****HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA CÔNG NGHỆ THÔNG TIN 1

****

**BÁO CÁO BÀI TẬP LỚN**

**CÁC KỸ THUẬT GIẤU TIN**

**Đề tài: Giám sát và phát hiện các mối đe dọa an ninh dữ liệu**

**Giảng viên hướng dẫn: Đỗ Xuân Chợ**

**Nhóm lớp: 3**

**Nhóm bài tập: 11**

**Thành viên nhóm:**

**Nguyễn Văn Quân - B19DCAT146**

**Hoàng Vũ Hiến - B19DCAT062**

**Nguyễn Hoàng Hải - B19DCAT057**

***Hà Nội, 2023***

**MỤC LỤC**

[I. Tổng quan về DLP 3](#_Toc134181039)

[1. DLP là gì? 3](#_Toc134181040)

[2. DLP hoạt động như thế nào? 3](#_Toc134181041)

[3. Tầm quan trọng của DLP 4](#_Toc134181042)

[4. Có những loại kỹ thuật DLP phổ biến nào? 4](#_Toc134181043)

[5. Tại sao nên lựa chọn sử dụng DLP? 4](#_Toc134181044)

[6. Những yếu tố quan trọng hỗ trợ triển khai DLP 5](#_Toc134181045)

[7. Các công cụ và công nghệ DLP phổ biến 5](#_Toc134181046)

[II. Wazuh 6](#_Toc134181047)

[1. Giới thiệu về Wazuh 6](#_Toc134181048)

[2. Các thành phần 7](#_Toc134181049)

[2.1. Wazuh agent 7](#_Toc134181050)

[2.2. Wazuh server 9](#_Toc134181051)

[3. Ưu điểm và Nhược điểm 11](#_Toc134181052)

[3.1. Ưu điểm 11](#_Toc134181053)

[3.2. Nhược điểm 11](#_Toc134181054)

[III. Cài đặt và chạy thử 12](#_Toc134181055)

[1. Cài đặt wazuh 12](#_Toc134181056)

[2. Kiểm soát truy cập tài khoản 15](#_Toc134181057)

[3. Kiểm soát file truy cập 18](#_Toc134181058)

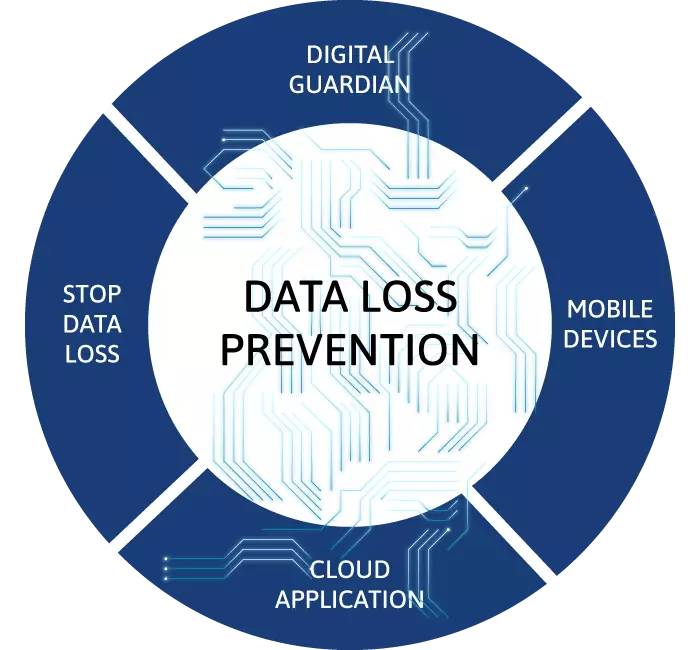
[4. Gửi cảnh báo qua email 21](#_Toc134181059)

[5. Chuyển tiếp nhật ký Windows Defender sang Wazuh 23](#_Toc134181060)

[IV. TỔNG KẾT 26](#_Toc134181061)

[V. TÀI LIỆU THAM KHẢO 26](#_Toc134181062)

1. **Tổng quan về DLP**
2. **DLP là gì?**

****

**DLP – Data Loss Prevention là một loại công nghệ sử dụng các công cụ phần mềm hỗ trợ và kỹ thuật nâng cao để bảo vệ dữ liệu quan trọng khỏi các truy cập trái phép.** Cụ thể DLP tiến hành áp dụng các chính sách bảo vệ tự động cho các phần khác nhau của một đối tượng dữ liệu đã được phân chia trước đó.

