CYBER EDGE

CYBER EDGE

Group 4

THE TEAM

Group 4

- PRIYANSHU DAS
- ASHISH SRIVASTAVA
- RAKESH CHOUDHARY
- HARISH PRAKASH SINGH

AGENDA

Problem Statement

Proposed Solution

Technical Details

Demo

Further Enhancements

Q&A

PROBLEM STATEMENT

Objective

Managing the security posture of multiple servers and virtual machines (VMs) in an enterprise environment is challenging. Administrators often struggle to keep track of security vulnerabilities, outdated software, and unpatched systems.

Additionally, conducting compliance checks using OpenSCAP and CIS benchmarks requires manual intervention, making it inefficient and error-prone. There is a need for an automated, centralized, and user-friendly solution that provides real-time security insights and compliance reports for all managed servers.

```
ion:absolute;z-index:99
x 5px #ccc}.gbrtl .gbm{
;display:block;position
pacity:1;*top:-2px;*lef
/;top:-4px\0/;left:-6px
ne-box;display:inline-b
isplay:block;list-styl
ne-block;line-height:27p
pointer;display:block;t
tive;z-index:1000}.gbts
padding-right:9px}#gbz
d:url(//
```

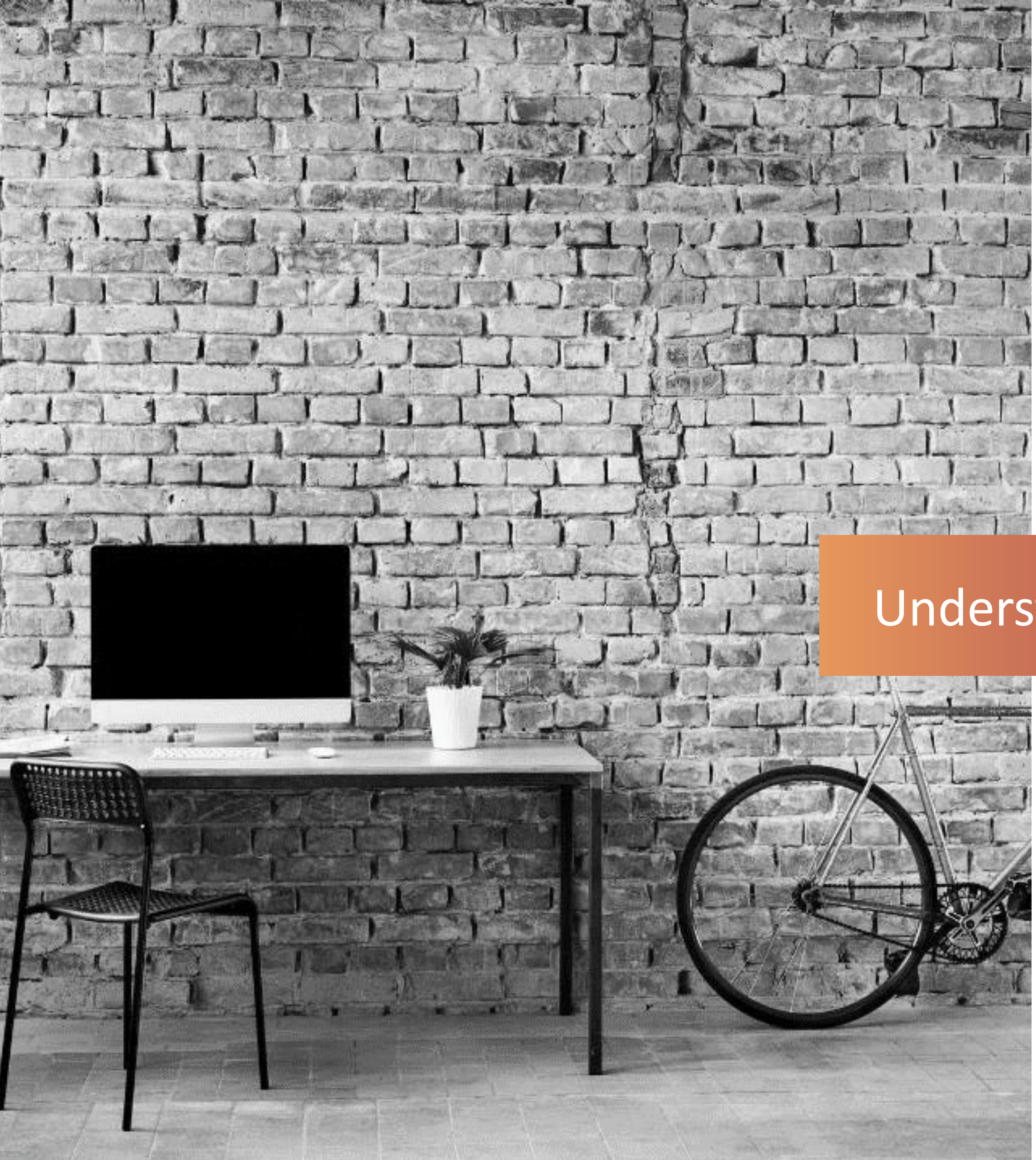
PROPOSED SOLUTION

LET’S DIVE IN

SOLUTION

The **Security-Centric Server & VM Management Tool** is a web-based platform that enables administrators to monitor and enforce security best practices across multiple servers. It consists of the following components:

