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. **ELK Stack** 3
2. **Shuffle** 3
3. **Wazuh** 3
4. **Greenbone Community edition** 7
5. **OpenCTI** 9
6. **MISP** 9
7. **GLPI** 10
8. **NetBox** 12
9. **DFIR IRIS – area: Ticketing** 12
10. **DFIR IRIS – area: Recording and management of incidents** ..Chyba! Záložka nie je definovaná.
11. **Kibana (ELK)** 12
12. **Wiki.js** 13

BRAIN:IT

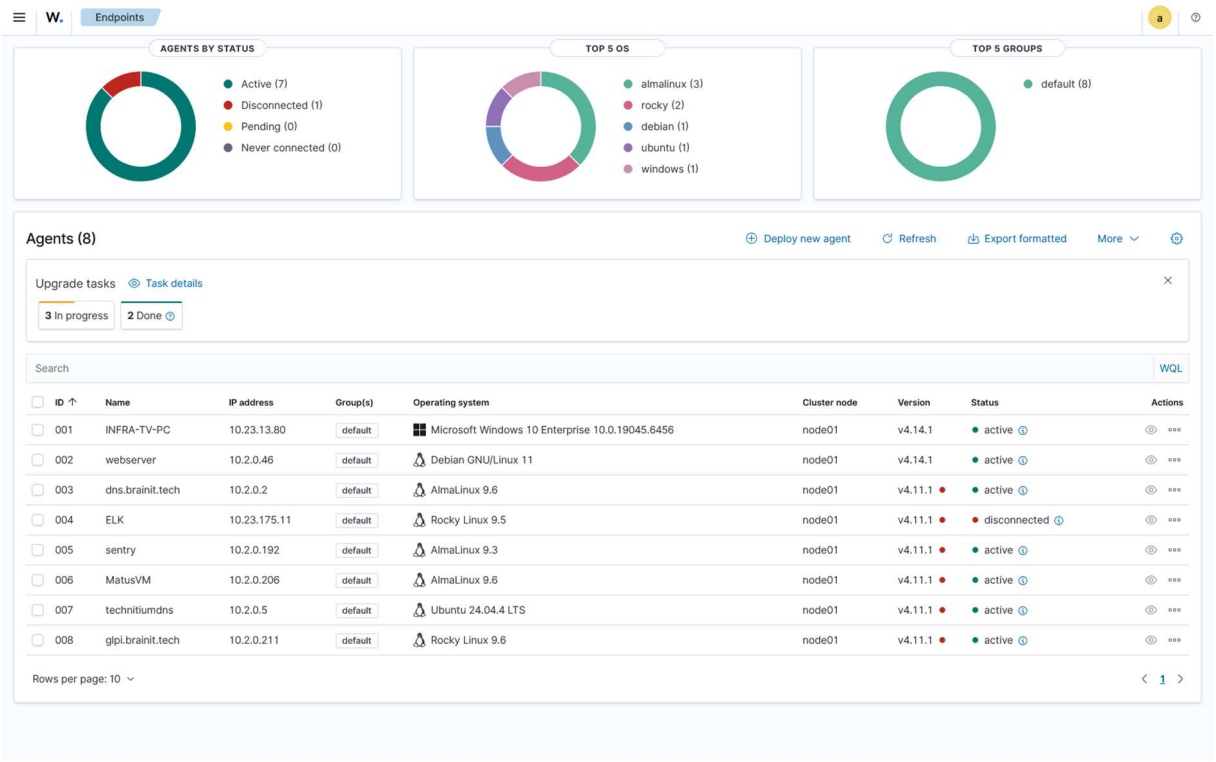
FRI

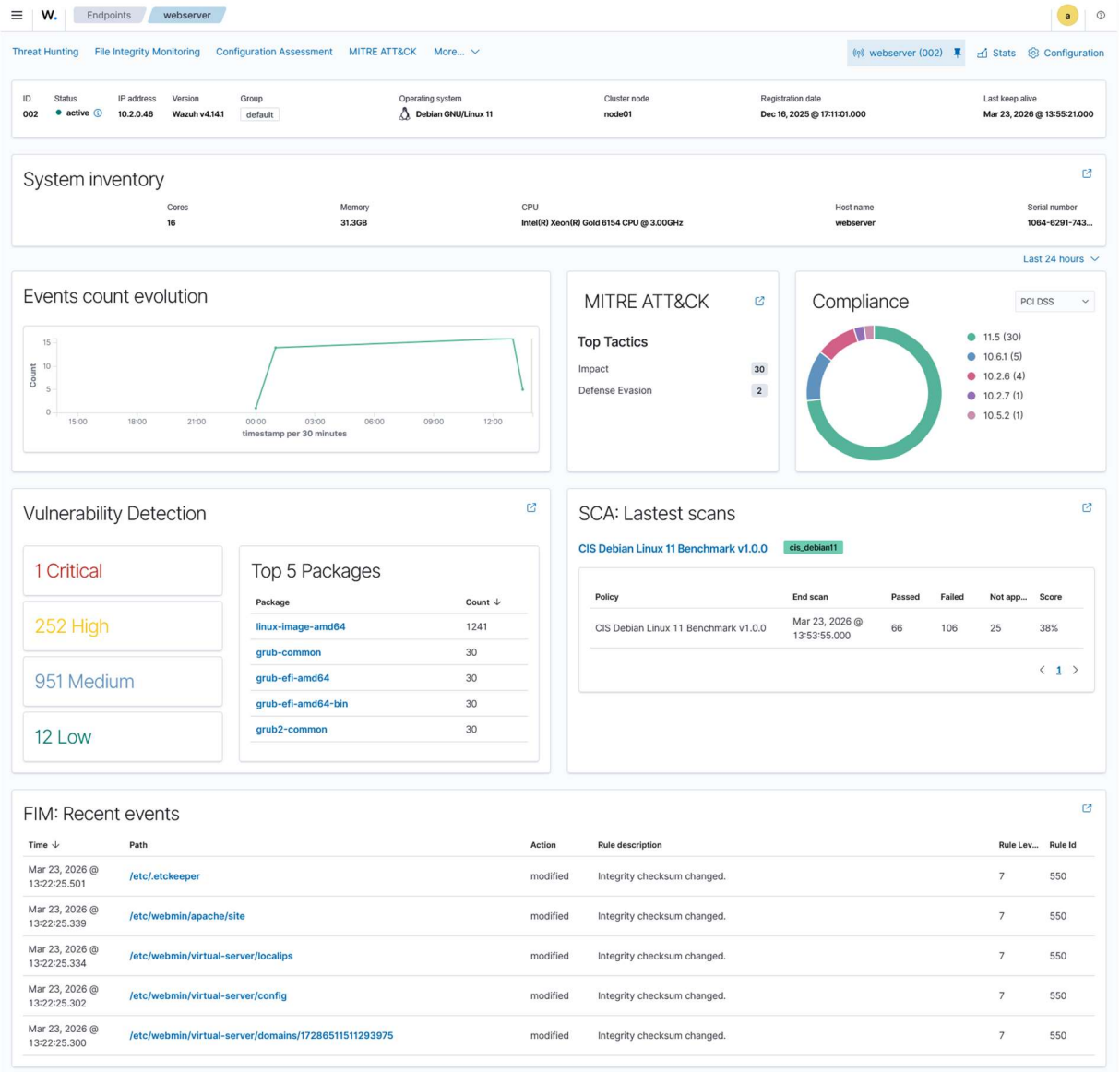
1. ELK STACK

test

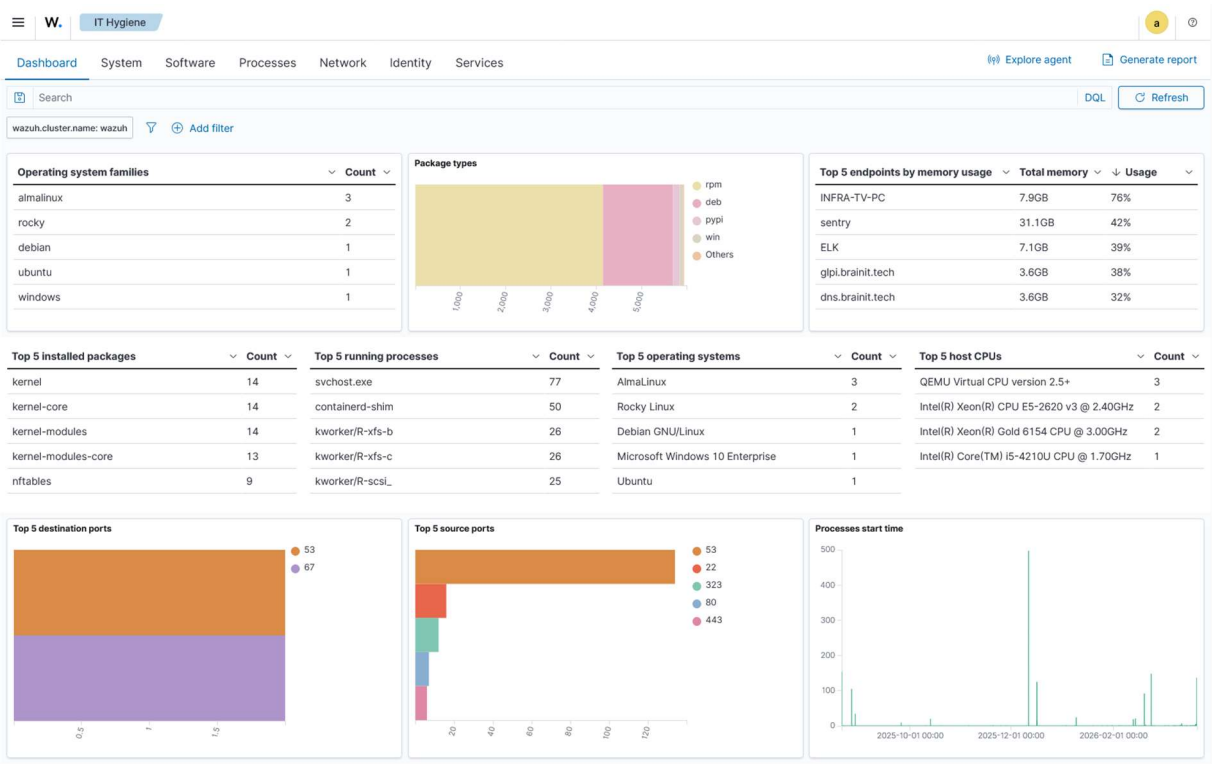
2. SHUFFLE

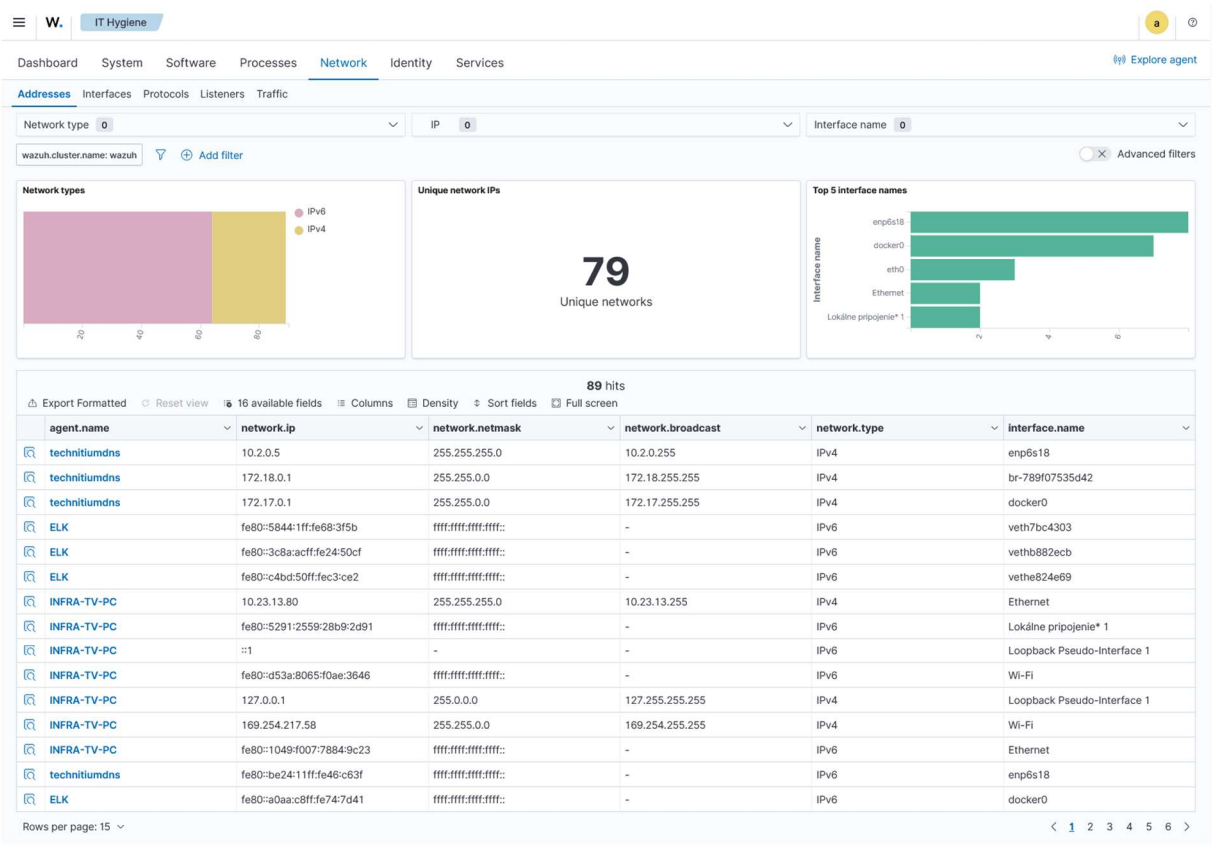
3. WAZUH

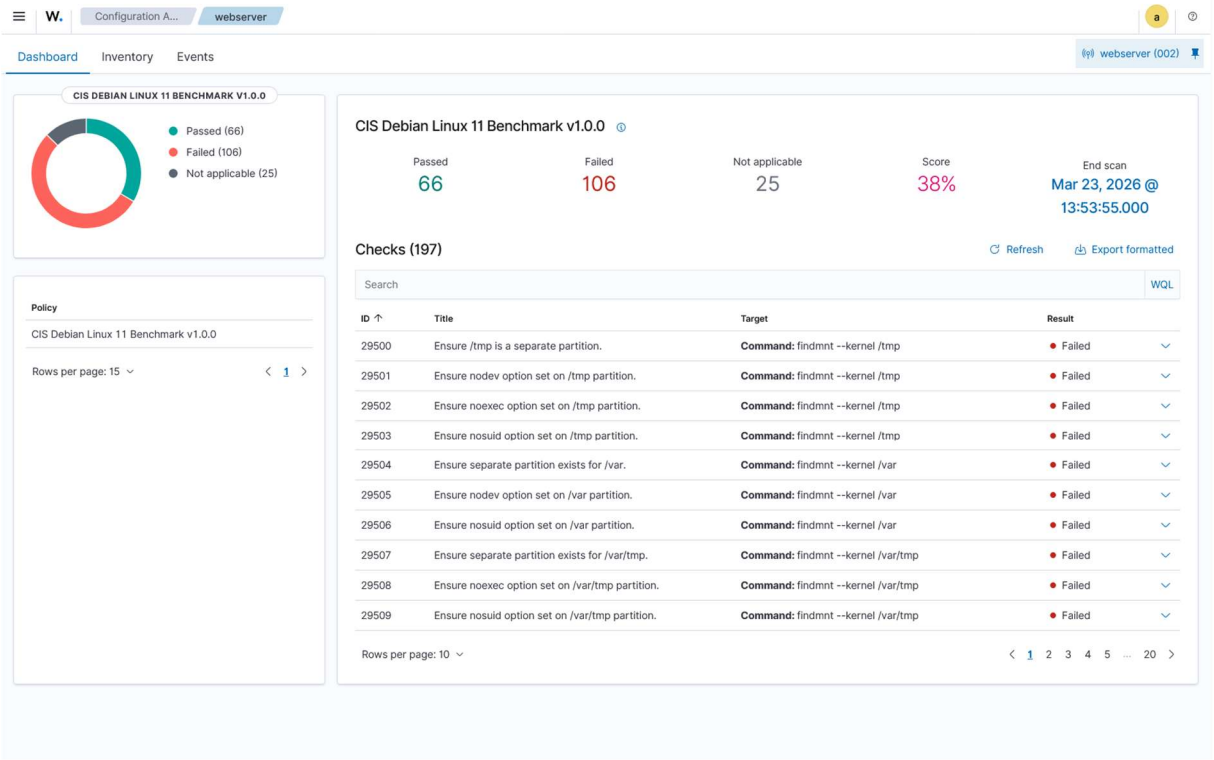




Funded by the European Union
NextGenerationEU
RECOVERY AND RESILIENCE PLAN
GOVERNMENT OFFICE OF THE SLOVAK REPUBLIC

