PROJECT

Multi-tenant cybersecurity operations centre designed as an open cloud service with machine learning elements

V16 Functional PoC

KPB5 – Implementation of the solution

type – documentation

month of submission – M22

Funded by the European Union
NextGenerationEU

RECOVERY AND RESILIENCE PLAN

GOVERNMENT OFFICE OF THE SLOVAK REPUBLIC

Contents

1 Introduction 3
1.1 Purpose of the document 3
1.2 Starting points and inputs to the PoC 3
1.3 Scope of the PoC 3
1.4 PoC operating environment 4
1.5 Limitations of the PoC 4
2 Components implemented in the INNOSOC PoC 5
2.1 SIEM - ELK Stack 5
2.2 Shuffle 5
2.3 Wazuh 5
2.4 Greenbone Community edition 9
2.5 OpenCTI 11
2.6 MISP 11
2.7 GLPI 12
2.8 NetBox 14
2.8.1 Role of NetBox in the PoC 14
2.8.2 Deployment and basic configuration of NetBox 15
2.8.3 Use of NetBox within the PoC 16
2.8.4 Current status and limitations of NetBox in the PoC 20
2.9 DFIR IRIS 20
2.10 Kibana (ELK) 20
2.11 Wiki.js 21
3 Deployment and basic configuration of the PoC 24
3.1 Deployment model 24
3.2 Virtual machines and services used 24
3.3 Basic integration links 24
4 Conclusion 25
4.1 XX 25

1 INTRODUCTION

1.1 Purpose of the document

The purpose of this document is to document the functional PoC within work package KPB5 – Implementation of the solution of the INNOSOC project. The document follows on from the project's previous architectural and implementation outputs and summarizes the state in which the proposed solution is implemented as a functional experimental concept.

The document captures the functional state of the implemented solution as an integrated whole, i.e. as a multi-tenant SOC-type cloud service that is deployed in experimental mode and ready for formal verification. Its main objective is to demonstrate that the proposed solution has been implemented in a functional and operational form within the scope of the PoC, and it constitutes the technical and operational documentation of the experimentally created solution..

1.2 Starting points and inputs to the PoC

The PoC builds on the results of the previous work packages and on the follow-up outputs of the project. The basic framework for implementation was created in KPB4 – Architecture of the solution, the aim of which was to create a coherent technological concept on the basis of the previous analytical and design outputs. Within KPB4, the functional and non-functional requirements, the business architecture, the technological architecture and the final DNR – Detailed design of the solution were defined, which represent a direct input to the KPB5 implementation stage.

The results of the project's previous design and analytical activities must also be regarded as substantive inputs to the implementation of the PoC, in particular the design of the virtualization solution, the design of the SOCaaS service and the design of the integration architecture of the individual components. The project plan lists among the main implementation tasks the configuration of the infrastructure, the installation of software applications, their integration and the testing of the proposed solution. The PoC is the result of building step by step on the project's previous architectural, technological and infrastructure outputs.

1.3 Scope of the PoC

The PoC described here captures the implemented parts of the proposed solution to the extent necessary to verify the basic functionality of the service. The subject of this output is mainly a description of the deployed components, their basic links and their operational arrangement in the project environment. The document focuses on what was actually deployed, configured and verified within KPB5. The PoC does not represent a final production solution or a complete commercial service. It is an experimental concept whose purpose is to demonstrate the technical feasibility of the proposed architecture and the basic operability of the solution as a whole. The scope of the PoC is therefore deliberately limited to the functions that it was possible to implement and verify under laboratory conditions.

1.4 PoC operating environment

The PoC is operated on a private OpenStack cloud environment, which forms the basic infrastructure layer of the solution. The individual components are deployed in virtual machines, with containerization by means of Docker and Docker Compose also used depending on the nature of the specific tool. This model makes it possible to separate the individual functional blocks of the solution, simplify their management and at the same time retain flexibility in experimental deployment. The PoC operating environment has the character of a test and verification environment. Its purpose is not to provide a fully fledged production service, but to create a functional platform for the integration, configuration and verification of the proposed components and their mutual cooperation. The environment is therefore designed to enable repeated deployment, configuration changes and the execution of test scenarios.

1.5 Limitations of the PoC

The PoC is provides an experimental proof of concept. Not all planned components and integration links had been brought to the final level of functionality at the time this output was prepared. In some cases, components were successfully deployed on their own, but their integration was only partially implemented. The document thus captures the actual state of implementation, not the final state of the architecture. The limitations concern mainly the degree of completion of individual integrations, the scope of verified scenarios and the overall level of operational maturity of the solution. However, the PoC provides a sufficient basis for technical verification of the concept and for the subsequent evaluation of the results achieved in a further output of the project.

.

