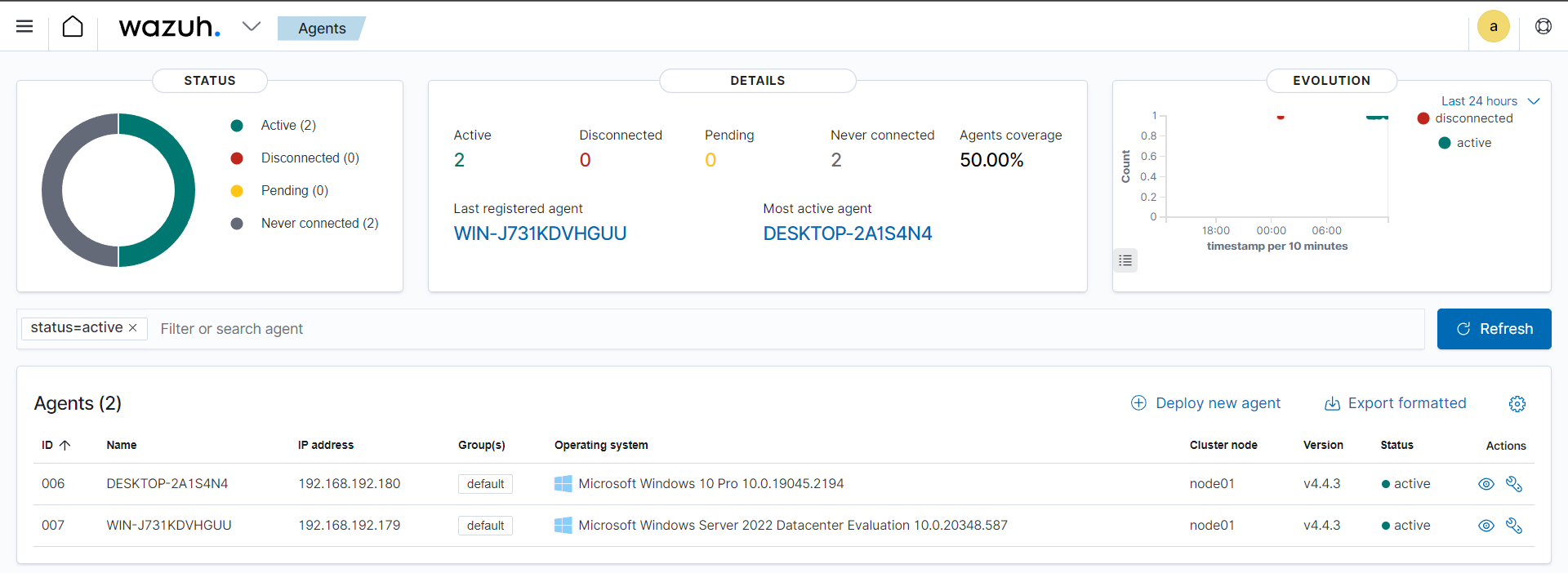
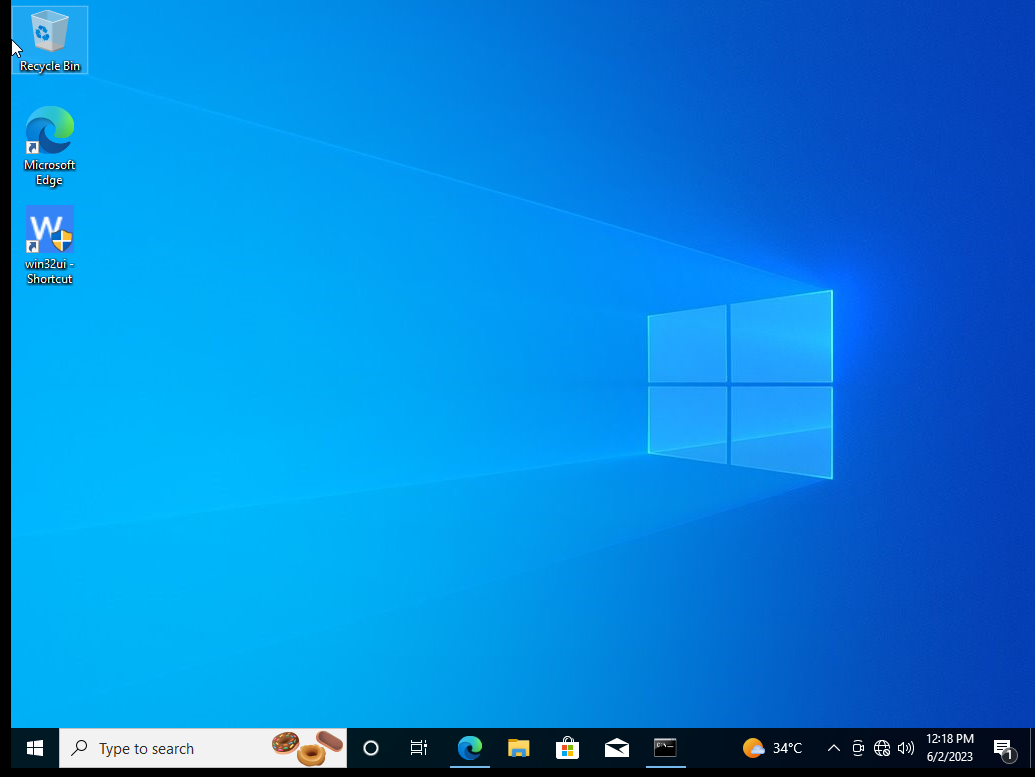
**Thực hiện tích hợp(chuyển tiếp) Window Defender Logs sang Wazuh**