Đặc biệt, DLP sử dụng chiến lược bảo mật với nhiều lớp khác nhau đảm bảo cho các thông tin nhạy cảm luôn được bảo vệ trong [tường lửa](https://bkhost.vn/blog/firewall/). Điều này đồng thời cũng hỗ trợ các tổ chức có thể thực hiện nhiều công việc khác nhau như xem xét, cập nhật lưu trữ một cách linh hoạt.

Theo nghiên cứu cho thấy, cho đến năm 2021 đã có hơn 90% tổ chức lớn nhỏ áp dụng công nghệ DLP tích hợp. Con số này đã tăng 50% so với năm 2017. Nguyên nhân là do nhiều người dùng có nhu cầu làm việc tại nhà đi kèm với nguy cơ bị tấn công cao. Do đó, việc chuẩn bị một DLP là một biện pháp bảo vệ an toàn và hiệu quả.

1. **DLP hoạt động như thế nào?**

Phần mềm DLP có khả năng phát hiện và ngăn chặn các dữ liệu nhạy cảm có hiện tượng di chuyển bất thường. Trong đó bao gồm cả việc giám sát các dữ liệu đi vào hay di chuyển ra khỏi mạng công ty. Ngoài ra, DLP còn có thể ngăn chặn các hành vi sao chép trái phép từ các thiết bị máy tính thành viên bằng cách từ chối quyền đọc và ghi vào ổ USB.

Thông thường, DLP sẽ tự động cung cấp cho các tổ chức một tùy chọn gắn cờ nội dung không nhất quán. Điều này nhằm hỗ trợ người dùng có thể tự kiểm tra và ngăn chặn nội dung đó một cách dễ dàng. Các nhà phát triển đã cải tiến DPL bằng cách sử dụng [trí tuệ nhân tạo](https://bkhost.vn/blog/ai-tri-tue-nhan-tao/) dựa trên [Machine Learning](https://bkhost.vn/blog/machine-learning/) cho phép người dùng vừa học vừa cải thiện phương pháp bảo vệ dữ liệu.

1. **Tầm quan trọng của DLP**

Dữ liệu là yếu tố quan trọng nhất của các tổ chức hay doanh nghiệp. Nó quyết định đến các hoạt động kinh doanh và phát triển của doanh nghiệp đó. Vì thế, nếu doanh nghiệp đánh mất dữ liệu thì sẽ có nguy cơ bị phá sản và ngừng hoạt động.

Đối với cá nhân nếu làm mất dữ liệu sẽ phải đền bù tiền thiệt hại hoặc thậm chí phải chịu trách nhiệm hình sự. Một số giám đốc điều hành tại Target và Equifax đã phải từ chức sau những vi phạm dữ liệu và phải trả hàng triệu USD tiền phạt.

Do đó, việc bảo vệ dữ liệu luôn được chú trọng và quan tâm hàng đầu hiện nay. Bên cạnh đó là nhu cầu sử dụng các công cụ hiện đại để có thể hỗ trợ bảo vệ an toàn cho các dữ liệu. DLP là một trong những công cụ được nhiều người dùng và tổ chức săn đón nhất.

1. **Có những loại kỹ thuật DLP phổ biến nào?**

DLP mạng bao gồm tập hợp nhiều kỹ thuật có khả năng bảo vệ dữ liệu. Cụ thể như sau:

