**TIỂU LUẬN CHUYÊN NGÀNH**

1. **Lý thuyết**
2. Tổng quát về hệ thống giám sát mạng (SIEM)
3. Các điểm tối ưu của SIEM
4. Các giải pháp giám sát an ninh mạng

* Security Information Management (SIM)
* Security Event Managerment (SEM)
* Security Information and Event Management (SIEM)

1. Các dịch vụ của SIEM
2. Các thành phần của SIEM

* Thiết bị nguồn (Source device)
* Thu thập Log (Log collection)
* Phân tích, Chuẩn hóa Log (Parsing normalization)
* Kỹ thuật tương quan sự kiện (Rule engine | correlation engine)
* Lưu trữ Log (Log storage)
* Theo dõi và giám sát (Monitoring)

1. Cách hoạt động của SIEM
2. Hệ thống qradar SIEM
3. **Thực hành**

* Tìm hiểu cách vận hành của SIEM và chạy thử trên ứng dụng mở.