- React-based Web Dashboard
- Host Agent (Backend Server)
- Guest Agent (Client Script)



Background Details

Understanding OpenSCAP Workbench

What is OpenSCAP Workbench

OpenSCAP Workbench is a powerful tool designed for compliance assessment and security automation. It is part of the OpenSCAP ecosystem, which supports the Security Content Automation Protocol (SCAP) framework. Here are the core aspects of OpenSCAP Workbench:

- **Compliance Checking:** It assesses system configurations against predefined security policies and standards, such as CIS Benchmarks or DISA STIGs.
- **Customizable Profiles**: Users can modify security policies by enabling or disabling specific rules and saving these changes as tailoring files.
- **Automated Reports**: It generates detailed reports that summarize compliance results, highlighting areas that need remediation.
- **Remediation Support**: Based on the scan results, it provides recommendations or scripts to fix identified issues.
- **Efficient Scanning**: It can perform system scans to identify security vulnerabilities and non-compliant configurations.

Utilization of OpenSCAP Workbench in the Project

- **Compliance Checks**: Validates system configurations against CIS benchmarks.
- **Automated Scanning**: Assists in system assessment by collecting data via agents.
- **Report Analysis**: Offers actionable insights for compliance enforcement.
- **Guidance**: Facilitates decisions for system hardening and regulatory adherence.

Checking Compliance with CIS Benchmark

The CIS (Center for Internet Security) Benchmarks are a set of best practices and guidelines developed to help organizations secure their systems and data. These benchmarks are widely recognized standards that provide specific configuration recommendations to improve the security posture of various IT systems, applications, and devices. Key Features of CIS Benchmarks:

- **Platform-Specific Guidelines**: Benchmarks are available for operating systems, cloud environments, databases, and network devices.
- **Customizable**: Recommendations can be adapted to fit an organization's unique needs and requirements.
- **Community-Driven**: Developed and maintained by cybersecurity experts and practitioners from around the world.

Using CIS Benchmarks helps ensure that systems are configured securely, reducing vulnerabilities and strengthening defenses against cyber threats.

FEATURE BREAKDOWN

- 📝 **OpenSCAP Hardening Reports**
  - Runs compliance scans and sends results to the host.
- 🔓 **Open Ports Scan**
  - Lists open network ports.
- 📦 **Patching Status**
  - Checks for available updates.
- 🛠️ **Third-Party Software Inventory**
  - Lists installed packages.

KEY BENEFITS

✅ **Centralized Security Management**: Monitor multiple servers from a single dashboard.

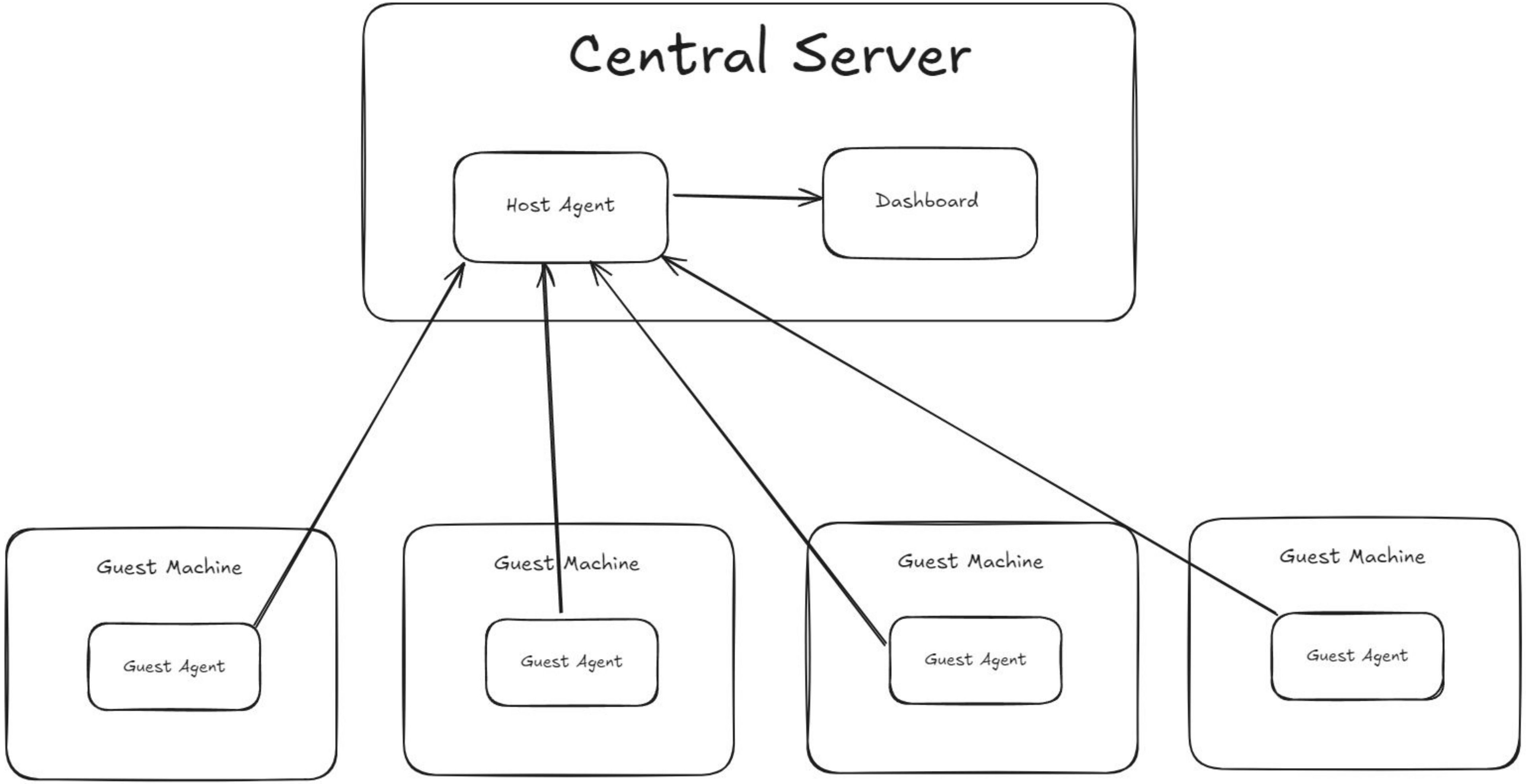
✅ **Automated Compliance Reporting**: Uses OpenSCAP with CIS benchmarks for security hardening.