BRAIN:IT

FRI

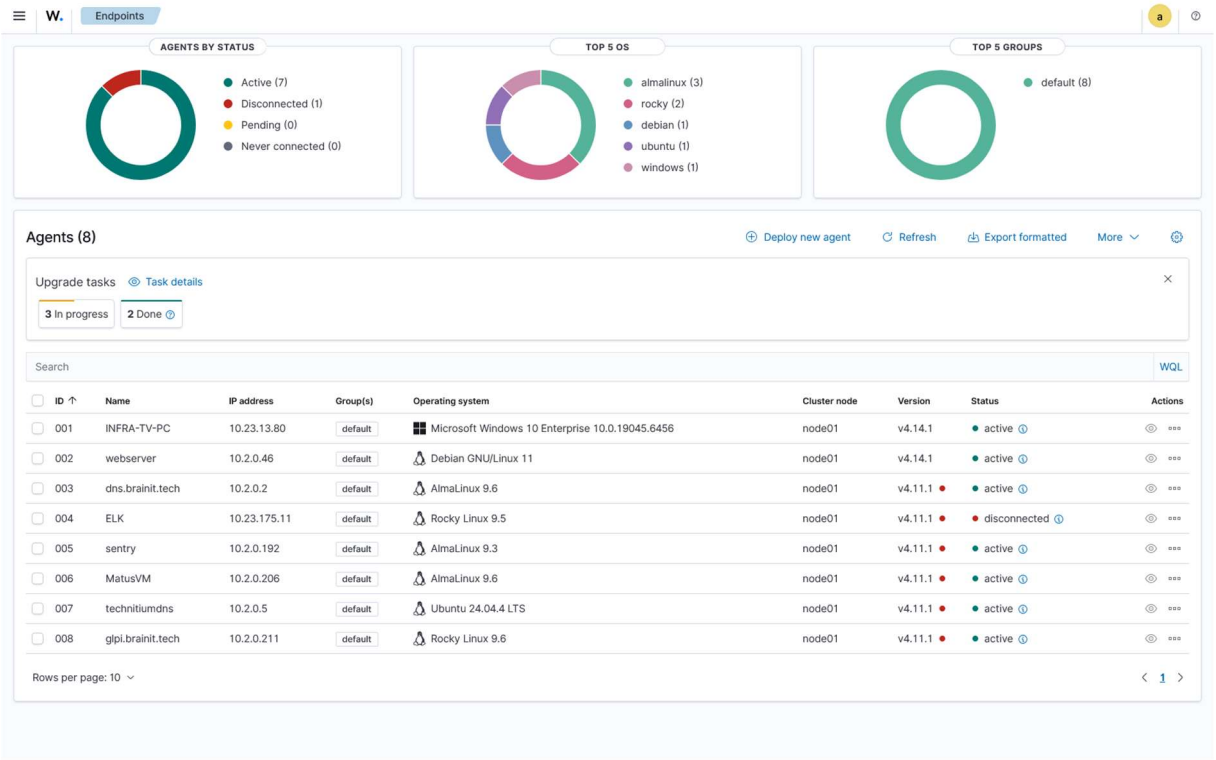
2 COMPONENTS IMPLEMENTED IN THE INNOSOC POC

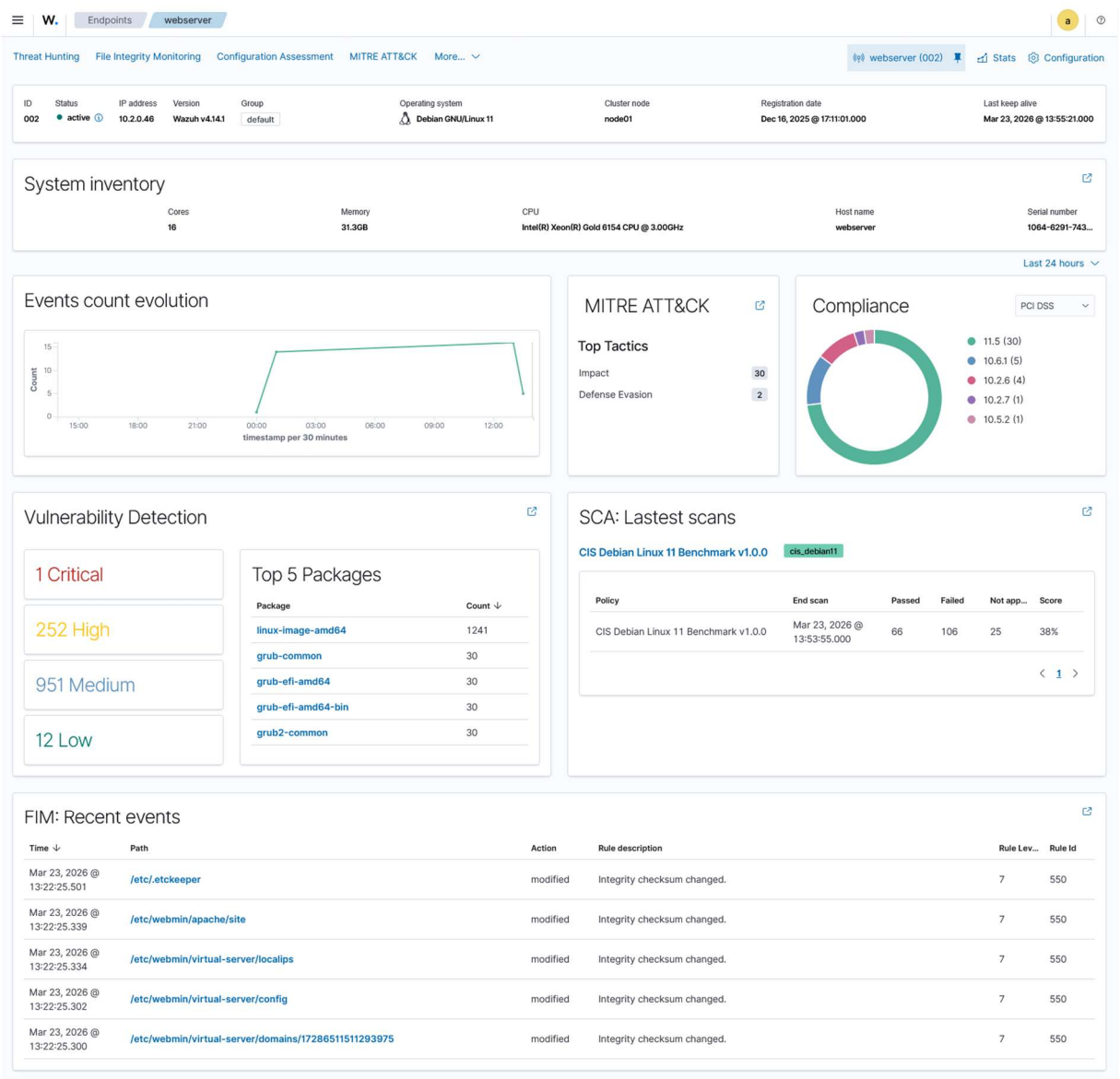
2.1 SIEM - ELK Stack

test

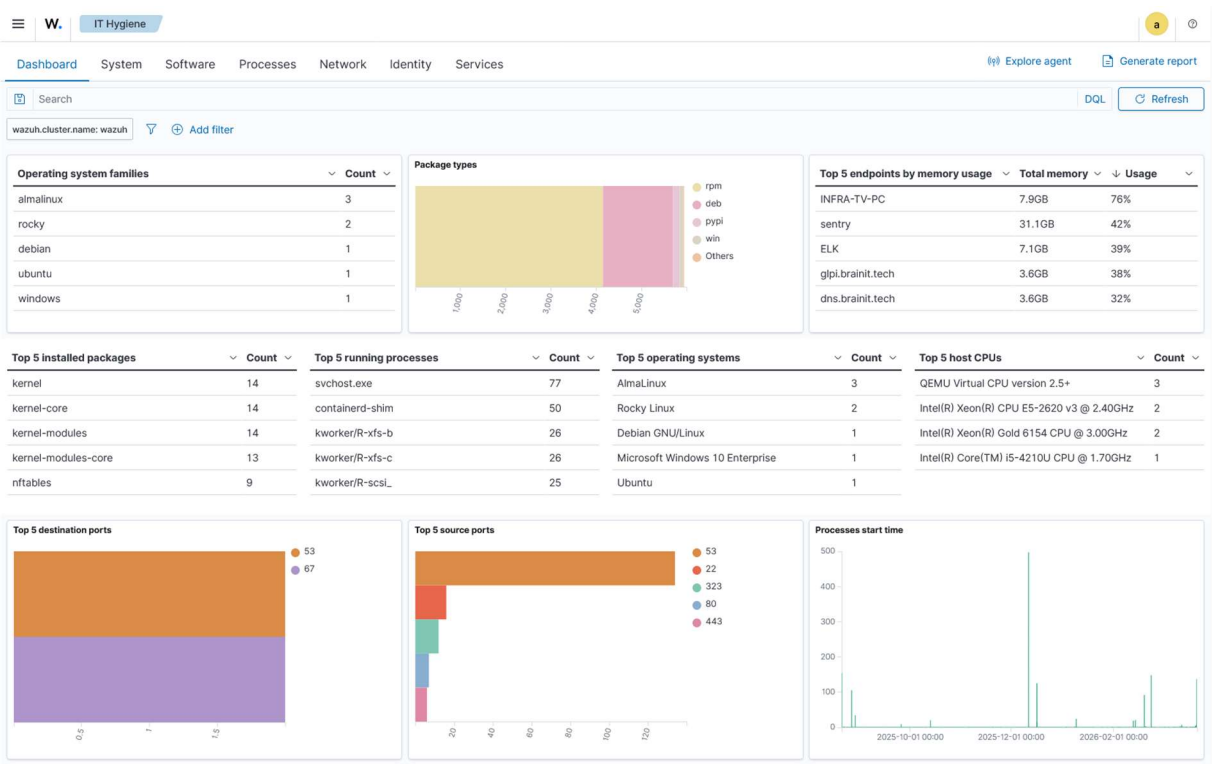
2.2 Shuffle

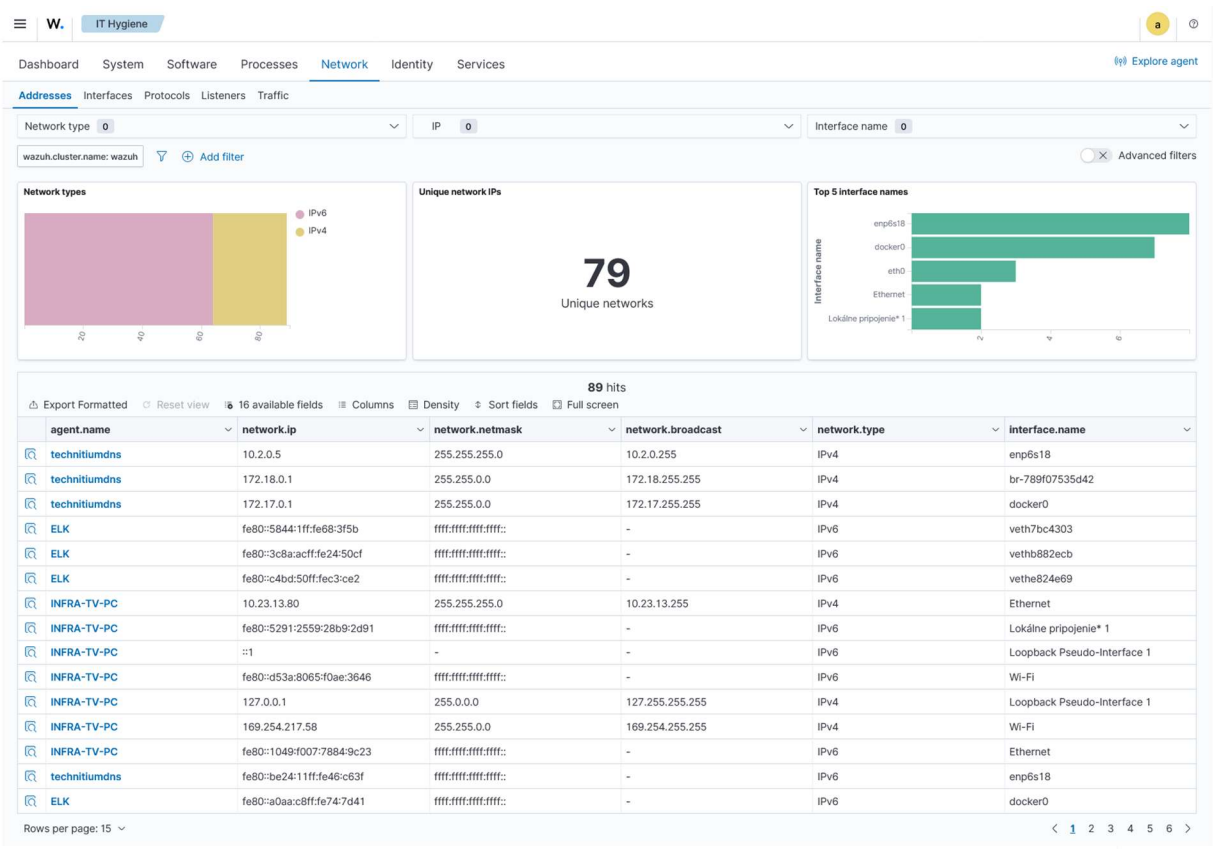
2.3 Wazuh

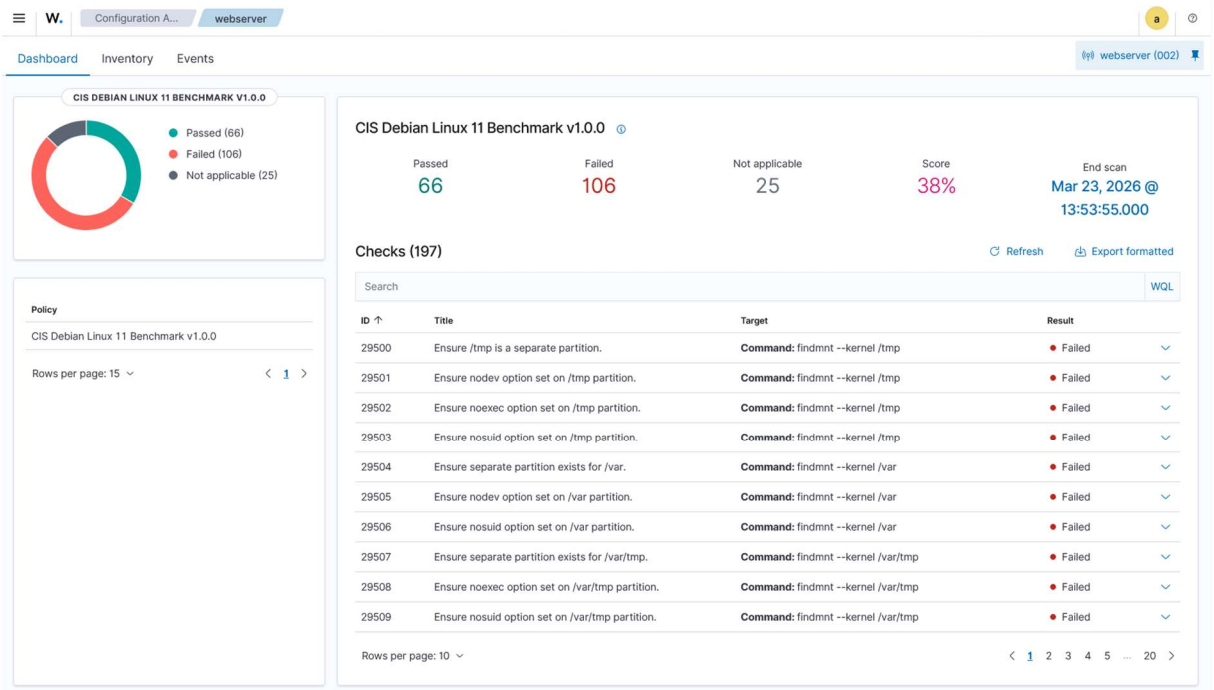




Funded by the European Union
NextGenerationEU
RECOVERY AND RESILIENCE PLAN
GOVERNMENT OFFICE OF THE SLOVAK REPUBLIC