* DLP với kỹ thuật nhận dạng dữ liệu đảm bảo rằng chúng đều an toàn và không phải nhạy cảm. Các doanh nghiệp nên lựa chọn các công cụ có tính năng tự động phân loại và xác định dữ liệu đáng tin cậy.
* Phần mềm PLD có tính năng bảo vệ dữ liệu luôn được định tuyến an toàn trong quá trình di chuyển, bao gồm nội bộ và các phạm vi hoạt động bên ngoài.
* Kỹ thuật bảo vệ dữ liệu khi trong trạng thái nghỉ của DLP thực sự hữu ích. Điều này đảm bảo an toàn cho các dữ liệu nằm trong cơ sở dữ liệu, ứng dụng, kho [lưu trữ đám mây](https://bkhost.vn/blog/luu-tru-dam-may/), thư mục máy tính hay trên các phương tiện lưu trữ khác.
* Endpoint DLP là một loại tính năng giúp bảo vệ dữ liệu ở các thiết bị đầu cuối trên điện thoại và máy tính. Đồng thời, nó còn có thể ngăn chặn việc sao chép hay [mã hóa](https://bkhost.vn/blog/ma-hoa/) các dữ liệu trái phép trong quá trình di chuyển từ vị trí này đến vị trí khác.
* Kỹ thuật phát hiện dữ liệu bị rò rỉ và tiến hành tìm kiếm các hành vi gây ra tình trạng này.
* Cloud DLP là loại kỹ thuật phổ biến được sử dụng nhiều nhất giúp quản lý và bảo vệ các dữ liệu nhạy cảm trong [phần mềm ứng dụng](https://bkhost.vn/blog/phan-mem-ung-dung/) hoặc cơ sở hạ tầng dưới dạng dịch vụ.

1. **Tại sao nên lựa chọn sử dụng DLP?**

Theo nghiên cứu năm 2022 của Gartner cho thấy rằng có đến 35% các doanh nghiệp không thể triển khai DLP. Điều này khiến cho họ phải chịu các tổn hại lớn như đóng tiền phạt, chịu hình phạt pháp luật hay bị mất danh tiếng. Do đó, việc sử dụng DLP là quan trọng và cần thiết. Cụ thể như sau:

* Tránh các mức phạt lớn do vi phạm dữ liệu.
* Tuân thủ các quy định an toàn về nhu cầu mở rộng và quản lý dữ liệu.
* Giúp bảo vệ khối lượng lớn các dữ liệu quan trọng của công ty và doanh nghiệp khỏi mục tiêu tấn công của kẻ lừa đảo muốn đánh cắp để kiếm lời. Chẳng hạn như đánh cắp danh tính, gian lận bảo hiểm hay lừa đảo quảng cáo.
* Các tổ chức và doanh nghiệp lựa chọn CISO để xây dựng các chính sách quản trị nhằm bảo vệ quyền sở hữu trí tuệ cũng như một số thông tin độc quyền khác.
* Các tổ chức có xu hướng sử dụng DLP để bù đắp sự thiếu hụt về các chuyên gia bảo mật có nhiều kinh nghiệm.
* DPL bảo vệ các dịch vụ đám mây, thiết bị đầu cuối và các công cụ từ nhà cung cấp bên thứ ba khỏi các cuộc tấn công Ransomware hay các mối đe dọa [an ninh mạng](https://bkhost.vn/blog/an-ninh-mang-cyber-security/) khác.

1. **Những yếu tố quan trọng hỗ trợ triển khai DLP**

Để có thể triển khai các chương trình DLP hiệu quả nhất thì các tổ chức hay người dùng cần đảm bảo được các bước sau đây:

* Cần kiểm tra và xác thực các vấn đề về dữ liệu bằng cách sử dụng DLP từ các nhà cung cấp như Barracuda Networks, Cisco và McAfee.
* Các tổ chức nên sử dụng một [Framework](https://bkhost.vn/blog/framework/) để phân loại dữ liệu, bao gồm dữ liệu có cấu trúc, dữ liệu không có cấu trúc, thông tin nhận dạng cá nhân, dữ liệu tài chính, dữ liệu quy định và dữ liệu sở hữu trí tuệ.
* Cần thiết lập các chính sách xử lý và khắc phục dữ liệu đúng cách giúp quá trình quản lý trở nên dễ dàng hơn.
* Bắt đầu triển khai một chương trình DLP tập trung duy nhất cho nhiều đơn vị kinh doanh khác nhau. Điều này giúp quản lý các dữ liệu một cách nhất quán và tổng thể.
* Cần hướng dẫn và đào tạo đội ngũ chuyên viên về các chính sách và thủ tục bảo mật về DLP.

1. **Các công cụ và công nghệ DLP phổ biến**

Trên thị trường công nghệ có mắt hai phiên bản DLP chính đó là chuyên dụng và tích hợp. Trong đó DLP chuyên dụng bao gồm các sản phẩm phần mềm độc quyền có tính chuyên sâu và khá phức tạp. DLP tích hợp khá cơ bản và có thể hoạt động với nhiều công cụ bảo mật khác nhau. Đặc biệt, loại DLP này giúp tiết kiệm chi phí sử dụng hiệu quả hơn so với DLP chuyên dụng.