# Chuẩn bị:

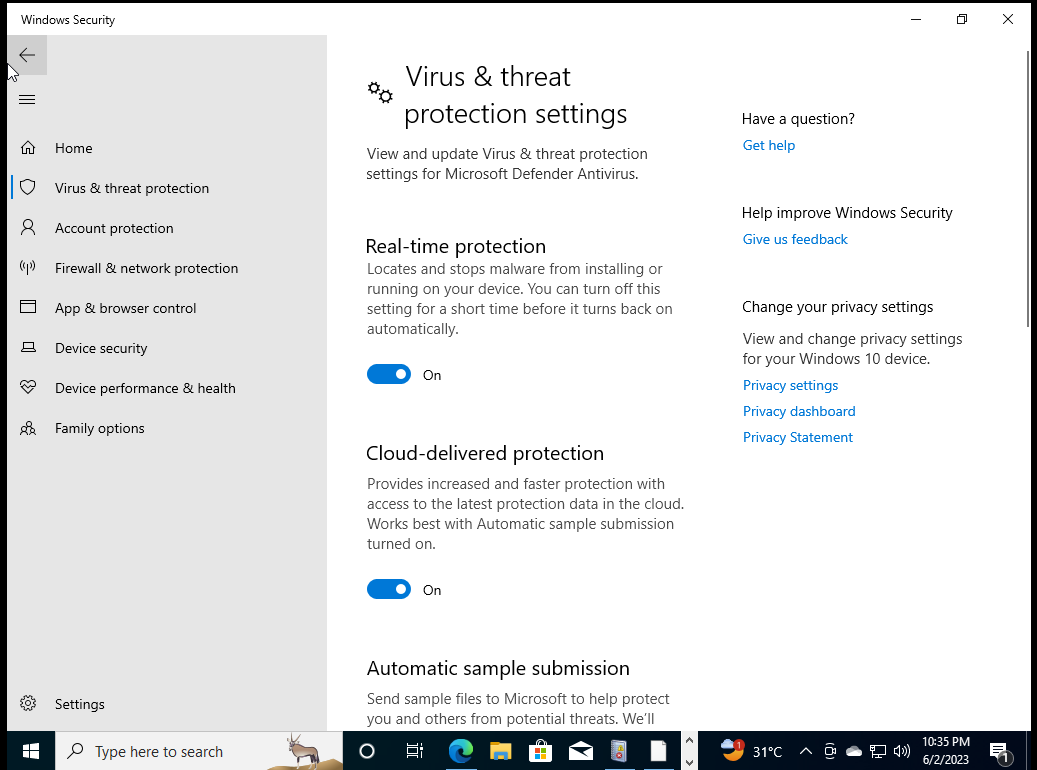
* Chuẩn bị Wazuh Server và một Window Agent đã được kết nối :





