Here's a guide on securing MongoDB installation on Ubuntu following the CIS benchmarks:

1. Update and Upgrade:

- Begin by ensuring your system is up-to-date with the latest security patches:

```
sudo apt update
sudo apt upgrade
```

2. Install MongoDB Package:

- Use the APT package manager to install the desired MongoDB package. Refer to the official MongoDB documentation for specific versions and package names: https://www.mongodb.com/docs/manual/tutorial/install-mongodb-on-ubuntu/

3. Create Dedicated User and Group:

- Create a dedicated user and group for running the MongoDB service:

```
sudo groupadd mongodb
sudo useradd -g mongodb mongodb
```

4. Secure Directory Permissions:

- Change ownership of the MongoDB data directory (/var/lib/mongodb by default) to the newly created user and group:

```
sudo chown mongodb:mongodb /var/lib/mongodb -R
```

- Set appropriate permissions for the data directory. The CIS benchmarks might recommend:

```
sudo chmod 750 /var/lib/mongodb
```

5. Edit MongoDB Configuration:

- Edit the MongoDB configuration file (/etc/mongodb.conf) using a text editor with root

privileges.

6. Security Settings in Configuration:

- **Bind Address:** Restrict access to the MongoDB server by setting the bind_ip option to 127.0.0.1 (localhost) to only accept connections from the same machine.
- **Authentication:** Enable authentication for MongoDB access. The CIS benchmarks likely recommend using either:
  - **SCRAM-SHA-1 Authentication:** A secure authentication method using username and password.
  - **LDAP Authentication:** Integrate with your existing LDAP server for user authentication.
- **Authorization:** Implement authorization controls to restrict user access to specific databases and collections within MongoDB.

7. Enable Authorization (Example):

```
security:
  authorization: enabled
```

8. Additional Considerations:

- **TLS/SSL Encryption (Optional):** For enhanced security, consider using TLS/SSL encryption for communication between client applications and the MongoDB server.
- **Audit Logging:** Enable audit logging to record user activities and potential security events within MongoDB.

9. Restart MongoDB Service:

- After making configuration changes, restart the MongoDB service:

```
sudo systemctl restart mongod
```

Additional Resources:

- CIS MongoDB Security Benchmarks (reference guides that mention them): While not available directly online, you can find references and explanations in security guides that reference CIS benchmarks. Search for "CIS MongoDB Security Benchmarks Ubuntu".
- MongoDB Documentation: https://www.mongodb.com/docs/
- Ubuntu Documentation on Users and Groups: https://www.cyberciti.biz/faq/create-a-user-account-on-ubuntu-linux/

Remember:

- These are general guidelines. Refer to the official CIS MongoDB benchmarks for your Ubuntu version for detailed security recommendations.
- Regularly update MongoDB packages to address vulnerabilities.
- Secure your client applications to ensure proper authentication and authorization when connecting to the MongoDB server.