LibreOffice Conf.
Asia
UbuCon Asia 2023

Surakarta | October, 8th 2023

UBUNTU SECURITY BEST PRACTICE

LERN HOW TO IMPLEMENT SECURITY ON LINUX

Yusuf Hadiwinata Sutandar
yusuf@biznetgio.com

https://www.biznetgio.com
https://louca.id

Yusuf Hadiwinata S.

Linux Geek, Opensource Enthusiast, Security Hobbies

RHCT, RHCSAv5-v7, RHCEv5-v7, RHCVA, RHCI, RHCX, RHCSA-RHOS, RHCJA, CEI, CEH, CHFI, CND, EDRP, CCNA, MCTCNA, Security+, Network+, VCA, vExpert 2017-2018

Vice President Operation & Services – PT Biznet Gio Nusantara

CYBER SECURITY 101

1

An Introduction about Cyber Security Perimeter in general

LINUX SECURITY

2

Learn more about security Principal on Linux Operating System

HARDENING

3

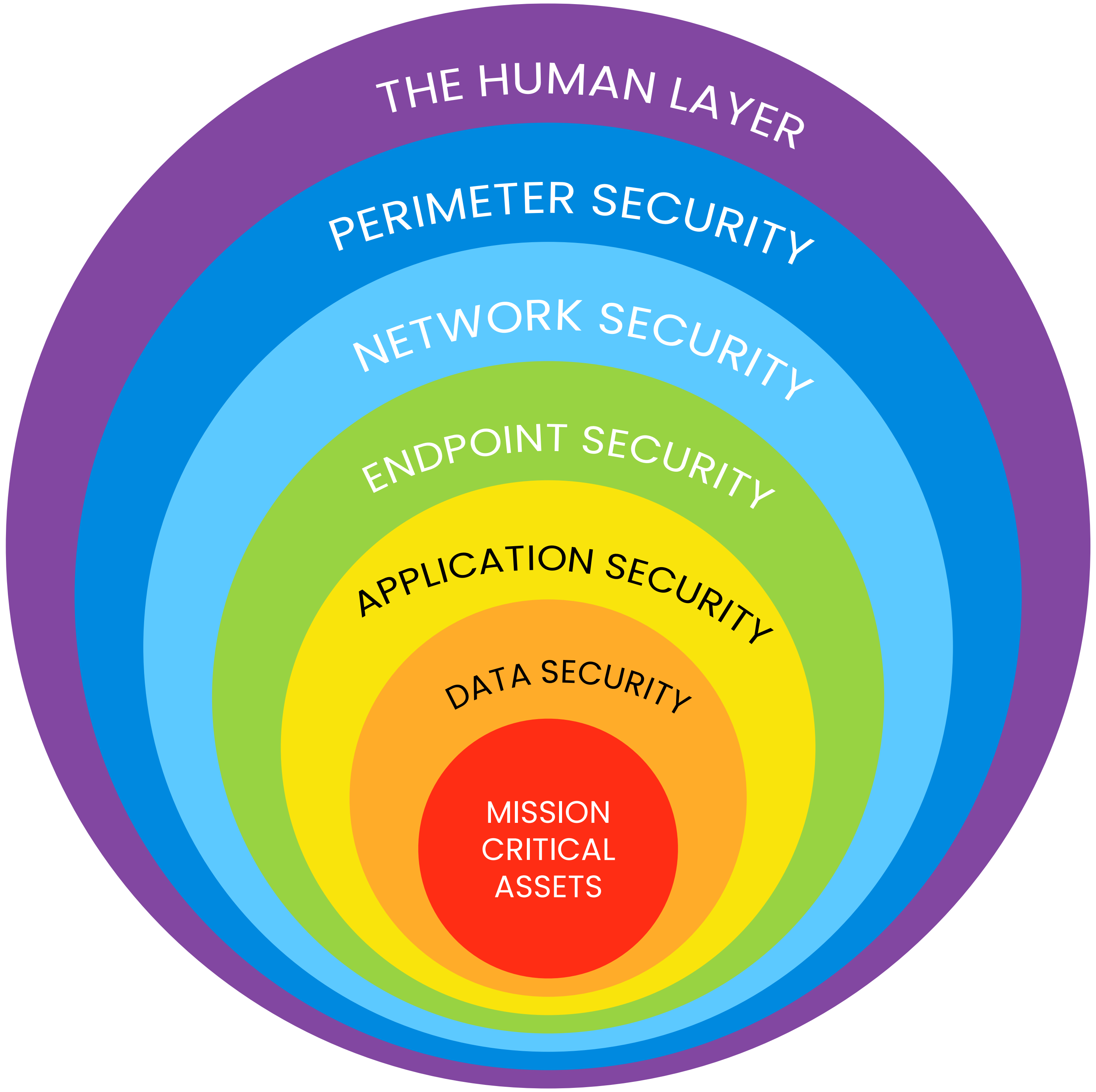
Deep dive learn about security implementation on Ubuntu Operating System

Q & A

4

Ask a question and win merchandize from Biznet Gio

CYBER SECURITY 101



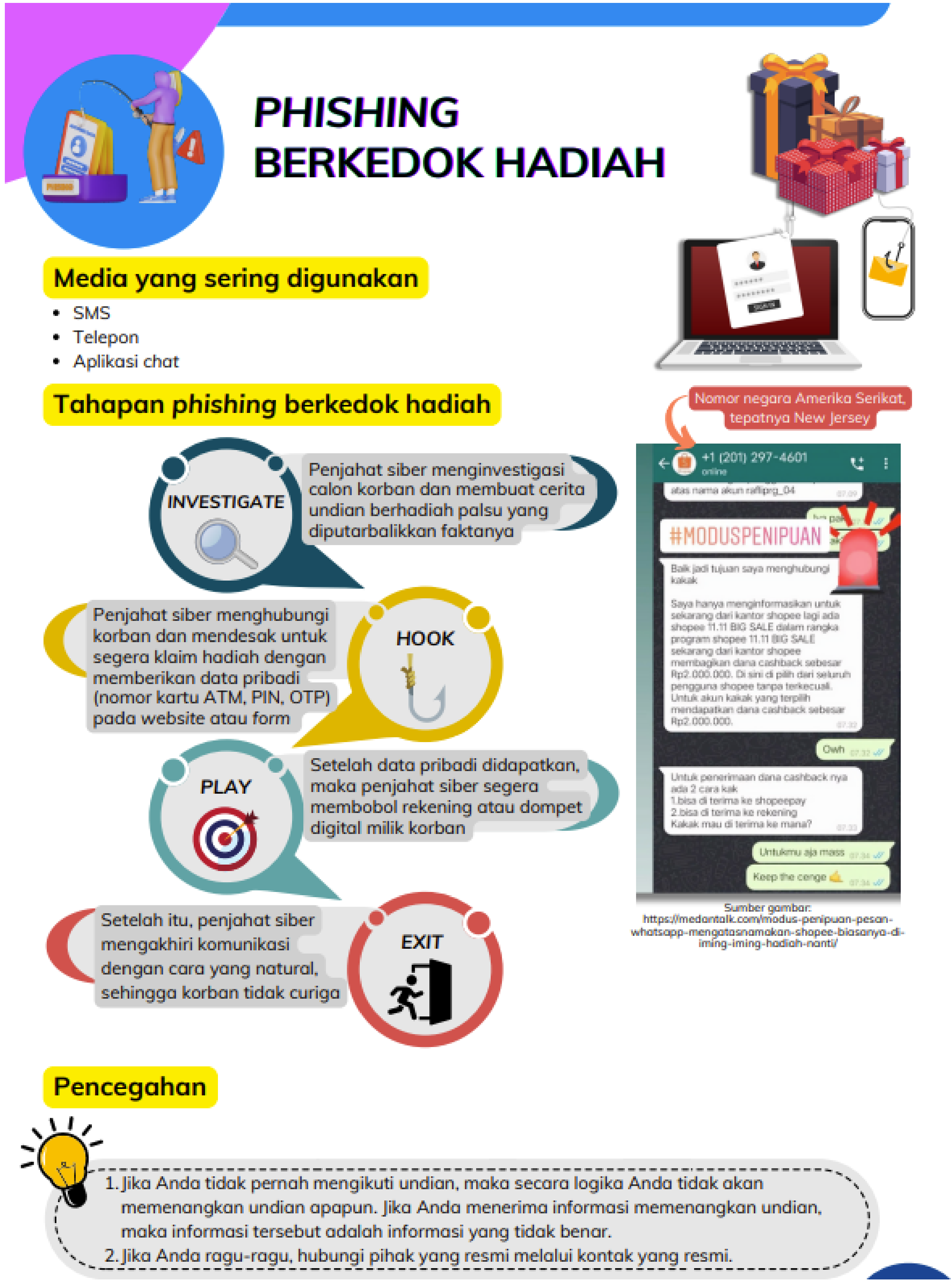
1. Human Layer: Training
2. Perimeter: Firewalls, Spamfilters, Instrusion Detection / Prevention
3. Network: Secure Design & Topology, VLANs, Multi-Layer Firewalls/Switchers
4. Endpoint: Anti-virus, Software Firewalls, Breach Detection Agents
5. Application: Patching, Updates
6. Data: Encryption at rest and in motion
7. Mission Critical: Backups, Response and Recovery Plans

1

Human Layer: Training

Security awareness training is a **strategy used by IT and security professionals** to prevent and mitigate user risk. These programs are designed **to help users and employees understand the role** they play in helping to combat information security breaches.

Ex: Certified Secure Computer User (CSCU)



PHISHING BERKEDOK HADIAH

Media yang sering digunakan

- SMS
- Telepon
- Aplikasi chat

Tahapan *phishing* berkedok hadiah

INVESTIGATE: Penjahat siber menginvestigasi calon korban dan membuat cerita undian berhadiah palsu yang diputarbalikkan faktanya

HOOK: Penjahat siber menghubungi korban dan mendesak untuk segera klaim hadiah dengan memberikan data pribadi (nomor kartu ATM, PIN, OTP) pada website atau form

PLAY: Setelah data pribadi didapatkan, maka penjahat siber segera membobol rekening atau dompet digital milik korban

EXIT: Setelah itu, penjahat siber mengakhiri komunikasi dengan cara yang natural, sehingga korban tidak curiga

Nomor negara Amerika Serikat, tepatnya New Jersey

+1 (201) 297-4601
online

atas nama akun rafliprg_04

#MODUSPENIPUAN

Baik jadi tujuan saya menghubungi kakak

Saya hanya menginformasikan untuk sekarang dari kantor shopee lagi ada shopee 11.11 BIG SALE dalam rangka program shopee 11.11 BIG SALE sekarang dari kantor shopee membagikan dana cashback sebesar Rp2.000.000. Di sini di pilih dari seluruh pengguna shopee tanpa terkecuali. Untuk akun kakak yang terpilih mendapatkan dana cashback sebesar Rp2.000.000.

Owh

Untuk penerimaan dana cashback nya ada 2 cara kak
1.bisa di terima ke shopeepay
2.bisa di terima ke rekening
Kakak mau di terima ke mana?

Untukmu aja mass

Keep the cenge 👍

Sumber gambar: https://medantalk.com/modus-penipuan-pesan-whatsapp-mengatasnamakan-shopee-biasanya-di-iming-iming-hadiah-nanti/

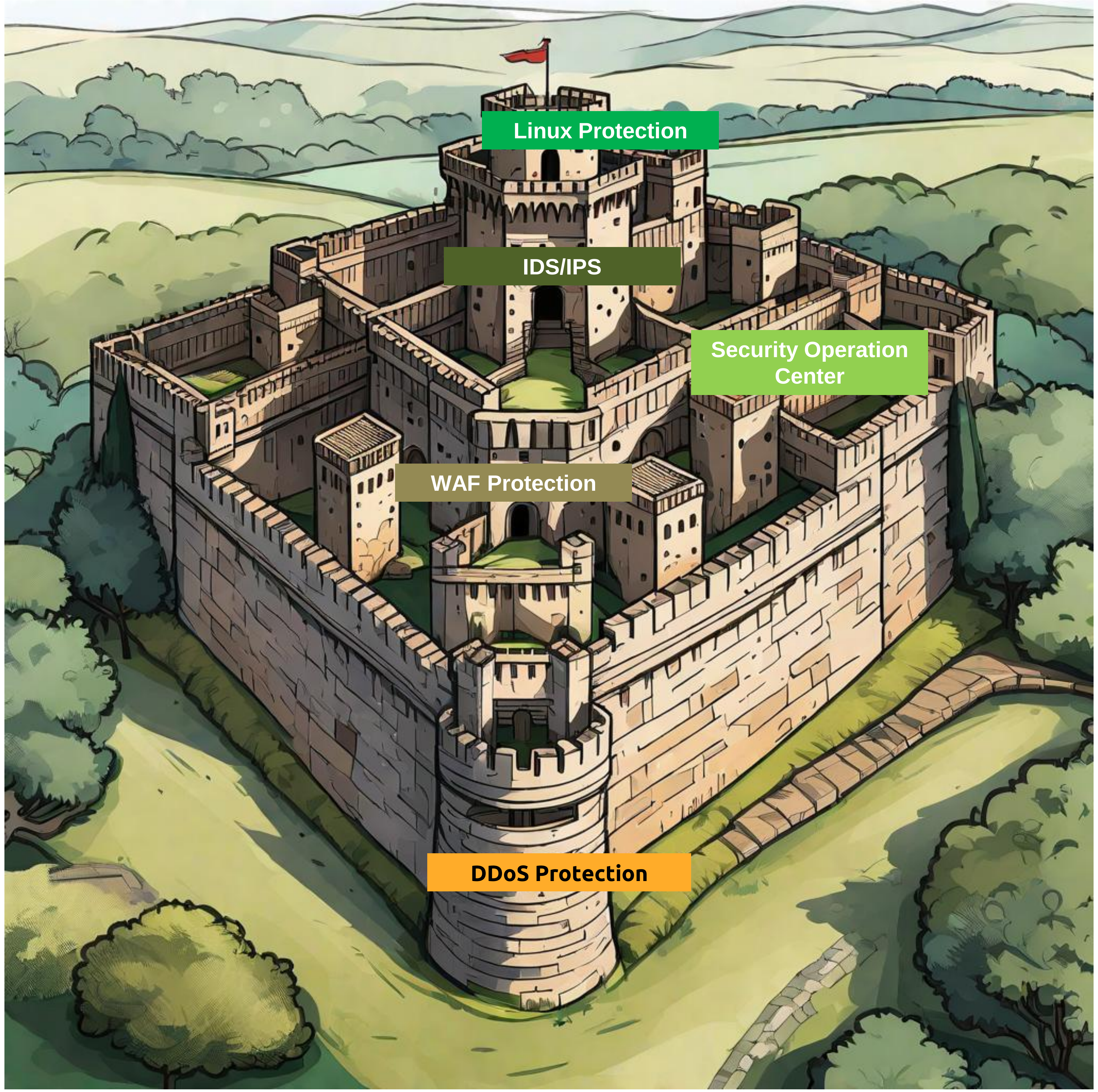
Pencegahan

1. Jika Anda tidak pernah mengikuti undian, maka secara logika Anda tidak akan memenangkan undian apapun. Jika Anda menerima informasi memenangkan undian, maka informasi tersebut adalah informasi yang tidak benar.
2. Jika Anda ragu-ragu, hubungi pihak yang resmi melalui kontak yang resmi.

