|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Cơ chế | Ưu | Hạn chế | Tóm tắt |
| Signature-based | -Sử dụng signature  -so sánh vs các sự kiện quan sát đc | Hiệu quả phát hiện known at  Tỉ lệ sai thấp | K phát hiện đc cái mới   * Dễ bị bypass | so sánh với các mẫu đã biết |
| Anomaly-based | -Định nghĩa bình thường  -cái nào khác là bất thường | Phát hiện đc tấn công chưa biết | -Dễ bị nhận biết sai do không định nghĩa đủ  -ít hiệu quả  -mất tgian định nghĩa | tìm kiếm các hành vi không bình thường |
| Specification-based | -So sánh hành vi  vs cái đc định nghĩa trc  -thu thập hđ |  |  | sử dụng quy tắc hoặc thông số đã xác định trước để phân loại hành vi |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IDPS |  |  |  |  |
| Network-based | Theo dõi lưu lượng mạng | Triển khai ở biên  -Gồm nh sensor đặt tè le trong mạng |  | Sensor |
| Host-based | Theo dõi 1 host riêng lẻ | Lưu lượng , logs , process,apps,thay đổi , của host | Đc triển khai trên host quan trọng | Agent |
| Hybrid IDPS | Tích hợp cả 2 cái trên |  |  |  |
| Server quản lí | Nhận thông tin từ sensor,agent |  |  |  |
| Server CSDL | Lưu trữ thông tin nhận |  |  |  |
| Consoles | Cung cấp giao diện IDPS cho người dùng |  |  |  |
| Connect | Các tp IDSP kết nối thông qua mạng chuẩn (standards network) | =>Độc lập vs mạng doanh nghiệp  -che dấu đc sự tồn tại trc attacker | -Tránh bị ảnh hưởng khi attacker tấn công | -Mất tiền  -bất tiện cho user và admin |
| Sensor | 1 interface kết nối với Server management | Còn lại là interface theo dõi |  |  |
| Logs | Lưu ở nhiều nơi | Đảm bảo tính toàn vẹn, sẵn sàng |  |  |
| Thresholds | Ngưỡng để phát hiện : bthg và bất thg | anomaly-based | phân tích các stateful protocol. |  |
| IDPS giao tiếp | -Hệ thống cung cấp (DMZ Server,log server tập trung,email-server,…) | Hệ thống để thực hiện các phản ứng ngăn chặn(vd., tường lửa, routers, switches) | Hệ thống quản lý các thành phần IDPS (vd. phần mềm quản lý mạng hay bản vá) |  |
| Bảo vệ IDPS | Tạo tk riêng biệt cho IDPS | Cấp quyền vừa đủ  -cấu hình firewall hạn chế truy cập trực tiếp  -các giao tiếp vs IDPS phải đc bảo vệ | IDPS thường đc sử dụng thông qua GUI-giao diện |  |
| Khả năng IDPS | Thu thập tt , ghi logs,chỉnh sửa mã nguồn | , phát hiện tấn công(sd thresholds,black-list,whitelists) | Thiết lập cảnh báo |  |
| Cần | Thiết kế kiến trúc | Thực hiện ktra các tp IDPS | Triển khai và bảo vệ nó |  |