* Setup Window Defender

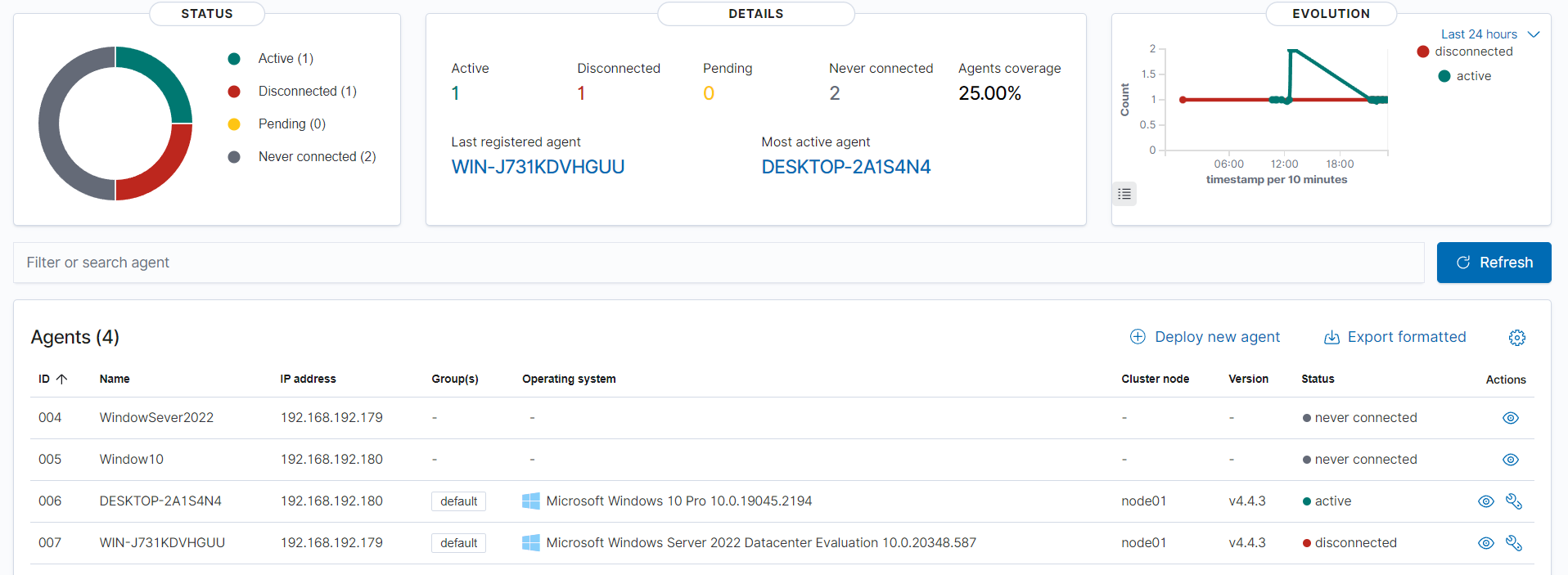
Bật Real-time protection

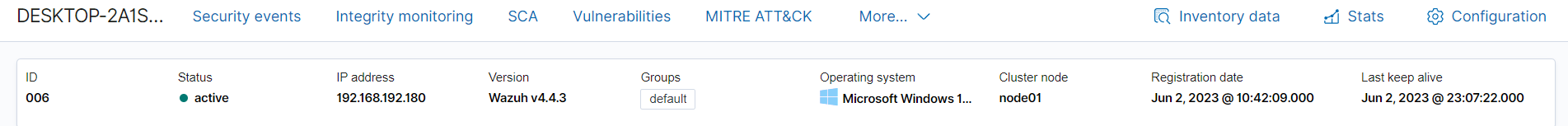


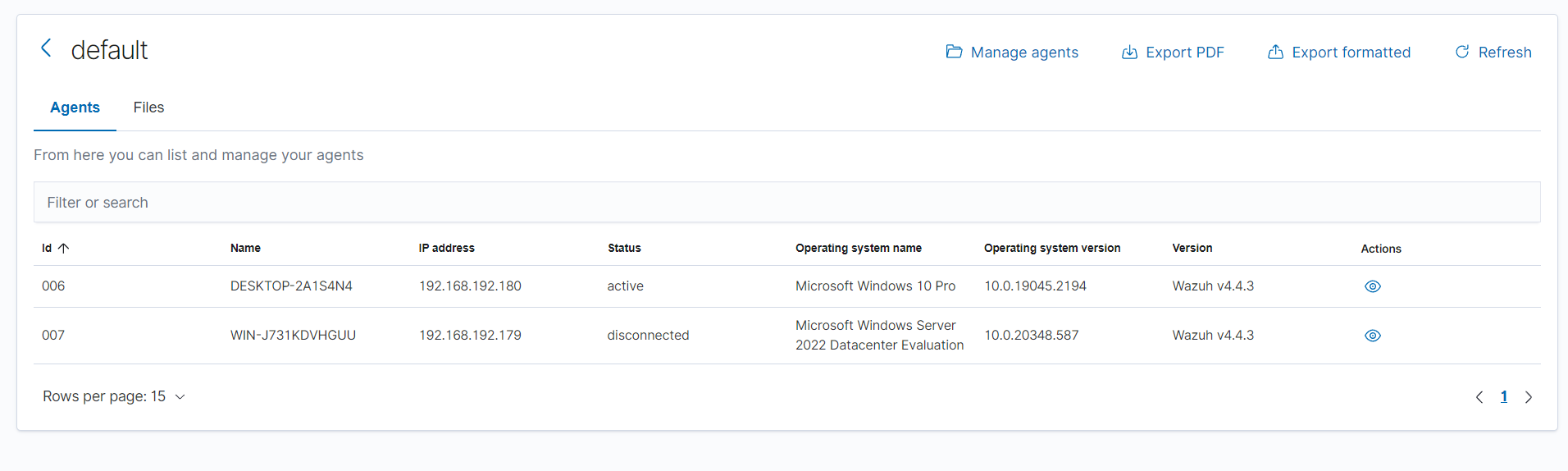
Real-time protection hoạt động như một hệ thống chống malware liên tục giúp ngăn chặn và loại bỏ các mối đe dọa độc hại trước khi chúng có thể gây hại cho máy tính.