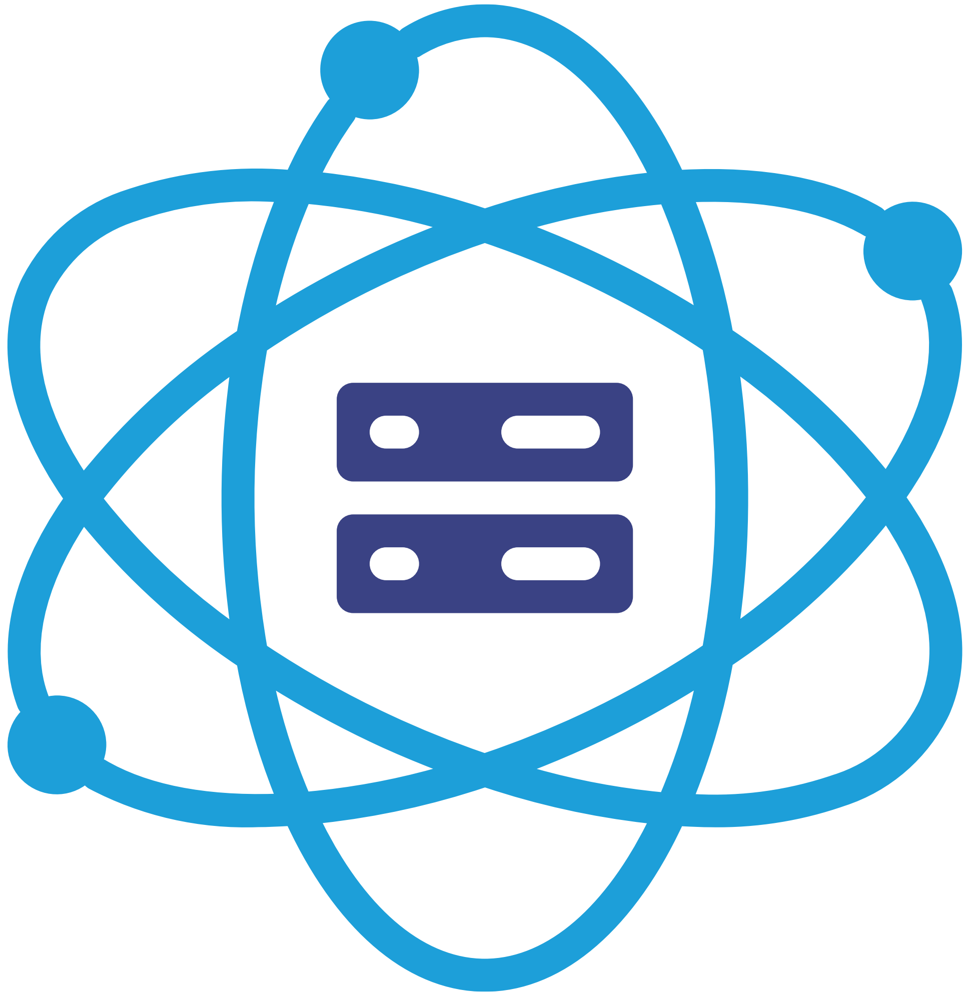
2

Perimeter: Firewalls, Spamfilter, Intrusion Detection/Prevention, WAF, etc

The perimeter layer stops most attackers.
It stops the spam, the petty thief, the automatic scanning tools ran by anonymous curious cats



LINUX SECURITY



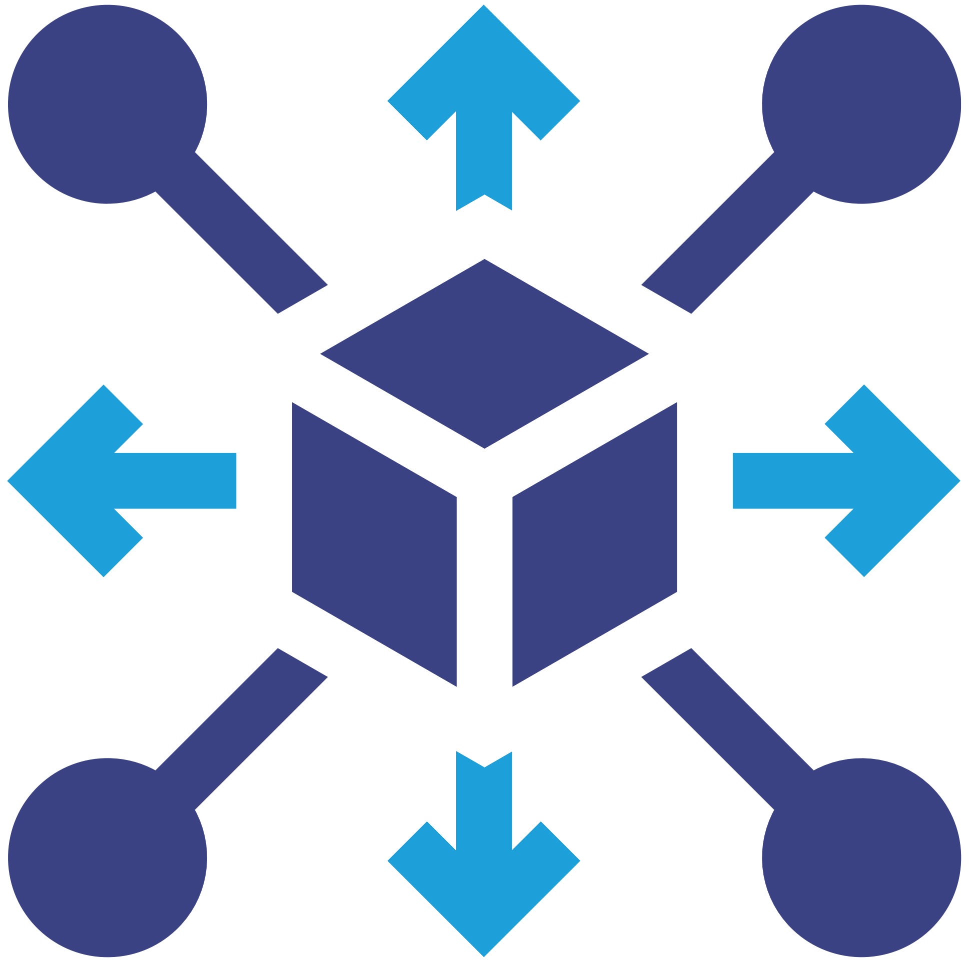
Know your system(s)

The first principle is about knowing what your system is supposed to do.
What is its primary role, what software packages does it need and who needs access?

Security Measures:

- Password policy
- Proper software patch management
- Configuration management
- Documentation

LINUX SECURITY



Least Amount of Privilege

Each process running, or package installed, might become a target. Security professionals call this the **“attack surface”**.
What you want is to minimize this attack surface by removing unneeded components, limit access and by default use a “deny unless” strategy.

Security Measures:

- Use minimal/basic installation
- Only allow access to people who really need it

LINUX SECURITY

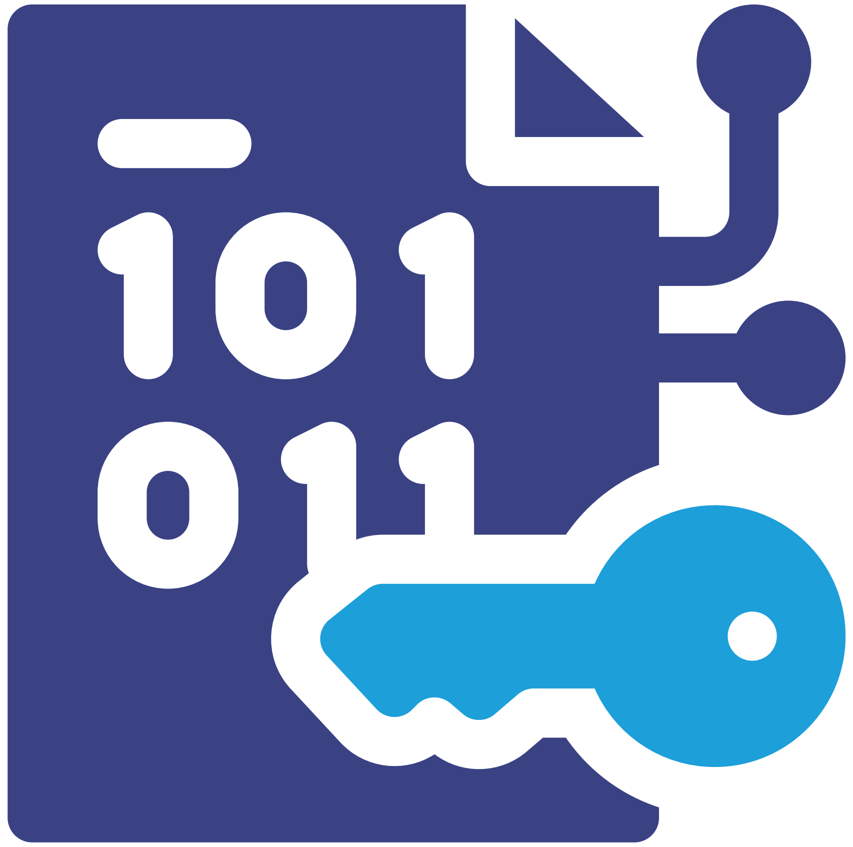
Perform Defense in Depth

Protect the system by applying several layers of security. This principle is named **“defense in depth”** and can be compared with an onion: to get to the core, you have to peel of **layer by layer.**
One broken defense might help us protect against full compromise.

Security Measures:

- IPtables / Nftables
- Hardening of software components

LINUX SECURITY



Protection is Key, Detection is a Must

Security focuses on the protection of assets. While this is a primary objective, we should consider that one day our defenses are broken.
Therefore we want to know this as soon as possible, so we can properly act. This is where principle 3 and 4 both are linked. **Set-up proper detection methods, similar to the trip wires used by the military.**

Security Measures:
- Linux audit framework
- Remote Logging
- Create backups and test them

LINUX SECURITY

Know your Enemy

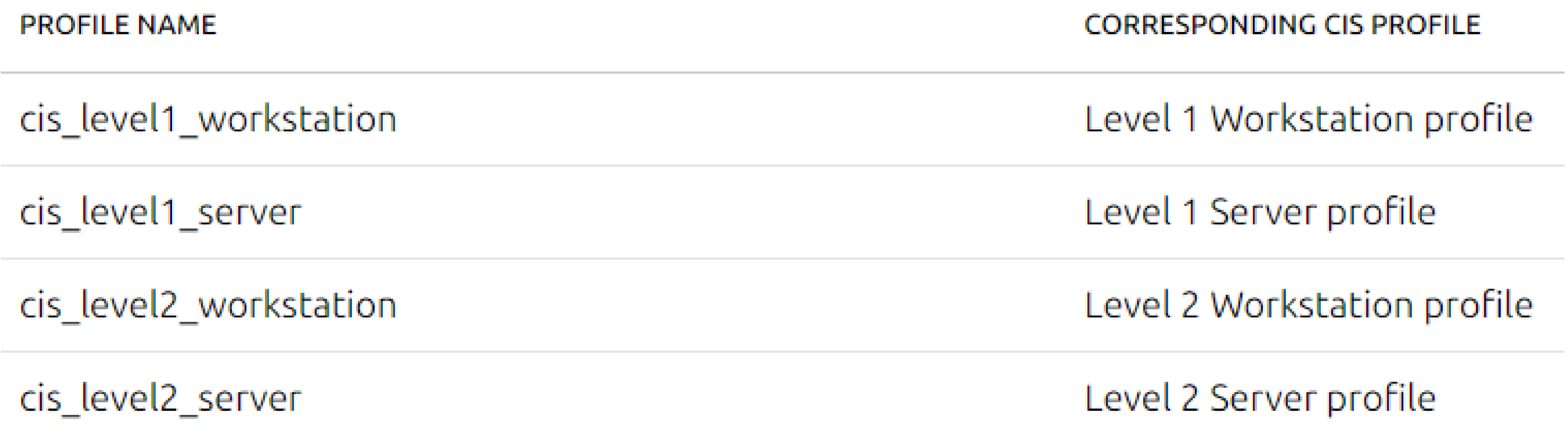
You can only protect a system the right way.
If you know what threats you are facing.
Why would this system be a target and who would be targeting it?
Perform a risk analysis and determine what potential threats your system might endure.

CIS HARDENING

CIS compliance with Ubuntu Pro Plan

Ubuntu contains native tooling to automate compliance and auditing with the Center for Internet Security (CIS) benchmarks.
The Center for Internet Security (CIS), develops the CIS benchmark documents for Ubuntu LTS releases. As these documents contain a large number of hardening rules, compliance and auditing can be very efficient when using the Ubuntu native tooling that is **available to subscribers of Ubuntu Pro.**

With Ubuntu 20.04 we introduce the **Ubuntu Security Guide (USG)** an easy to use tool **for compliance and auditing that replaces our older tooling**. See the following sections for more information.