✅ **Real-time Insights**: Helps administrators quickly identify and address vulnerabilities.

✅ **User-friendly Interface**: Provides a clean and intuitive UI for easy navigation.

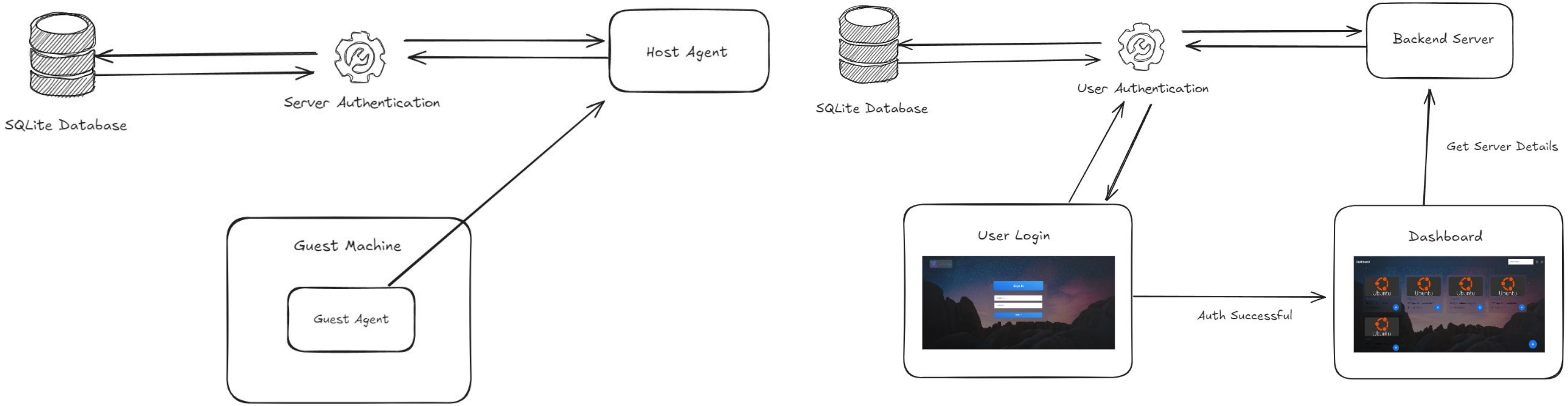
✅ **Lightweight & Efficient**: Uses SQLite, React, and Node.js for a scalable and low-resource solution.

