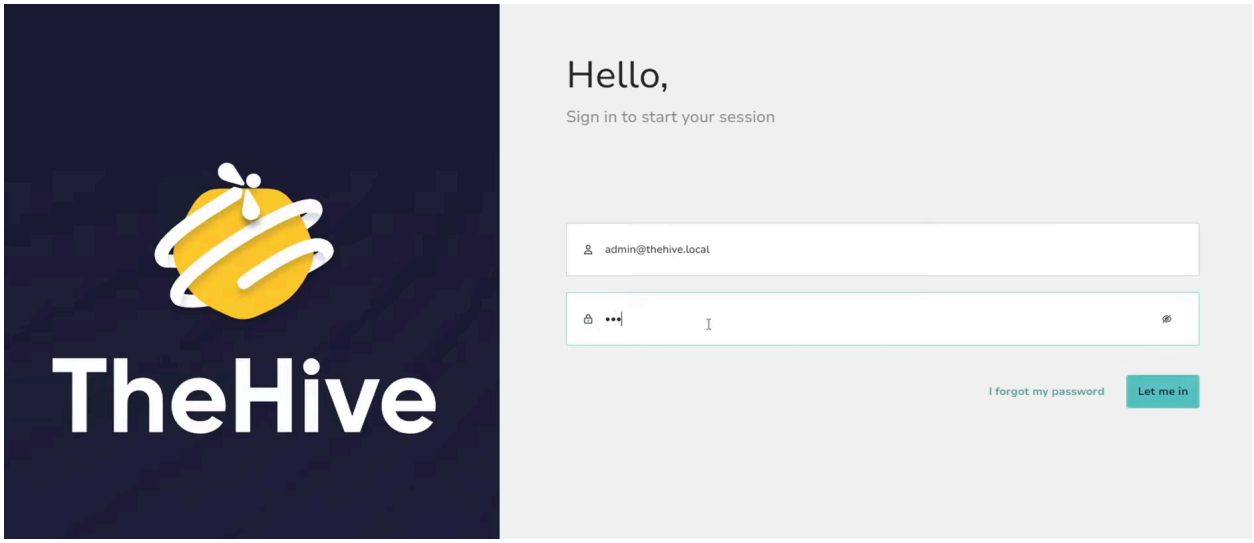
5. TheHive Incident Response Platform Setup

TheHive allows case creation and incident tracking after detection events.



Dependencies installed:
- Cassandra (database)
- ElasticSearch
- TheHive application

Steps overview:

1. Install Cassandra and update configuration:
    - Change cluster name
    - Set listen_address and rpc_address to the VM IP
    - Restart Cassandra
2. Install ElasticSearch:
    - Modify elasticsearch.yml with correct IP and cluster name
    - Restart ElasticSearch
3. Install TheHive:

- Update application.conf with:
    - Public IP
    - Correct cluster name
    - ElasticSearch host
- Start TheHive
- Access via: http://YOUR_IP:9000

Default credentials:
admin@thehive.local
secret

TheHive is now operational.