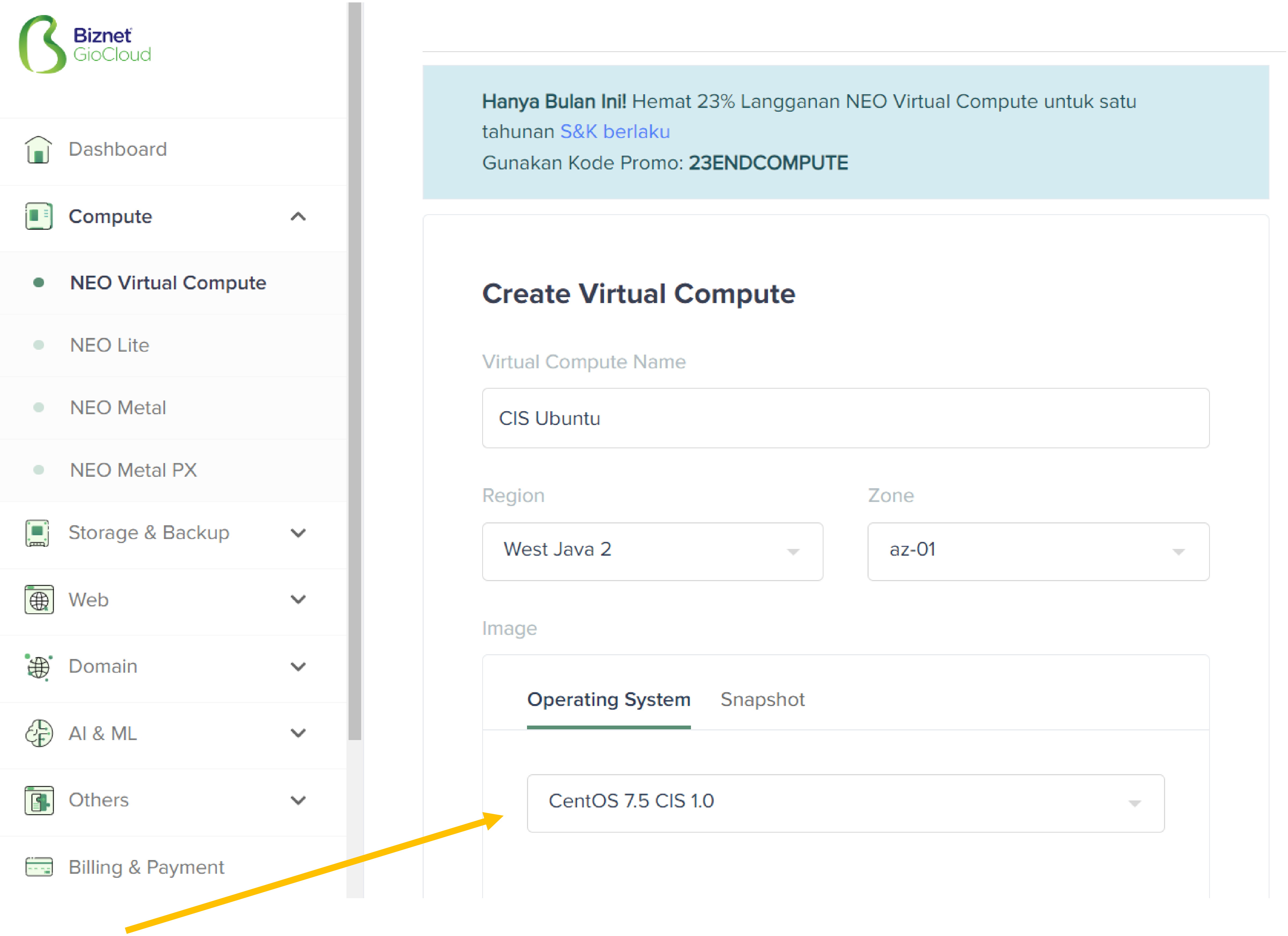
PROFILE NAME	CORRESPONDING CIS PROFILE
cis_level1_workstation	Level 1 Workstation profile
cis_level1_server	Level 1 Server profile
cis_level2_workstation	Level 2 Workstation profile
cis_level2_server	Level 2 Server profile

https://ubuntu.com/security/certifications/docs/usg/cis
https://ubuntu.com/security/certifications/docs/usg/cis/compliance
https://github.com/francsw/ubuntu2204_cis

CIS HARDENING

Use Cloud Provider CIS Image

Many cloud provider like Biznet Gio Cloud provide CIS Hardened image, this is the easy way to use Secure Image in the Cloud Environment



Hanya Bulan Ini! Hemat 23% Langganan NEO Virtual Compute untuk satu tahunan S&K berlaku
Gunakan Kode Promo: **23ENDCOMPUTE**

Create Virtual Compute

Virtual Compute Name: CIS Ubuntu

Region: West Java 2

Zone: az-01

Image: CentOS 7.5 CIS 1.0

CIS HARDENING

CIS Ubuntu Linux 22.04 LTS Benchmark

CIS Benchmarks focus on technical configuration settings used **to maintain and/or increase the security of the addressed technology,** and they should be used in conjunction with other essential cyber hygiene tasks like:

- Monitoring the base operating system for vulnerabilities and quickly updating with the latest security patches
- Monitoring applications and libraries for vulnerabilities and quickly updating with the latest security patches

At the CIS Benchmarks are designed as a key component of a comprehensive cybersecurity program.

CIS HARDENING

CIS Ubuntu Linux 22.04 LTS Benchmark

Initial Setup	**Items in this section are advised for all systems,** but may be difficult or require extensive preparation after the initial setup of the system
Services	While applying system updates and patches helps correct known vulnerabilities, one of the best ways to protect the system against as yet unreported vulnerabilities is to **disable all services that are not required for normal system operation**

CIS HARDENING

CIS Ubuntu Linux 22.04 LTS Benchmark

Networking Configuration	This section **provides guidance** on for securing the network configuration of the system through kernel parameters, access list control, and firewall settings
Access	**Authentication and Authorization**
System Maintenance	Recommendations in this section are intended as **maintenance and are intended to be checked** on a frequent basis to ensure system stability

CIS HARDENING

CIS CAS Lite (free version)

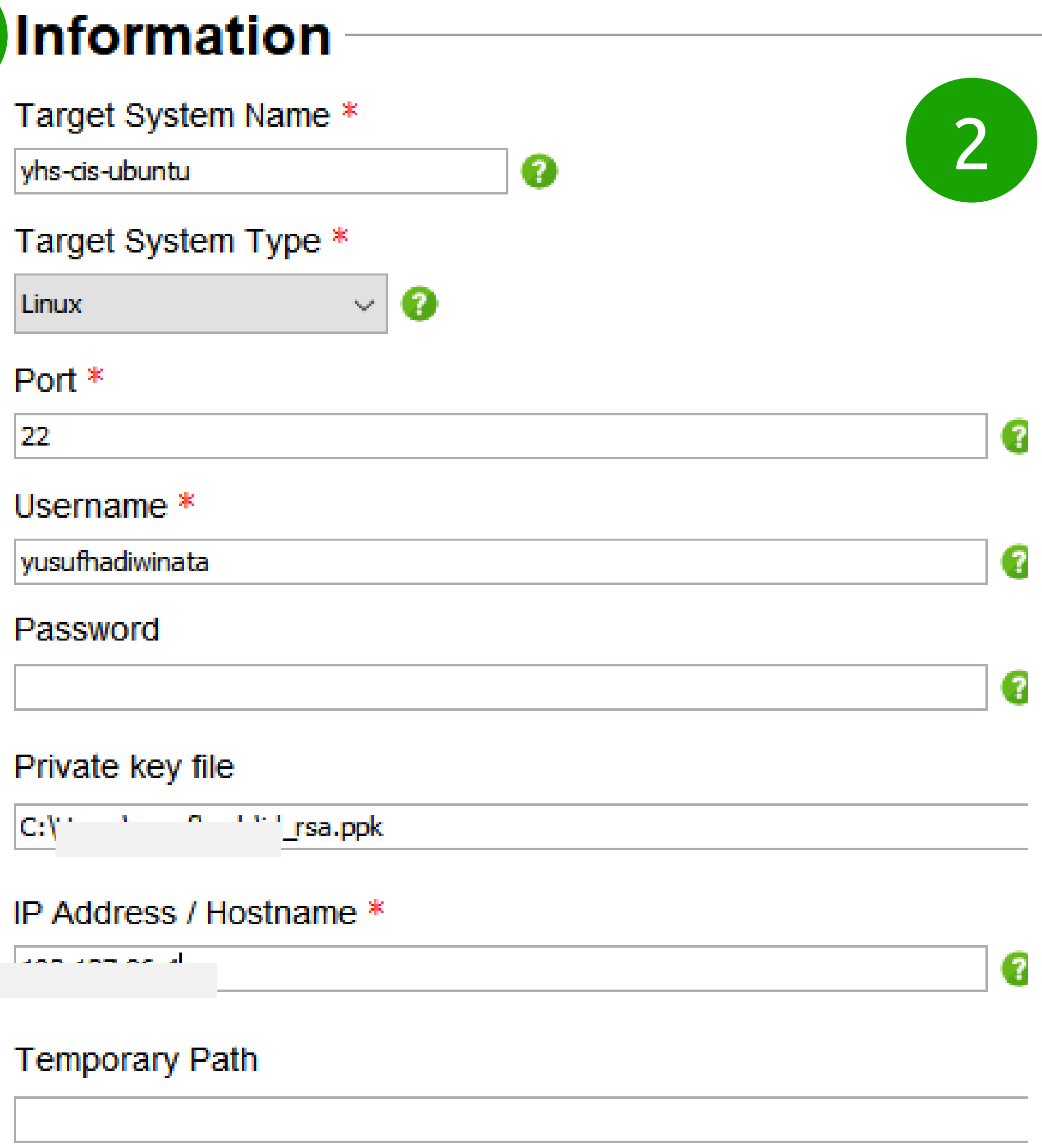
CIS-CAT Lite is the free **assessment tool developed by the CIS** (Center for Internet Security, Inc.).
CIS-CAT Lite helps users implement secure configurations for multiple technologies. With unlimited scans available via CIS-CAT Lite.

With CIS-CAT Lite, We Can Easily:

- Instantly check your systems against CIS Benchmarks.
- Receive a compliance score 1-100.
- Follow remediation steps to improve your security.

CIS HARDENING

CIS CAS Lite (free version)



1

Information

Target System Name *

yhs-cis-ubuntu

Target System Type *

Linux

Port *

22

Username *

yusufhadiwinata

Password

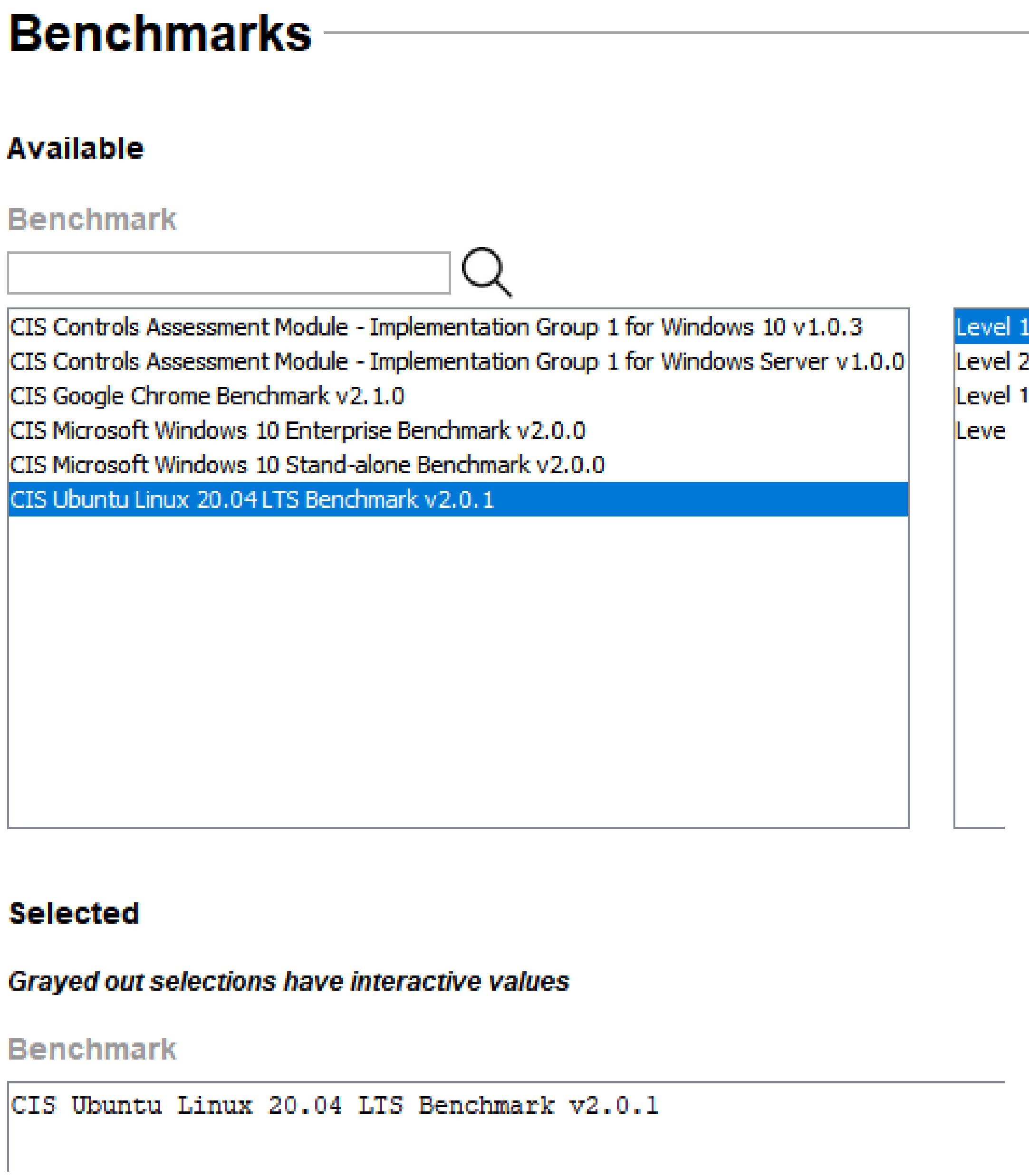
Private key file

C:\[redacted]_rsa.ppk

IP Address / Hostname *

[redacted]

Temporary Path



2

Benchmarks

Available

Benchmark

CIS Controls Assessment Module - Implementation Group 1 for Windows 10 v1.0.3
CIS Controls Assessment Module - Implementation Group 1 for Windows Server v1.0.0
CIS Google Chrome Benchmark v2.1.0
CIS Microsoft Windows 10 Enterprise Benchmark v2.0.0
CIS Microsoft Windows 10 Stand-alone Benchmark v2.0.0
CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.1