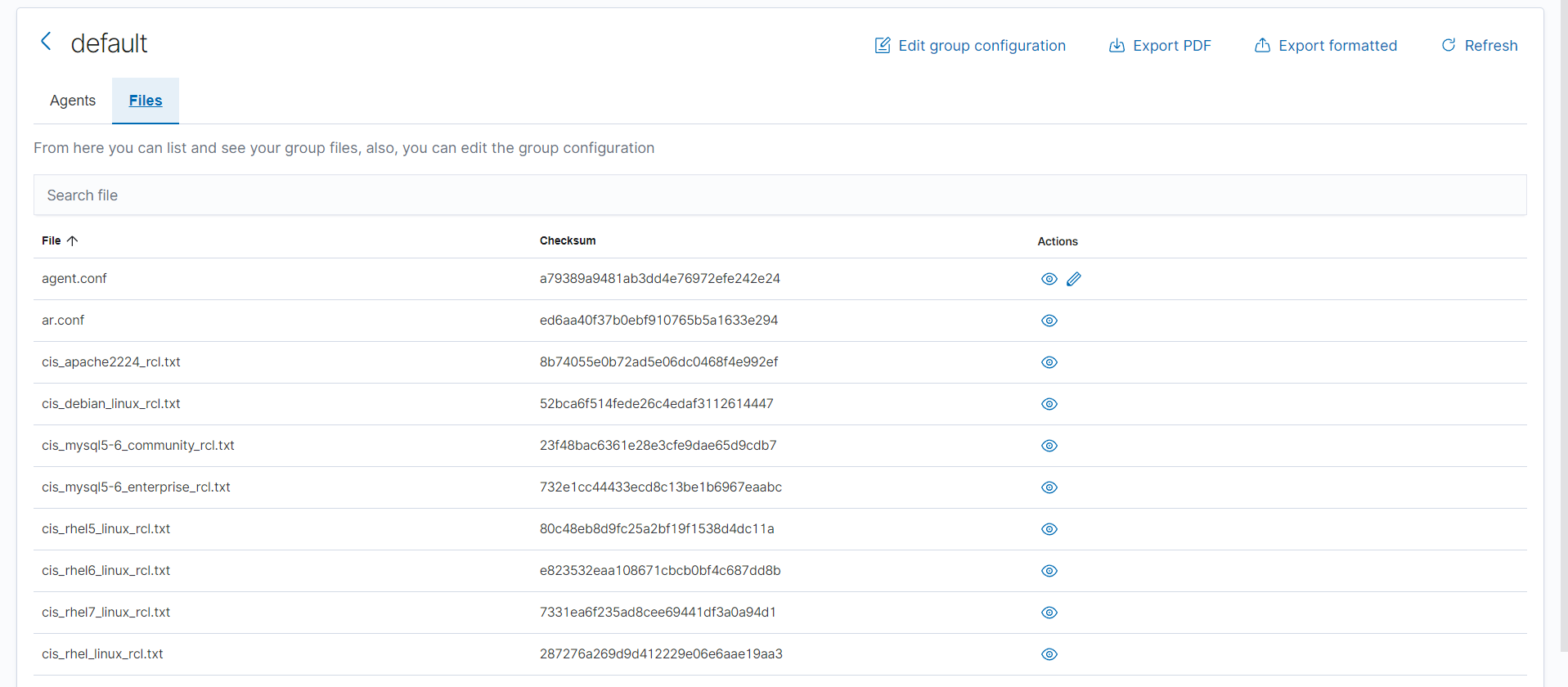
# Thực hiện

* Từ GUI của Wazuh Server ta thiết lập rule để thu thập log của window defender với agent win10: Chọn default group -> file -> edit agent.conf :

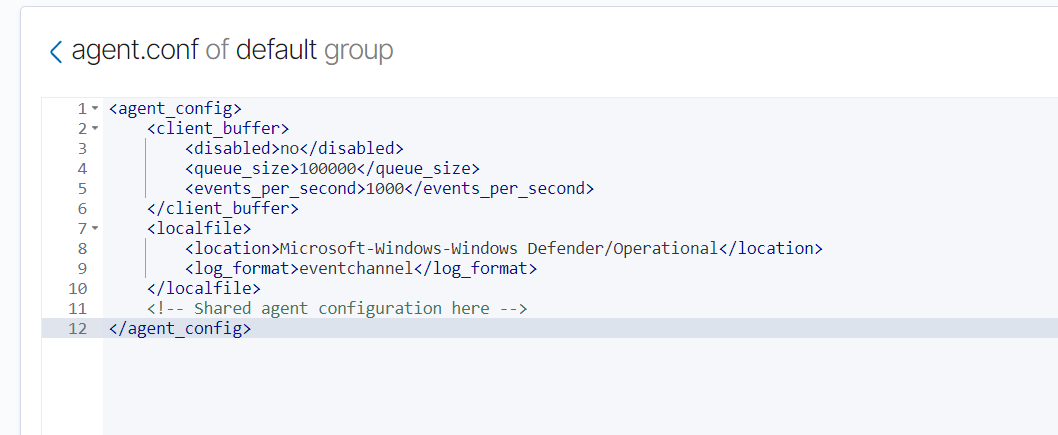








* Sau đó ta cấu hình rule như sau :



Cấu hình Client\_buffer :