Việc sở hữu một công cụ giúp bảo vệ các dữ liệu khỏi tầm ngắm của kẻ tấn công là điều rất quan trọng. Hiện nay có rất nhiều nhà cung cấp DLP nổi tiếng và được ưa chuộng. Cụ thể như sau:

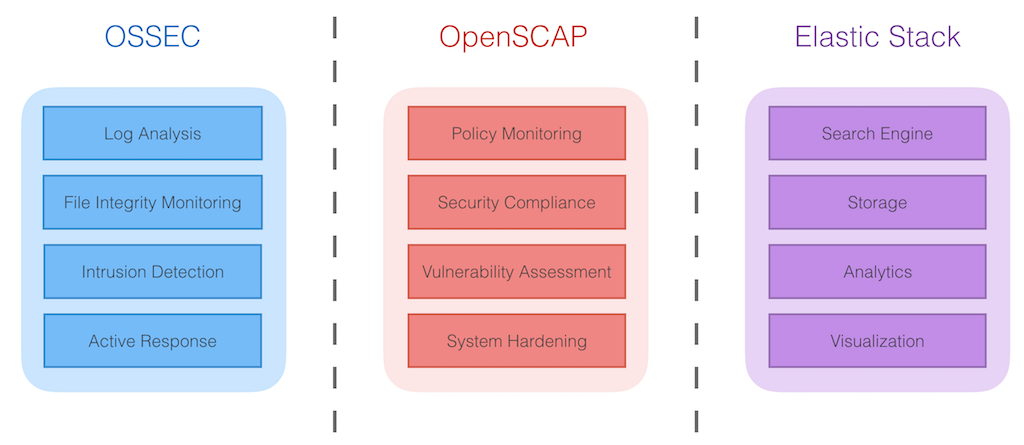
* Broadcom Symantec Data Loss Prevention cung cấp thiết bị đầu cuối, trung tâm dữ liệu và dịch vụ đám mây.
* Check Point Data Loss cung cấp các công cụ chuyên lọc dữ liệu tại các phạm vi cụ thể.
* CoSoSys Endpoint Protector cung cấp trình bảo vệ tích hợp dành cho Windows, Apple và [Linux](https://bkhost.vn/blog/he-dieu-hanh-linux/).
* ManageEngine Device Control Plus cung cấp trình bảo vệ điểm cuối và bảo mật USB.
* McAfee Total Protection for DLP cung cấp các công cụ giúp khám phá, theo dõi và phòng ngừa.
* SolarWinds Data Loss Prevention with [Access](https://bkhost.vn/blog/microsoft-access/) Rights Manager cung cấp trình quản lý quyền truy cập tốt nhất hiện nay.
* Viking Cloud Endpoint Protection cung cấp các công cụ chịu trách nhiệm về các rủi ro nội bộ.

1. **Wazuh**
2. **Giới thiệu về Wazuh**

Wazuh là một giải pháp an ninh mở và miễn phí được phát triển trên nền tảng Elastic Stack. Nó cung cấp cho người dùng các tính năng để giám sát và phát hiện các mối đe dọa an ninh trong môi trường máy chủ và ứng dụng.

Wazuh được thiết kế để cung cấp các tính năng chuyên môn cho việc quản lý an ninh, bao gồm phát hiện xâm nhập, giám sát chính sách bảo mật, quản lý sự kiện và phân tích các cảnh báo an ninh. Wazuh cũng hỗ trợ các tính năng để phát hiện các mối đe dọa phổ biến như tấn công từ chối dịch vụ (DoS), tấn công dò tìm xung đột (port scan), tấn công tìm lỗ hổng (vulnerability scan) và tấn công tràn đổ bộ nhớ đệm (buffer overflow).

Wazuh là 1 project mã nguồn dùng cho việc bảo vệ an ninh. Được xây dựng từ các thành phần : OSSEC HIDS, OpenSCAP và Elastic Stack.

****

OSSEC HIDS : host-based Intrusion Detection System (HIDS) được dùng cho việc phát hiện xâm nhập, hiển thị và giám stas. Nó dựa vào 1 multi-platform agent cho việc đẩy dữ liệu hệ thống (log message, file hash và phát hiện bất thường) tới 1 máy quản lý trung tâm, nơi sẽ phân tích và xử lý, dựa trên các cảnh báo an ninh. Các agent truyền event data event data tới máy quản lý trung tâm thông qua kênh được bảo mật và xác thực. OSSEC HIDS cung cấp syslog server trung tâm và hệ thống giám sát không cần agent, cung cấp việc giám sát tới các event và thay đổi trên các thiết bị không cài được agent như firewall, switch, router, access point, thiết bị mạng....