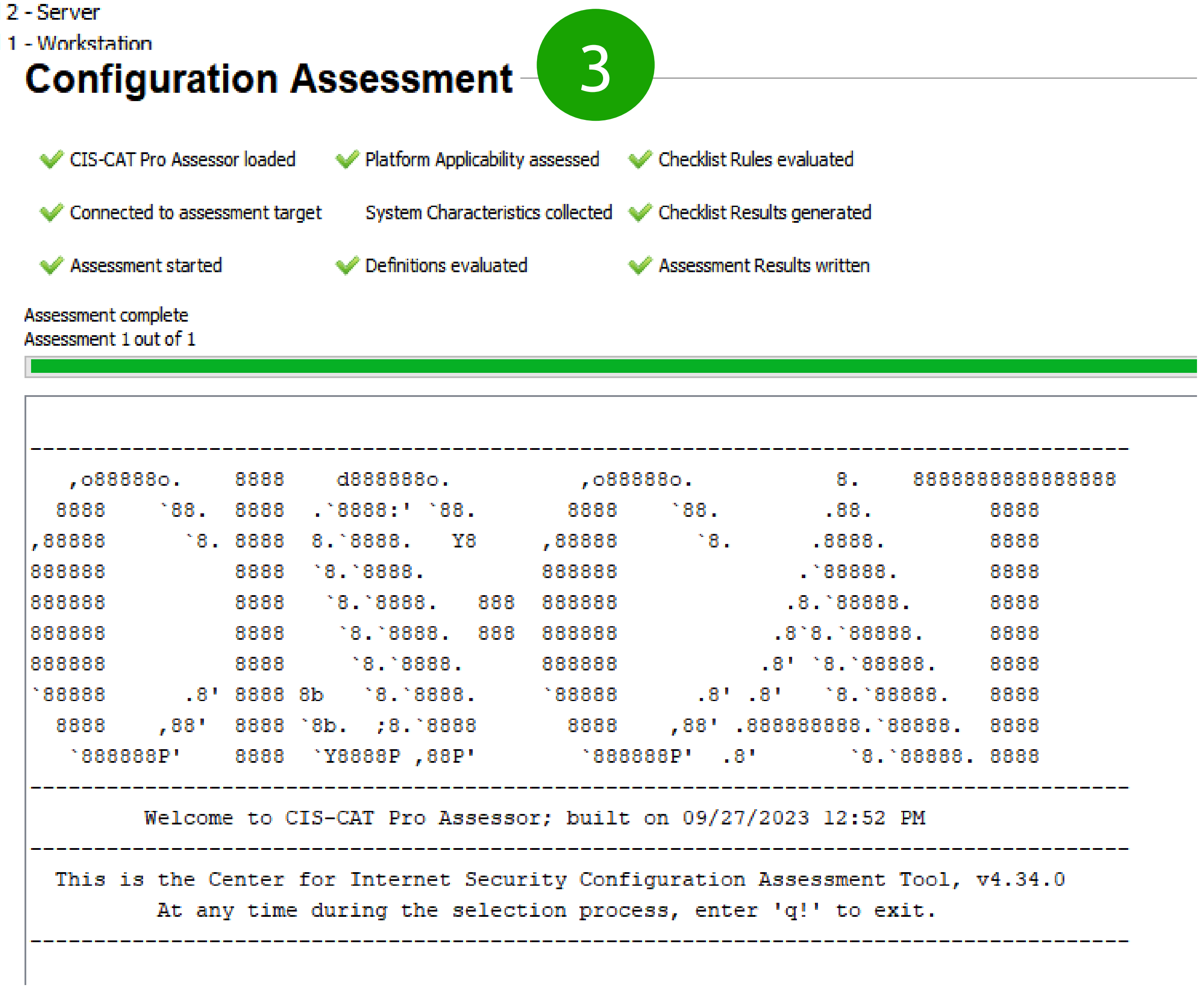
Level 1 - Server
Level 2 - Server
Level 1 - Workstation
Leve

Selected

Grayed out selections have interactive values

Benchmark

CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.1



Configuration Assessment

3

✓ CIS-CAT Pro Assessor loaded
✓ Connected to assessment target
✓ Assessment started
✓ Platform Applicability assessed
System Characteristics collected
✓ Definitions evaluated
✓ Checklist Rules evaluated
✓ Checklist Results generated
✓ Assessment Results written

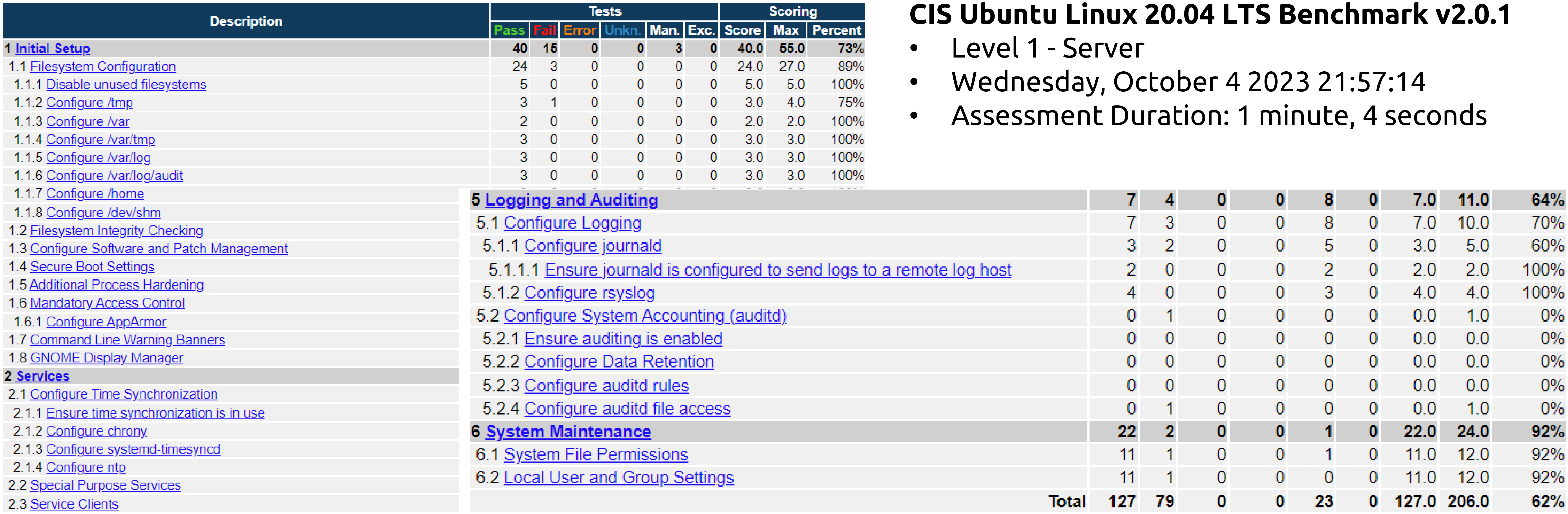
Assessment complete
Assessment 1 out of 1

```
----------------------------------------------------------------------------------------
   ,o88888o.    8888     d888888o.          ,o88888o.            8.    8888888888888888
  8888    `88.  8888   .`8888:' `88.       8888     `88.        .88.         8888
,88888      `8. 8888   8.`8888.   Y8     ,88888       `8.      .8888.        8888
888888          8888   `8.`8888.         888888               .`88888.       8888
888888          8888    `8.`8888.   888  888888              .8.`88888.      8888
888888          8888     `8.`8888.  888  888888             .8`8.`88888.     8888
888888          8888      `8.`8888.      888888            .8' `8.`88888.    8888
`88888      .8' 8888 8b    `8.`8888.     `88888       .8' .8'   `8.`88888.   8888
  8888    ,88'  8888 `8b.   ;8.`8888       8888     ,88' .888888888.`88888.  8888
   `888888P'    8888   `Y8888P ,88P'        `888888P'   .8'       `8.`88888. 8888
----------------------------------------------------------------------------------------
         Welcome to CIS-CAT Pro Assessor; built on 09/27/2023 12:52 PM
----------------------------------------------------------------------------------------
  This is the Center for Internet Security Configuration Assessment Tool, v4.34.0
          At any time during the selection process, enter 'q!' to exit.
----------------------------------------------------------------------------------------
```

CIS HARDENING

CIS CAS Lite (free version)

Summary :



Description	Tests						Scoring		
	Pass	Fail	Error	Unkn.	Man.	Exc.	Score	Max	Percent
1 Initial Setup	**40**	**15**	**0**	**0**	**3**	**0**	**40.0**	**55.0**	**73%**
1.1 Filesystem Configuration	24	3	0	0	0	0	24.0	27.0	89%
1.1.1 Disable unused filesystems	5	0	0	0	0	0	5.0	5.0	100%
1.1.2 Configure /tmp	3	1	0	0	0	0	3.0	4.0	75%
1.1.3 Configure /var	2	0	0	0	0	0	2.0	2.0	100%
1.1.4 Configure /var/tmp	3	0	0	0	0	0	3.0	3.0	100%
1.1.5 Configure /var/log	3	0	0	0	0	0	3.0	3.0	100%
1.1.6 Configure /var/log/audit	3	0	0	0	0	0	3.0	3.0	100%
1.1.7 Configure /home									
1.1.8 Configure /dev/shm									
1.2 Filesystem Integrity Checking									
1.3 Configure Software and Patch Management									
1.4 Secure Boot Settings									
1.5 Additional Process Hardening									
1.6 Mandatory Access Control									
1.6.1 Configure AppArmor									
1.7 Command Line Warning Banners									
1.8 GNOME Display Manager									
2 Services									
2.1 Configure Time Synchronization									
2.1.1 Ensure time synchronization is in use									
2.1.2 Configure chrony									
2.1.3 Configure systemd-timesyncd									
2.1.4 Configure ntp									
2.2 Special Purpose Services									
2.3 Service Clients									

5 Logging and Auditing	**7**	**4**	**0**	**0**	**8**	**0**	**7.0**	**11.0**	**64%**
5.1 Configure Logging	7	3	0	0	8	0	7.0	10.0	70%
5.1.1 Configure journald	3	2	0	0	5	0	3.0	5.0	60%
5.1.1.1 Ensure journald is configured to send logs to a remote log host	2	0	0	0	2	0	2.0	2.0	100%
5.1.2 Configure rsyslog	4	0	0	0	3	0	4.0	4.0	100%
5.2 Configure System Accounting (auditd)	0	1	0	0	0	0	0.0	1.0	0%
5.2.1 Ensure auditing is enabled	0	0	0	0	0	0	0.0	0.0	0%
5.2.2 Configure Data Retention	0	0	0	0	0	0	0.0	0.0	0%
5.2.3 Configure auditd rules	0	0	0	0	0	0	0.0	0.0	0%
5.2.4 Configure auditd file access	0	1	0	0	0	0	0.0	1.0	0%
6 System Maintenance	**22**	**2**	**0**	**0**	**1**	**0**	**22.0**	**24.0**	**92%**
6.1 System File Permissions	11	1	0	0	1	0	11.0	12.0	92%
6.2 Local User and Group Settings	11	1	0	0	0	0	11.0	12.0	92%
Total	**127**	**79**	**0**	**0**	**23**	**0**	**127.0**	**206.0**	**62%**

Note: Actual scores are subject to rounding errors. The sum of these values may not result in the exact overall score.

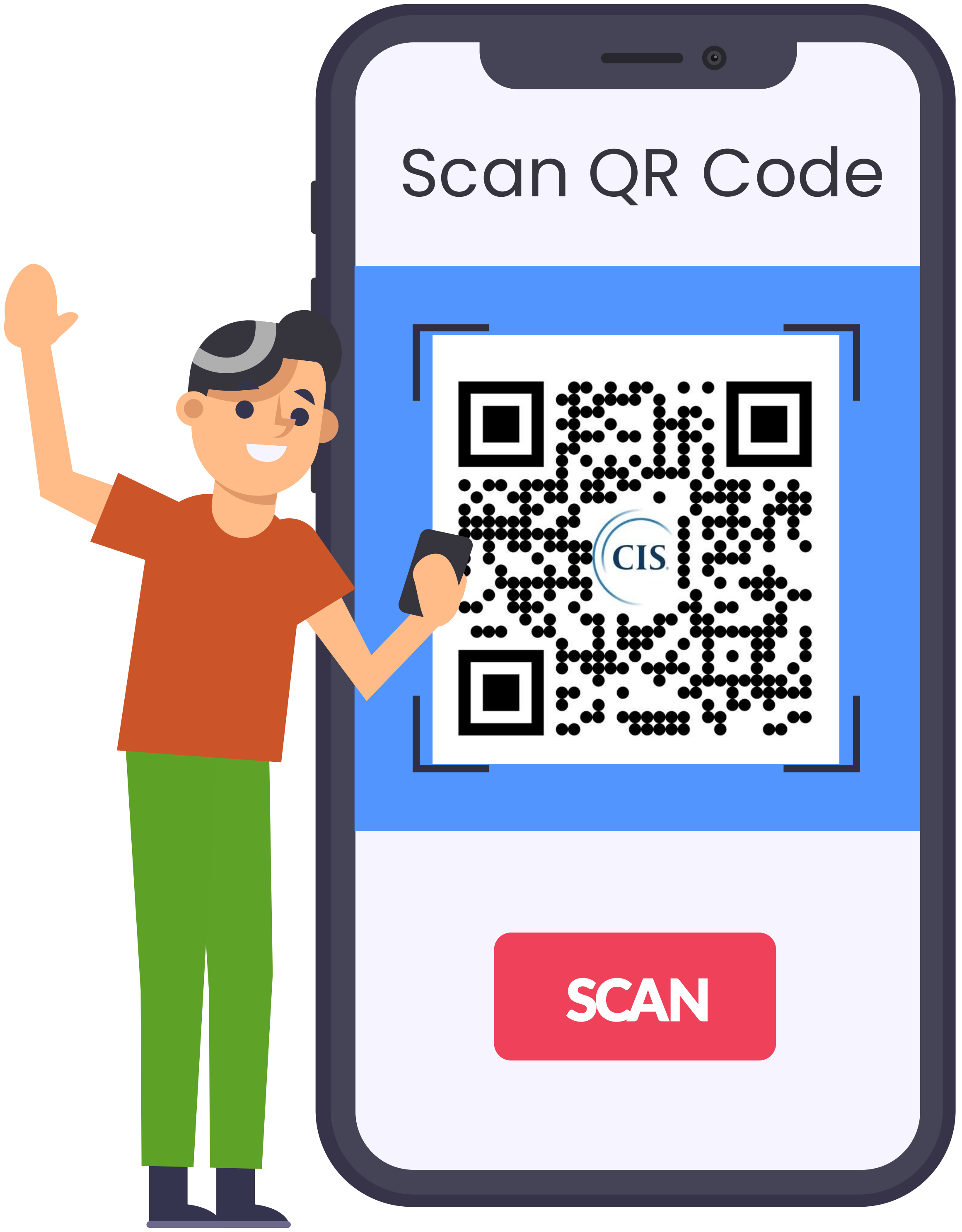
The 'Exc' column only applies to Exceptions that are generated using CIS-CAT Pro Dashboard and is not utilized by CIS-CAT Pro Assessor.

CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.1

- Level 1 - Server
- Wednesday, October 4 2023 21:57:14
- Assessment Duration: 1 minute, 4 seconds

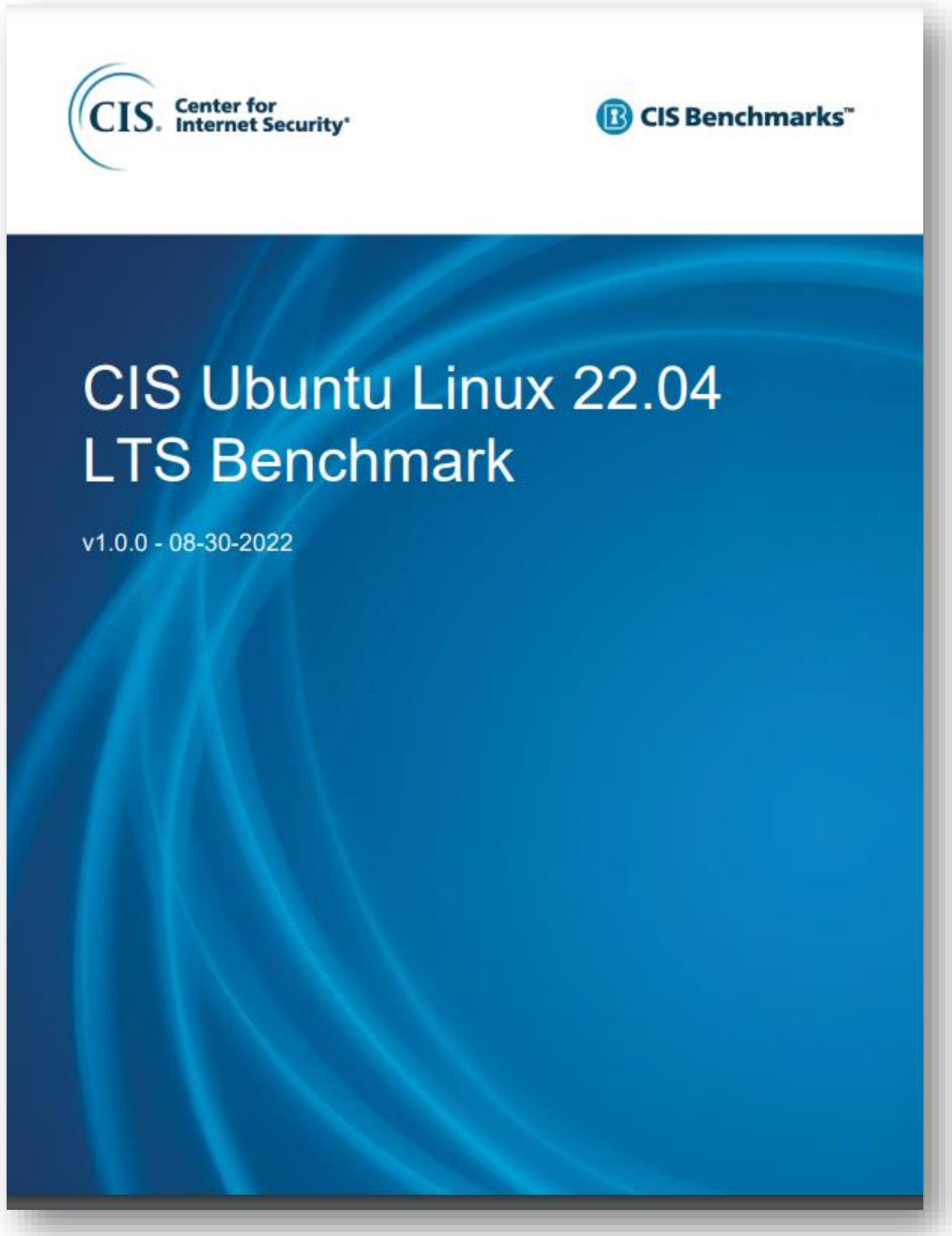
yhs-cis-ubuntu-CIS_Ubuntu_Linux_20.04_LTS_Benchmark-20231004T215819Z.html

