Định nghĩa HTGS

SIEM là hệ thống nhiều thành phần

Buổi 2

Chức năng: Thực hiện thu thập dữ liệu từ nhiều nguồn 🡺 tổng hợp 🡺 phân tích 🡺 phát hiện xâm nhập

SIEM ⬄ IPS/IDS

Hệ thống GSATTT = 3 thành phần ( TP thu thập DL, TP phân tích và lưu trữ, TP quản trị tập trung )

Mô hình triển khai

Thành phần thu thập { Collector, Agent }

Chức năng: thu thập dữ liệu từ nhiều nguồn khác nhau gửi về thành phần quản lý tập trung

Nguồn dữ liệu thu thập: Thiết bị bảo mật, thiết bị mạng, máy chủ, ứng dụng (Log)

Chuẩn hoá dữ liệu: