActiveX Collaboration External Remote Services Malware Remote Services Software Libraries Web Services 	<ul style="list-style-type: none"> ActiveX Collaboration External Remote Services Malware Remote Services Software Libraries Web Services 	<ul style="list-style-type: none"> ActiveX Collaboration External Remote Services Malware Remote Services Software Libraries Web Services 	<ul style="list-style-type: none"> ActiveX Collaboration External Remote Services Malware Remote Services Software Libraries Web Services 	<ul style="list-style-type: none"> ActiveX Collaboration External Remote Services Malware Remote Services Software Libraries Web Services 	<ul style="list-style-type: none"> ActiveX Collaboration External Remote Services Malware Remote Services Software Libraries Web Services

MITRE D3FEND™ Knowledge Graph

Model				Harden				Detect				Isolate		Deceive		Evict				
Asset Inventory	Network Mapping	Operational Activity Mapping	System Mapping	Application Hardening	Credential Hardening	Message Hardening	Platform Hardening	File Analysis	Identifier Analysis	Message Analysis	Network Traffic Analysis	Platform Monitoring	Process Analysis	User Behavior Analysis	Execution Isolation	Network Isolation	Decoy Environment	Decoy Object	Credential Eviction	Process Eviction
Configuration Inventory	Logical Link Mapping	Access Modeling	Data Exchange Mapping	Application Configuration Hardening	Biometric Authentication	Message Authentication	Bootloader Authentication	Dynamic Analysis	Homograph Detection	Sender MTA Reputation Analysis	Administrative Network Activity Analysis	Firmware Behavior Analysis	Database Query String Analysis	Authentication Event Thresholding	Executable Allowlisting	Broadcast Domain Isolation	Connected Honeynet	Decoy File	Account Locking	Process Termination
Data Inventory	Active Logical Link Mapping	Operational Dependency Mapping	Service Dependency Mapping	Dead Code Elimination	Certificate-based Authentication	Message Encryption	Disk Encryption	Emulated File Analysis	URL Analysis	Sender Reputation Analysis	Byte Sequence Emulation	Firmware Embedded Monitoring Code	File Access Pattern Analysis	Authorization Event Thresholding	Executable Denylisting	DNS Allowlisting	Integrated Honeynet	Decoy Network Resource	Authentication Cache Invalidation	
Software Inventory	Link Mapping	Operational Risk Assessment	System Dependency Mapping	Exception Handler Pointer Validation	Certificate Pinning	Transfer Agent Authentication	Driver Load Integrity Checking	File Content Rules	Identifier Reputation Analysis	Sender Reputation Analysis	Certificate Analysis	Firmware Verification	Indirect Branch Call Analysis	Credential Compromise Scope Analysis	Hardware-based Process Isolation	DNS Denylisting	Standalone Honeynet	Decoy Process		
Asset Vulnerability Enumeration	Passive Logical Link Mapping	Organization Mapping	System Vulnerability Assessment	Pointer Authentication	Credential Transmission Sniffing		File Encryption	File Hashing	Domain Name Reputation Analysis	Active Certificate Analysis	Peripheral Firmware Verification	Process Code Segment Verification	Domain Account Monitoring	Kernel-based Process Isolation	ICQ Post Restriction	Forward Resolution Domain Denylisting	Decoy Public Release			
Network Node Inventory	Physical Link Mapping			Process Segment Execution Prevention	Domain Trust Policy		Local File Permissions	File Hash Reputation Analysis	File Hash Reputation Analysis	Passive Certificate Analysis	System Firmware Verification	Process Self-Modification Detection	Job Function Access Pattern Analysis	Mandatory Access Control	Hierarchical Domain Denylisting	Decoy Session Token				
Hardware Component Inventory	Active Physical Link Mapping			Segment Address Offset Randomization	Multi-factor Authentication		RF Shielding	Software Update	IP Reputation Analysis	Client-server Payload Profiling	Operating System Monitoring	Process Spawn Analysis	Local Account Monitoring		Homograph Denylisting	Forward Resolution IP Denylisting	Decoy User Credential			
	Network Traffic Policy Mapping			Stack Frame Canary Validation	One-time Password		System Configuration Permissions	System Configuration Permissions	URL Reputation Analysis	Connection Attempt Analysis	Endpoint Health Beacon	Process Lineage Analysis	Resource Access Pattern Analysis		System Call Filtering	Reverse Resolution IP Denylisting				
				User Account Permissions			TPM Boot Integrity			DNS Traffic Analysis	Input Device Analysis	Script Execution Analysis	Session Duration Analysis			Encrypted Tunnels				
										File Carving	Memory Boundary Tracking	Shadow Stack Comparisons	User Data Transfer Analysis			Network Traffic Filtering				
										Inbound Session Volume Analysis	Scheduled Job Analysis	System Call Analysis	User Geolocation Logon Pattern Analysis			Network Traffic Filtering				
										IPC Traffic Analysis	System Daemon Monitoring	File Creation Analysis	Web Session Activity Analysis			Inbound Traffic Filtering				
										Network Traffic Community Deviation	System File Analysis	Service Binary Verification	System Int Config Analysis			Outbound Traffic Filtering				
										Per Host Download/Upload Ratio Analysis	Protocol Metadata Anomaly Detection	User Session Int Config Analysis								
										Remote Terminal Session Detection	RPC Traffic Analysis									

MITRE D3FEND™ Knowledge Graph

Model			Harden			
Asset Inventory		Asset Inventory	Application Hardening	Credential Hardening	Message Hardening	Platform Hardening
Configuration Inventory		Configuration Inventory	Application Configuration Hardening	Biometric Authentication	Message Authentication	Bootloader Authentication
Data Inventory		Data Inventory	Dead Code Elimination	Certificate-based Authentication	Message Encryption	Disk Encryption
Software Inventory		Software Inventory	Exception Handler Pointer Validation	Certificate Pinning	Transfer Agent Authentication	Driver Load Integrity Checking
Asset Vulnerability Enumeration		Asset Vulnerability Enumeration	Pointer Authentication	Credential Transmission Scoping		File Encryption
Network Node Inventory		Network Node Inventory	Process Segment Execution Prevention	Domain Trust Policy		Local File Permissions
Hardware Component Inventory		Hardware Component Inventory	Segment Address Offset Randomization	Multi-factor Authentication		RF Shielding
		Network Traffic Policy Mapping	Stack Frame Canary	One-time Password		Software Update
				Strong Password Policy		System Configuration Permissions
						TDM Post

Jak.

Geografická data

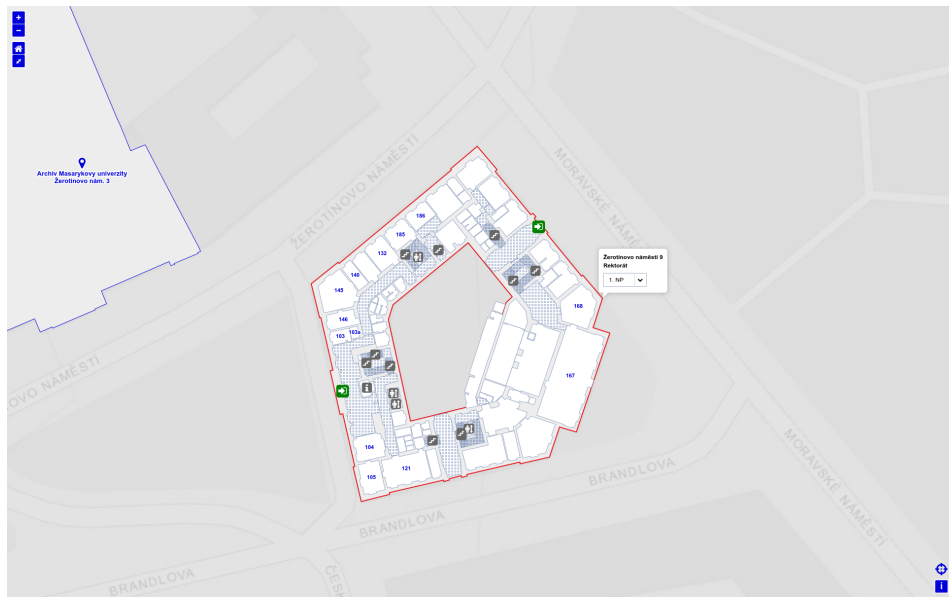
Příklady

- 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

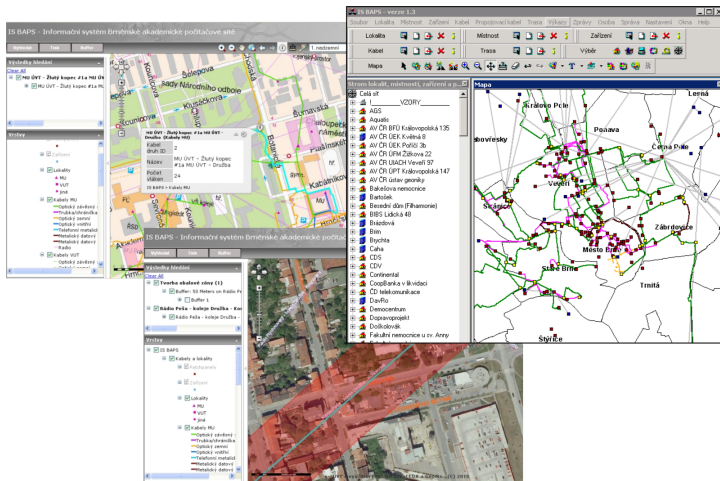
Přínosy

- 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

The screenshot displays the Globema NetStork software interface, which is used for network design and visualization. The main window is titled "NetStork - Globema NetStork" and contains several panels:

- Editor (Left):** Contains a tree view of the network structure, a list of ports (Post 1 to Post 39), and a detailed configuration panel for the selected object "ODF Stojan R1 (levý: optika a srv.)". The configuration includes fields for "Rok", "Roz", "Označení", "Typ", "Šířka [mm]", "Výška [mm]", "Výrobce", "Vzdálenost jednotky [mm]", "Vzdálenost od stěny [mm]", "Schéma", "Rozložení", "Zaměření zařízení", "Bod vstupu", "Text uvnitř", "Dokumenty", "Měřítko", "Nápisce", and "Poznámky".
- Mapa (Center):** A satellite map showing the physical location of the network components, with a red outline indicating the layout of the ODF Stojan R1.
- Kabely (Right):** A terminal view showing the connection between the ODF Stojan R1 (left) and the server rack (right). The connections are color-coded and labeled with numbers 1 through 10.

The status bar at the bottom of the window indicates "ODF Stojan R1 (levý: optika a srv.)".

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 infrastruktury
 - Kontakty různého druhu
- Zachování jisté volnosti
 - Vlastní atributy
 - Některé koncepty lze ohnout požadovaným směrem
- Infrastrukturní agent (o agentech dále)
- Globální vyhledávání
- Řízení přístupu na úrovni objektů
- Zdroj pravdy, velmi omezeně pak příjemce pravdy
- Rozšiřitelnost
 - Python + Django, Python knihovna
 - GraphQL API pro čtení, REST API (OpenAPI)

NetBox – IP prefixy

netbox

- Organization
- Devices
- Connections
- IPAM
 - IP ADDRESSES
 - IP Addresses
 - IP Ranges
 - PREFIXES
 - Prefixes
 - Prefix & VLAN Roles
 - AGGREGATES
 - Aggregates
 - RIRs
 - VRFS
 - Route Targets
 - VLANs
 - VLANs
 - VLAN Groups
 - SERVICES
 - Services
 - Virtualization
 - Circuits
 - Power
 - Other