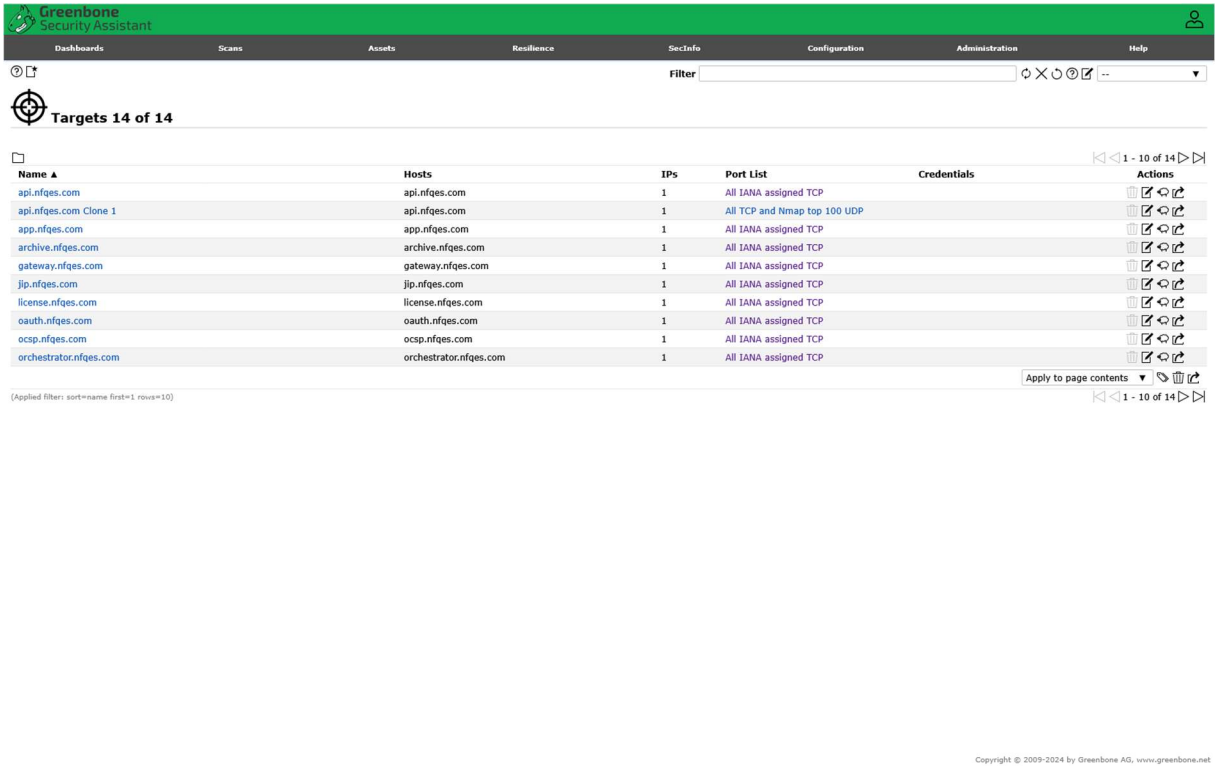

W.
IT Hygiene
a
Dashboard
System
Software
Processes
Network
Identity
Services
Explore agent
Generate report
Search
DQL
Refresh
wazuh.cluster.name: wazuh
Add filter
Operating system families
Count
almalinux 3
rocky 2
debian 1
ubuntu 1
windows 1
Package types
rpm
deb
pypi
win
Others
1,000
2,000
3,000
4,000
5,000
Top 5 endpoints by memory usage
Total memory
Usage
INFRA-TV-PC 7.9GB 76%
sentry 31.1GB 42%
ELK 7.1GB 39%
glpi.brainit.tech 3.6GB 38%
dns.brainit.tech 3.6GB 32%
Top 5 installed packages
Count
kernel 14
kernel-core 14
kernel-modules 14
kernel-modules-core 13
nftables 9
Top 5 running processes
Count
svchost.exe 77
containerd-shim 50
kworker/R-xfs-b 26
kworker/R-xfs-c 26
kworker/R-scsi_ 25
Top 5 operating systems
Count
AlmaLinux 3
Rocky Linux 2
Debian GNU/Linux 1
Microsoft Windows 10 Enterprise 1
Ubuntu 1
Top 5 host CPUs
Count
QEMU Virtual CPU version 2.5+ 3
Intel(R) Xeon(R) CPU E5-2620 v3 @ 2.40GHz 2
Intel(R) Xeon(R) Gold 6154 CPU @ 3.00GHz 2
Intel(R) Core(TM) i5-4210U CPU @ 1.70GHz 1
Top 5 destination ports
53
67
0.5
1
1.5
Top 5 source ports
53
22
323
80
443
20
40
60
80
100
120
Processes start time
500
400
300
200
100
0
2025-10-01 00:00
2025-12-01 00:00
2026-02-01 00:00

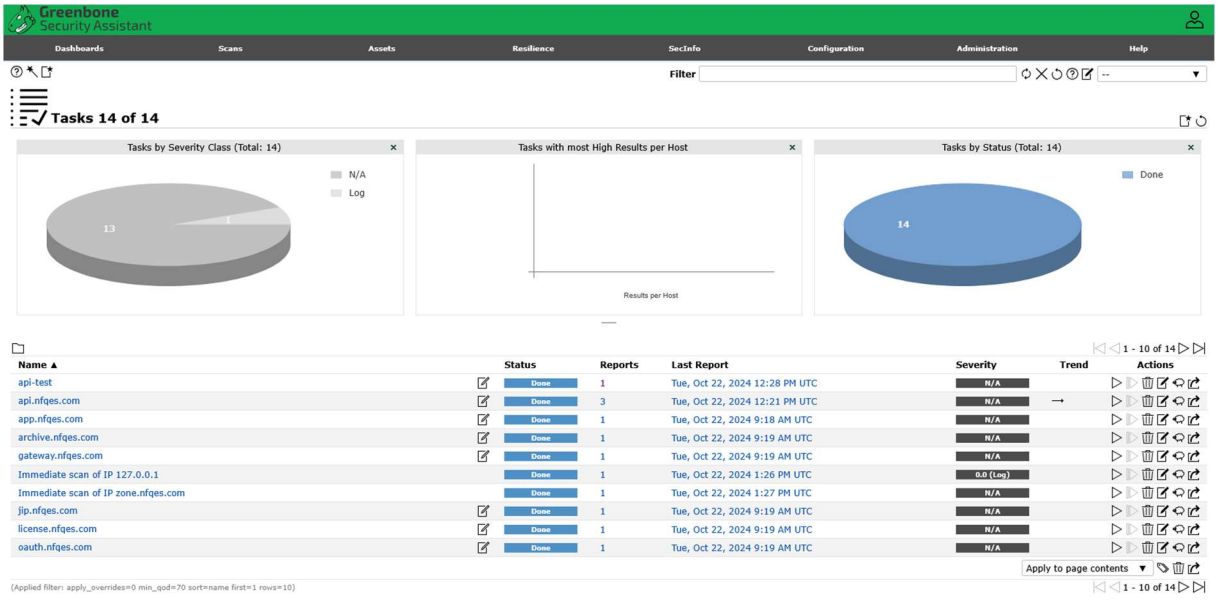




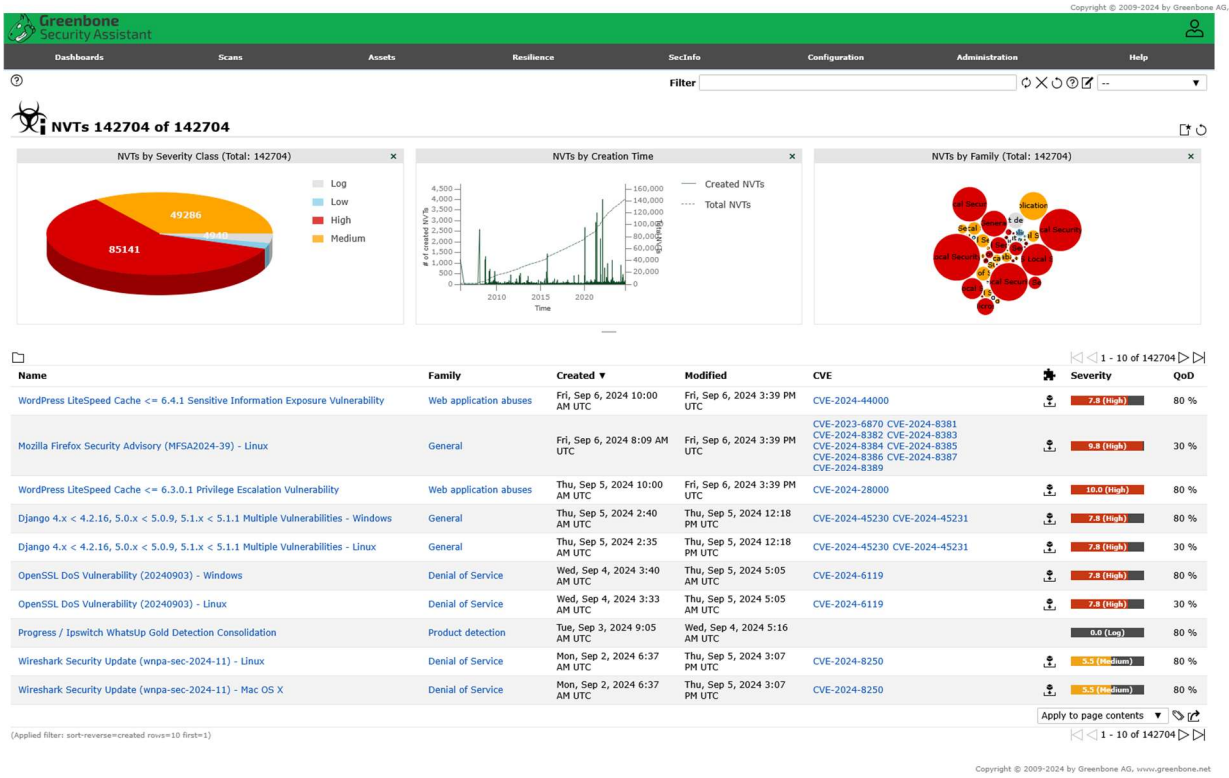
Funded by the European Union
NextGenerationEU
RECOVERY AND RESILIENCE PLAN
GOVERNMENT OFFICE OF THE SLOVAK REPUBLIC

