Concrete Architecture

Client

Visualization module

Communication module

Web Server

Data Sources

System Scan

Response

Communication module

Service

Communication module

Plan Recognition

Attack Tree Database

Alert Correlation

Attack Scenario Database

Ontology Database

Alert Aggregation

Alert Normalization

Vulnerability Matching Module

Vulnerability Normalization Module

Vulnerability Database