Search All Objects

Prefixes

Records 37 Filters

Quick find

<input type="checkbox"/> Prefix	Status	Children	VRF	Utilization	Tenant	Site	VLAN	Role	Description
<input type="checkbox"/> 4.122.55.0/24	Active	0	Global	<div><div style="width: 5%;">5%</div></div>	—	—	—	—	—
<input type="checkbox"/> 10.0.0.0/16	Active	0	Global	<div><div style="width: 0%;">0%</div></div>	—	—	—	—	—
<input type="checkbox"/> 10.1.0.0/16	Active	5	Global	<div><div style="width: 0%;">0%</div></div>	Customer 1	—	—	—	—
<input type="checkbox"/> * 10.1.1.0/24	Active	0	Global	<div><div style="width: 0%;">0%</div></div>	—	—	—	—	—
<input type="checkbox"/> * 10.1.2.0/24	Active	0	Global	<div><div style="width: 2%;">2%</div></div>	—	—	—	—	—
<input type="checkbox"/> * 10.1.3.0/24	Active	0	Global	<div><div style="width: 1%;">1%</div></div>	—	—	—	—	—
<input type="checkbox"/> * 10.1.4.0/24	Active	0	Global	<div><div style="width: 3%;">3%</div></div>	—	—	—	—	—
<input type="checkbox"/> * 10.1.5.0/24	Active	0	Global	<div><div style="width: 0%;">0%</div></div>	—	—	—	—	—
<input type="checkbox"/> 10.2.0.0/16	Active	4	Global	<div><div style="width: 0%;">0%</div></div>	—	—	—	—	—
<input type="checkbox"/> * 10.2.2.0/24	Active	0	Global	<div><div style="width: 0%;">0%</div></div>	—	—	—	—	—
<input type="checkbox"/> * 10.2.3.0/24	Active	0	Global	<div><div style="width: 0%;">0%</div></div>	—	—	—	—	—
<input type="checkbox"/> * 10.2.4.0/24	Active	0	Global	<div><div style="width: 0%;">0%</div></div>	—	—	—	—	—
<input type="checkbox"/> * 10.2.5.0/24	Active	0	Global	<div><div style="width: 0%;">0%</div></div>	—	—	—	—	—
<input type="checkbox"/> 10.3.0.0/16	Active	5	Global	<div><div style="width: 0%;">0%</div></div>	—	—	—	—	—
<input type="checkbox"/> * 10.3.1.0/24	Active	0	Global	<div><div style="width: 0%;">0%</div></div>	—	—	—	—	—
<input type="checkbox"/> * 10.3.2.0/24	Active	0	Global	<div><div style="width: 0%;">0%</div></div>	—	—	—	—	—
<input type="checkbox"/> * 10.3.3.0/24	Active	0	Global	<div><div style="width: 0%;">0%</div></div>	—	—	—	—	—
<input type="checkbox"/> * 10.3.4.0/24	Active	0	Global	<div><div style="width: 0%;">0%</div></div>	—	—	—	—	—
<input type="checkbox"/> * 10.3.5.0/24	Active	0	Global	<div><div style="width: 0%;">0%</div></div>	—	—	—	—	—
<input type="checkbox"/> 10.4.0.0/16	Active	5	Global	<div><div style="width: 0%;">0%</div></div>	—	—	—	—	—
<input type="checkbox"/> * 10.4.1.0/24	Active	0	Global	<div><div style="width: 0%;">0%</div></div>	—	—	—	—	—
<input type="checkbox"/> * 10.4.2.0/24	Active	0	Global	<div><div style="width: 0%;">0%</div></div>	—	—	—	—	—
<input type="checkbox"/> * 10.4.3.0/24	Active	0	Global	<div><div style="width: 0%;">0%</div></div>	—	—	—	—	—
<input type="checkbox"/> * 10.4.4.0/24	Active	0	Global	<div><div style="width: 0%;">0%</div></div>	—	—	—	—	—

NetBox – pohled na rack

netbox

Organization

SITES
Sites
Regions
Site Groups
Locations

RACKS
Racks
Rack Roles
Reservations
Elevations

TENANCY
Tenants
Tenant Groups

Devices
Connections
IPAM
Virtualization
Circuits
Power
Other

Search

All Objects

admin

dcim_rack-1

Previous Next Clone Edit Delete

Racks > Brno CSIRT-MU

Rack ERA.42

Created 2023-02-03 · Updated 2 days, 23 hours ago

Rack Journal Change Log

Site	Brno CSIRT-MU
Location	None
Facility ID	—
Tenant	None
Status	Active
Role	None
Serial Number	—
Asset Tag	—
Devices	4
Space Utilization	16%
Power Utilization	0%

Type	None
Width	19 inches
Height	24U (ascending)
Outer Width	—
Outer Depth	—

Tags

No tags assigned

Comments

None

Images and Labels

Front

Download SVG

Rear

Download SVG

Non-Racked Devices

None

+ Add a Non-Racked Device

NetBox – detail typu zařízení

netbox

Organization

Devices

DEVICES

Device Roles

Platforms

Virtual Chassis

DEVICE TYPES

Device Types

Manufacturers

DEVICE COMPONENTS

Interfaces

Front Ports

Rear Ports

Console Ports

Console Server Ports

Power Ports

Power Outlets

Device Bays

Inventory Items

Connections

IPAM

Virtualization

Circuits

Power

Other

Search

All Objects

admin

device devicetype:9 (cisco-catalyst-2960x-48td-l)

+ Add Components Clone Edit Delete

Device Types > CISCO

CISCO Cisco Catalyst 2960X-48TD-L

Created 2023-02-03 · Updated 2 days, 23 hours ago

Device Type [Journal](#) [Change Log](#)

Chassis

Manufacturer [CISCO](#)


Model Name [Cisco Catalyst 2960X-48TD-L](#)
cisco-catalyst-2960x-48td-l


Part Number —

Height (U) 1

Full Depth

Parent/Child —

Front Image 

Rear Image 

Instances 1

Tags

No tags assigned

Comments

None

[Interfaces](#) 2 [Front Ports](#) [Rear Ports](#) [Console Ports](#) [Console Server Ports](#) [Power Ports](#) [Power Outlets](#) [Device Bays](#)


Interfaces

<input type="checkbox"/> Name	Label	Management Only	Type	Description	
<input type="checkbox"/> Port1	—	<input checked="" type="checkbox"/>	1000BASE-T (1GE)	—	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
<input type="checkbox"/> Port2	—	<input checked="" type="checkbox"/>	1000BASE-T (1GE)	—	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>