HIGH LEVEL DESIGN

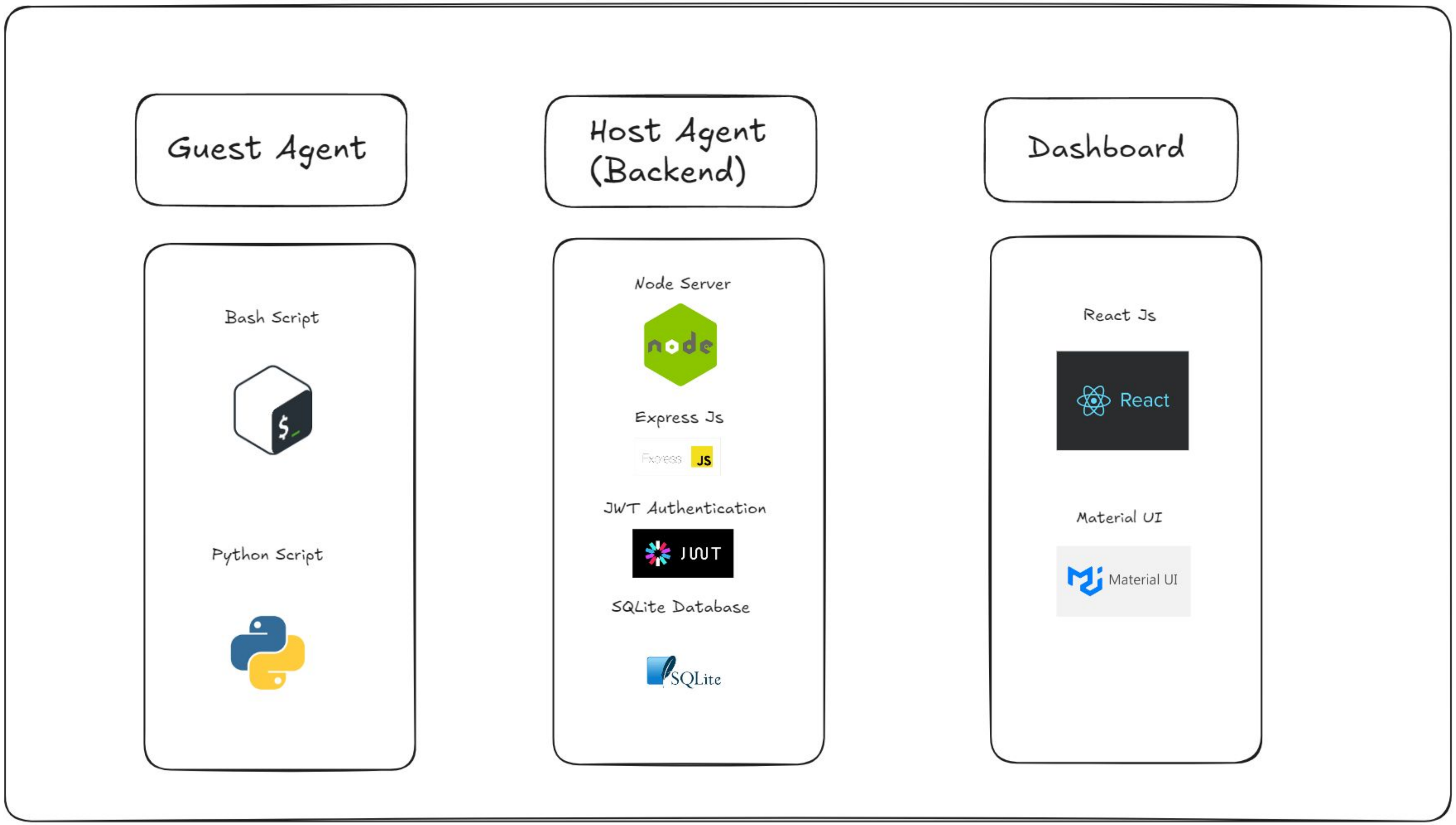


TECHNICAL DETAILS

SYSTEM DESIGN



TECH STACK



Guest Agent

Bash Script

Python Script

Host Agent (Backend)

