* Tìm kiếm các endpoint trên ActiveDirectory

Host-based Malware Protection

• Signature-based – Phát hiện các đặc điểm khác nhau của những file malware đã biết

• Heuristics-based – Phát hiện các tính năng chung thường được sử dụng bởi các loại malware

• Behavior-based – dựa trên việc phân tích các hành vi đáng ngờ

**Cấu hình tập trung**

* Agent đc triển khai trên các host quan trọng : servers , ..
* Agent gửi data (event) đến servers
* Hiệu suất của host không bị ảnh hưởng bởi IDPS
* Các cảnh báo có thể không theo thời gian thực

➔ Yêu cầu ít CPU, RAM, ổ cứng trên các host

**Cấu hình phân tán**

• Việc xử lý các sự kiện được phân tán giữa host và console

• Host tạo và phân tích sự kiện theo thời gian thực

• Giảm hiệu suất trên các host

➔ Các host nên được trang bị tối đa CPU, RAM, ổ cứng

Về cấu hình của HIDPS, có thể có cả hai cấu hình tập trung hoặc phân tán**, tùy thuộc vào yêu cầu của hệ thống và mục đích sử dụng của HIDPS.**

Trong cấu hình tập trung, các dữ liệu và cấu hình của HIDPS được quản lý và lưu trữ trên một máy chủ tập trung. Các máy tính được bảo vệ được kết nối với máy chủ này để truy cập cấu hình và nhận các cập nhật và thông báo từ HIDPS. Việc quản lý tập trung này giúp cho việc theo dõi và phát hiện các hoạt động xâm nhập trên các máy tính được dễ dàng hơn.

Trong cấu hình phân tán, các máy tính được bảo vệ sẽ lưu trữ và quản lý các dữ liệu và cấu hình của HIDPS. Các cảm biến HIDPS được cài đặt trên mỗi máy tính để phát hiện và ngăn chặn các hoạt động xâm nhập trên máy tính đó. Việc phân tán này giúp giảm bớt tải cho một máy chủ tập trung và giúp cho các máy tính được bảo vệ có khả năng tự phòng thủ hơn.

Những hạn chế

* Nhiều thì trùng lặp và conflict

Ưu điểm :

• Phát hiện các sự kiện trên hệ thống host, phát hiện thay đổi trong các file, bộ nhớ và ứng dụng

• Có thể xử lý lưu lượng đã bị mã hoá (encrypted) để phát hiện các tấn công mà NIDS không thể phát hiện

Có thể so sánh các record lưu trong log theo dõi

Nhược điểm :

• Thêm vấn đề quản lý , cần triển khai agent trên mỗi host muốn giám sát

• Có thể chịu các tấn công trực tiếp hoặc tấn công vào host, dễ bị 1 số tấn công DoS

• Cần một không gian ổ đĩa lớn , có thể ảnh hưởng đến hiệu suất của host