Rename Edit Delete [+ Add Interfaces](#)

2023-02-06 14:20 UTC orion-netbox-678d76b6-mk46h (v3.0.11)

Netbox – integrace s ostatními nástroji



Overview

Assets

Observables

Monitoring

IPFIX

User Accounting

Case Management

Cases

Labels

Templates

Knowledge Base

TTPs

Device Detail

Home » Assets » Devices » Device #24

Device #24 created 2 days ago updated 2 days ago [Open in Netbox](#)

SRV-DB-BT1

Overview CVEs **Cases** Tasks

Related Cases

Title	State	Priority	Due Date	Assignees	Updated
[CVE-2024-22570] - Affected Assets #3 - created 2 days ago vulnerability	RESOLVED	None	None	None	2 days ago

Organization

Devices

Connections


Wireless

IPAM

Virtualization

Circuits

Power



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

This research was supported by the Security Research Programme of the Czech Republic 2015-2022 (BV III/1 – V5) granted by the Ministry of the Interior of the Czech Republic under No. VI20202022164 – Advanced Security Orchestration and Intelligent Threat Management (ORION).

0.1.61

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



VO manager

[Select VO](#)[fedcloud.egi.eu](#)[Members](#)[Groups](#)[Resources](#)[Applications](#)[Application form](#)[Resource tags](#)[Resources state](#)[Settings](#)[Managers](#)[External sources](#)<< [hide advanced](#)

Group manager



User



CHAIN-REDS: groups x

fedcloud.egi.eu x



fedcloud.egi.eu

Short name:
fedcloud.egi.eu[Overview](#)[Members](#)[Groups](#)[Resources](#)[Applications](#)[Application form](#)[Settings](#)[Managers](#)[External sources](#)**Quick tools**

Add member

Add new member into your VO. Candidates can be searched for in VO's external sources or among user already existing in Perun.



Create service member

Create new member which represent service account (account usually used by more users with separate login and password).



Add manager

Add new manager which can manage your VO in Perun.



Create group

Create new group in your VO.



Add member to resource

Add selected member to specific resource (grant some type of access to Facility resources).

**Statistics**

Members	111
- valid	110
- invalid	0
- suspended	1
- expired	0
- disabled	0
Resources	3
Groups	2

Perun (CESNET), MUNI instance

≡ MUNI

🔔 👤 Imeno uzivatele

- 🏠 Home
- 👤 Access management
- 🏢 Facilities management
- 🔍 My profile

Home site

🏢 Manager in Organizations ⌵

Filter

Id	Name ↑
...	Testovací

Items per page: 10 1 - 1 of 1 < >

🏢 Sponsor in Organizations ⌵

Filter

Id	Name ↑
...	Testovací

Items per page: 10 1 - 1 of 1 < >

👤 Manager in Groups ⌵

Filter

Id	Organization	Name ↑	Description
...	Testovací	Testovací	Testovací

Items per page: 10 1 - 1 of 1 < >

🏢 Group creator in Organizations ⌵

Filter

Id	Name ↑
...	Testovací

Items per page: 10 1 - 1 of 1 < >

🏢 Manager in Facilities ⌵

Filter

Id	Name ↑
----	--------

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 Application 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

- Dashboard
- Node management
 - Nodes
 - Node search
 - Pending nodes
 - Groups
 - Data sources
 - Node External Reports
- Configuration policy
 - Rules
 - Directives
 - Techniques
 - Parameters
- Patch Management**
 - System updates**
 - Update campaigns
 - Security management ▾
 - Utilities ▾
 - Administration ▾
 - Plugins ▾

Rudder 7.2.3

© Normation 2022

System Updates

Filter

Showing 11 of 11 Nodes.

dev-www-01.lab.rudder.io	
prod-app-02.lab.rudder.io	
prod-infra-01.lab.rudder.io	
prod-windows-2016.demo.normation.com	
rudder.demo.normation.com	



rudder.demo.normation.com - details

Information [Package List](#)