Node Server

Express Js

JWT Authentication

SQLite Database

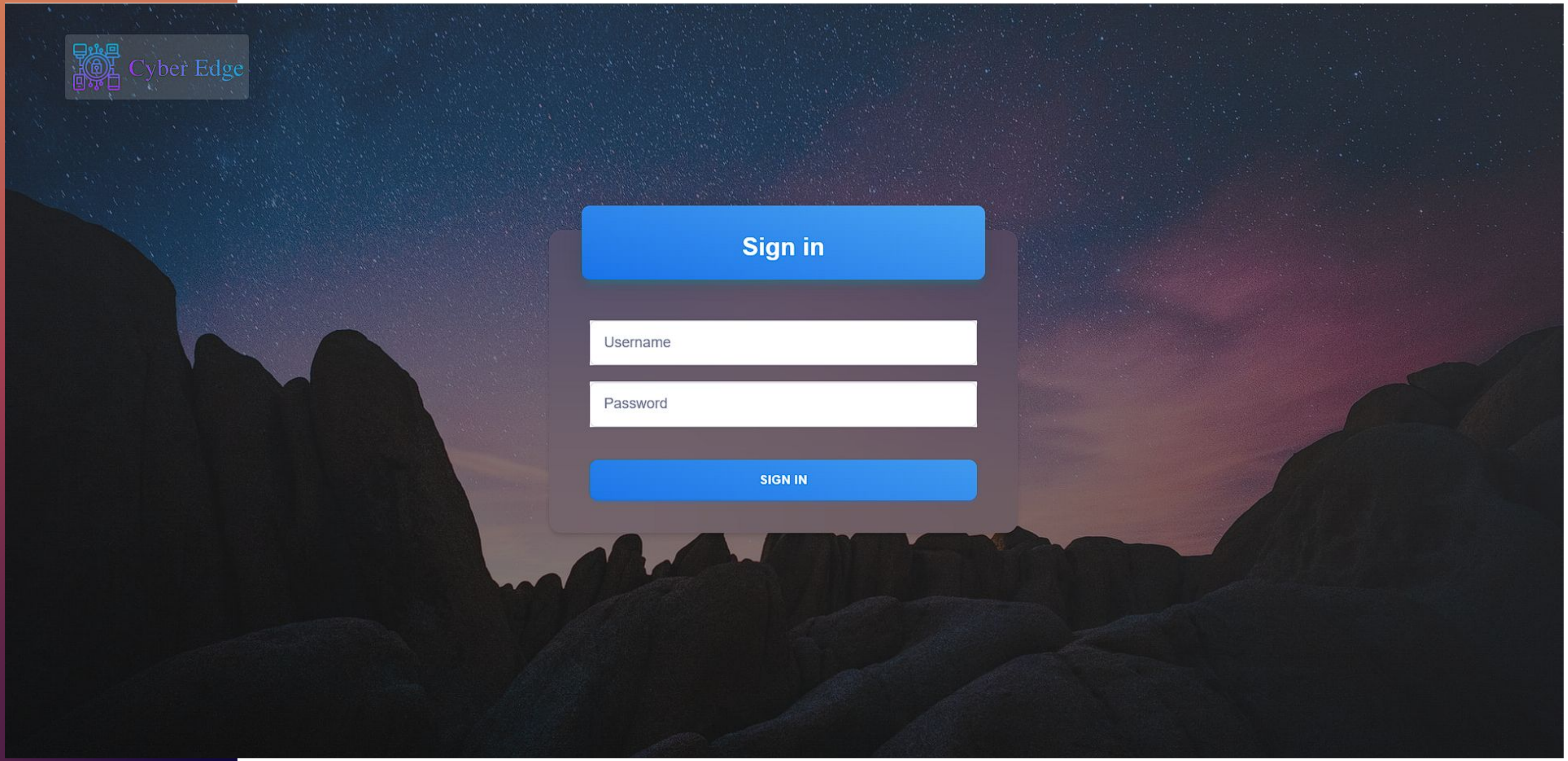
Dashboard

React Js

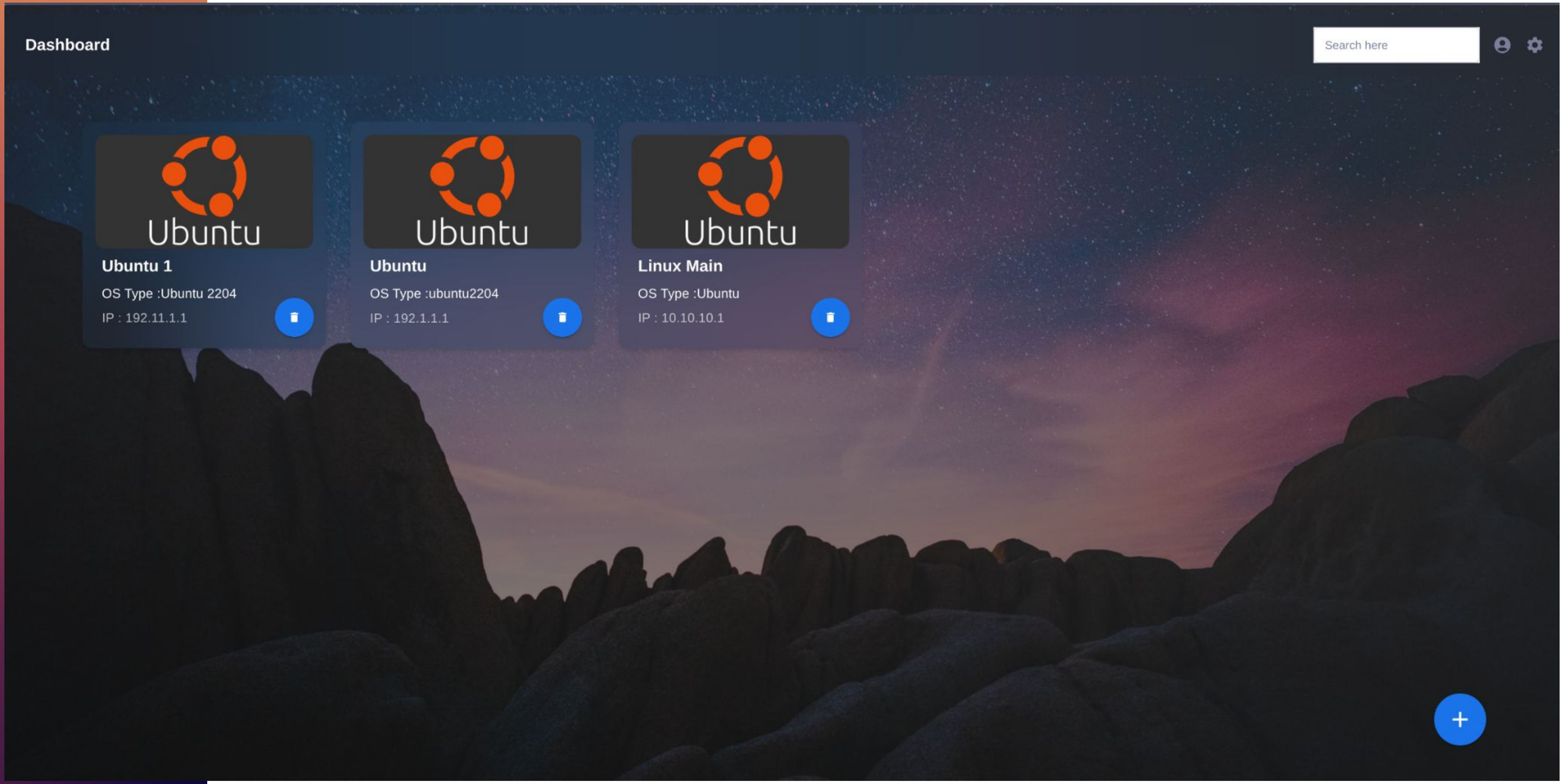
Material UI

DEMO

LOGIN PAGE



DASHBOARD



Ubuntu 1

OS Type :Ubuntu 2204

IP : 192.11.1.1

Ubuntu

OS Type :ubuntu2204

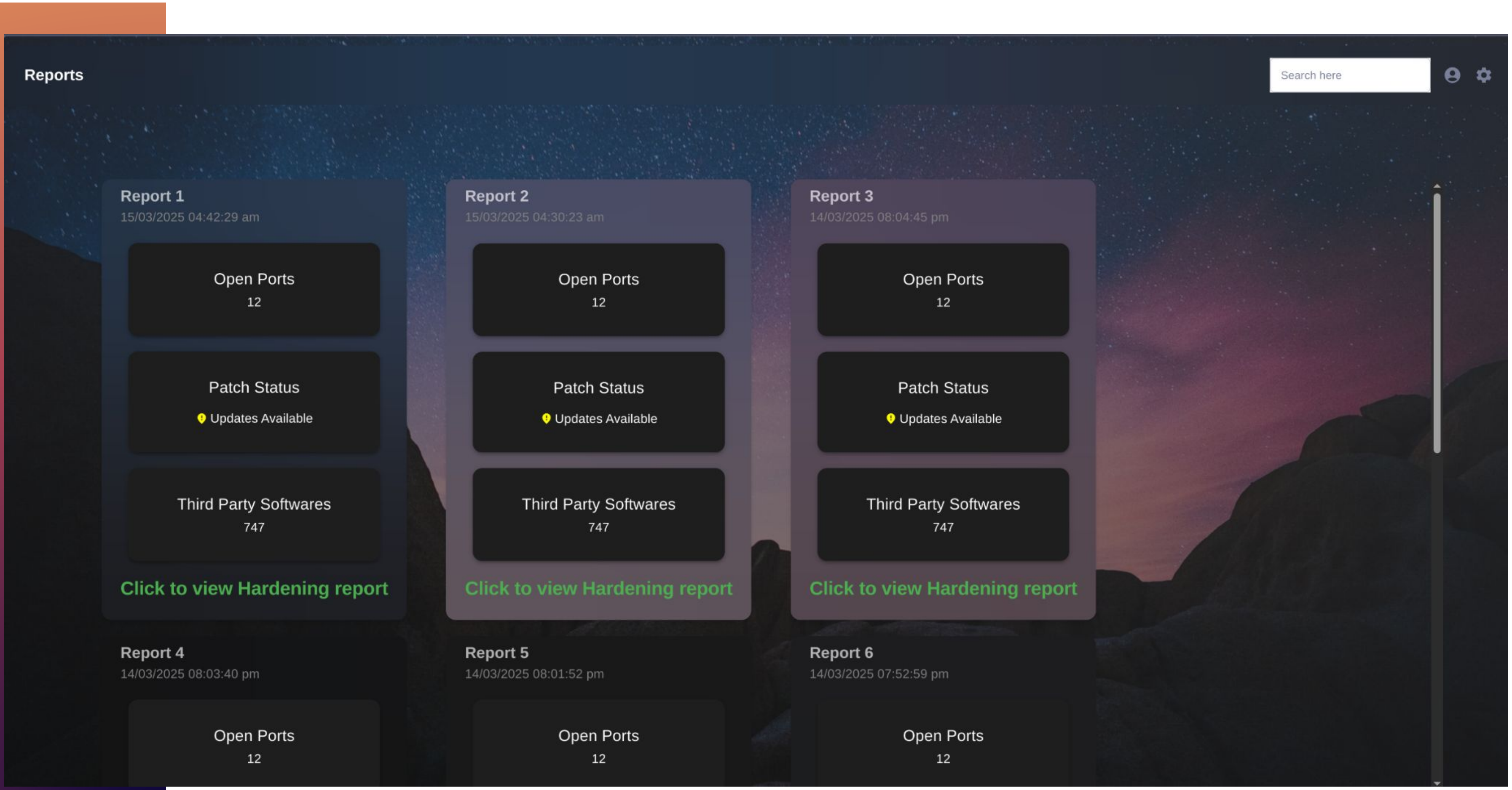
IP : 192.1.1.1

Linux Main

OS Type :Ubuntu

IP : 10.10.10.1

REPORTS



Reports

Search here

Report 1
15/03/2025 04:42:29 am

Open Ports
12

Patch Status
● Updates Available

Third Party Softwares
747

Click to view Hardening report

Report 2
15/03/2025 04:30:23 am

Open Ports
12

Patch Status
● Updates Available

Third Party Softwares
747

Click to view Hardening report

Report 3
14/03/2025 08:04:45 pm

Open Ports
12

Patch Status
● Updates Available

Third Party Softwares
747

Click to view Hardening report

Report 4
14/03/2025 08:03:40 pm

Open Ports
12

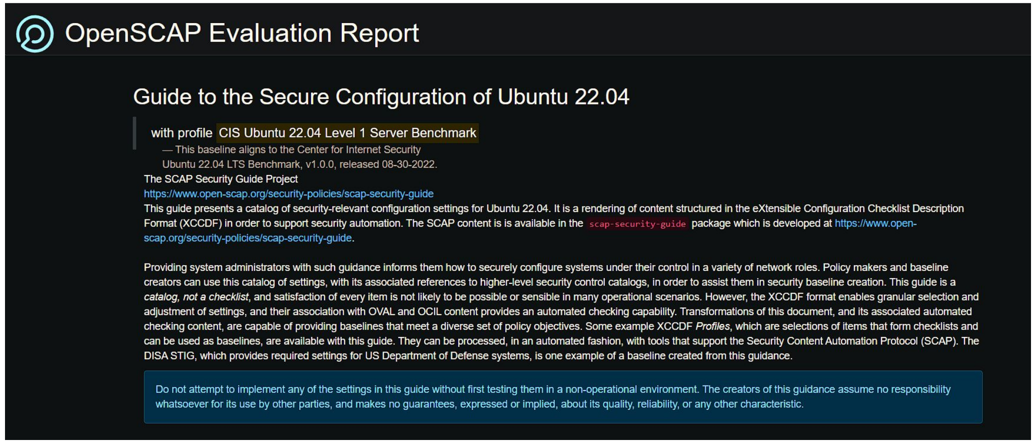
Report 5
14/03/2025 08:01:52 pm

Open Ports
12

Report 6
14/03/2025 07:52:59 pm

Open Ports
12