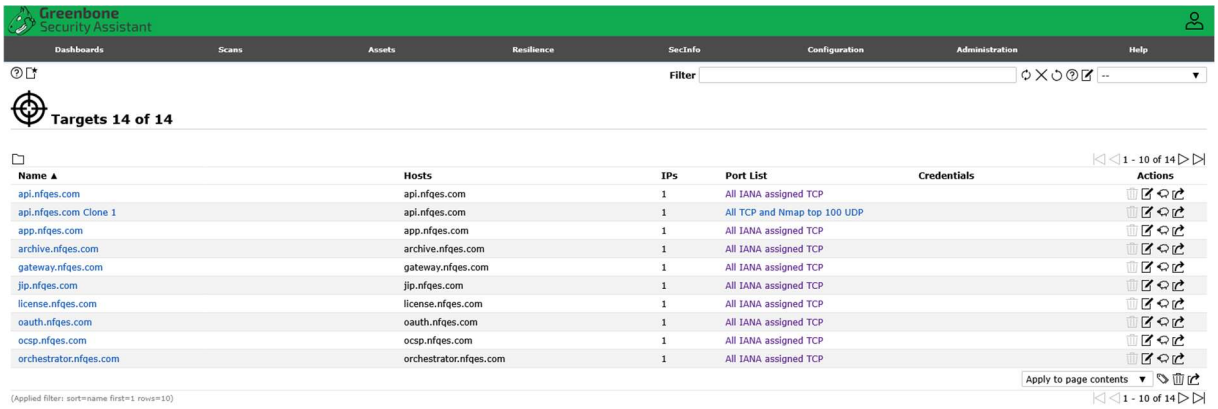

W.
IT Hygiene
Dashboard
System
Software
Processes
Network
Identity
Services
Explore agent
Generate report
Search
DQL
Refresh
wazuh.cluster.name: wazuh
Add filter
Operating system families
Count
almalinux 3
rocky 2
debian 1
ubuntu 1
windows 1
Package types
rpm
deb
pypi
win
Others
1,000
2,000
3,000
4,000
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