Filter

Only available updates ▾

Package name	Type	Current version	Available version
almlinux-release		8.6-1.el8	8.6-2.el8
bash		4.4.20-3.el8	4.4.20-4.el8_6
ca-certificates		2021.2.50-80.0.el8_4	2022.2.54-80.2.el8_6
curl		7.61.1-22.el8	7.61.1-22.el8_6.4
dbus		1.1.12.8-18.el8	1.1.12.8-18.el8_6.1
dbus-common		1.1.12.8-18.el8	1.1.12.8-18.el8_6.1
dbus-daemon		1.1.12.8-18.el8	1.1.12.8-18.el8_6.1
dbus-libs		1.1.12.8-18.el8	1.1.12.8-18.el8_6.1
dbus-tools		1.1.12.8-18.el8	1.1.12.8-18.el8_6.1
device-mapper		8:1.02.181-3.el8	8:1.02.181-3.el8_6.2
device-mapper-event		8:1.02.181-3.el8	8:1.02.181-3.el8_6.2
device-mapper-event-libs		8:1.02.181-3.el8	8:1.02.181-3.el8_6.2
device-mapper-libs		8:1.02.181-3.el8	8:1.02.181-3.el8_6.2
dracut		049-201.git20220131.el8	049-202.git20220511.el8_6
dracut-config-rescue		049-201.git20220131.el8	049-202.git20220511.el8_6
dracut-network		049-201.git20220131.el8	049-202.git20220511.el8_6
dracut-squash		049-201.git20220131.el8	049-202.git20220511.el8_6
epel-release		8-15.el8	8-17.el8
expat		2.2.5-8.el8	2.2.5-8.el8_6.2
gnupp2		2.2.20-2.el8	2.2.20-3.el8_6
gnupp2-smime		2.2.20-2.el8	2.2.20-3.el8_6
htop		3.0.5-1.el8	3.2.1-1.el8
httpd		2.4.37-47.module_el8.6.0+2872+fe0ff7aa.1.alma	2.4.37-47.module_el8.6.0+2935+fb177b09.2
httpdfilesystem		2.4.37-47.module_el8.6.0+2872+fe0ff7aa.1.alma	2.4.37-47.module_el8.6.0+2935+fb177b09.2

Rudder – přehled zranitelnosti

Rudder Platform Use cases Pricing Community Company **Contact** English

Search anything Status Documentation admin

Common Vulnerabilities and Exposures

Filter

Group by: Nodes

Severity: 102 929 1196 103 0 505

Order by: Hostname Asc Desc

Show completely remediated items

Showing 6 of 8 Nodes.

prod-app-02.lab.rudder.io	11
prod-infra-01.lab.rudder.io	342
prod-www-01.lab.rudder.io	25
prod-www-02.lab.rudder.io	9
prod-zabbix-01.lab.rudder.io	1
rudder.demo.northern.com	149

rudder.demo.northern.com - details

Information **CVE List 149** **Vulnerable Packages 64** History

Show only active (non-remediated) CVE-

Filter

CVE	Severity	State	Packages
CVE-2022-34903 - details	7	Active	gnupp2, gnupp2-urmime
CVE-2020-35527 - details	9.8	Active	sqlite, sqlite-libs
CVE-2021-3773 - details	9.8	Active	kernel
CVE-2022-1292 - details	9.8	Active	openssl, openssl-libs
CVE-2022-1927 - details	9.8	Active	vim-common, vim-enhanced, vim-filesystem, vim-minimal
CVE-2022-2068 - details	9.8	Active	openssl, openssl-libs
CVE-2022-27404 - details	9.8	Active	freetype
CVE-2022-37434 - details	9.8	Active	rsync
CVE-2022-40674 - details	9.8	Active	expat
CVE-2021-46848 - details	9.1	Active	libblas1
CVE-2022-1586 - details	9.1	Active	pcrc2
CVE-2021-4093 - details	8.8	Active	kernel
CVE-2022-2801 - details	8.8	Active	grub2-common, grub2-pc, grub2-pc-modules, grub2-tools, grub2-tools-efi, grub2-tools-extra, grub2-tools-minimal
CVE-2022-1012 - details	8.2	Active	kernel, kernel-core, kernel-modules, kernel-tools, kernel-tools-libs
CVE-2022-22576 - details	8.1	Active	curl, libcurl
CVE-2021-4157 - details	8	Active	kernel
CVE-2020-13974 - details	7.8	Active	kernel
CVE-2021-29154 - details	7.8	Active	kernel
CVE-2021-3612 - details	7.8	Active	kernel
CVE-2021-4037 - details	7.8	Active	kernel
CVE-2021-41864 - details	7.8	Active	kernel
CVE-2021-4197 - details	7.8	Active	kernel
CVE-2022-1011 - details	7.8	Active	kernel

Lansweeper – diagram prvku

You are currently in a Lansweeper demo. Start your free trial to discover your data. [START MY FREE TRIAL](#)

NT-diagram_demo_Corporate [PREVIEW](#) Network topology

Our updated subscription plans will affect the availability of diagrams. If you'd like to give feedback, you can join the [diagram conversation](#).