2.4 Greenbone Community edition

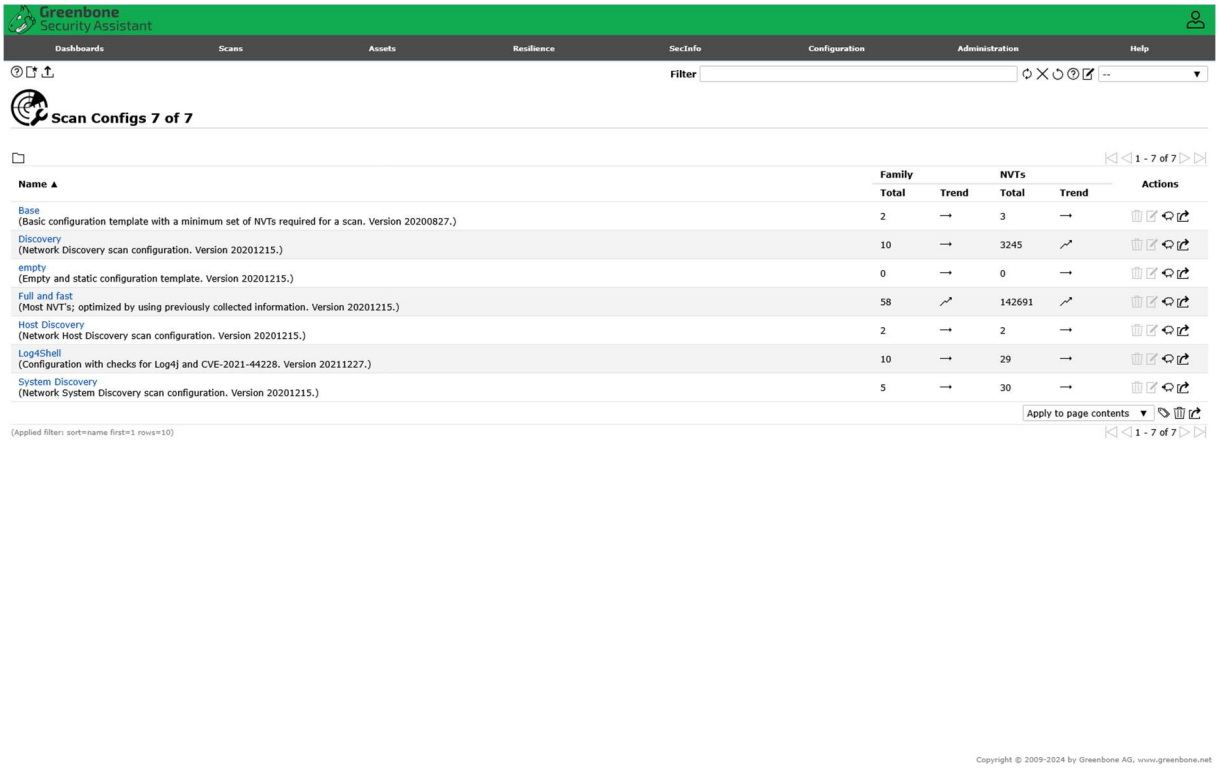




Copyright © 2009-2024 by Greenbone AG, www.greenbone.net



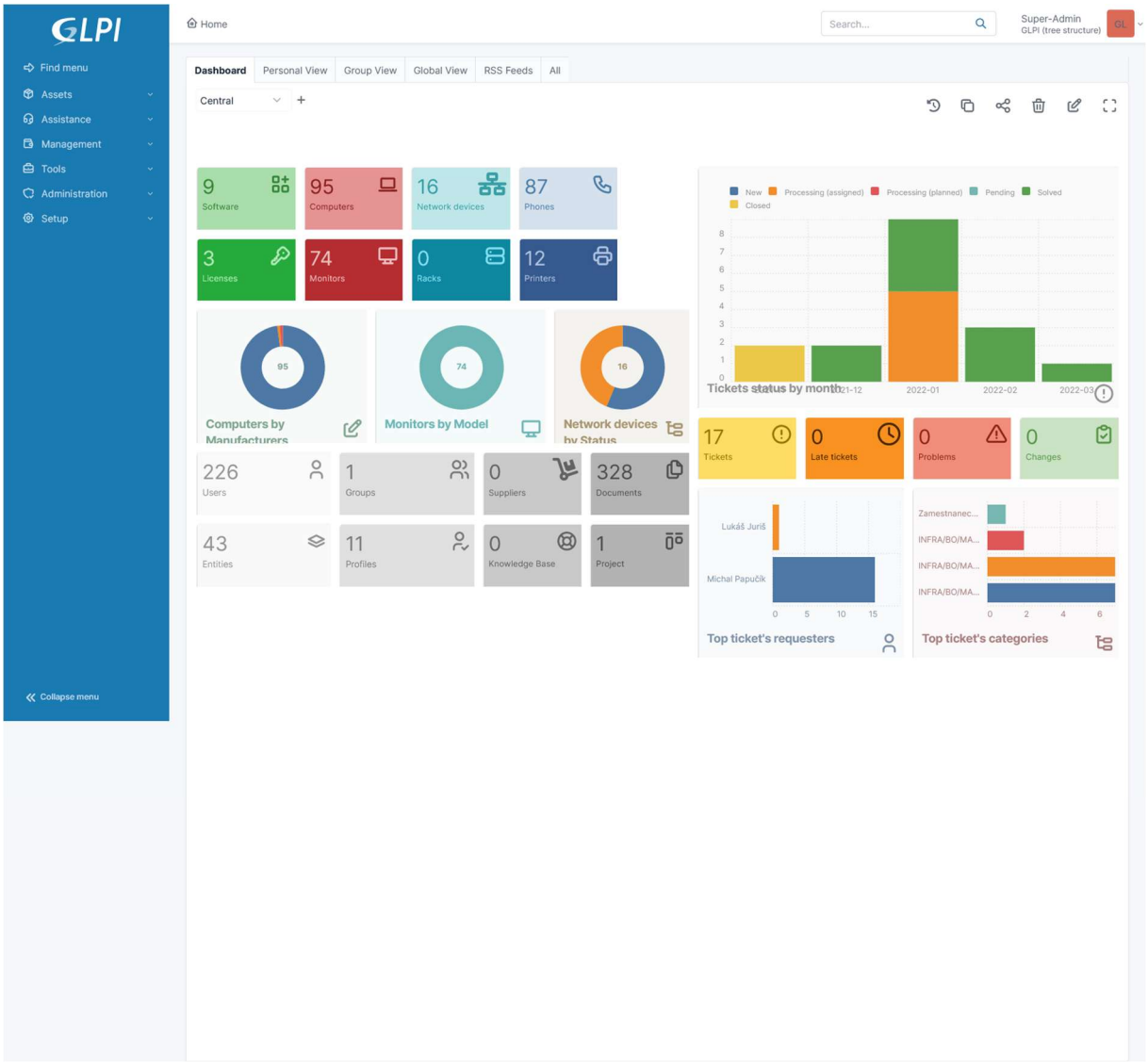
Copyright © 2009-2024 by Greenbone AG, www.greenbone.net