+ Đây là bộ đệm dùng để giữ các log trước khi log được gửi đến hệ thống sự kiện

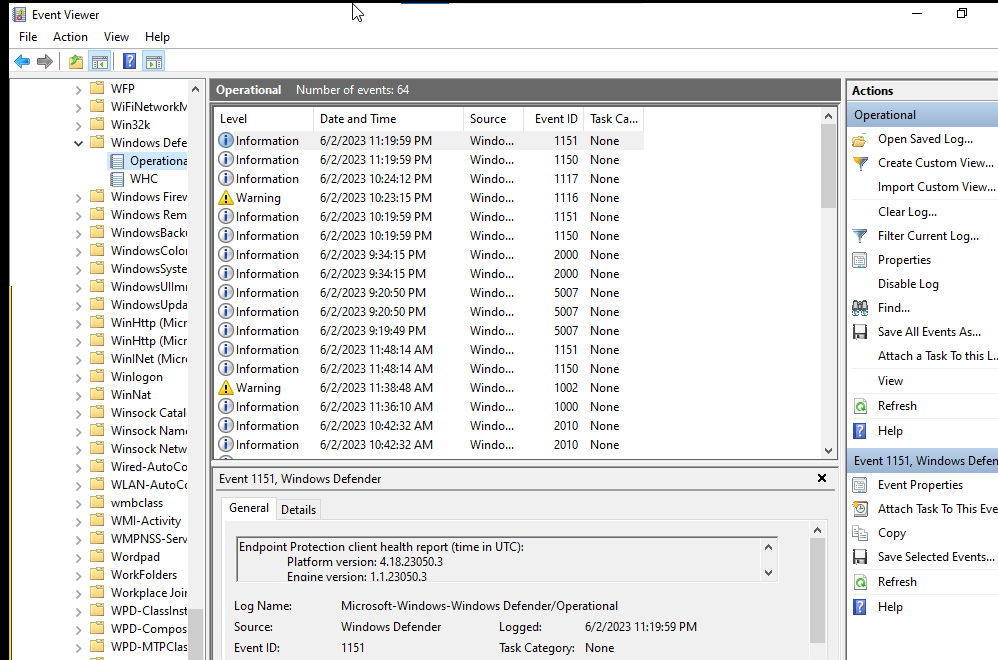
+ Cấu hình 3 thuộc tính : disabled: xác định Client\_buffer có bị vô hiệu hóa không , queue\_size: kích thước bộ đệm , số log tối đa mà bộ đệm có thể lưu trữ , events\_per\_second :số sự kiện tối đa mà client có thể gửi đến hệ thống

Cấu hình local\_file :

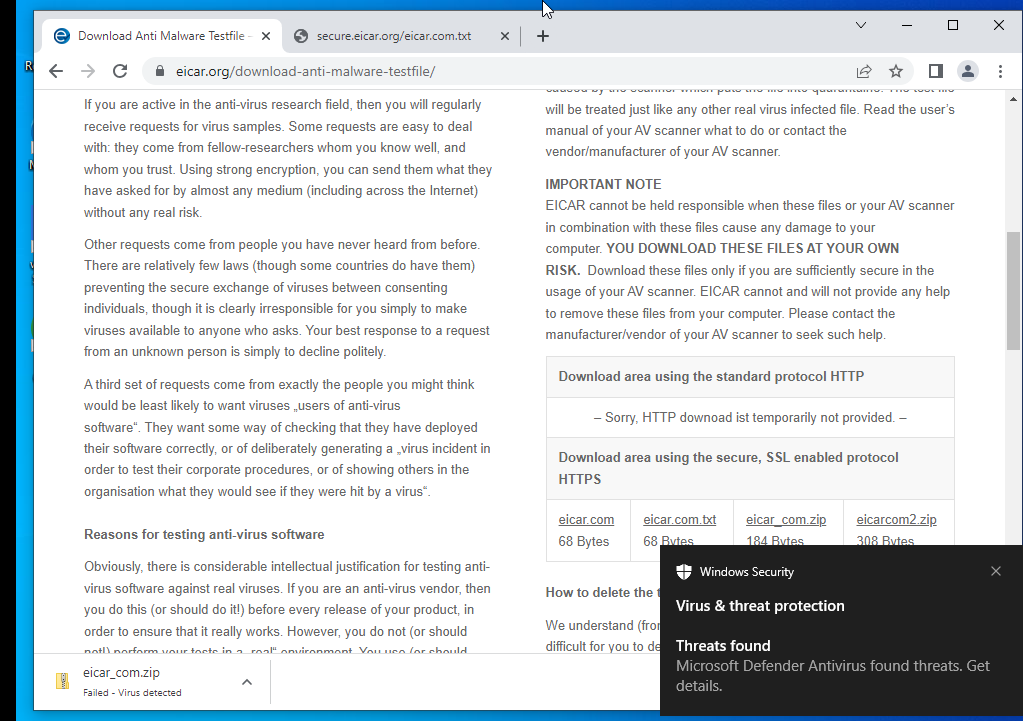
+ Việc cấu hình local\_file để ta có thể thu thập các log từ một tập tin