Diagram viewer

The diagram shows a central switch (CONHQSW01) connected to several servers (CONHQWS01-04), a printer (CONHQPRN01), and a laptop (CONHQL01). The switch is also connected to a server rack (CONHQSRV01) and a server (CONHQSRV02). The switch is connected to a server (CONHQSRV03) and a server (CONHQSRV04). The switch is connected to a server (CONHQSRV05) and a server (CONHQSRV06). The switch is connected to a server (CONHQSRV07) and a server (CONHQSRV08). The switch is connected to a server (CONHQSRV09) and a server (CONHQSRV10). The switch is connected to a server (CONHQSRV11) and a server (CONHQSRV12). The switch is connected to a server (CONHQSRV13) and a server (CONHQSRV14). The switch is connected to a server (CONHQSRV15) and a server (CONHQSRV16). The switch is connected to a server (CONHQSRV17) and a server (CONHQSRV18). The switch is connected to a server (CONHQSRV19) and a server (CONHQSRV20). The switch is connected to a server (CONHQSRV21) and a server (CONHQSRV22). The switch is connected to a server (CONHQSRV23) and a server (CONHQSRV24). The switch is connected to a server (CONHQSRV25) and a server (CONHQSRV26). The switch is connected to a server (CONHQSRV27) and a server (CONHQSRV28). The switch is connected to a server (CONHQSRV29) and a server (CONHQSRV30). The switch is connected to a server (CONHQSRV31) and a server (CONHQSRV32). The switch is connected to a server (CONHQSRV33) and a server (CONHQSRV34). The switch is connected to a server (CONHQSRV35) and a server (CONHQSRV36). The switch is connected to a server (CONHQSRV37) and a server (CONHQSRV38). The switch is connected to a server (CONHQSRV39) and a server (CONHQSRV40). The switch is connected to a server (CONHQSRV41) and a server (CONHQSRV42). The switch is connected to a server (CONHQSRV43) and a server (CONHQSRV44). The switch is connected to a server (CONHQSRV45) and a server (CONHQSRV46). The switch is connected to a server (CONHQSRV47) and a server (CONHQSRV48). The switch is connected to a server (CONHQSRV49) and a server (CONHQSRV50).

CONHQSW01
10.40.0.4 - BB:D4:E7:ED:D3:30

Asset type	Switch
IP Location	Corporate
Manufacturer	Hewlett-Packard
Model	JL366A HPE 1920S 48G PPs+ (370W) Switch
State	Active
Serial Number	CN0GKPGZKX
Scan Server	labadmwin05
Installation	Demo


ATTACHMENTS COMMENTS

Lansweeper – detail prvku

You are currently in a Lansweeper demo. Start your free trial to discover your data. [START MY FREE TRIAL](#)

CONHQSW01 | 10.40.0.4 - Aruba Instant On 1930 24G Class4 PoE 45FP/SFP+ 370W Switch JL684A, InstantOn_1930_1.0.70 (141), Linux 4.4.120, U-Boot 2013.01 (V1.01.30)

Summary

MANUFACTURER Hewlett-Packard 	Model	JL386A HPE 1920S 48G PPoE+ (370W) Switch	Memory	-
	Serial Number	CN06KPG2KX	Processor	-
WARRANTY END DATE	System SKU	-	Device Version	-
	Express Code	-	Hardware Version	-
	SSH Server	-	Software Version	-
SERVER Info	HTTP Server	-	FTP Server	-
	HTTP Title	ARUBA - Login Form	SMTP	-

OID: 1.3.6.1.4.1.11.2.3.7.11.198

Scan Server	labdmzwt03	Created at	2022-09-19 14:43:07
Installation	demo	Last Successful	2025-01-01 11:00:27

Network

NAME	MAC ADDRESS	IP ADDRESS	SUBNET	MASK	GATEWAY	CONNECTION	LAST SEEN
-	BB:D4:E7:ED:D3:30	10.40.0.4	-	-	-	-	-

Lifecycle

Feature preview: Lifecycle Insights is in a preview phase with no known showstopper-class bugs. Changes could still be made to expand capabilities.

HARDWARE: HPE OfficeConnect 1920S... **Status** - General availability > ⚠️ 2020-10-31 End of sale > 2025-10-31 End of support

Financial Information

PO NUMBER	PO Date	-	Vendor Name	-
	Purchase Date	-	Invoice Number	-
	Cost Center	-	Acquisition Type	-

Custom fields | This item does not have any data

Asset location | This item does not have any data

Last synced 2 days ago

Snipe-IT – přehledová obrazovka

SNPIE-IT

Lookup by Asset Tag

Create New Admin

- Dashboard
- Assets
- Licenses
- Accessories
- Consumables
- Components
- Predefined Kits
- People
- Import
- Settings
- Reports
- Requestable

Dashboard

DDMO MODE: Some features are disabled for this installation.