CIS HARDENING DOC



CIS Ubuntu Linux 22.04 LTS Ben

UBUNTU HARDENING

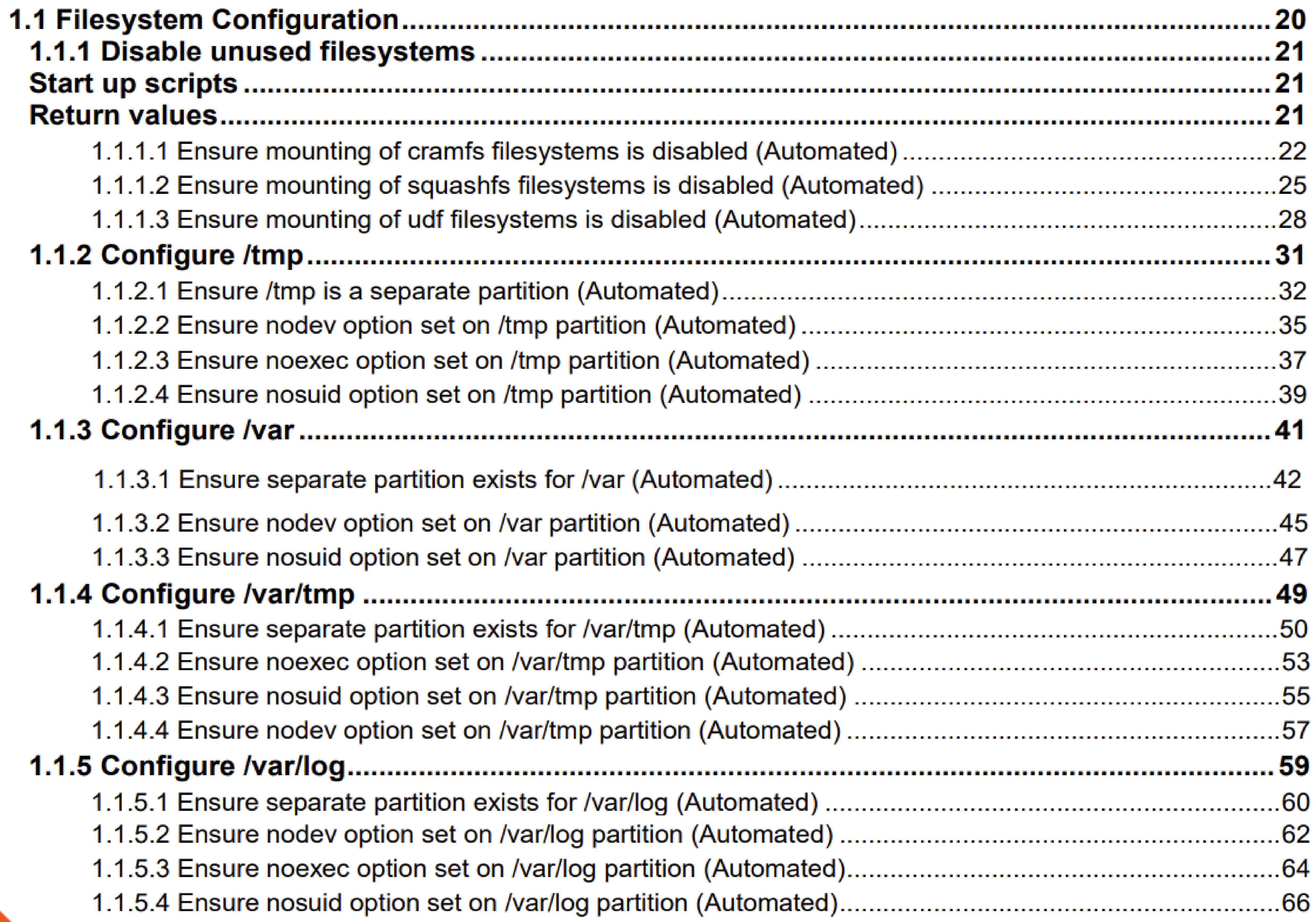


CIS Center for Internet Security

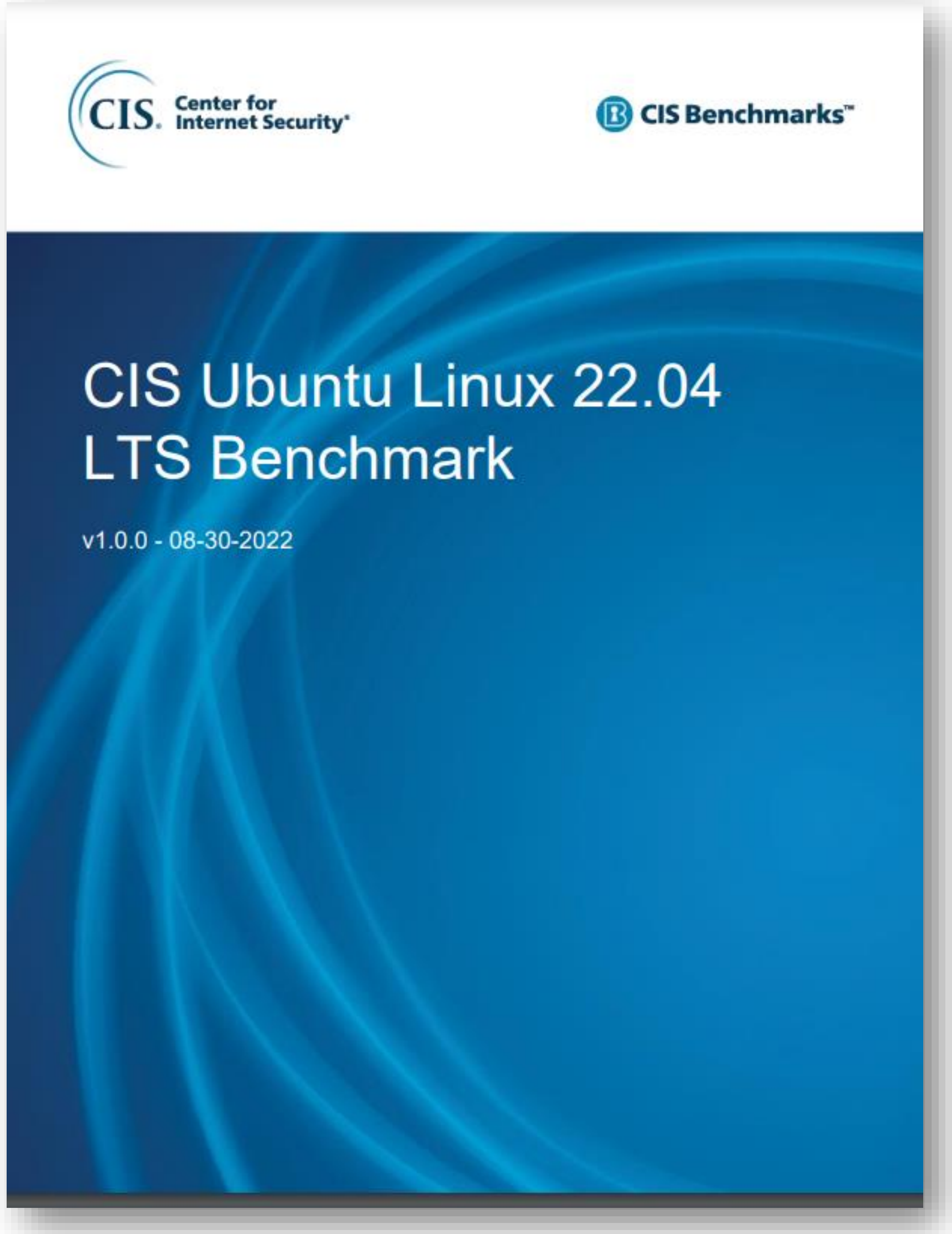
CIS Benchmarks

CIS Ubuntu Linux 22.04
LTS Benchmark

v1.0.0 - 08-30-2022



UBUNTU HARDENING

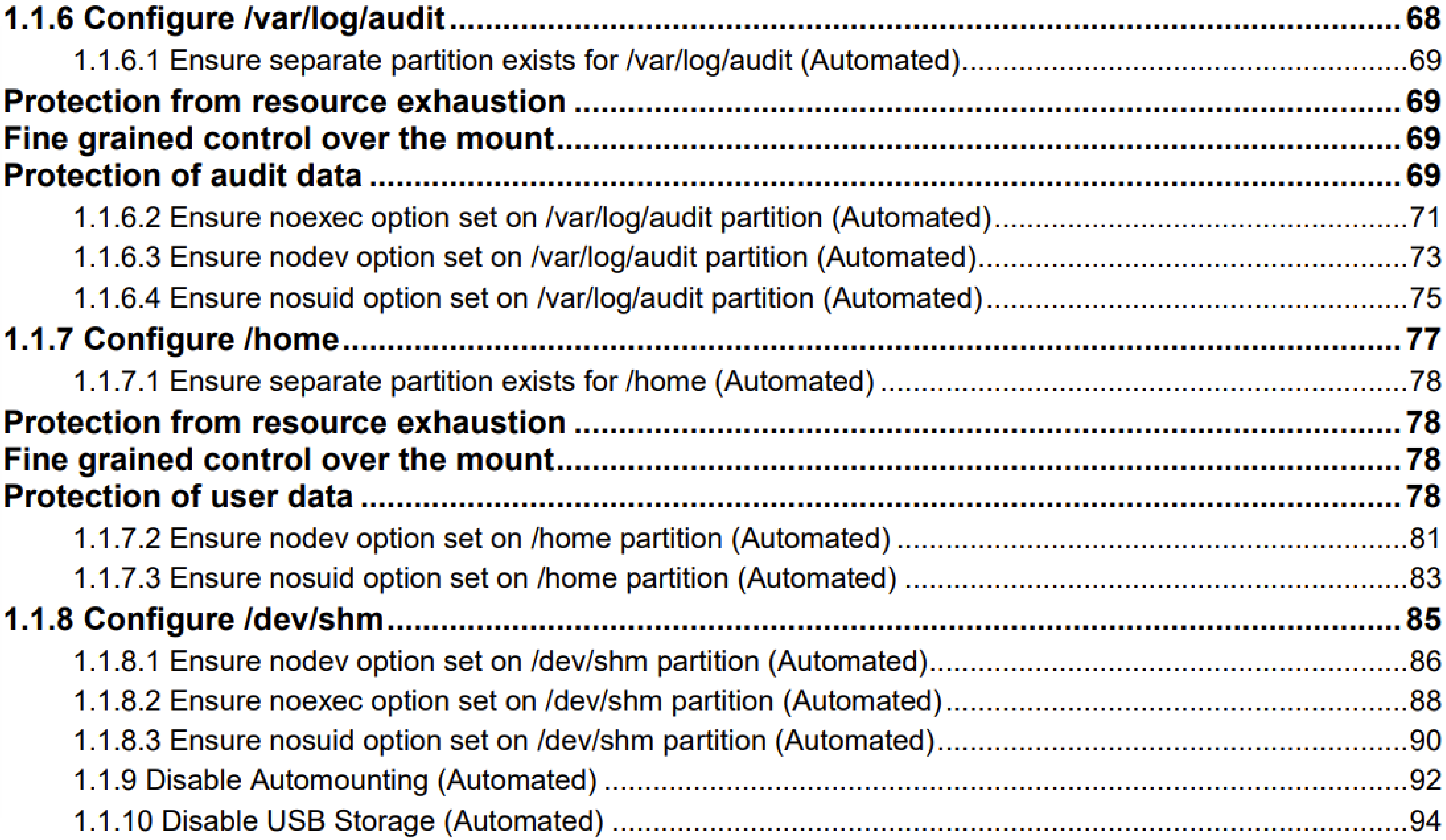


CIS. Center for Internet Security®

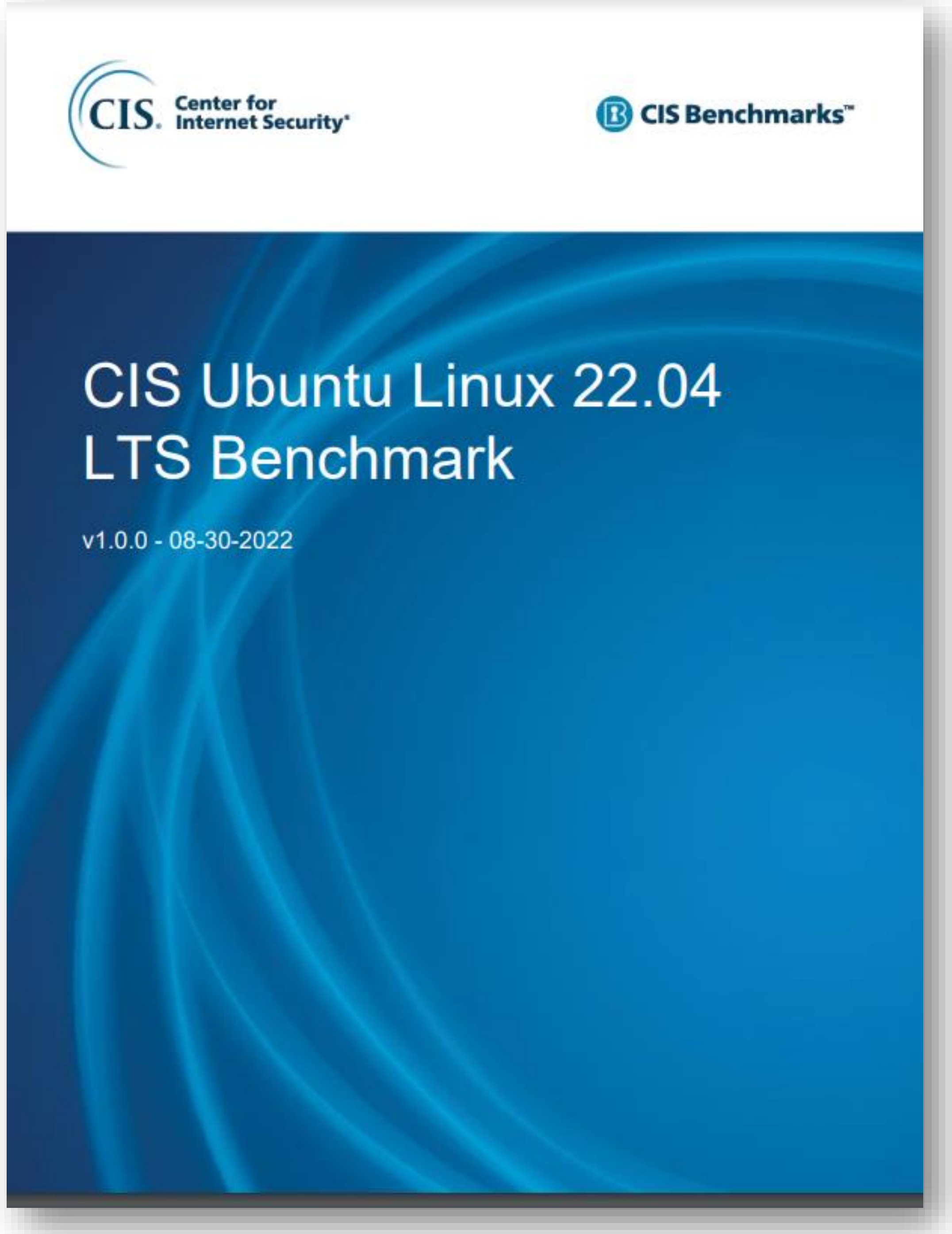
CIS Benchmarks™

CIS Ubuntu Linux 22.04
LTS Benchmark

v1.0.0 - 08-30-2022



UBUNTU HARDENING

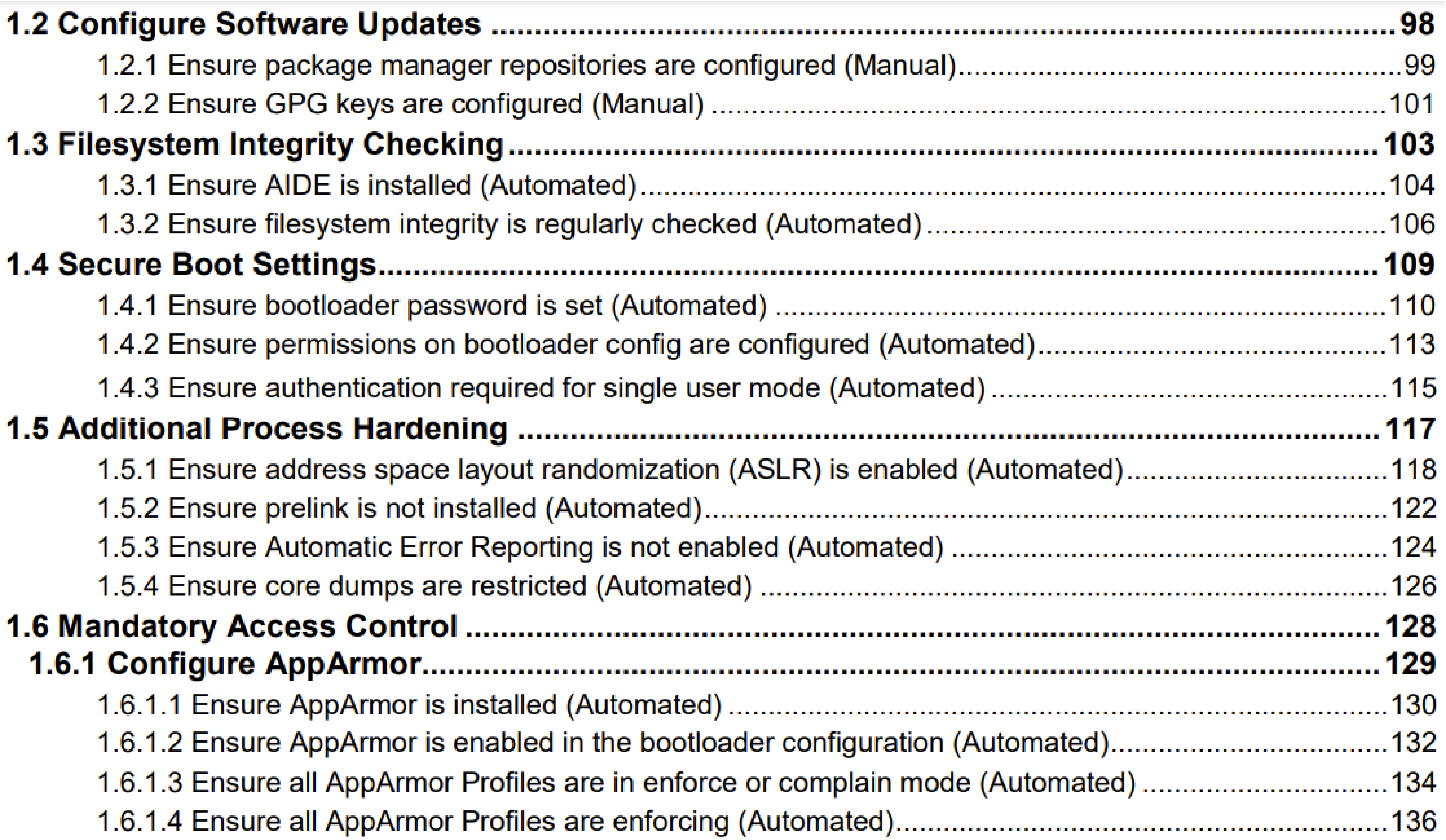


CIS. Center for Internet Security®

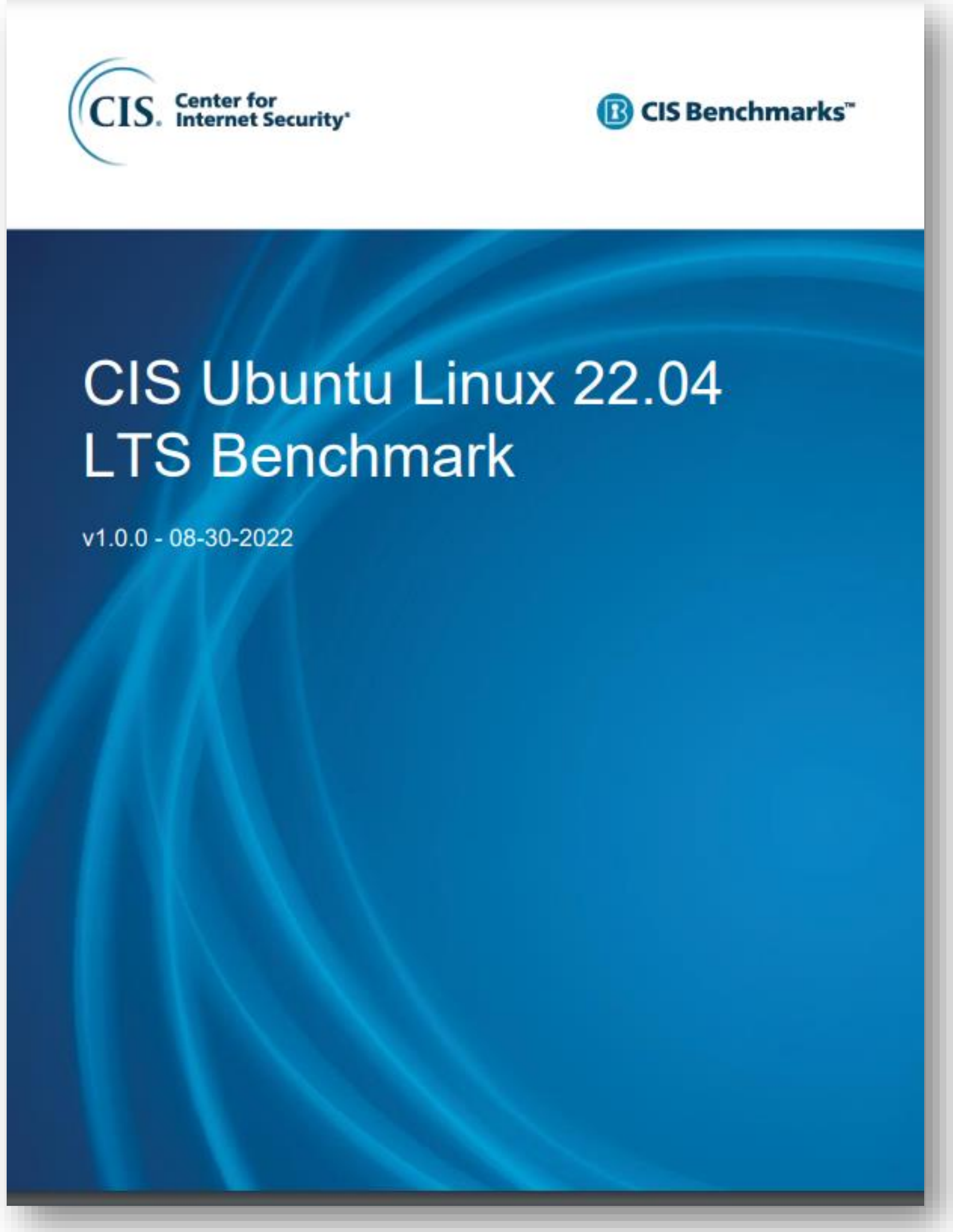
CIS Benchmarks™

CIS Ubuntu Linux 22.04
LTS Benchmark

v1.0.0 - 08-30-2022



UBUNTU HARDENING



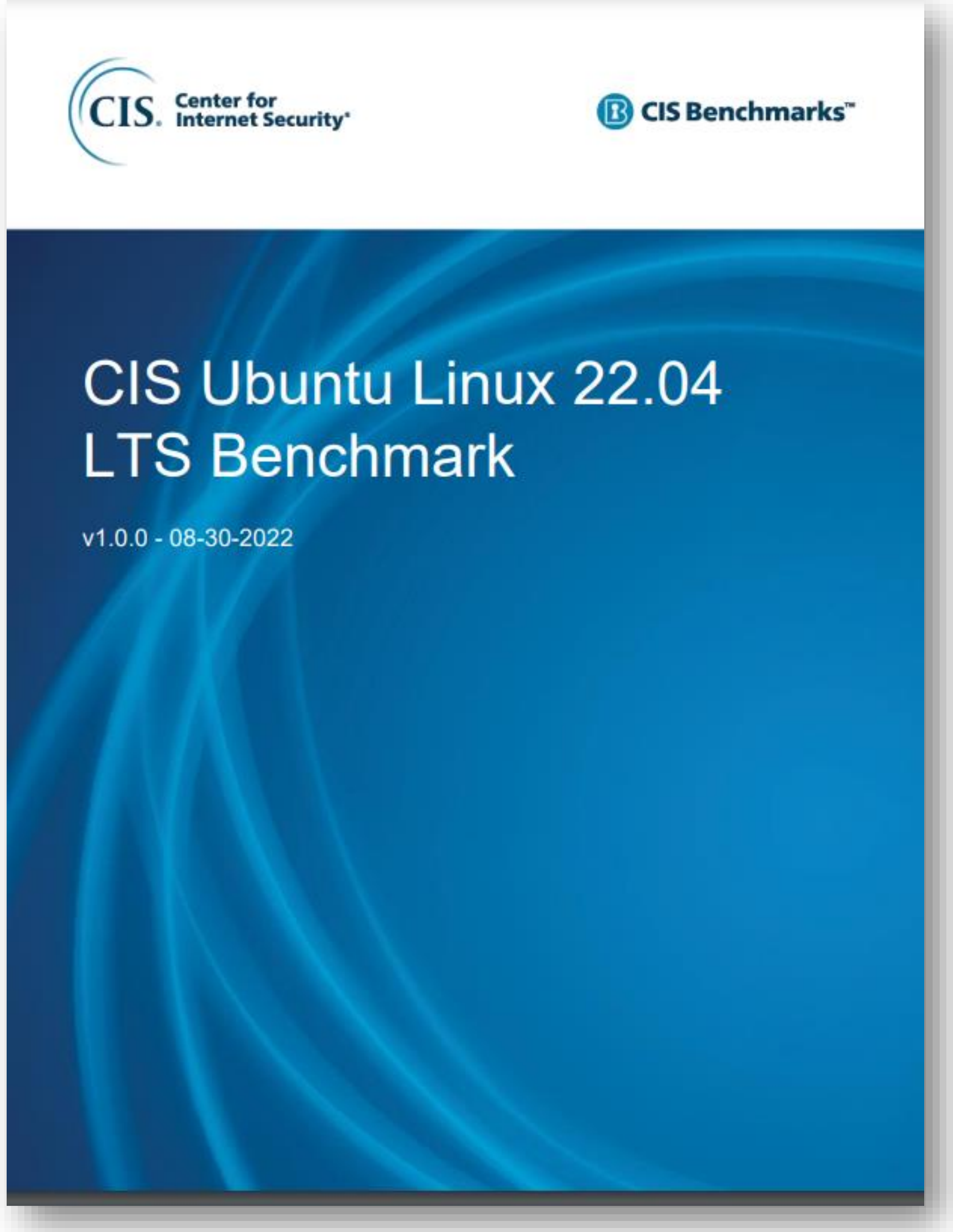
CIS. Center for Internet Security®

