|  |  |  |  |
| --- | --- | --- | --- |
|  | Hoạt động | Khả năng phát hiện tấn công | Độ chính xác |
| HIDPS | -Signature-based  -anomaly-based (so sánh với mô hình baseline đc đc học) | -Phân tích code : không cho malware thực thi  -Theo dõi system call  -Phân tích lưu lượng mạng : vào và ra host  -Theo dõi hệ thống file : ngăn việc thay đổi , xóa file ,… từ  -Giới hạn các thiết bị removeable (usb,..)  -Giám sát các thiết bị trên host (camera , mic ,…)  -Host hardening : gỡ bỏ các apps không cần thiết  -Theo dõi trạng thái của tiến trình | -Nên kết hợp vs các kĩ thuật khác  -Xem các records quản lý thay đổi , thay đổi và cấu hình policy để ngăn false positives  - hỗ trợ black list,whitelist  -xác định hành động với mỗi cảnh báo |
| Hạn chế | -Độ trễ khi tạo cảnh báo và báo cáo tập trung  -sử dụng tài nguyên của host  -Xung đột với các cơ chế kiểm soát an ninh đang có (chức năng bị trùng lặp) |  |  |
| Ưu | Phát hiện các sự kiện đang diễn ra trên host | Có thể xử lý các lưu lượng bị mã hóa | Có thể so sánh các records |
| Nhược | -Cần triển khai mỗi agent trên thiết bị cần giám sát | Dễ bị tấn công Ddos | Cần 1 không gian ổ đĩa lớn   * ảnh hưởng tới hiệu suất của host |
| Một số nền tảng HIDPS | Wazuh,OSSEC |  |  |