* Chuẩn hóa các alert từ các data sources
* Cách kết hợp các alert thành hyper-alert sau khi đã chuẩn hóa
* Cách xác định pre-post của các hyper-alert
* Cách kết hợp các hyper-alert tạo thành attack tree
* Cách trừu tượng các bước trong attack tree thành các class
* Cách kết hợp ontology vào hệ thống
* Ngôn ngữ đặc tả attack tree
* Các match giữa causal network
* Các phương pháp visualize
* Các thông tin cần cung cấp để visualize
* Xác định lỗ hổng bảo mật của hệ thống