1,374 assets

view all

50 licenses

view all

4 accessories

view all

4 consumables

view all

4 components

view all

60 people

view all

Recent Activity

Date	Admin	Action	Item	Target
Sun Feb 05, 2023 10:25PM	Admin User	checkout	Cardstock (White)	Jayne Batz
Sun Feb 05, 2023 10:11PM	Admin User	checkout	Acrobat	Hope Balistreri
Sun Feb 05, 2023 9:38PM	Admin User	checkout	Cardstock (White)	twm bmn
Sun Feb 05, 2023 9:37PM	Admin User	checkout	Laserjet Paper (Ream)	Admin User
Sun Feb 05, 2023 9:33PM	Admin User	requested	(963021783) - MacBook Pro 13"	Admin User
Sun Feb 05, 2023 9:33PM	Admin User	update	(963021783) - MacBook Pro 13"	Admin User
Sun Feb 05, 2023 9:02PM	Admin User	create new	(024847) - OptiFlex	
Sun Feb 05, 2023 8:14PM	Admin User	checkout	Paperclips	asas sssss

View All

Assets by Status Type

Ready to Deploy (1189) Deployed (103) Archived (00)
Pending (49) Un-deployable (3)

Asset Locations

Showing 1 to 11 of 11 rows 20 rows per page

Name	Assets	Assigned	Requestable
North Melissaart	150	17	0
East Samantabury	142	9	0
Lake Ariborough	141	9	0
Lake Allamouth	138	10	0
Marquardside	135	12	0
South Crystelhaven	134	5	0

Asset Categories

Showing 1 to 17 of 17 rows 20 rows per page

Name	Type	Assets	Assigned	Requestable	Consumables	Components	Predefined Kits
Laptops	Asset	1172	0	0	0	0	0
Desktops	Asset	91	0	0	0	0	0
Mobile Phones	Asset	67	0	0	0	0	0
Displays	Asset	21	0	0	0	0	0
Tablets	Asset	16	0	0	0	0	0
VOIP Phones	Asset	7	0	0	0	0	0

Snipe-IT – detail prvku


SNIFE-IT Lookup by Asset Tag Create New Admin

View Asset 1092756431


DDMO MODE: Some features are disabled for this installation.

Info Licenses Components Assets History Maintenances Files Additional Files Upload

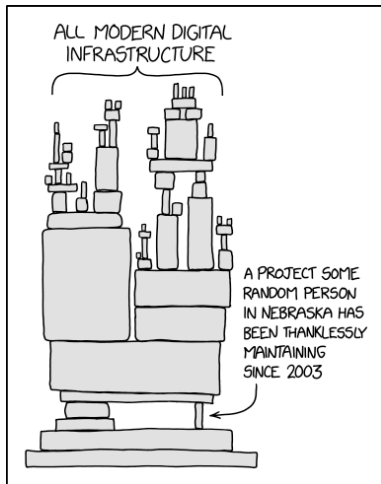
Status	● Ready to Deploy Deployed → South Hosea
Serial	cceaed1a5-6c4b-3c89-b002-d094f0147c16
Manufacturer	Dell <ul style="list-style-type: none">https://dell.comhttps://support.dell.com907-561-5974otorp@example.org
Category	Laptops
Model	XPS 13
Model No.	4716626270372
BYOD	✗ No
RAM	
CPU	
MAC Address	
Purchase Date	Thu Dec 29, 2022 - 0 years, 1 months and 7 days
Purchase Cost	OMR 2.941,51
Current Value	OMR 2.859,80
Order Number	#20103655
Supplier	Bauch Inc
Depreciation	Computer Depreciation (36 months)
Fully Depreciated	Mon Dec 29, 2025 - 2 years 10 months from now
EOL Rate	36 months
EOL Date	Mon Dec 29, 2025 - 2 years 10 months from now
Notes	Created by DB seeder
Location	South Hosea
Default Location	New Lavonside
Created At	Sun Feb 05, 2023 4:00PM
Updated at	Sun Feb 05, 2023 4:00PM



Checked Out To
South Hosea
South Hosea
410 Clair Expressway Suite 958 Suite 727
North Maximemouth, OK 97831



Software – knihovny a závislosti



■ Zdroj: <https://xkcd.com/2347/>

Software – knihovny a závislosti

Příklady

- Závislosti všeho 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