OSSEC:

1. Các hệ điều hành được hỗ trợ
   * GNU/Linux (all distributions, including RHEL, Ubuntu, Slackware, Debian, etc)
   * Windows 2000, XP, 2003, Vista, 2008
   * VMWare ESX 3.0,3.5 (including CIS checks)
   * FreeBSD (all versions)
   * OpenBSD (all versions)
   * NetBSD (all versions)
   * Solaris 2.7, 2.8, 2.9 and 10
   * AIX 5.3 and 5.3
   * Mac OS X 10.x

Chắc cơ bản chỉ cần Linux với Windows

1. Cấu trúc hệ thống
   * Cài đặt và hoạt động trực tiếp trên một máy local
   * Dạng client-server gồm:
     1. Phần quản lý cài ở máy chủ
     2. Agent có thể cài ở máy client hoặc cũng hổ trợ tính năng agentless <đối với hệ thống không thể cải agent được>
        + Agent có thể cài được trên máy ảo
     3. Có thể nhận log từ Firewalls, switches and routers
2. Một số tính năng chính:
   * Kiểm tra tính toàn vẹn:
     1. Có sử dụng MD5/SHA1 checksums , hỗ trợ cấu hình file được check …,tần suất ,thời gian ,…
     2. Có hỗ trợ check trong thời gian thực
   * Hỗ trợ phát hiện việc cài đặt rookit lên hệ thống <chỉ những hệ thống có cài agent> ,tự động kiểm tra sau một khoảng thời gian nhất định do người dùng định nghĩa, dựa trên cơ sở dữ liệu về trojan,rookit lưu dưới dạng txt
   * Log analysist:
     1. Hỗ trợ phân tích khá nhiều định dạng log,riêng windows hỗ trợ 2 dạng dưới:
        + Windows event logs (logins, logouts, audit information, etc)
        + Windows Routing and Remote Access logs
   * Alert output:
     1. syslog servers
     2. Qua email
     3. Ra database,hiện chỉ hỗ trợ hai dạng database sau:
        + MySQL or PgSQL
     4. Gửi tới prelude
     5. Cái cuối cùng là Picvis<hem hỉu nó là cái zì>
   * Về việc sinh alert từ log file cơ chế sẽ theo thứ tự :
     1. Phía agent sẽ có logcollector thu thập và gửi file log về cho server
     2. Phía server:
        + Nhận file log ,tùy loại file log sẽ có phần decoder <mặc định hoặc do người dùng định nghĩa>
        + Sau đó sẽ áp dụng các rule được thiết lập để sinh alert <phần rules này sẽ không phụ thuộc vào cấu trúc của log file ban đầu vì đã qua decoder>
3. Kết luận:

Cái này hạn chế việc không cài đặt server trên windows được ,nếu yêu cầu những tác vụ đơn giản mà có chương trình nào thực hiện được thì khỏi xài cái này.