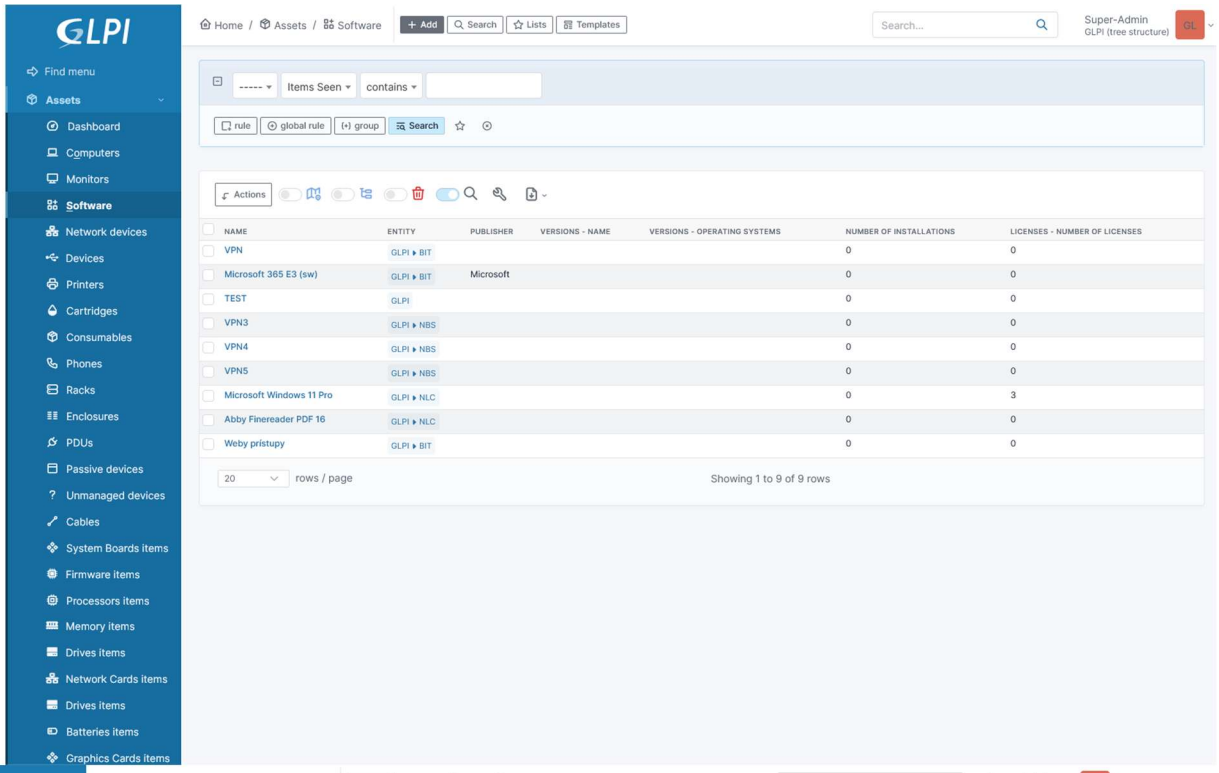


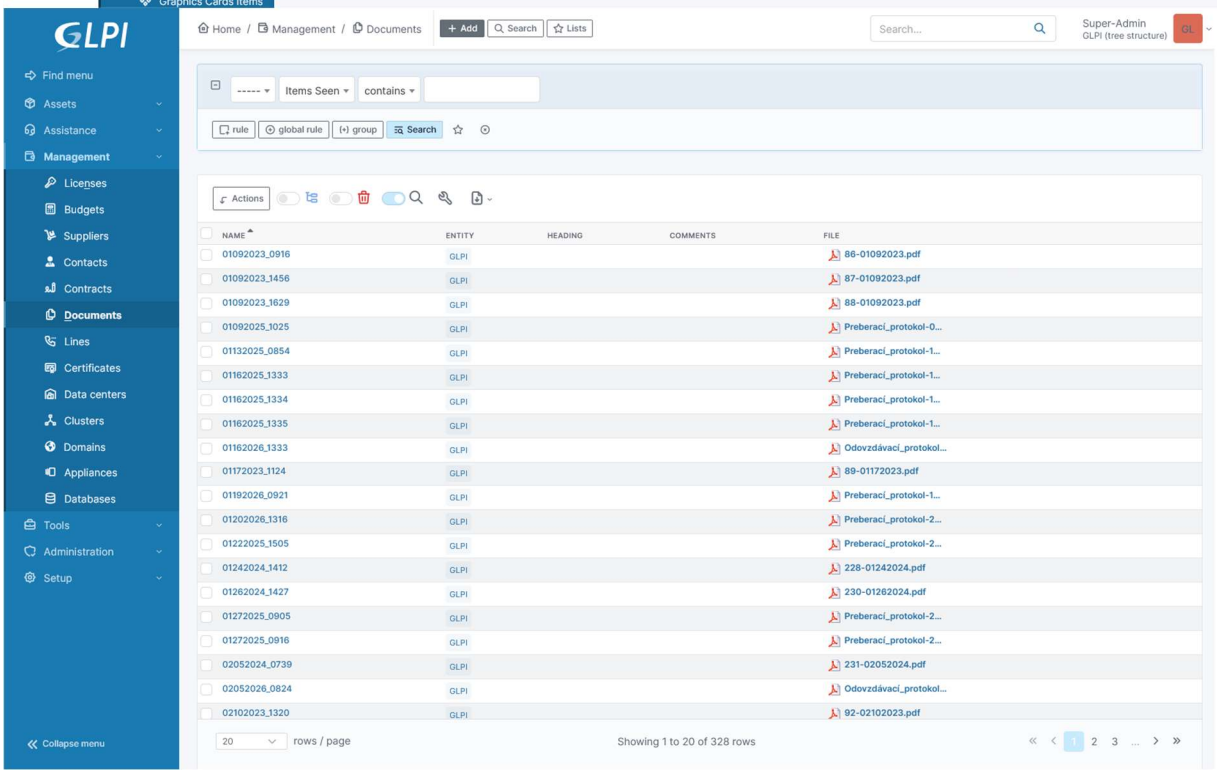
2.5 OpenCTI

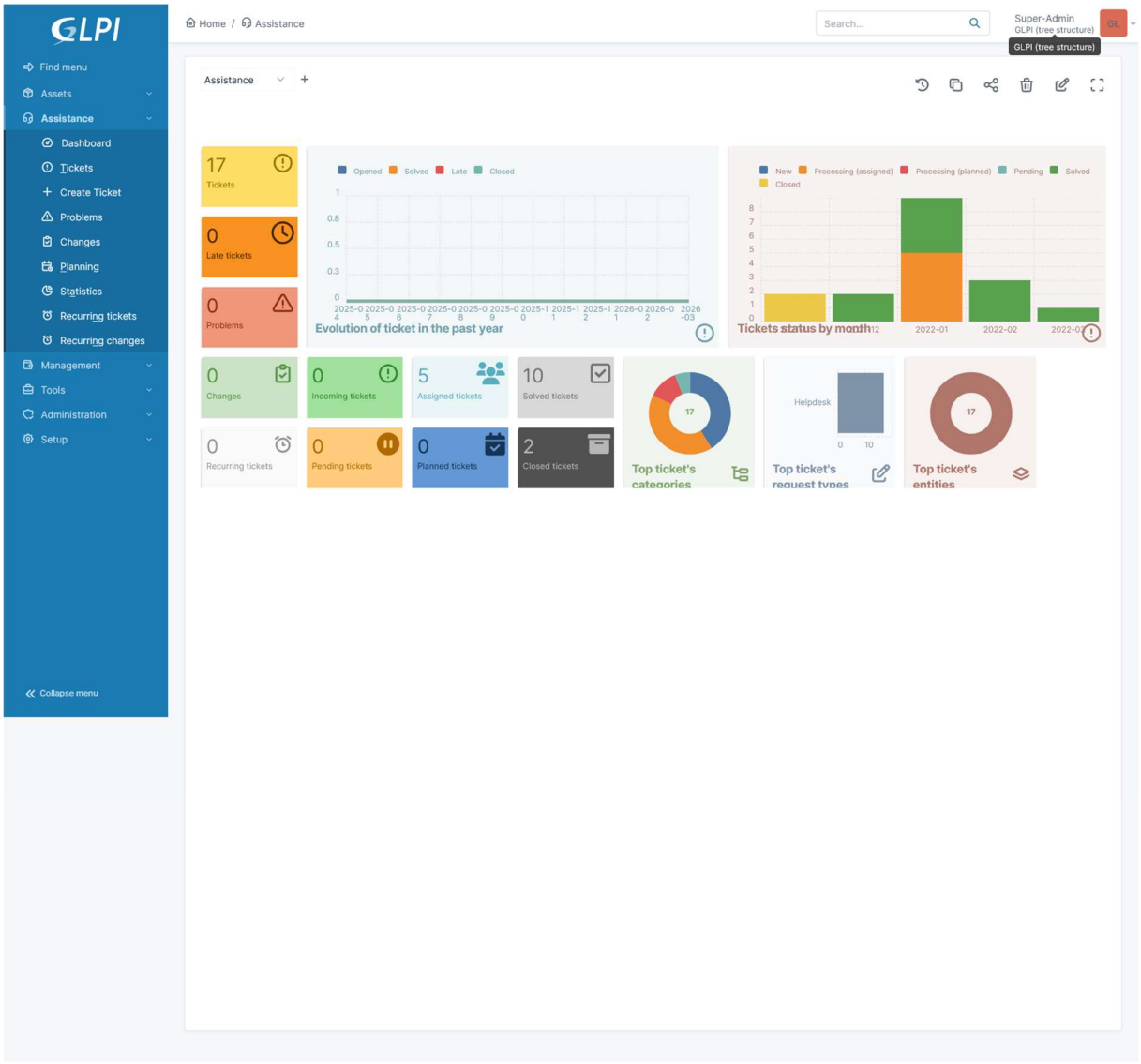
2.6 MISP

2.7 GLPI


GLPI
Home
Search...
Super-Admin
GLPI (tree structure)
Find menu
Assets
Assistance
Management
Tools
Administration
Setup
Collapse menu
Dashboard
Personal View
Group View
Global View
RSS Feeds
All
Central
9 Software
95 Computers
16 Network devices
87 Phones
3 Licenses
74 Monitors
0 Racks
12 Printers
Computers by Manufacturers
Monitors by Model
Network devices by Status
New
Processing (assigned)
Processing (planned)
Pending
Solved
Closed
Tickets status by month
2022-01
2022-02
2022-03
17 Tickets
0 Late tickets
0 Problems
0 Changes
226 Users
1 Groups
0 Suppliers
328 Documents
43 Entities
11 Profiles
0 Knowledge Base
1 Project
Lukáš Juriš
Michal Papučík
Top ticket's requesters
Zamestnanec...
INFRA/BO/MA...
Top ticket's categories


GLPI
Home / Assets / Software
+ Add
Search
Lists
Templates
Search...
Super-Admin
GLPI (tree structure)
Find menu
Assets
Dashboard
Computers
Monitors
Software
Network devices
Devices
Printers
Cartridges
Consumables
Phones
Racks
Enclosures
PDUs
Passive devices
Unmanaged devices
Cables
System Boards items
Firmware items
Processors items
Memory items
Drives items
Network Cards items
Drives items
Batteries items
Graphics Cards items
Items Seen
contains
rule
global rule
group
Search
Actions
NAME
ENTITY
PUBLISHER
VERSIONS - NAME
VERSIONS - OPERATING SYSTEMS
NUMBER OF INSTALLATIONS
LICENSES - NUMBER OF LICENSES
VPN
GLPI ▸ BIT
Microsoft 365 E3 (sw)
GLPI ▸ BIT
Microsoft
TEST
GLPI
VPN3
GLPI ▸ NBS
VPN4
GLPI ▸ NBS
VPN5
GLPI ▸ NBS
Microsoft Windows 11 Pro
GLPI ▸ NLC
Abby Finereader PDF 16
GLPI ▸ NLC
Weby prístupy
GLPI ▸ BIT
20
rows / page
Showing 1 to 9 of 9 rows


GLPI
Home / Management / Documents
+ Add
Search
Lists
Search...
Super-Admin
GLPI (tree structure)
Find menu
Assets
Assistance
Management
Licenses
Budgets
Suppliers
Contacts
Contracts
Documents
Lines
Certificates
Data centers
Clusters
Domains
Appliances
Databases
Tools
Administration
Setup
Collapse menu
Items Seen
contains
rule
global rule
group
Search
Actions
NAME
ENTITY
HEADING
COMMENTS
FILE
01092023_0916
GLPI
86-01092023.pdf
01092023_1456
GLPI
87-01092023.pdf
01092023_1629
GLPI
88-01092023.pdf
01092025_1025
GLPI
Preberací_protokol-0...
01132025_0854
GLPI
Preberací_protokol-1...
01162025_1333
GLPI
Preberací_protokol-1...
01162025_1334
GLPI
Preberací_protokol-1...
01162025_1335
GLPI
Preberací_protokol-1...
01162026_1333
GLPI
Odovzdávací_protokol...
01172023_1124
GLPI
89-01172023.pdf
01192026_0921
GLPI
Preberací_protokol-1...
01202026_1316
GLPI
Preberací_protokol-2...
01222025_1505
GLPI
Preberací_protokol-2...
01242024_1412
GLPI
228-01242024.pdf
01262024_1427
GLPI
230-01262024.pdf
01272025_0905
GLPI
Preberací_protokol-2...
01272025_0916
GLPI
Preberací_protokol-2...
02052024_0739
GLPI
231-02052024.pdf
02052026_0824
GLPI
Odovzdávací_protokol...
02102023_1320
GLPI
92-02102023.pdf
20
rows / page
Showing 1 to 20 of 328 rows
1
2
3



2.8 NetBox

2.8.1 Role of NetBox in the PoC

NetBox is used within the INNOSOC PoC solution as a supporting tool for recording and managing infrastructure context. In the proposed SOC solution, it does not act as a detection or response component, but serves as a source of information on assets, addressing, network segments and selected relationships between infrastructure elements. Its importance lies mainly in the fact that it makes it easier to understand which device, system or part of the network a particular event relates to. Within the PoC, NetBox is understood as a context layer that complements the technical data obtained from the other components of the solution. When analysing security events, it can thus be used to look up basic information about devices, IP ranges, sites or the logical placement of infrastructure elements. Such an approach increases the clarity of the solution and creates the prerequisite for a more accurate assessment of security situations.

NetBox in the SOC offers the context of the environment in which security logs and alerts originate. In this sense, it represents a ***complementary*** but important component of the solution, which supports orientation within the infrastructure and lays the groundwork for further integration use in extended scenarios.

2.8.2 Deployment and basic configuration of NetBox

Within the PoC, NetBox was deployed in the OpenStack environment as a standalone service intended for recording and managing infrastructure data. From an implementation perspective, it was containerized, using the application and supporting components required for it to run, in particular the database layer and cache/queue services. This deployment approach corresponds to the nature of an experimental deployment and at the same time allows easier administration, updating and repeatable deployment.

In the PoC, the basic configuration of NetBox focused on making the web interface accessible and on preparing the data model for recording selected infrastructure objects. In terms of configuration, the system was prepared to work with a PostgreSQL database and with a separate Redis layer for tasks and cache. Within the PoC, basic objects were entered into the system, in particular sites, devices, address spaces and the related infrastructure context.