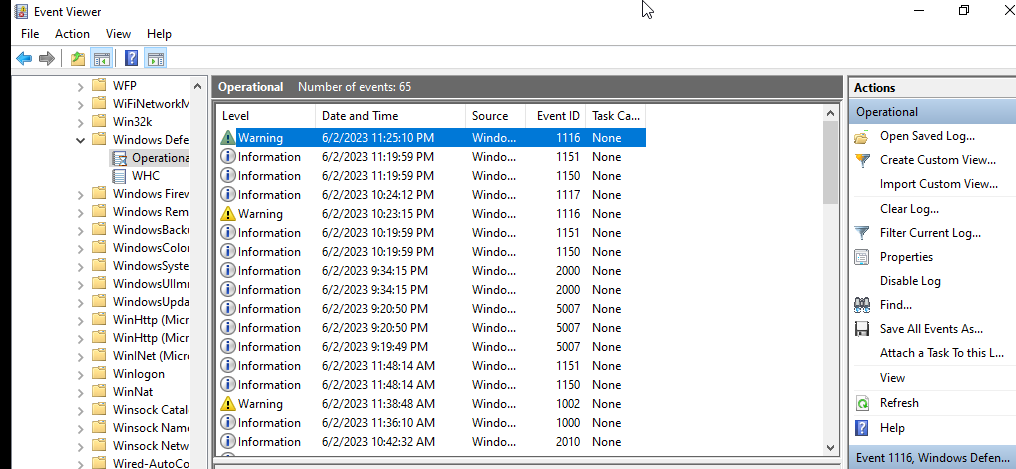
+ Cấu hình 2 thuộc tính : location: vị trí của tệp tin chưa log,log\_format: định dạng của log

* Sau khi cấu hỉnh rule , ta có thể xem log của Window Defender ở Win10 như sau : Event Viewer -> Application and Serivce Logs -> Microsoft -> Windows -> Window Defender -> Operational

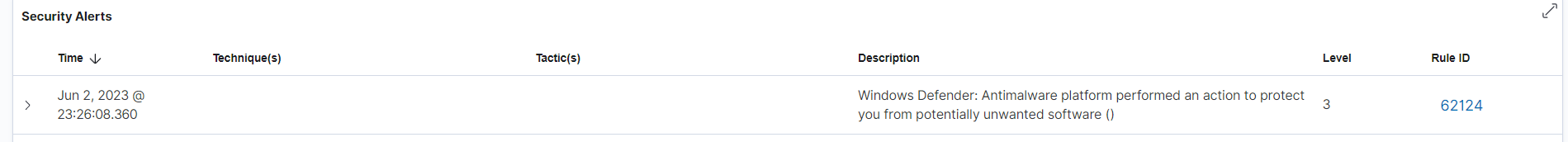


* Thực hiện tải một malware bất kỳ để xem log hiện thị ở Window Defender:





* Sau đó ta xem ở Wazuh có bắt được log tương tự hay không



Phát hiện thành công : log của wazuh cho ta biết các chi tiết cụ thể như sau :