CIS Benchmarks™

CIS Ubuntu Linux 22.04
LTS Benchmark

v1.0.0 - 08-30-2022

UBUNTU HARDENING



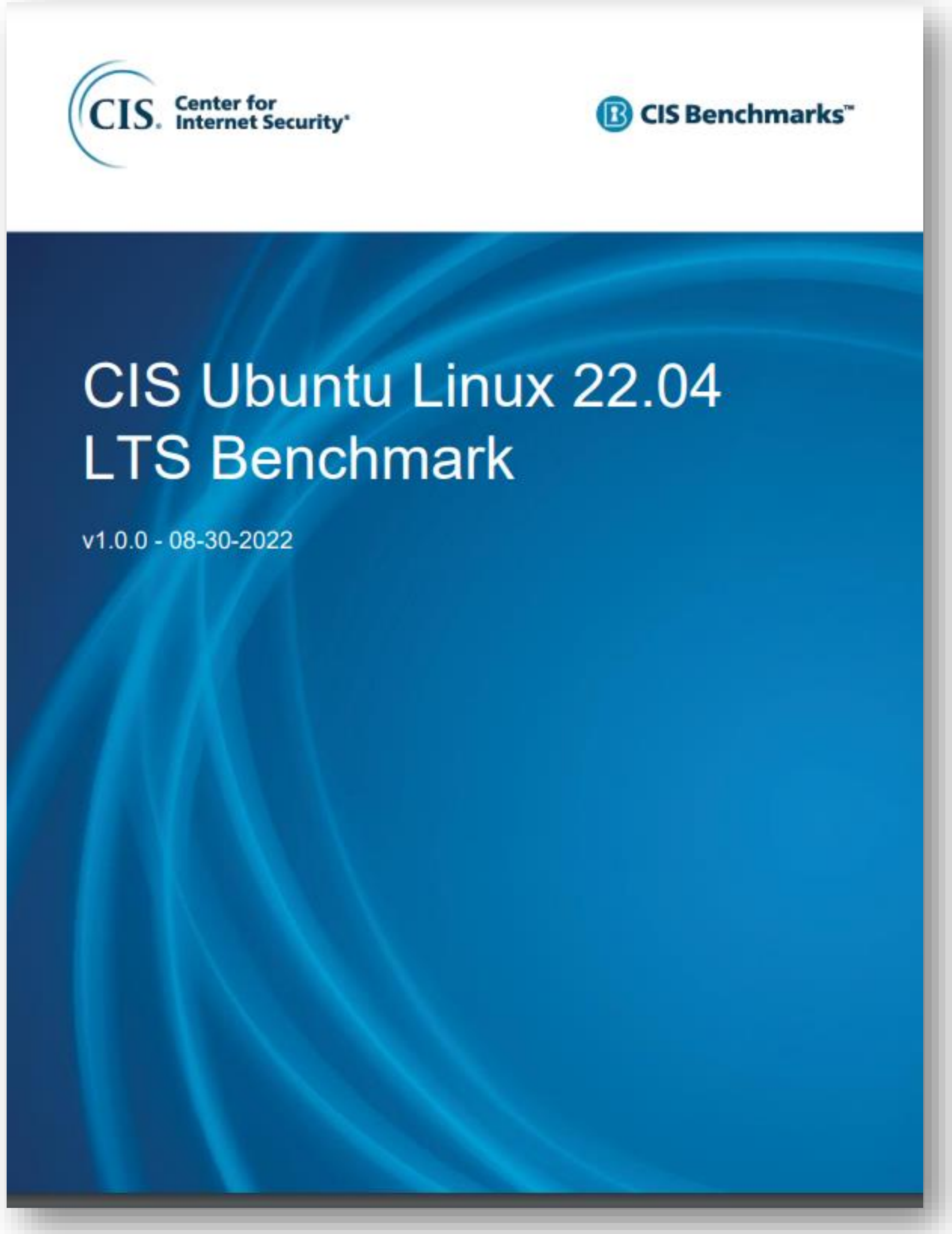
CIS Center for Internet Security

CIS Benchmarks

CIS Ubuntu Linux 22.04 LTS Benchmark

v1.0.0 - 08-30-2022

UBUNTU HARDENING

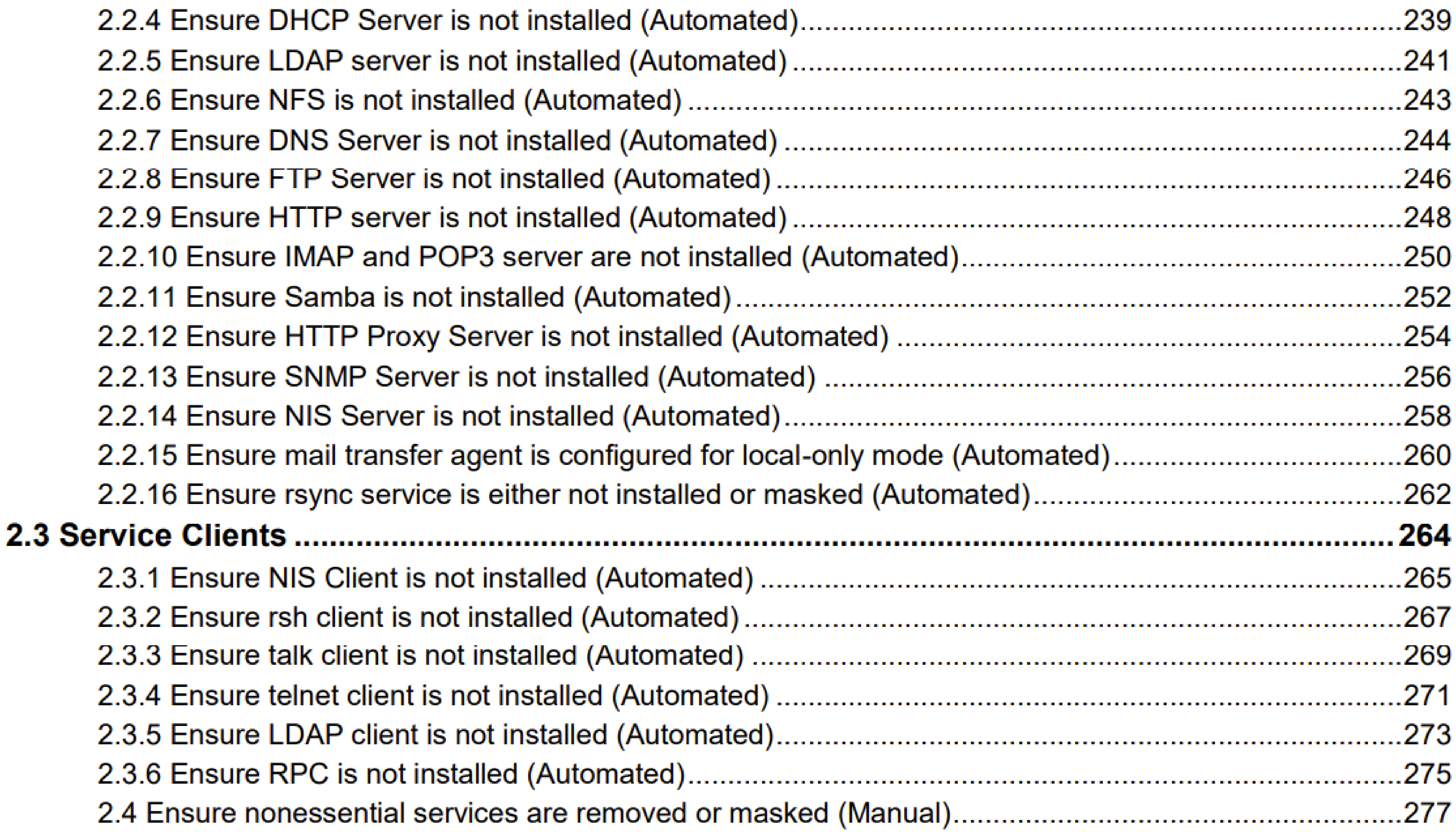


CIS. Center for Internet Security®

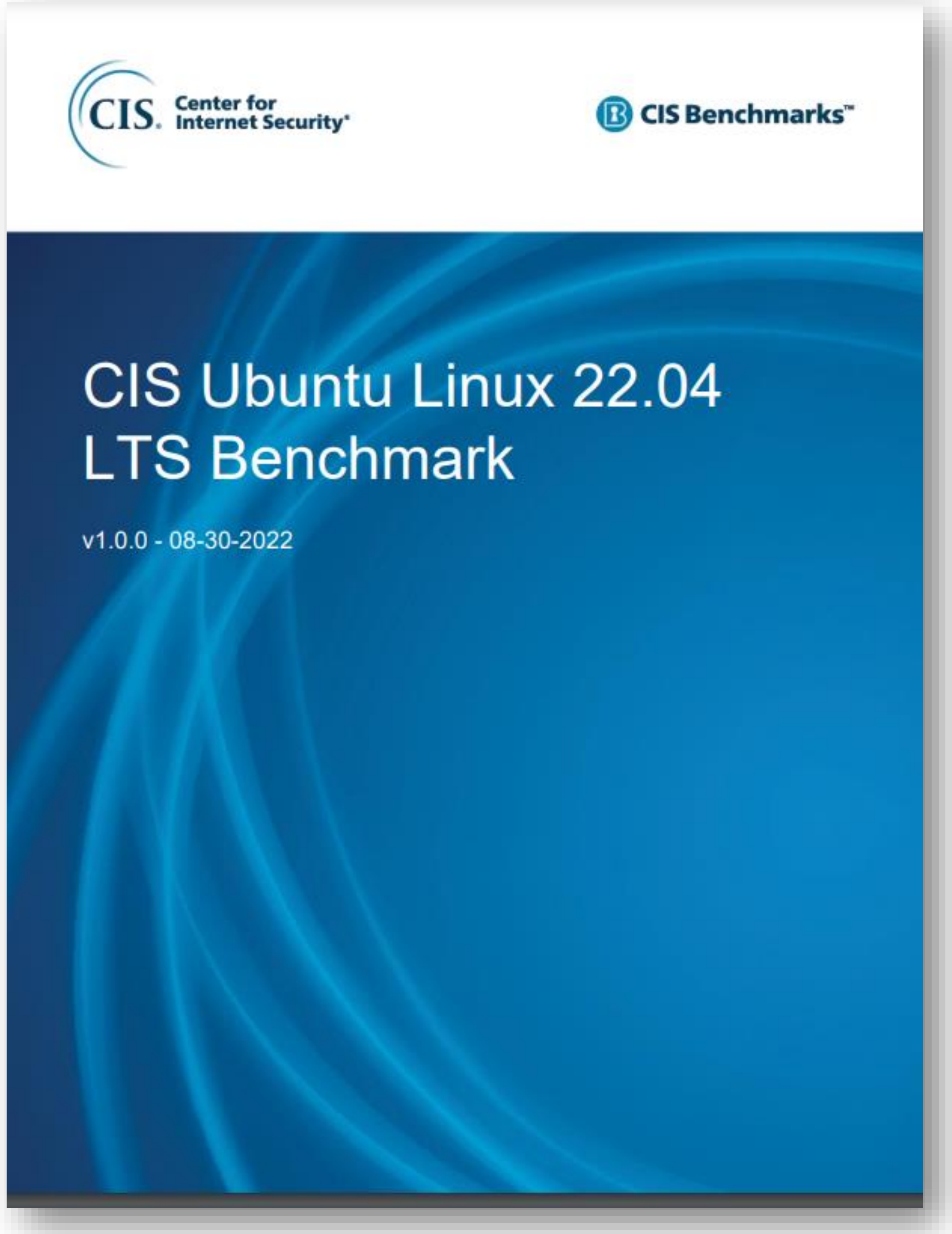
CIS Benchmarks™

CIS Ubuntu Linux 22.04 LTS Benchmark

v1.0.0 - 08-30-2022



UBUNTU HARDENING



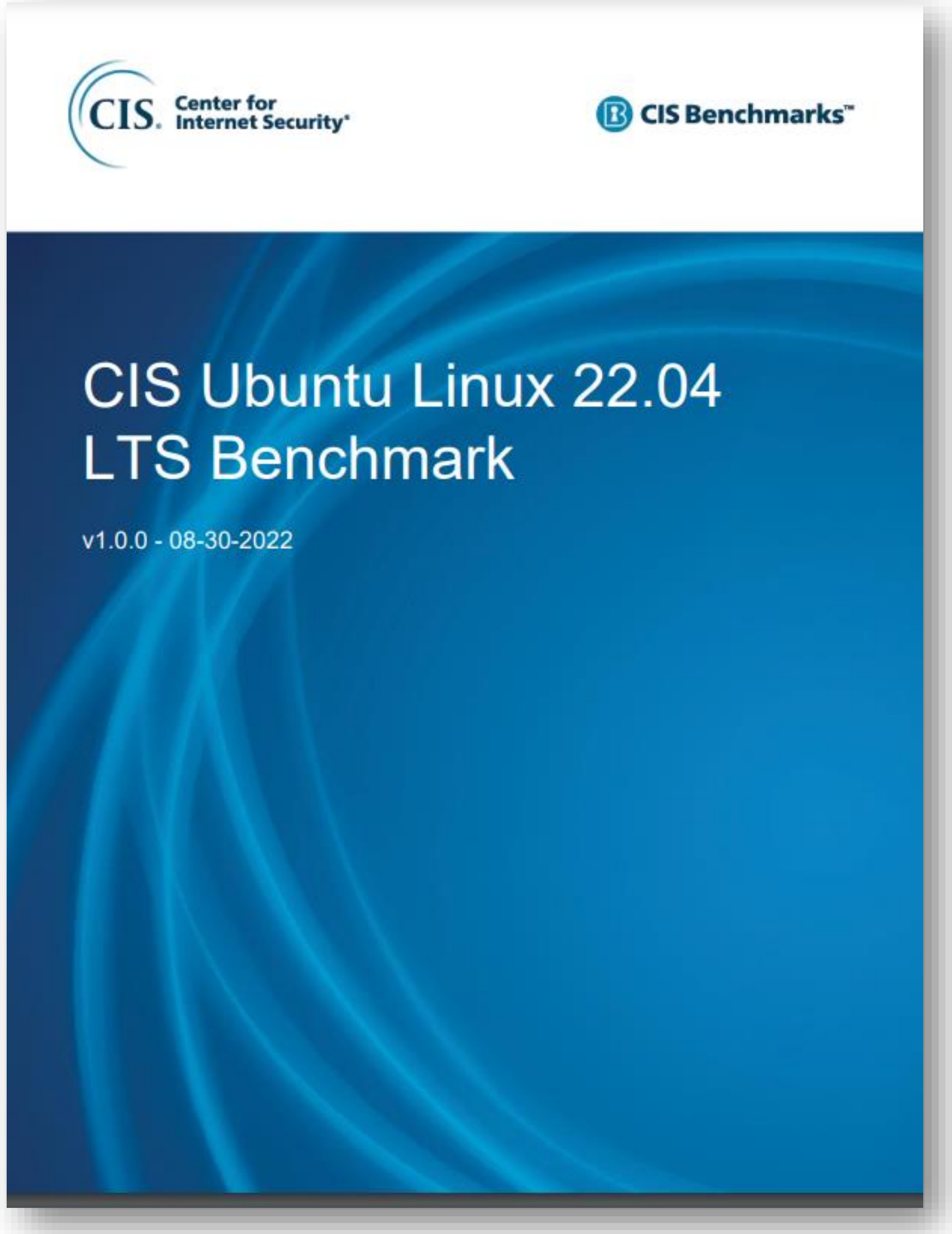
CIS. Center for Internet Security

CIS Benchmarks™

CIS Ubuntu Linux 22.04
LTS Benchmark

v1.0.0 - 08-30-2022

UBUNTU HARDENING



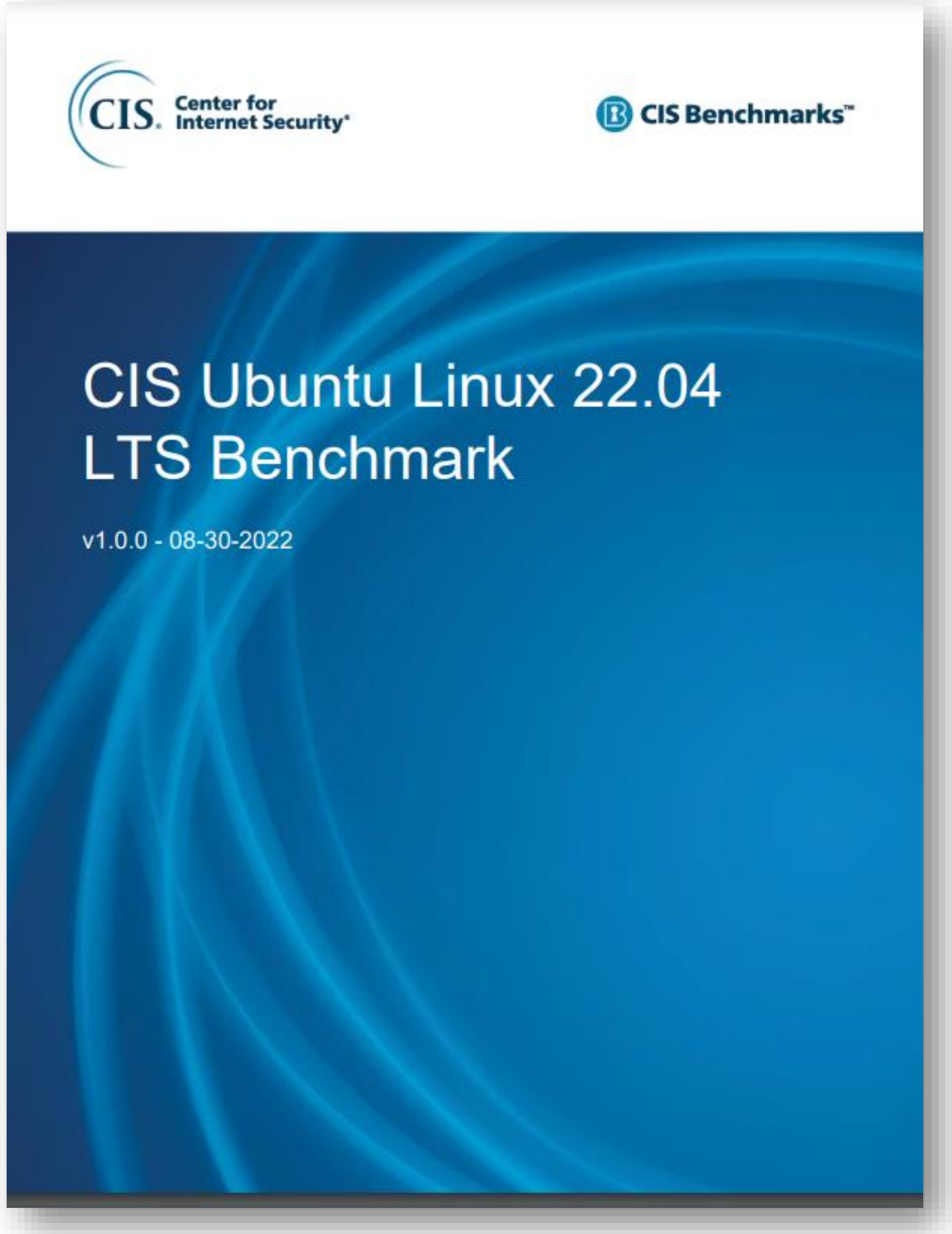
CIS. Center for Internet Security®

CIS Benchmarks™

CIS Ubuntu Linux 22.04 LTS Benchmark