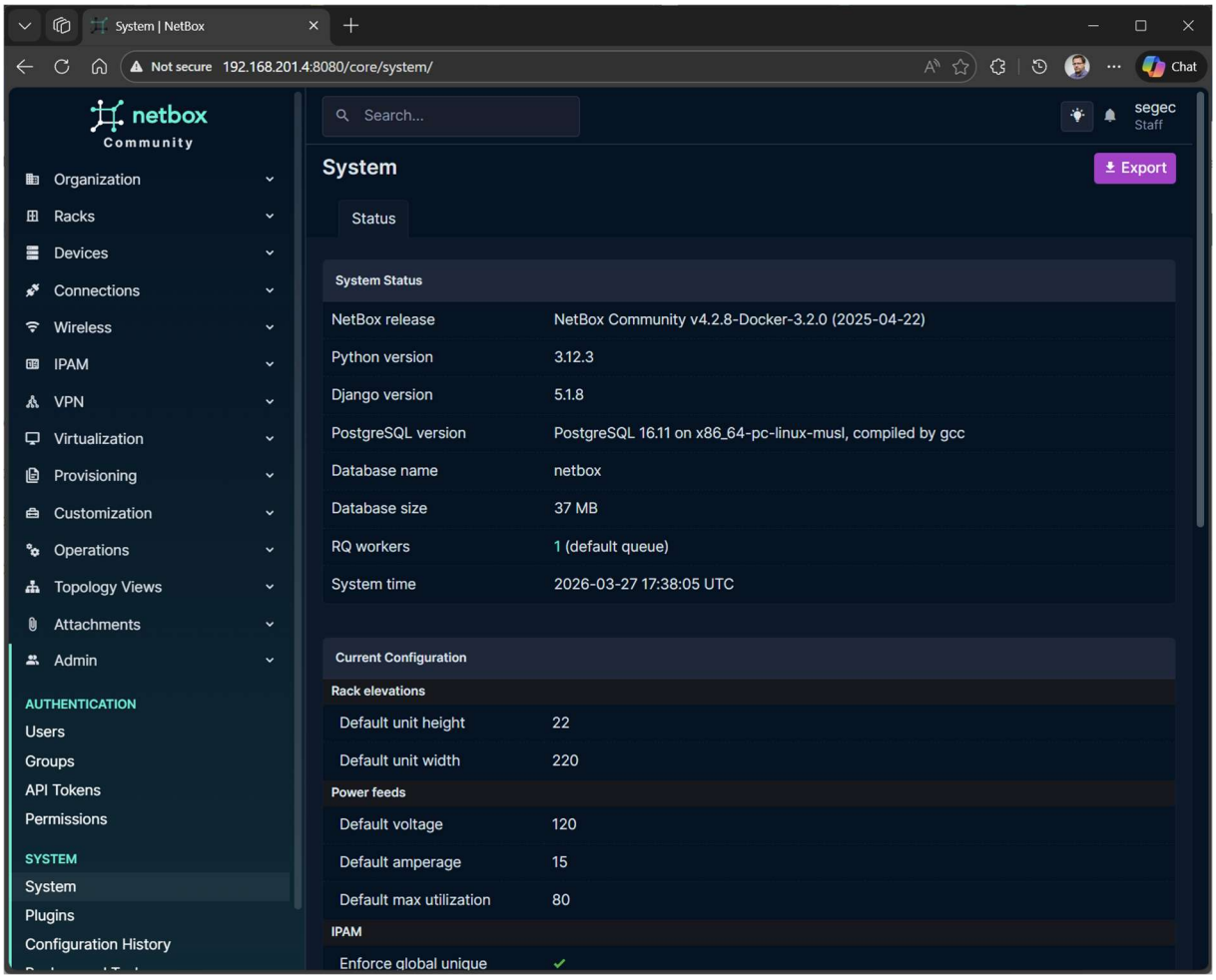


Figure 1 System information

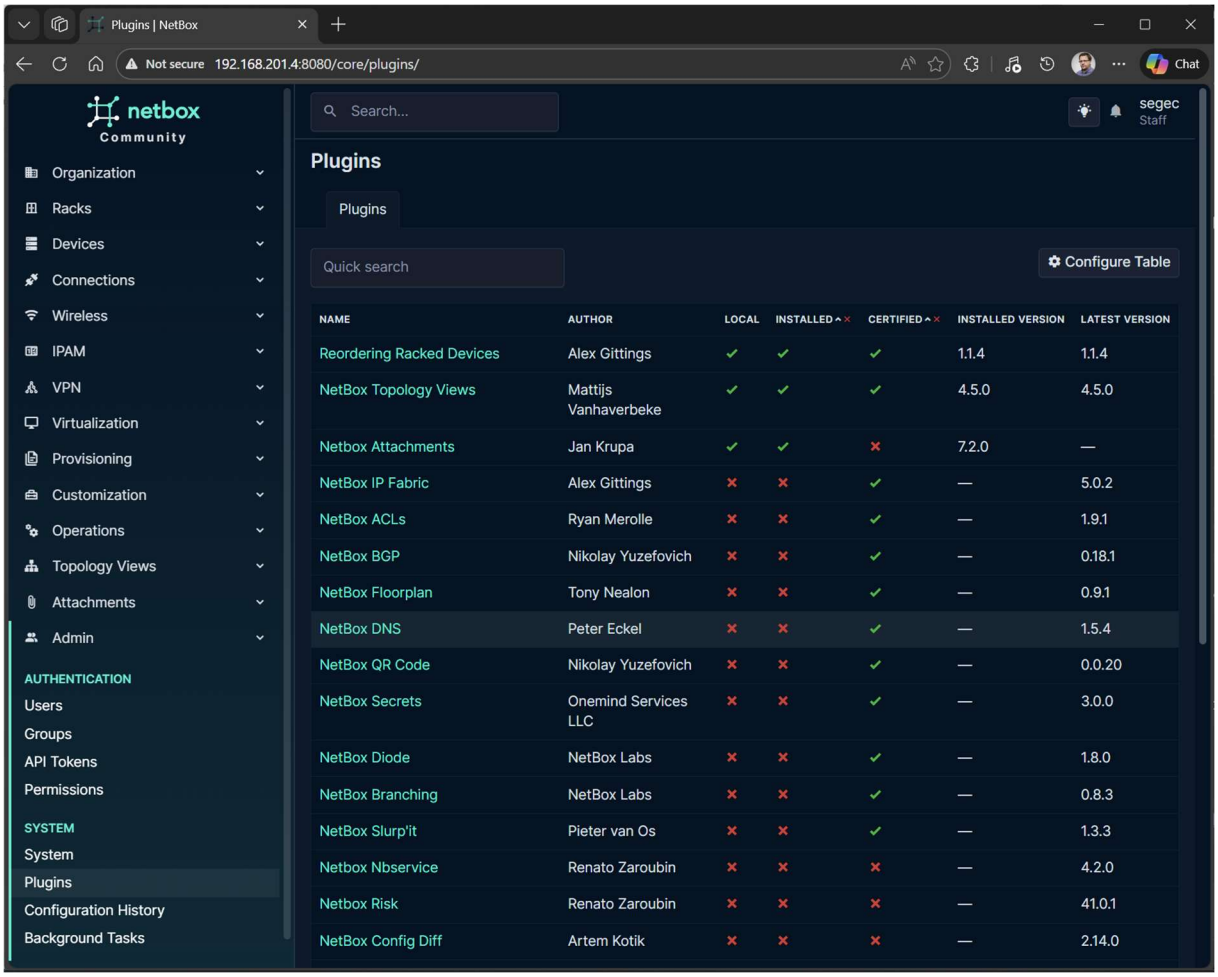


Figure 2 Plugins

The aim was not to create a complete production CMDB or a detailed model of the entire network, but to prepare a representative data set on which the use of NetBox in the proposed solution can be demonstrated.

2.8.3 Use of NetBox within the PoC

Within the PoC, NetBox was used as a supporting source of infrastructure context for the other parts of the solution. Its main contribution lay in the fact that it made it possible to look up basic information about devices, IP addressing, sites and network segments to which events or findings from other tools could be assigned.

Practical use of NetBox at this stage was oriented mainly towards record-keeping and manual or partially assisted context lookup. NetBox thus did not act as a detection or response tool, but complemented the solution with the data needed for a better understanding of the technical environment. To this extent, its deployment confirmed that it is a suitable complement to the PoC solution and a usable basis for further extension of integration scenarios.