OPENSCAP CIS BENCHMARK REPORT



OpenSCAP Evaluation Report

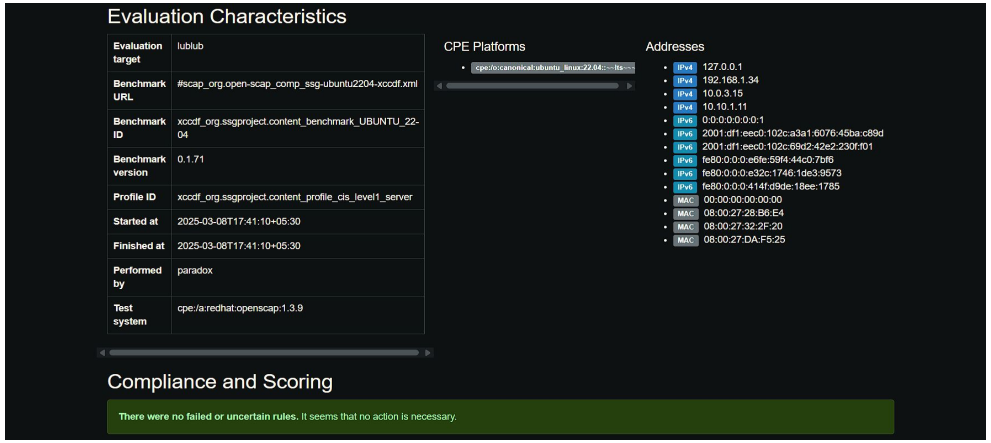
Guide to the Secure Configuration of Ubuntu 22.04

> with profile CIS Ubuntu 22.04 Level 1 Server Benchmark
>
> — This baseline aligns to the Center for Internet Security
> Ubuntu 22.04 LTS Benchmark, v1.0.0, released 08-30-2022.

The SCAP Security Guide Project
https://www.open-scap.org/security-policies/scap-security-guide
This guide presents a catalog of security-relevant configuration settings for Ubuntu 22.04. It is a rendering of content structured in the eXtensible Configuration Checklist Description Format (XCCDF) in order to support security automation. The SCAP content is is available in the `scap-security-guide` package which is developed at https://www.open-scap.org/security-policies/scap-security-guide.

Providing system administrators with such guidance informs them how to securely configure systems under their control in a variety of network roles. Policy makers and baseline creators can use this catalog of settings, with its associated references to higher-level security control catalogs, in order to assist them in security baseline creation. This guide is a *catalog, not a checklist*, and satisfaction of every item is not likely to be possible or sensible in many operational scenarios. However, the XCCDF format enables granular selection and adjustment of settings, and their association with OVAL and OCIL content provides an automated checking capability. Transformations of this document, and its associated automated checking content, are capable of providing baselines that meet a diverse set of policy objectives. Some example XCCDF *Profiles*, which are selections of items that form checklists and can be used as baselines, are available with this guide. They can be processed, in an automated fashion, with tools that support the Security Content Automation Protocol (SCAP). The DISA STIG, which provides required settings for US Department of Defense systems, is one example of a baseline created from this guidance.