OpenSCAP là 1 OVAL (Open Vulnerability Assesment Language) và XCCDF (Extensible Configuration Checklist Description Format) được dùng để kiểm tra cấu hình hệ thống và phát hiện các ứng dụng dễ bị tấn công. Nó được biết đến như là một công cụ được thiết kế để kiểm tra việc tuân thủ an ninh của hệ thống sử dụng các tiêu chuẩn an ninh dùng cho môi trường doanh nghiệp

ELK Stack Sử dụng cho việc thu thập, phân tích, index, store, search và hiển thị dữ liệu log.

1. **Các thành phần**
   1. **Wazuh agent**

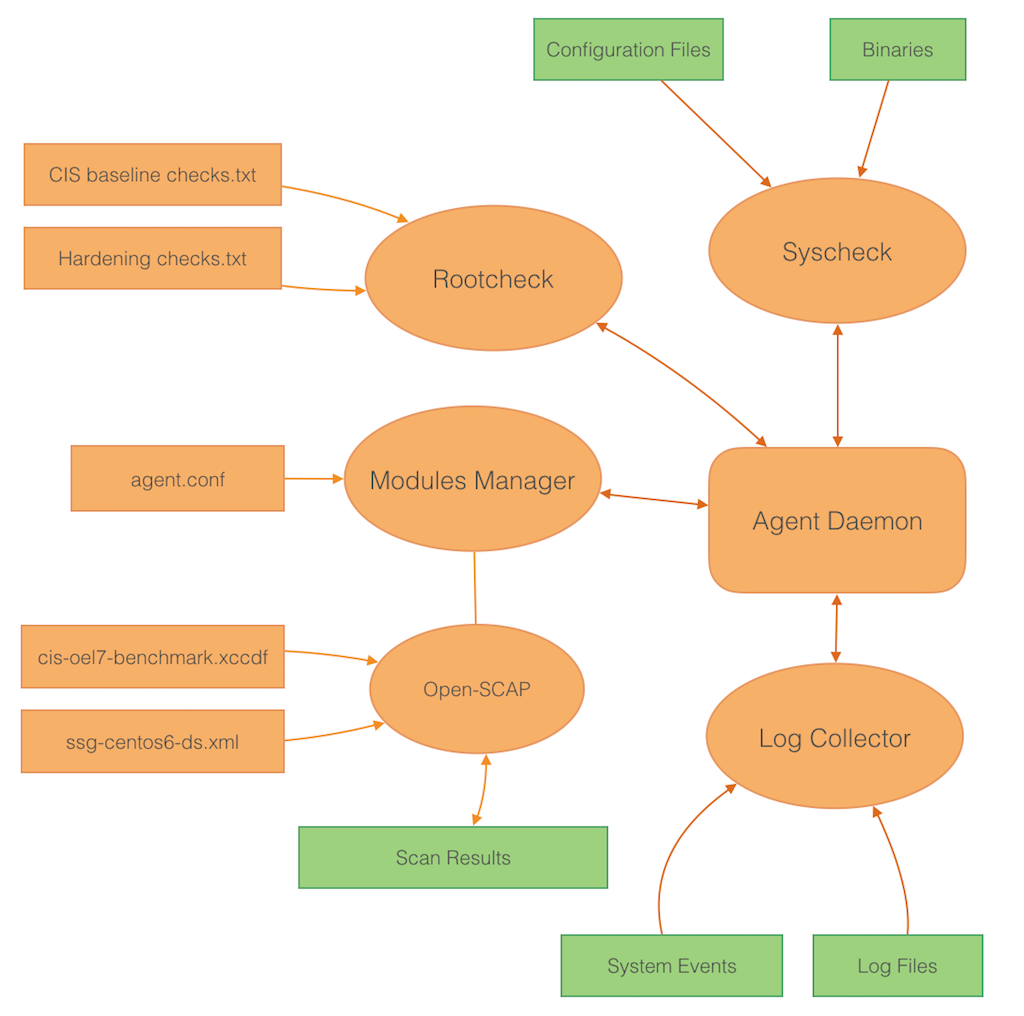
Chạy trên : Windows, Linux, Solaris, BSD hoặc MAC OS. Dùng thu thập các dạng khác nhau của dữ liệu hệ thống và ứng dụng. Dữ liệu được chuyển tới Wazuh server thông qua 1 kênh được mã hóa và xác thực. Để thiết lập kênh này, 1 quá trình đăng ký bao gồm pre-shared key duy nhất được thiết lập.