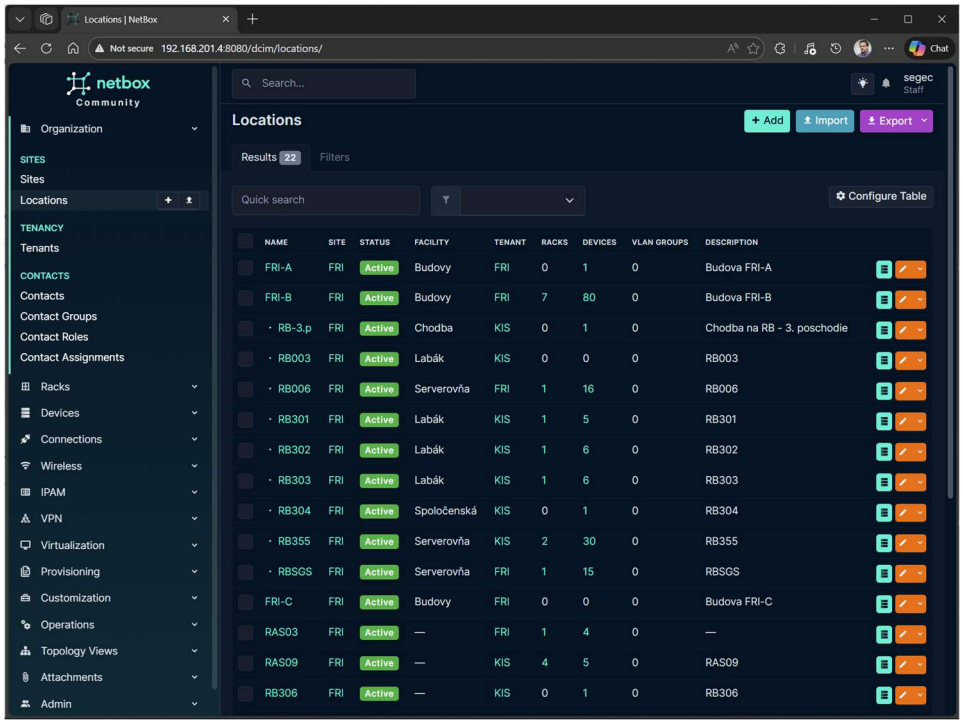


Figure 3 Modelling the organization

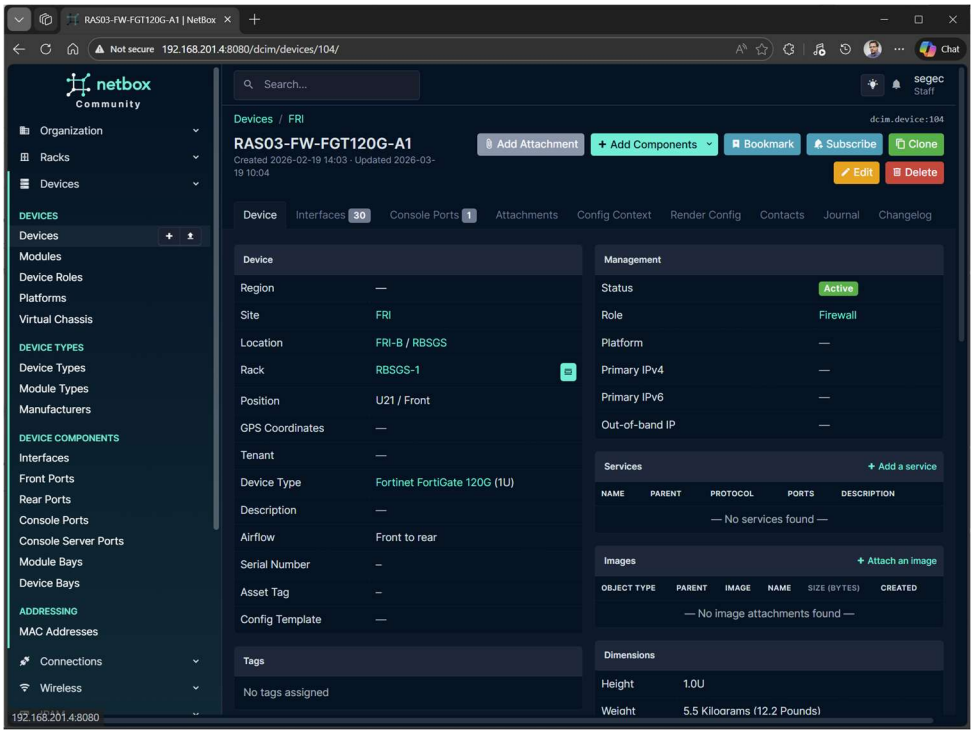


Figure 4 Modelling a device – Firewall

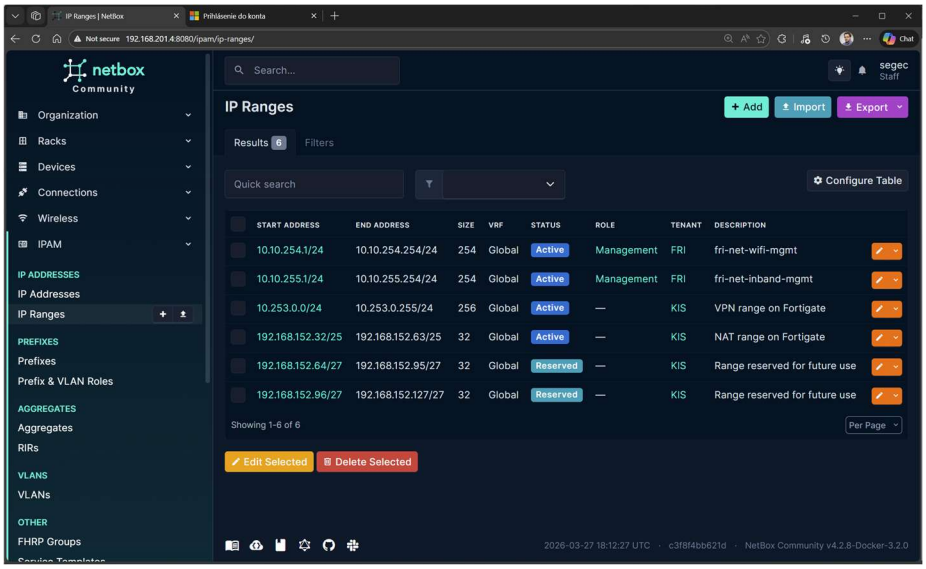
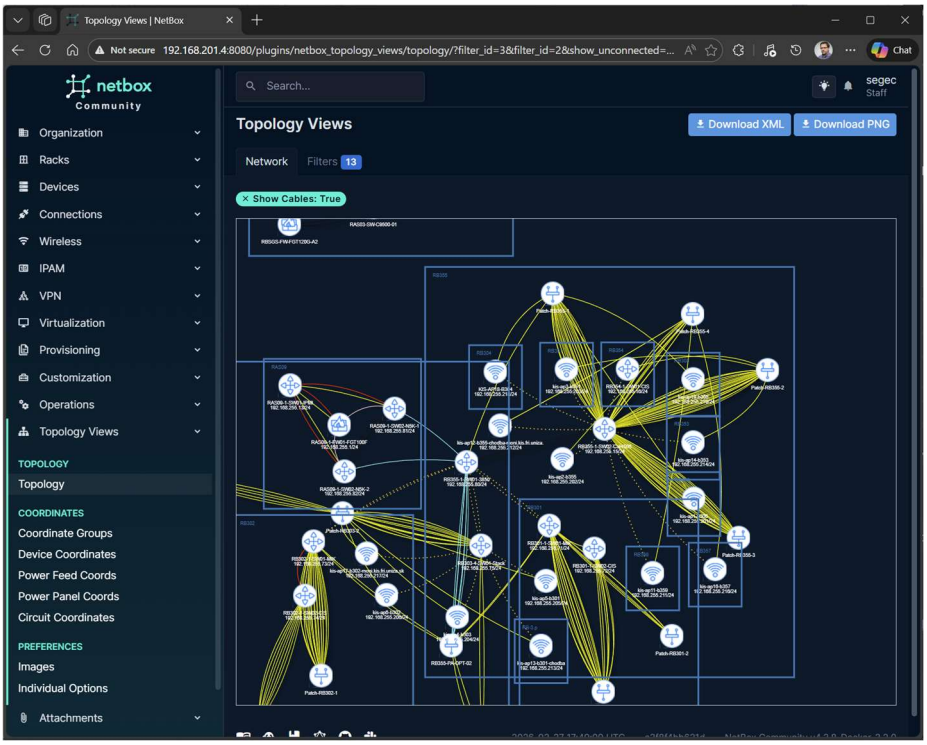


Figure 5 Address management



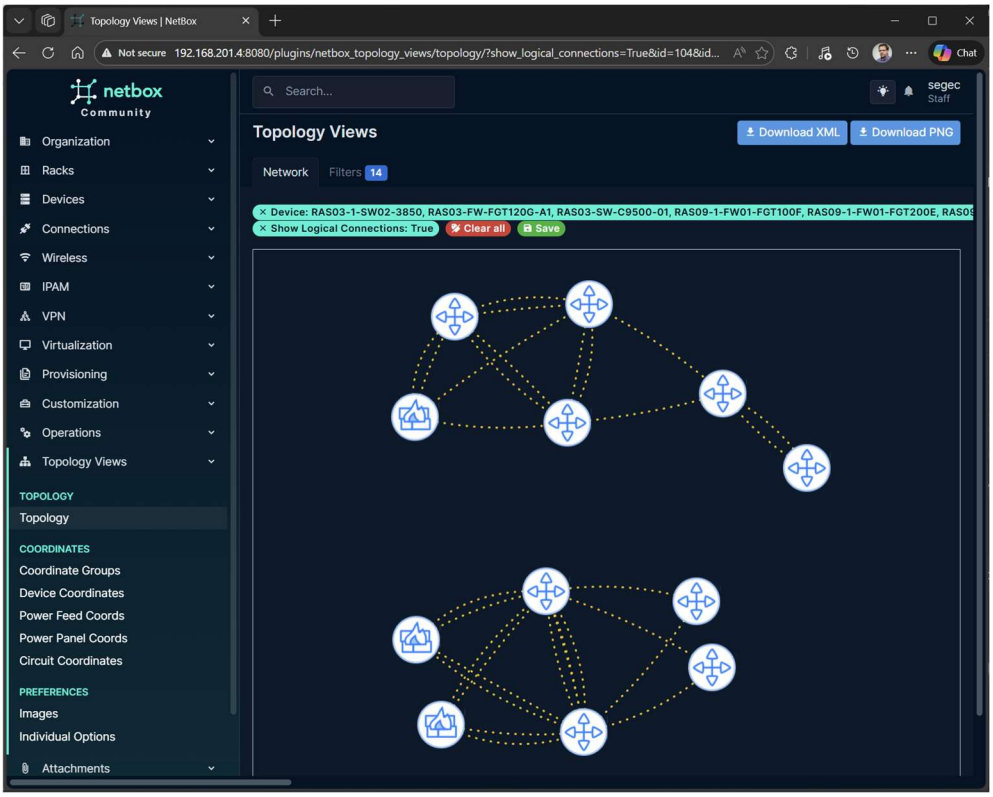


Figure 6 Topology generation

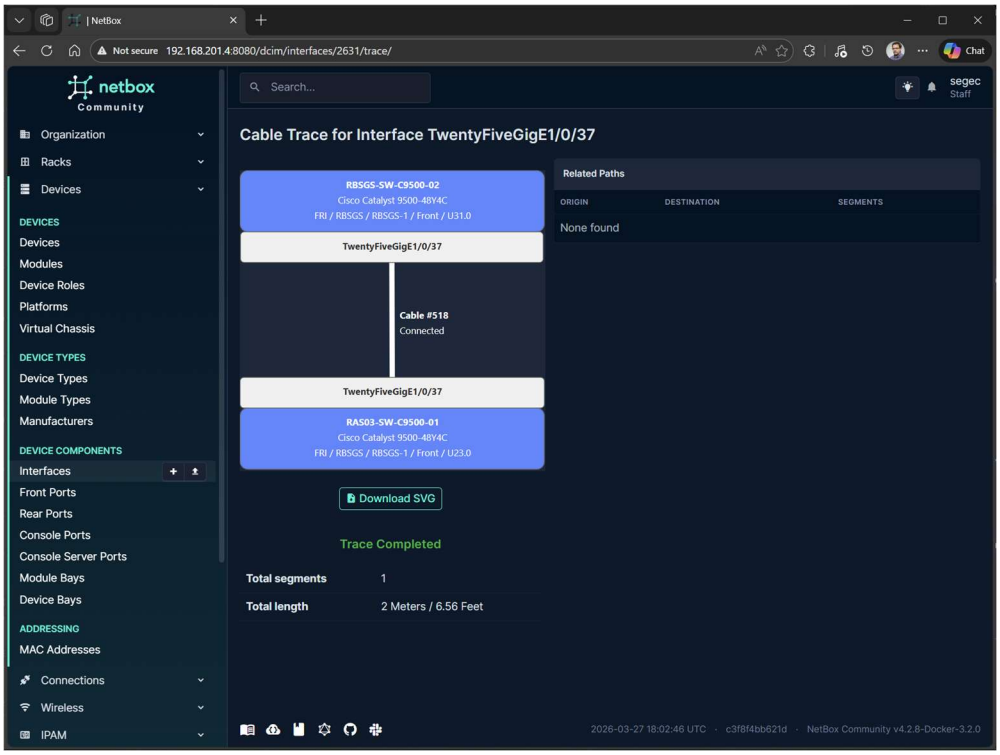


Figure 7 Cable tracing

2.8.4 Current status and limitations of NetBox in the PoC

Within the PoC, NetBox was successfully deployed and given a basic configuration as a functional tool for recording infrastructure data. In this state, it provides a usable basis for managing selected objects and for orientation within the environment of the proposed solution. From the PoC perspective, it was confirmed that NetBox is suitable for complementing the SOC solution with infrastructure context and for supporting work with assets and addressing.

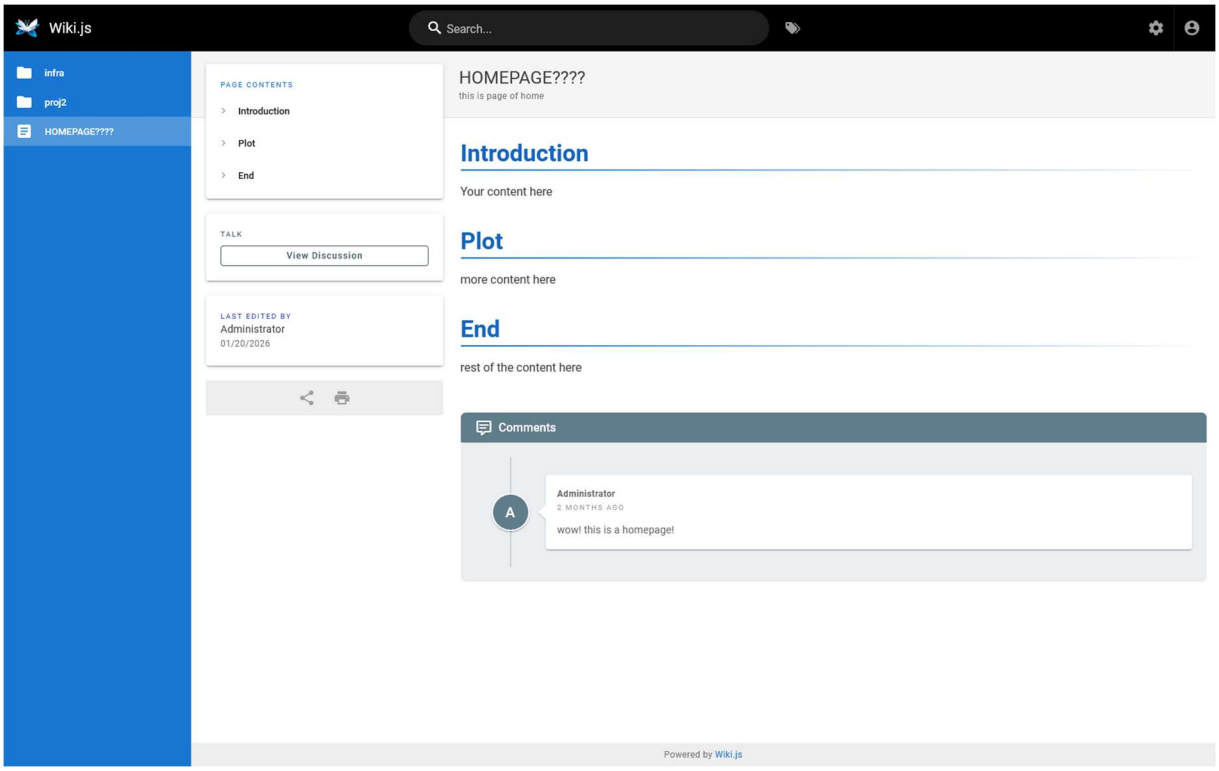
On the other hand, it should be noted that its use in the PoC remained at the level of basic record-keeping and partial context enrichment. Not all of the planned integration links to the other components of the solution were completed, and so at this stage NetBox does not function as a fully automated source of enrichment data. For the time being, its role is rather a supporting one, laying the groundwork for further extension in future stages of the project.