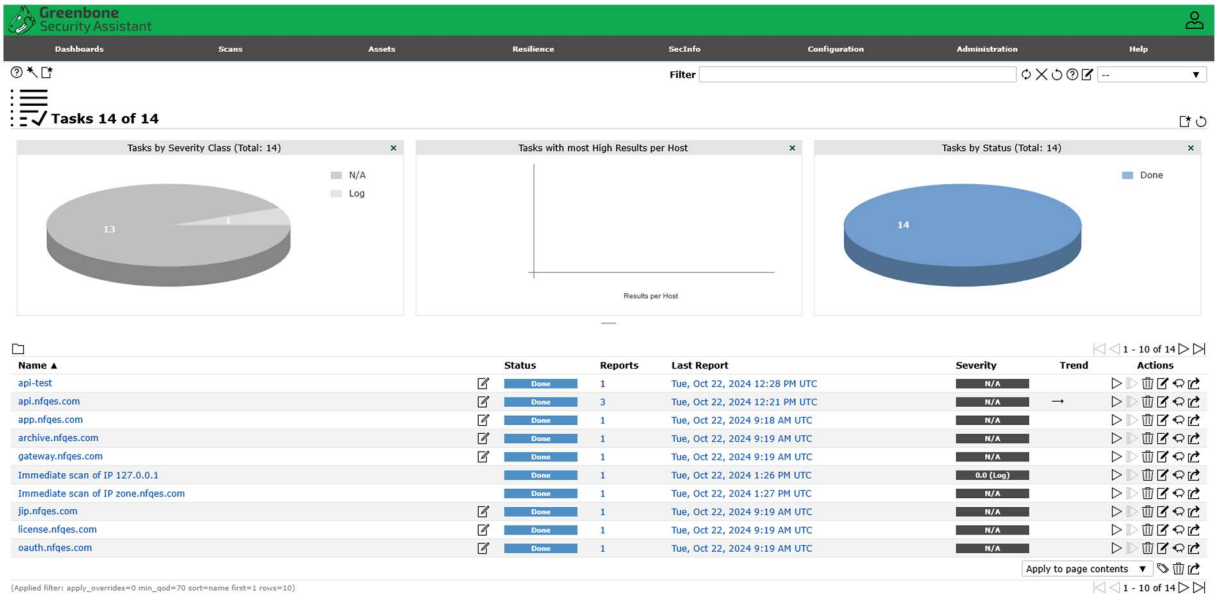




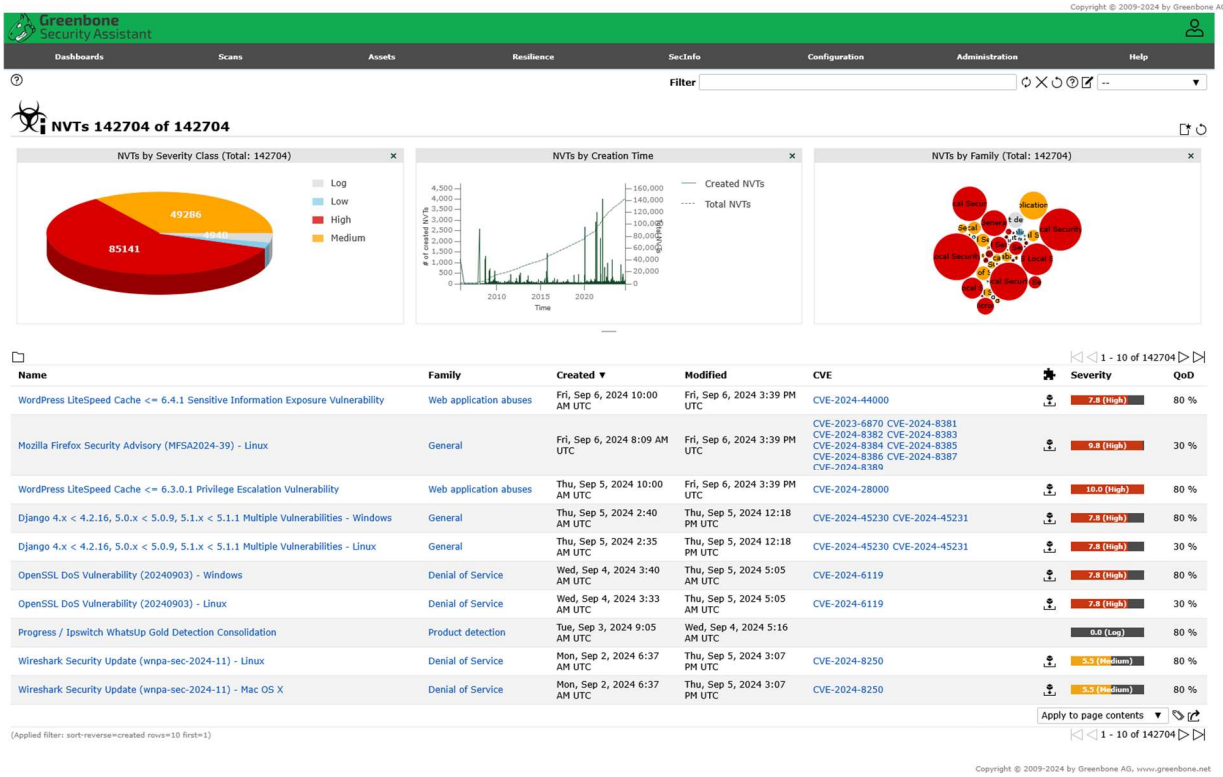
Funded by the European Union
NextGenerationEU
RECOVERY AND RESILIENCE PLAN
GOVERNMENT OFFICE OF THE SLOVAK REPUBLIC

