Deployment Guide

Accessing the SIEM

Local Testing

When deploying the SIEM locally for testing purposes:

Access the Frontend Interface:

- Open a web browser on your host machine.
- Navigate to `http://localhost:3000` or `http://127.0.0.1:3000`.
- This connects you directly to the SIEM frontend.

Send Test Syslog Messages:

- Use a syslog client to send test messages to localhost on UDP port 514.

Production Deployment

For deploying the SIEM in a production environment:

Domain and DNS Setup:

1. **Acquire a Domain Name:** Obtain a domain name (e.g., `yourdomain.com`).
2. **Configure DNS:** Create an A record pointing your domain to your server's public IP address.

Update Traefik Configuration:

- Ensure Traefik is set up to obtain SSL certificates, refer to the Traefik HTTPS Documentation.
- In your `docker-compose.yml`, update the Traefik service's command section if necessary.

Modify Service Labels:

Update the frontend and backend service labels to match your domain:

- **Frontend labels:**

  ```
  "traefik.http.routers.frontend.rule=Host(`yourdomain.com`)"
  ```

- **Backend labels:**

  ```
  "traefik.http.routers.backend.rule=Host(`api.yourdomain.com`)"
  ```

Ensure Firewall Settings:

- Open port 443 in your server's firewall to allow external access.

Access the SIEM Interface:

- Open a web browser and navigate to `https://yourdomain.com`.
- This connects you to the Traefik reverse proxy, which forwards HTTP requests to the frontend and API requests to the backend.

Configure Syslog Input:

- Set up your network devices or syslog clients to send logs to your server's internal IP address on port 514.