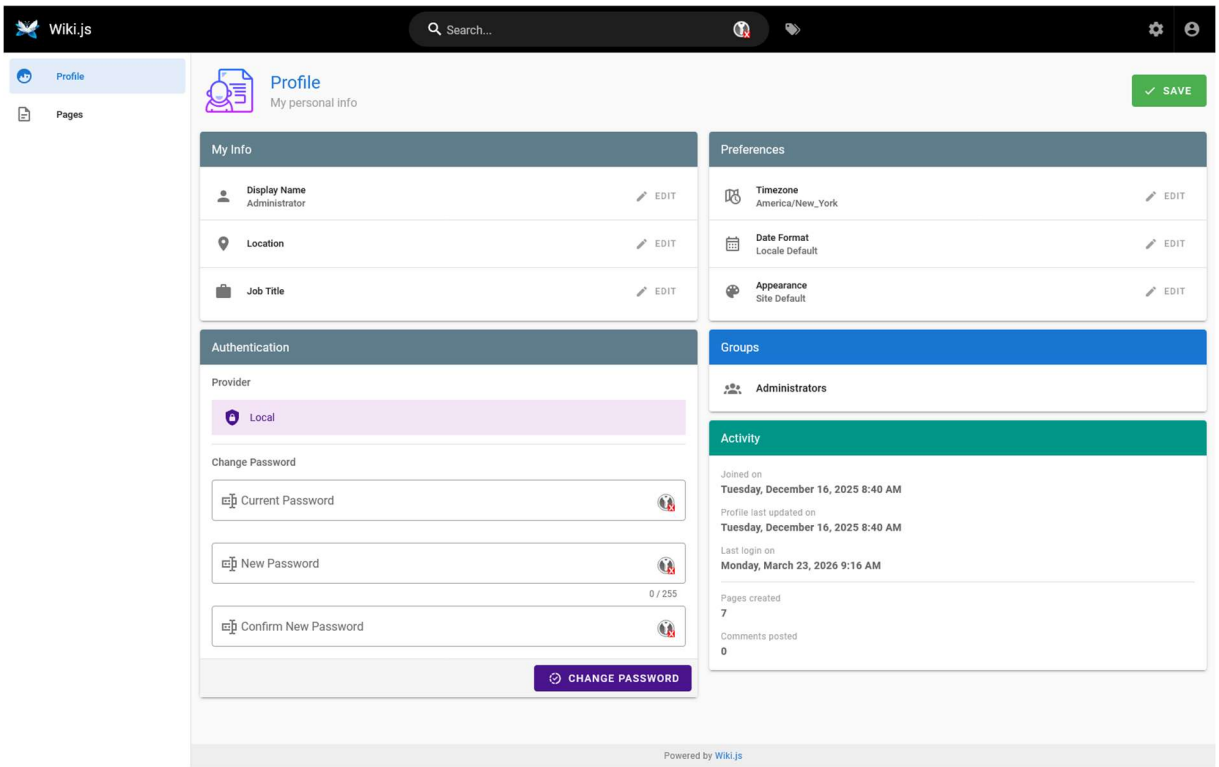
For this reason, NetBox in the PoC should be understood as a functional, but not yet fully developed, component. Nevertheless, its deployment demonstrated its practical usability in the proposed solution and confirmed the suitability of including it in the wider architecture of the SOC service.

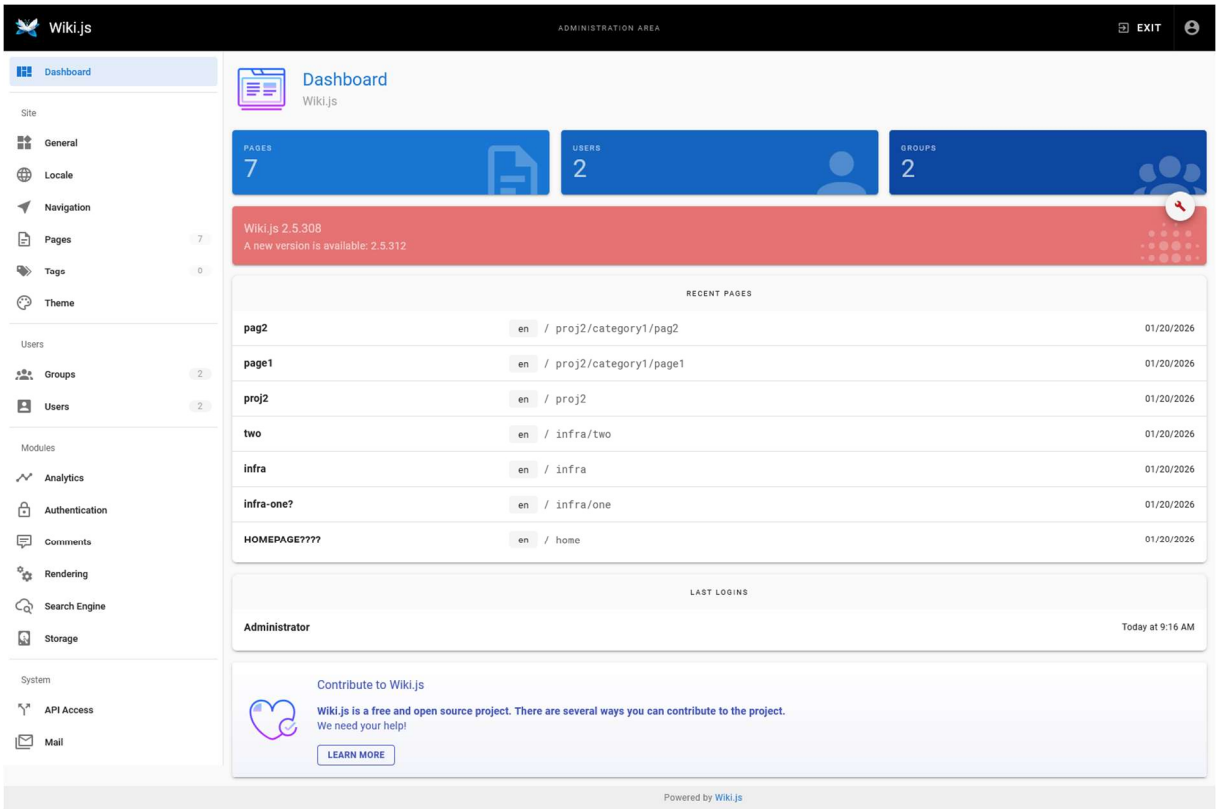
2.9 DFIR IRIS

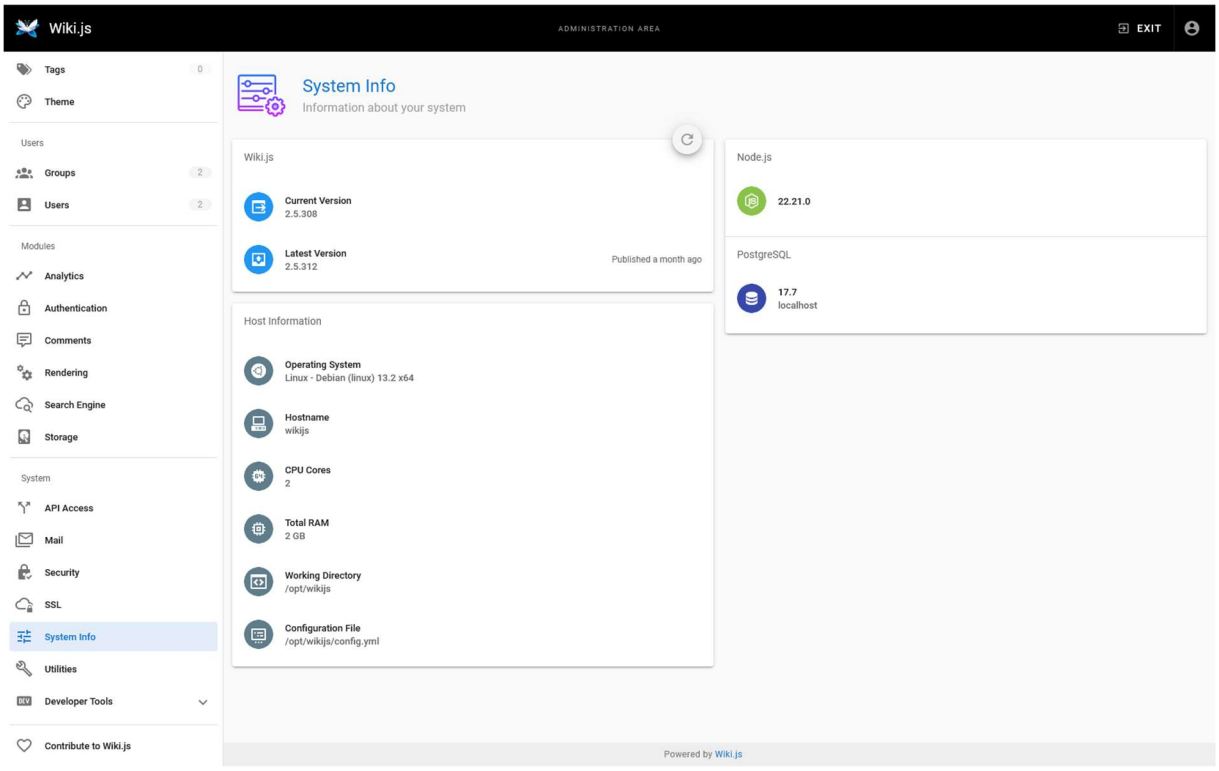
2.10 Kibana (ELK)

2.11 Wiki.js


Wiki.js
Search...
infra
proj2
HOMEPAGE????
PAGE CONTENTS
Introduction
Plot
End
TALK
View Discussion
LAST EDITED BY
Administrator
01/20/2026
HOMEPAGE????
this is page of home
Introduction
Your content here
Plot
more content here
End
rest of the content here
Comments
A
Administrator
2 MONTHS AGO
wow! this is a homepage!
Powered by Wiki.js


Wiki.js
Search...
Profile
Pages
Profile
My personal info
SAVE
My Info
Display Name
Administrator
EDIT
Location
EDIT
Job Title
EDIT
Preferences
Timezone
America/New_York
EDIT
Date Format
Locale Default
EDIT
Appearance
Site Default
EDIT
Authentication
Provider
Local
Change Password
Current Password
New Password
0 / 255
Confirm New Password
CHANGE PASSWORD
Groups
Administrators
Activity
Joined on
Tuesday, December 16, 2025 8:40 AM
Profile last updated on
Tuesday, December 16, 2025 8:40 AM
Last login on
Monday, March 23, 2026 9:16 AM
Pages created
7
Comments posted
0
Powered by Wiki.js





Plus, in the rest of the documentation there is also some screenshot of the e-mail settings or something like that, I think...

3 DEPLOYMENT AND BASIC CONFIGURATION OF THE POC

Briefly describe here how the PoC was deployed in the OpenStack environment, how the VMs were used and where Docker was used. Do not go into detail as in V14, just summarize the actual state.

3.1 Deployment model

3.2 Virtual machines and services used

3.3 Basic integration links

Funded by the European Union
NextGenerationEU
RECOVERY AND RESILIENCE PLAN
GOVERNMENT OFFICE OF THE SLOVAK REPUBLIC

4 CONCLUSION

4.1 XX