v1.0.0 - 08-30-2022

UBUNTU HARDENING



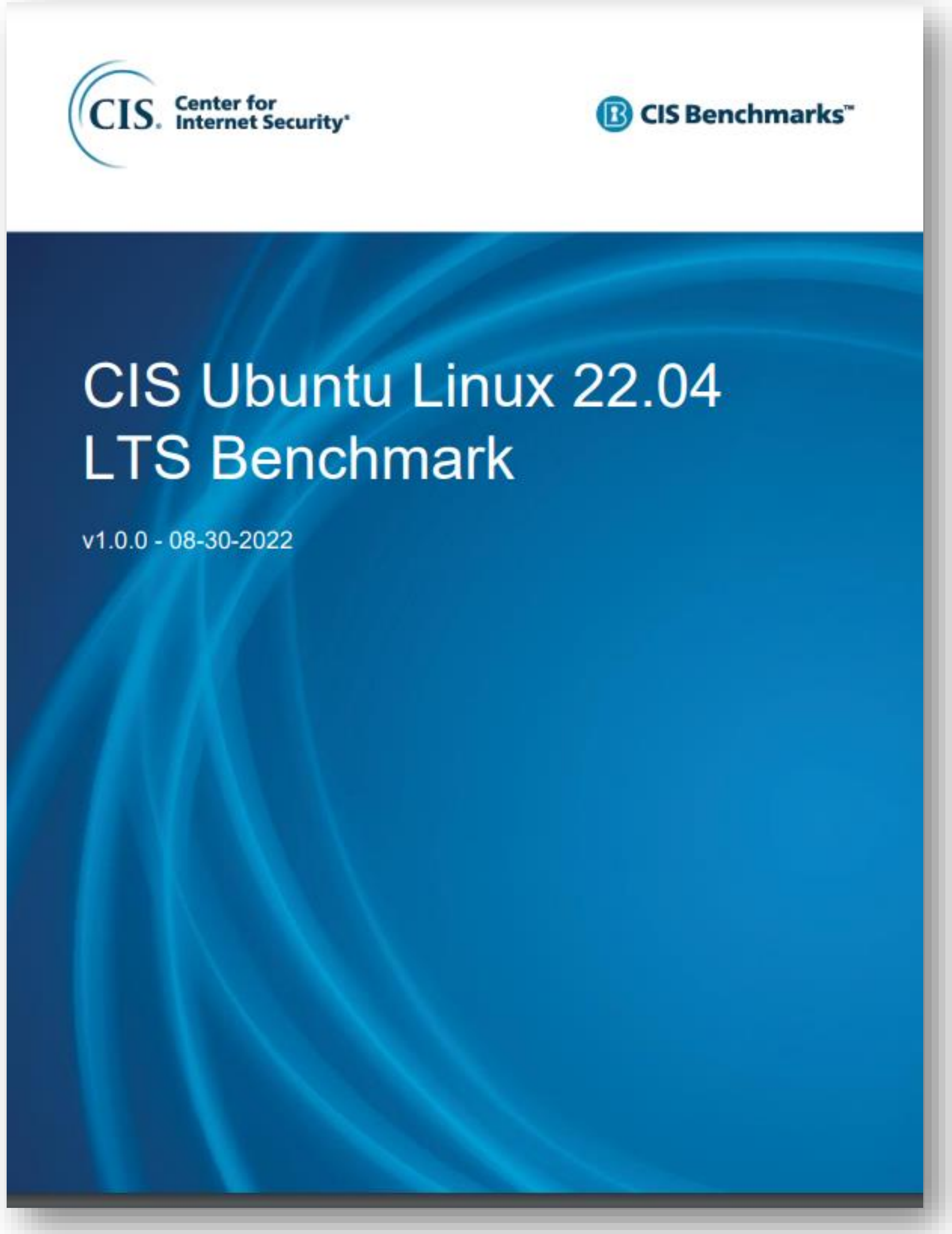
CIS Center for Internet Security

CIS Benchmarks™

CIS Ubuntu Linux 22.04
LTS Benchmark

v1.0.0 - 08-30-2022

UBUNTU HARDENING

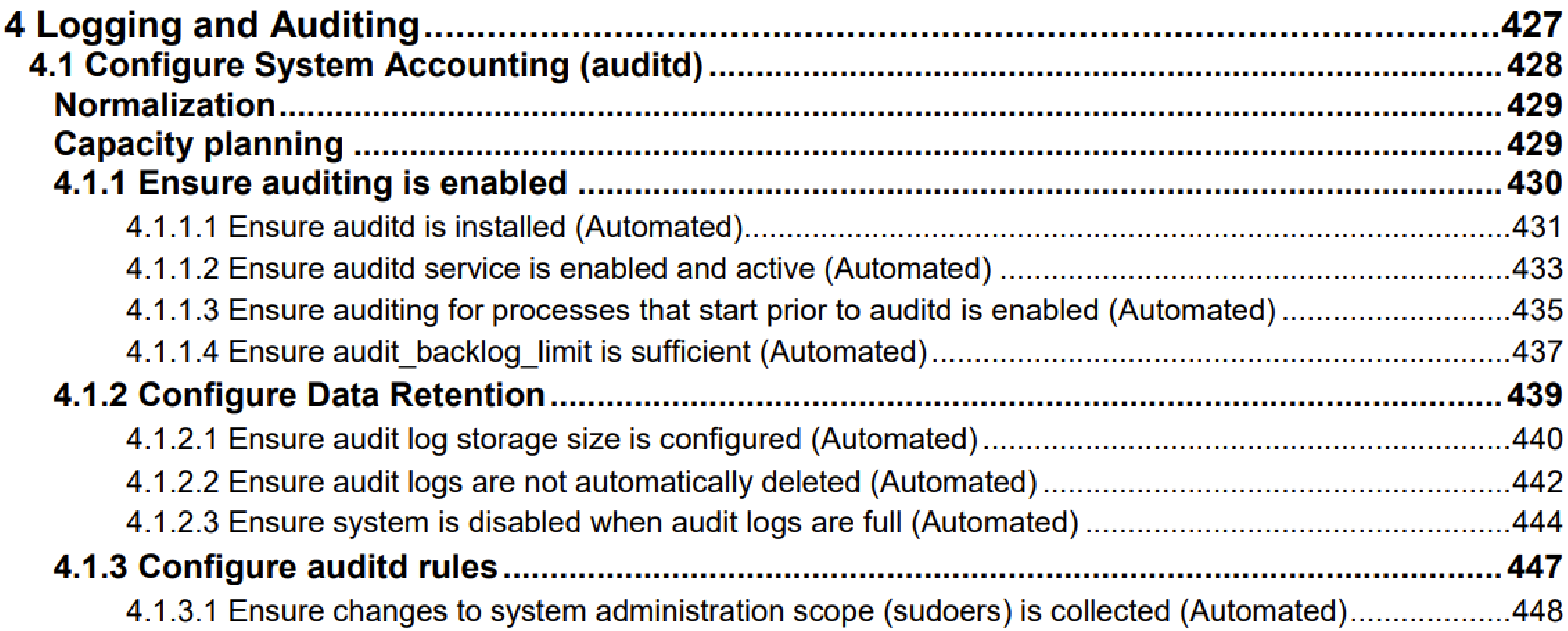


CIS. Center for Internet Security®

CIS Benchmarks™

CIS Ubuntu Linux 22.04
LTS Benchmark

v1.0.0 - 08-30-2022



Question?

Lets discuss and Win Merchandize or Voucher Neocloud

Thanks to Our Sponsors

Canonical
Ubuntu

LibreOffice
The Document Foundation

ONLYOFFICE

IndoBSD
Serving IT & Digital World Accurately

APJII
Asosiasi
Penyelenggara
Jasa
Internet
Indonesia
INDONESIA INTERNET SERVICE PROVIDER ASSOCIATION

IDNIC
indonesia
network
information
centre

Kopi Toedjoeh

nevacloud

Biznet
GioCloud

Ubuntu Korea