4. GREENBONE COMMUNITY EDITION



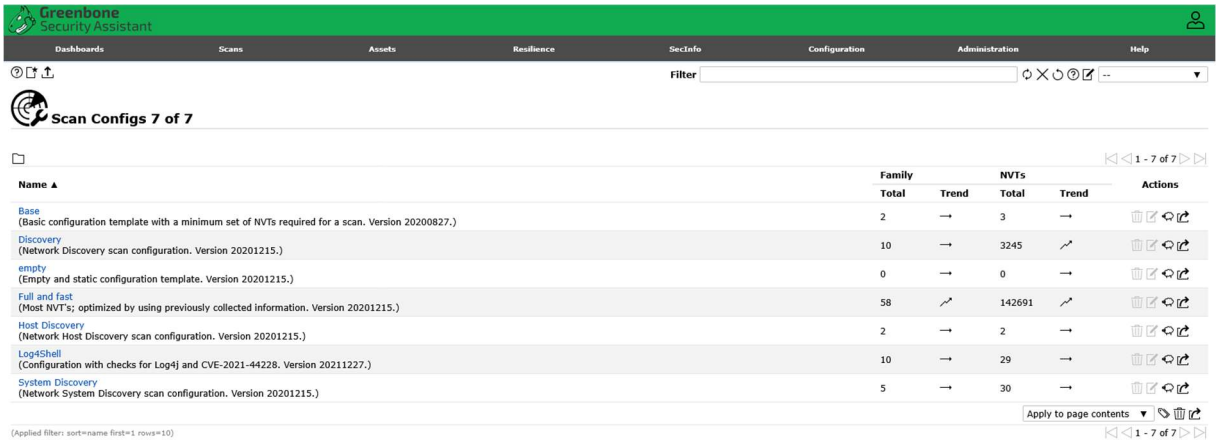


Copyright © 2009-2024 by Greenbone AG, www.greenbone.net



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

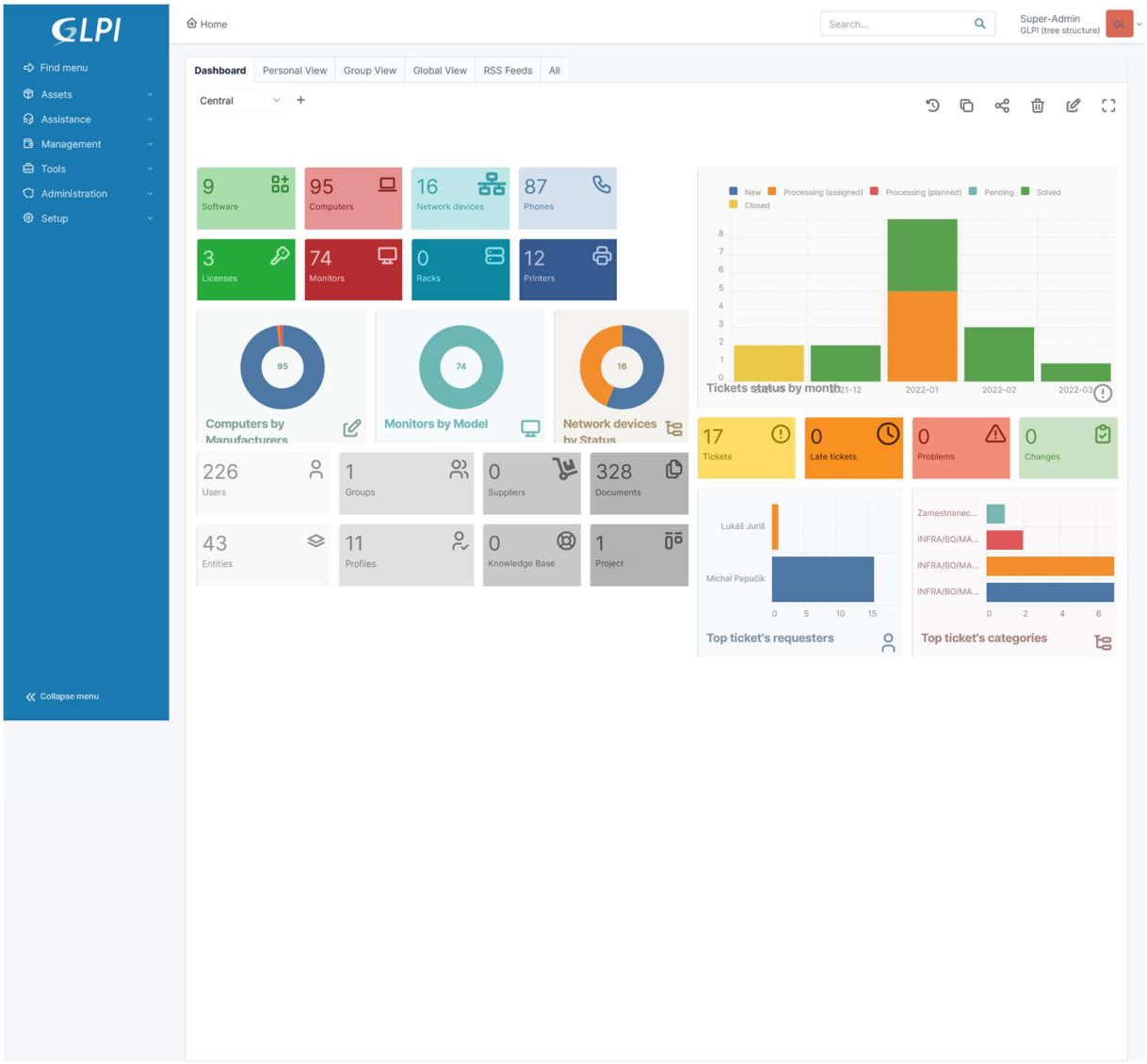
Funded by the European Union
NextGenerationEU
RECOVERY AND RESILIENCE PLAN
GOVERNMENT OFFICE OF THE SLOVAK REPUBLIC

