Assignment

I. Hosting Strategy

Host Site

The SOAR platform will be deployed on an Ubuntu 22.04 virtual machine hosted on Amazon Web Services (AWS) EC2.

Justification for Selecting AWS EC2

- Provides full operating system control required for backend orchestration.
- Supports scalable infrastructure suitable for high-volume alert processing.
- Enables secure API exposure using security groups and SSL certificates.
- Allows realistic simulation of enterprise-grade deployment.
- Supports persistent runtime necessary for stateful incident lifecycle management.

Rationale for Not Selecting Alternative Hosting Models

- Shared hosting does not support persistent backend services or API-based integrations.
- Serverless platforms were not selected due to the requirement for continuous orchestration and stateful processing.
- Local deployment was rejected because it lacks scalability, secure exposure, and production realism.

Deployment Strategy

1. Provision Ubuntu 22.04 EC2 instance.
2. Install Python runtime and required backend dependencies.
3. Configure isolated virtual environment.
4. Deploy SOAR backend services within the application runtime.
5. Install and configure PostgreSQL database.
6. Define REST API endpoints for alert ingestion, incident retrieval, and playbook execution.
7. Configure Nginx as reverse proxy.
8. Enable HTTPS using SSL certificates.
9. Restrict inbound traffic using AWS Security Groups (HTTPS allowed, SSH restricted).
10. Enable persistent audit logging for compliance.

Security Measures

- All communication secured using TLS encryption (HTTPS).
- Database access restricted to localhost.
- Role-based access control enforced at application level.
- Firewall rules configured through AWS Security Groups.
- Comprehensive audit logging of automated actions.