Các agent có thể dùng để giám sát server vật lý, máy ảo, cloud instance (AWS, Azure hoặc Google cloud). Các các cài đặt pre-compile agent có sẵn cho các OS : Linux, AIX, Solaris, Windows và Darwin (Mac OS X).

Trên các OS Unix-based, agent chạy trên multiple process, các process này liên lạc với nhau thông qua local Unix domain socket. 1 trong các process này phụ trách việc liên lạc và gửi dữ liệu tới Wazuh server. Trên Windows, chỉ có 1 agent process chạy trên multiple task sử dụng mutexes.

Các agent task hoặc process khác nhau được dùng để giám sát hệ thống theo các cách khác nhau (giám sát sự thay đổi về file, đọc log, quét các thay đổi hệ thống).

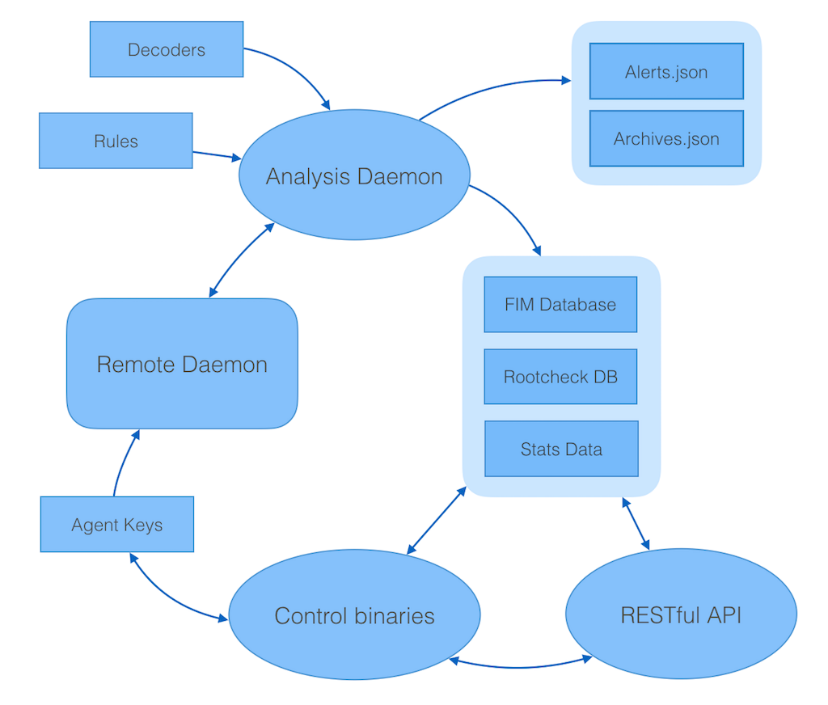
Sơ đồ sau thể hiện các internal task và process diễn ra trên các agent level.



Tất cả các process agent có mục tiêu và thiết lập khác nhau.

* Rootcheck : Thực hiện các task liên quan đến phát hiện về Rootkits, malware và các bất thường của hệ thống. Nó chạy 1 số công cụ kiểm tra an ninh cơ bản dựa vào các file cấu hình hệ thống.
* Log Collector: Dùng để đọc và thu thập các log message, bao gồm các các file flat log như Windows event log và thậm chí là Windows Event Channel. Nó cũng được cấu hình để chạy định kỳ và bắt 1 số output của các câu lệnh cụ thể.
* Syscheck : Process này thực hiện file integrity monitoring (FIM) (Giám sát tính toàn vẹn của file). Nó cũng có thể giám sát registry key trên Windows. Nó sẽ bắt các thay đổi về nội dung file, quyền và các thuộc tính khác, cũng như phát hiện việc tạo và xóa file.
* OpenSCAP : Được dùng để publish OVAL và XCCDF dựa vào các hồ sơ bảo mật cơ bản, định kỳ quét hệ thống, nó sẽ phát hiện được các ứng dụng và cấu hình sẽ bị tấn công, không tuân theo các chuẩn được xác định theo CIS (Center of Internet Security)
* Agent Daemon : Process nhận dữ liệu được tạo hoặc được thu thập bởi tất cả các thành phần agent khác. Nó nén, mã hóa và phân phối dữ liệu tới server thông qua kênh được xác thực. Process này chạy trên "chroot" enviroment được cô lập, có nghĩa rằng nó sẽ hạn chế truy cập tới các hệ thống được giám sát. Điều này cải thiện được an toàn cho agent vì process đó là process duy nhất kết nối tới mạng.
* Rootkits : Phần mềm hoặc công cụ phần mềm che giấu sự tồn tại của 1 phần mềm khác, thường là virus xâm nhập vào hệ thống.
* Malware : Mọi loại mã gây hại trên máy tính người dùng : spyware, trojan, virus...
  1. **Wazuh server**