Do not attempt to implement any of the settings in this guide without first testing them in a non-operational environment. The creators of this guidance assume no responsibility whatsoever for its use by other parties, and makes no guarantees, expressed or implied, about its quality, reliability, or any other characteristic.



Evaluation Characteristics

Evaluation target	lublub
Benchmark URL	#scap_org.open-scap_comp_ssg-ubuntu2204-xccdf.xml
Benchmark ID	xccdf_org.ssgproject.content_benchmark_UBUNTU_22-04
Benchmark version	0.1.71
Profile ID	xccdf_org.ssgproject.content_profile_cis_level1_server
Started at	2025-03-08T17:41:10+05:30
Finished at	2025-03-08T17:41:10+05:30
Performed by	paradox
Test system	cpe:/a:redhat:openscap:1.3.9

CPE Platforms

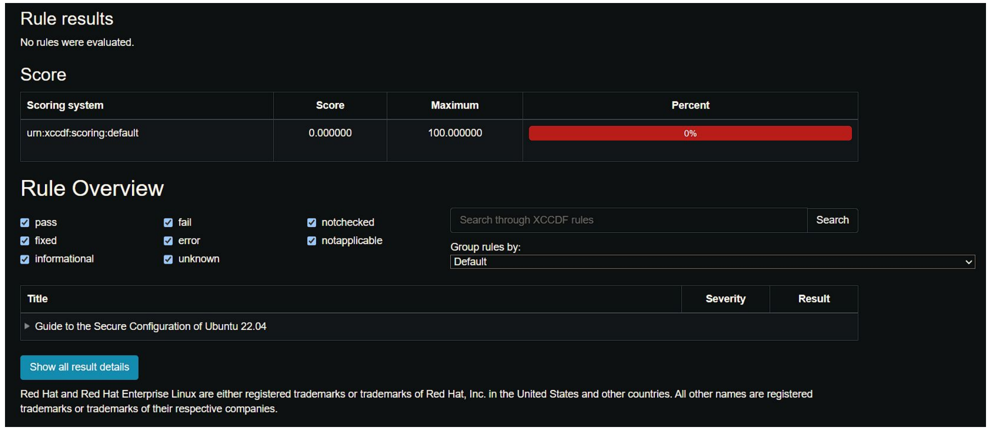
- cpe:/o:canonical:ubuntu_linux:22.04::~~lts~~~

Addresses

IPv4	127.0.0.1
IPv4	192.168.1.34
IPv4	10.0.3.15
IPv4	10.10.1.11
IPv6	0:0:0:0:0:0:0:1
IPv6	2001:df1:eec0:102c:a3a1:6076:45ba:c89d
IPv6	2001:df1:eec0:102c:69d2:42e2:230f:f01
IPv6	fe80:0:0:0:e6fe:59f4:44c0:7bf6
IPv6	fe80:0:0:0:e32c:1746:1de3:9573
IPv6	fe80:0:0:0:414f:d9de:18ee:1785
MAC	00:00:00:00:00:00
MAC	08:00:27:28:B6:E4
MAC	08:00:27:32:2F:20
MAC	08:00:27:DA:F5:25

Compliance and Scoring

There were no failed or uncertain rules. It seems that no action is necessary.



Rule results

No rules were evaluated.

Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	0.000000	100.000000	0%

Rule Overview

☑ pass ☑ fixed ☑ informational
☑ fail ☑ error ☑ unknown
☑ notchecked ☑ notapplicable

Search through XCCDF rules | Search

Group rules by: Default

Title	Severity	Result
▸ Guide to the Secure Configuration of Ubuntu 22.04		

Show all result details

Red Hat and Red Hat Enterprise Linux are either registered trademarks or trademarks of Red Hat, Inc. in the United States and other countries. All other names are registered trademarks or trademarks of their respective companies.

FUTURE ENHANCEMENTS

Vision

Many security policies are readily available online in the form of standardized SCAP checklists. However, a universally applicable security policy does not exist, as each organization has distinct security requirements and operational needs.

To enhance both the capabilities and user experience of the product, additional functionalities can be integrated. These include connecting the portal to an organizational repository or the web, enabling the retrieval of the latest security policies for download and installation on flagged client machines.

Furthermore, remote patch automation can be implemented, allowing seamless installation of security patches across multiple devices. This not only improves security and compliance but also enhances user experience by reducing manual effort, minimizing downtime, and ensuring a more efficient and intuitive patch management process.

- Cross-Platform Support: Improve compatibility for both Windows and Linux environments
- Advanced Threat Detection: Integrate AI for detecting intrusion and threats.
- Option to manage - Scheduled Scans & Alerts – configurable by Admin
- More In-Depth Scanning and Report Generation
- Email/Slack/SMS Notifications and reports
- System Telemetry, Graphical Data Visualization for quick overview and issue flagging.
- Role-based access for teams.
- Data Aggregation Enhancements.

Conclusion

Cyber Edge

ANY QUESTIONS?

THANK YOU

CYBER EDGE