Giám sát và phát hi?n s? c?

- **Sử dụng hệ thống quản lý thông tin và sự kiện an ninh (SIEM) để giám sát hoạt động mạng:**
  - Cấu hình SIEM để phát hiện các hành vì bất thường.
  - Đảm bảo log từ tất cả hệ thống quan trọng được gửi về SIEM.
  - Định kỳ xem xét và cập nhật quy tắc phát hiện trong SIEM.

- **Triển khai hệ thống phát hiện và ngăn chặn xâm nhập tại các điểm mạng quan trọng:**
  - Sử dụng hệ thống IDS/IPS để phát hiện và phản hồi nhanh chóng các mỗi đe dọa.
  - Cấu hình cảnh báo theo mức độ ưu tiên phù hợp.
  - Thực hiện kiểm tra định kỳ hiệu quả của IDS/IPS.

Revision #2
Created 17 September 2025 10:40:34 by Hieu Nguyen
Updated 27 October 2025 04:04:43 by Admin