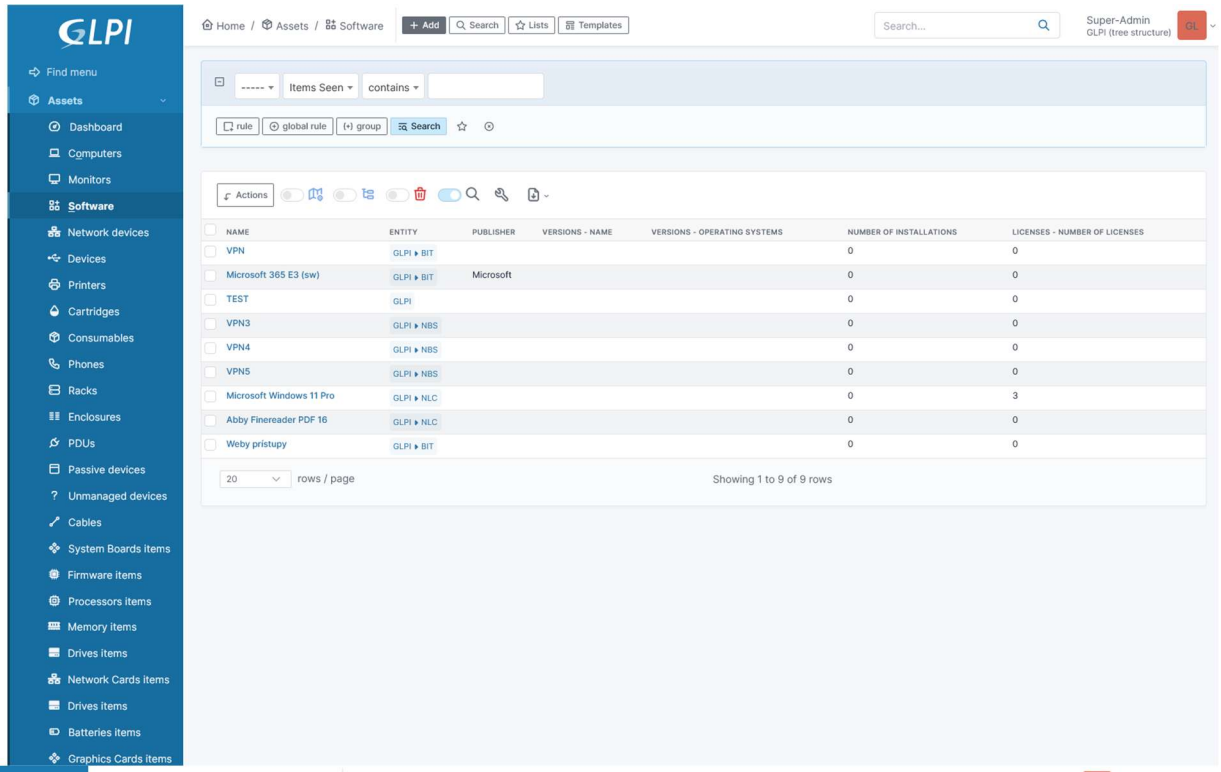


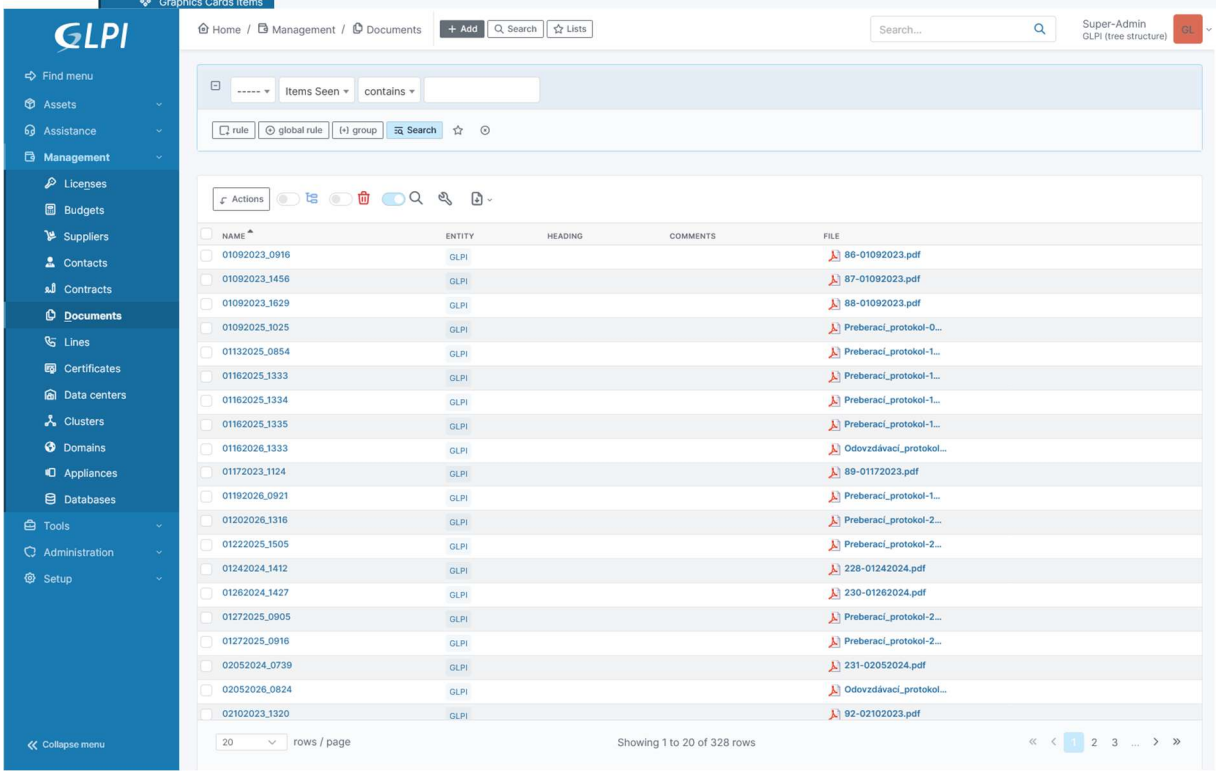
5. OPENCTI

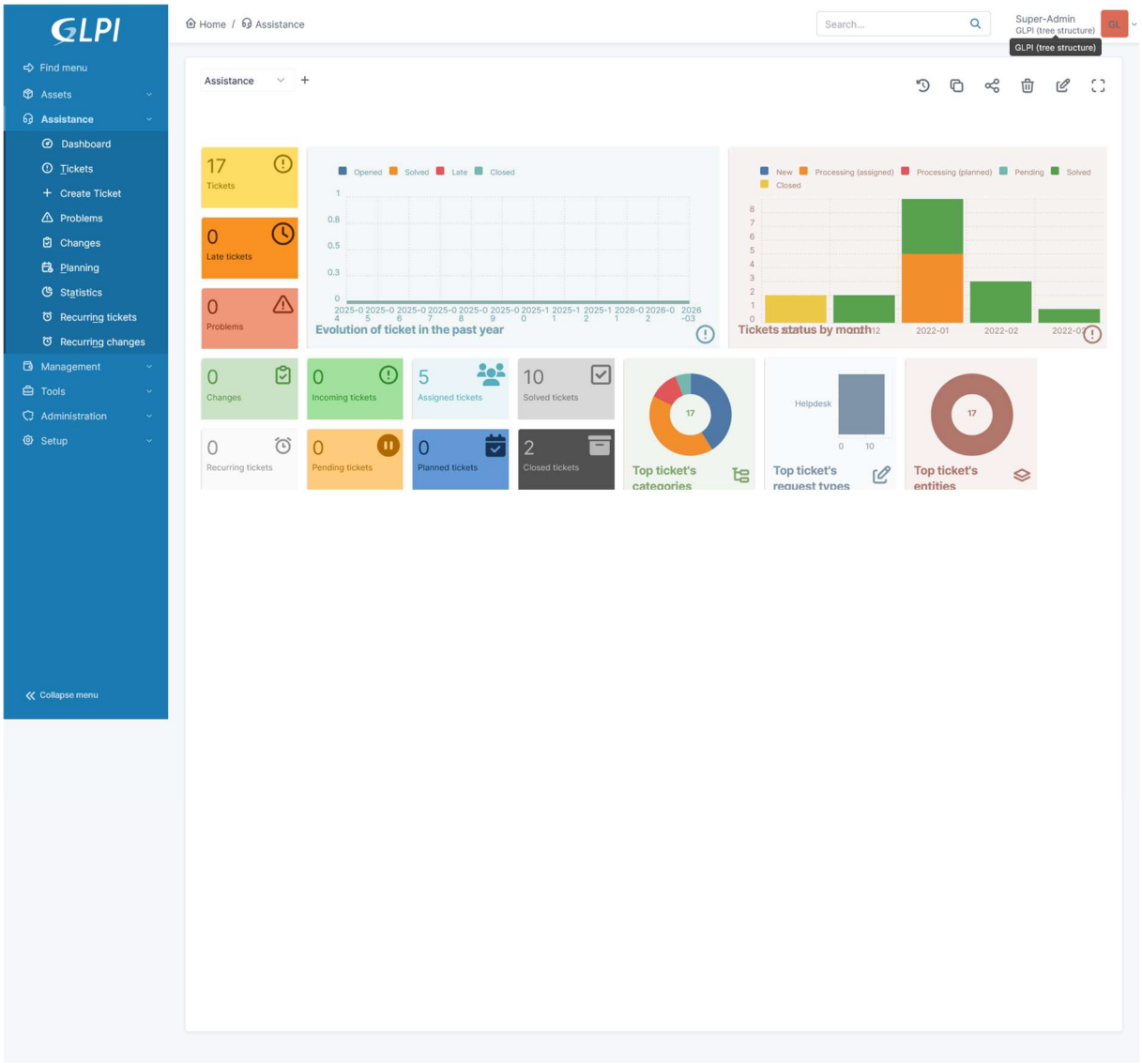
6. MISP

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...
INFRA/BO/MA...
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
Microsoft 365 E3 (sw)
TEST
VPN3
VPN4
VPN5
Microsoft Windows 11 Pro
Abby Finereader PDF 16
Weby prístupy
Microsoft
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
01092023_1456
01092023_1629
01092025_1025
01132025_0854
01162025_1333
01162025_1334
01162025_1335
01162026_1333
01172023_1124
01192026_0921
01202026_1316
01222025_1505
01242024_1412
01262024_1427
01272025_0905
01272025_0916
02052024_0739
02052026_0824
02102023_1320
86-01092023.pdf
87-01092023.pdf
88-01092023.pdf
Preberací_protokol-0...
Preberací_protokol-1...
Odovzdávací_protokol...
89-01172023.pdf
Preberací_protokol-2...
228-01242024.pdf
230-01262024.pdf
231-02052024.pdf
92-02102023.pdf
20
rows / page
Showing 1 to 20 of 328 rows

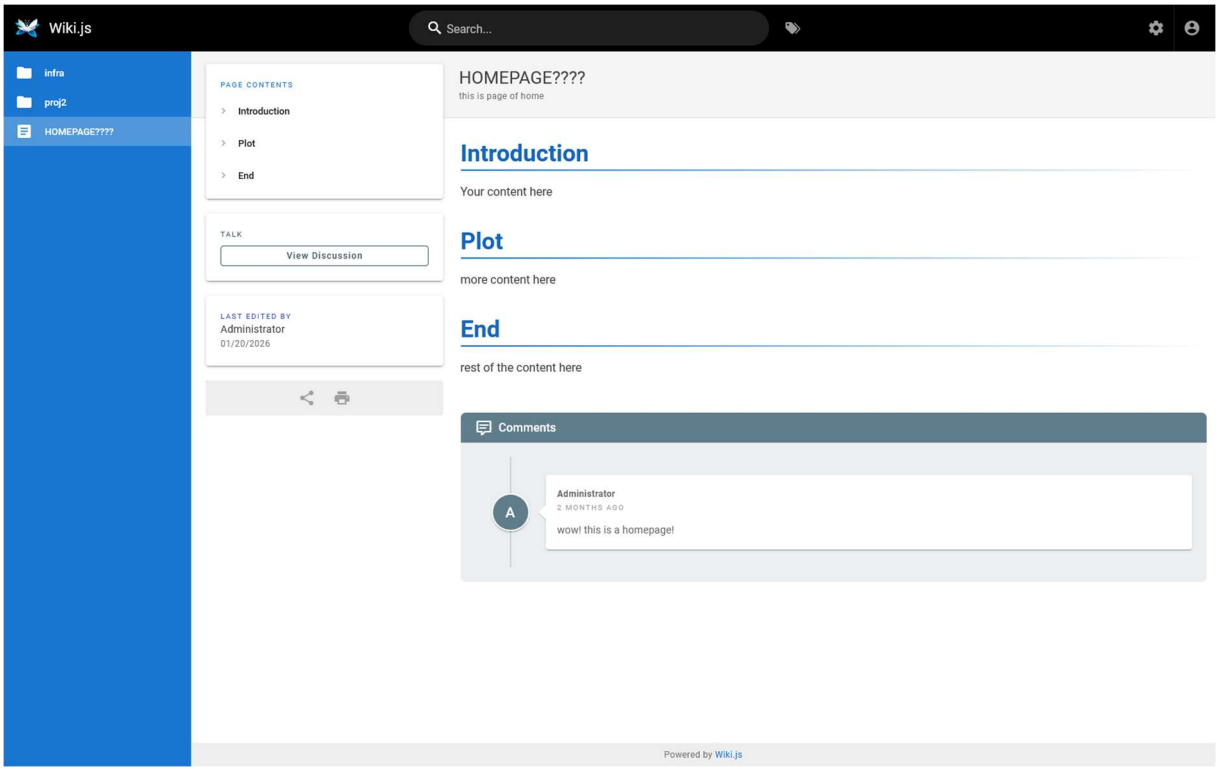


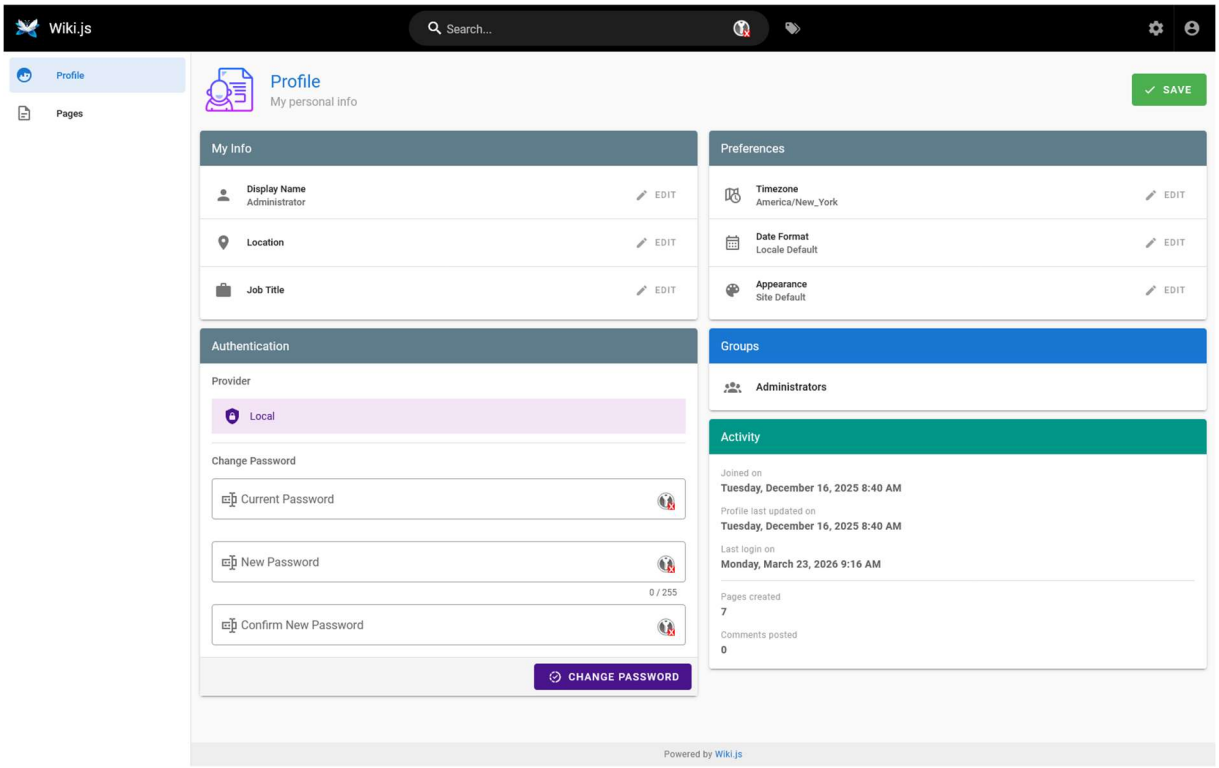
8. NETBOX

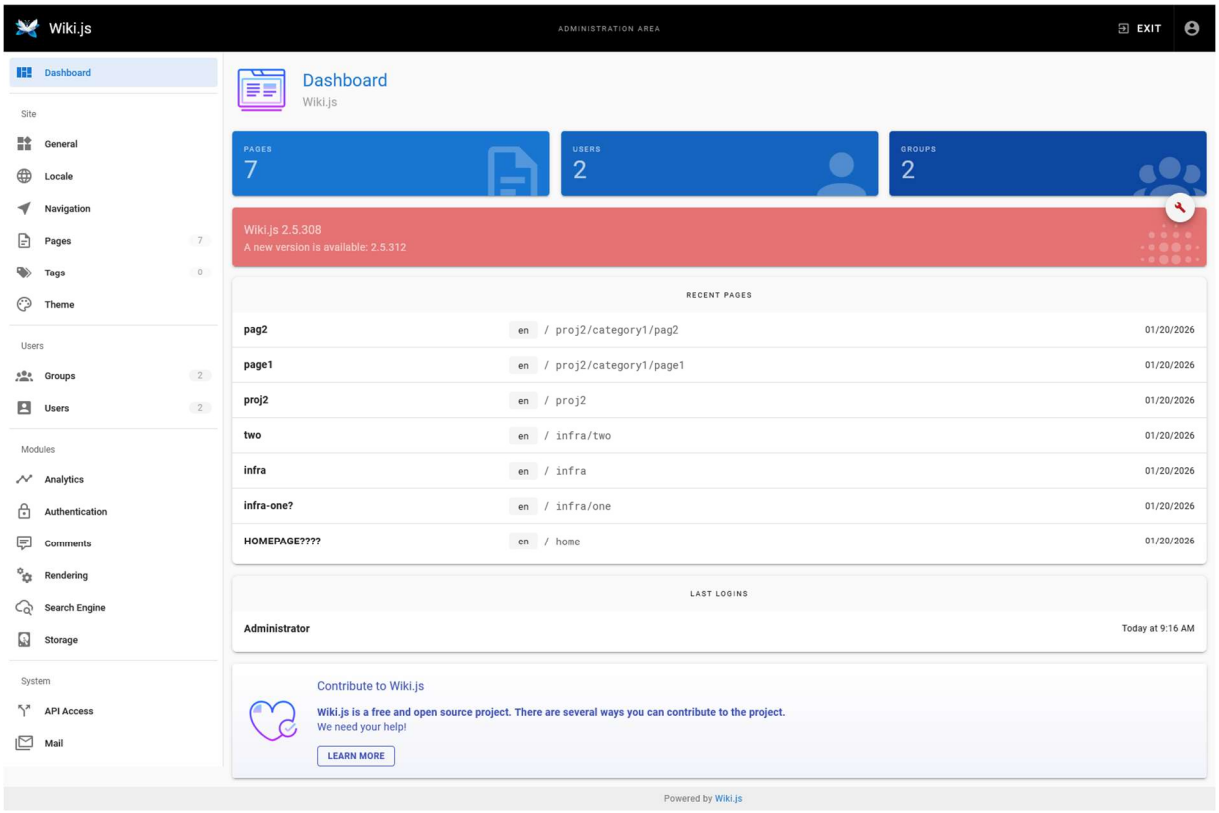
9. DFIR IRIS

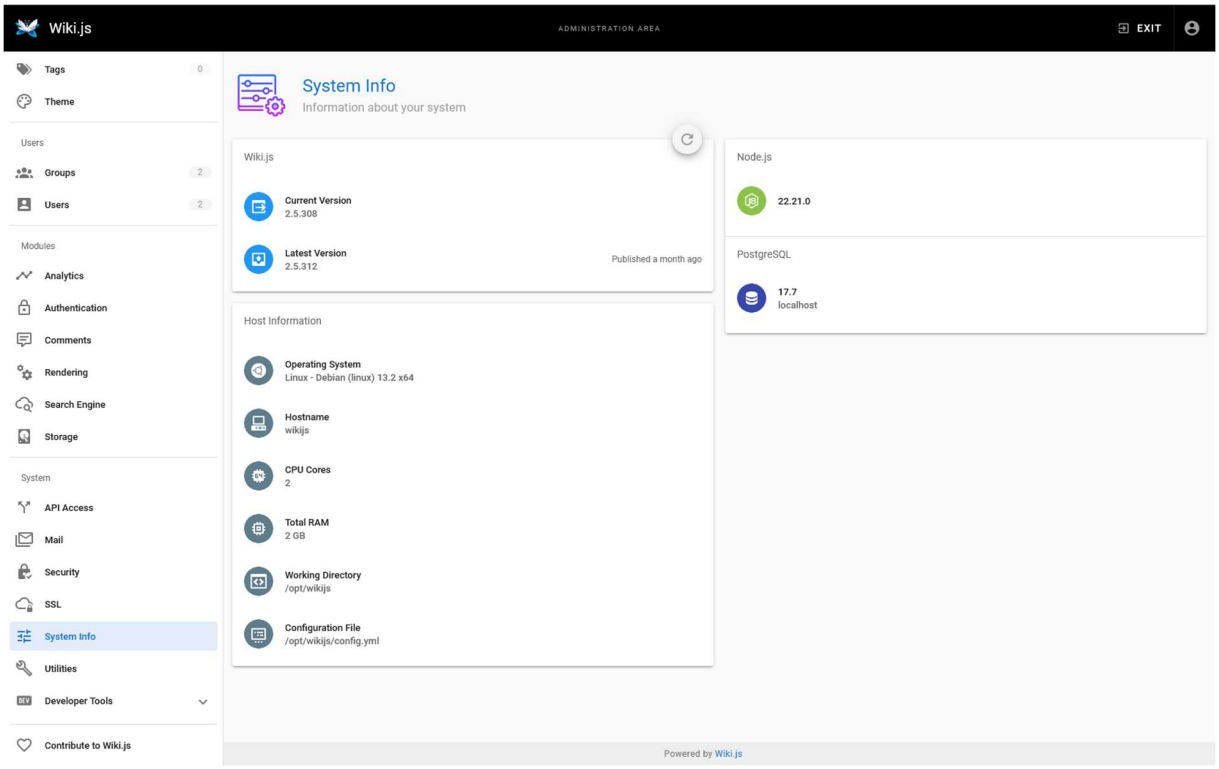
10. KIBANA (ELK)

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
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...

Funded by the European Union
NextGenerationEU

RECOVERY AND RESILIENCE PLAN

GOVERNMENT OFFICE OF THE SLOVAK REPUBLIC