Thành phần server phụ trách việc phân tích dữ liệu nhận từ agent, tạo các ngưỡng cảnh báo khi 1 event ánh xạ với rule (phát hiện xâm nhập, thay đổi file, cấu hình không tương thích với policy, rootfit...)



Server thông thường chạy các thành phần agent với mục tiêu giám sát chính nó. Một số thành phần server chính là :

* **Registration service** : Được dùng để register agent mới được việc cung cấp và phân phối các key xác thực pre-shared, các key này là độc nhất với mỗi agent. Process này chạy như 1 network service và hỗ trợ việc xác thực qua TLS/SSL với 1 fixed password.
* **Remote daemon service** : Service này nhận dữ liệu từ agent. Nó sử dụng pre-shared key để xác thực định danh của mỗi agent và mã hóa giao tiếp với chúng.
* **Analysis daemon** : Process này thực hiện việc phân tích dữ liệu. Nó sử dụng các bộ giải mã để nhận dạng thông tin được xử lý (các Windows event, SSHD logs...) và sau đó giải nén các yếu tố dữ liệu thích hợp từ log message (source ip, event id, user...) Sau đó, bằng cách sử dụng các rule được định nghĩa bằng cách pattern đặc biệt trên bộ giải mã, nó sẽ tạo các ngưỡng cảnh báo thậm chí ra lệnh để thực hiện các biện pháp đối phó như chặn IP trên firewall.
* **RESTful API** : Cung cấp interface để quản lý và giám sát cấ hình và trạng thái triển khai của các agent. Nó cũng được dùng bởi Wazuh web interface (Kibana)

Wazuh tích hợp với Elastic stack để cung cấp các log message đã được giải mã và đánh index bởi Elasticsearch, cũng như là 1 web console real-time cho việc cảnh báo và phân tích log. Wazuh web interface (chạy trên Kibana) có thể dùng để quản lý và giám sát hạ tầng Wazuh

Một Elasticsearch index là một tập hợp các document có một chút các đặc trưng tương tự nhau (như các trường chung hoặc các yêu cầu về data retention được chia sẻ). Wazuh sử dụng 3 index khác nhau, được tạo hàng ngày và lưu trữ các dạng event khác nhau :

* **Wazuh-alert** : Index cho các cảnh báo được sinh ra bởi Wazun server mỗi khi một event ứng với rule tạo ra.
* **Wazuh-events** : Index cho tất cả các event (archive data) được nhận từ các agent, bất kể có ứng với rule hay không.
* **Wazuh-monitoring**: Index cho dữ liệu liên quan đến trạng thái agent. Nó được dùng bởi web interface cho việc hiển thị agent đã hoặc đang "Active", "Disconnect" hoặc "Never connected"

Với các index trên, document là các cảnh báo, archived event hoặc status event riêng lẻ.

Một Elasticsearcg index được chia tới 1 hoặc nhiều shard, và mỗi shard có thể có 1 hoặc nhiều replica. Mỗi primary và replica shard là 1 Lucene index đơn lẻ. Vì vậy 1 Elasticsearch index được tạo bởi nhiều Lucene index. Khi 1 tìm kiếm chạy trên 1 Elasticsearch index, search đó được xử lý trên các shard song song, và kết quả được merge lại. Việc chia nhỏ các Elasticsearch tới nhiều shard và replica cũng được dùng với Elasticsearch cluster với mục tiêu là mở rộng việc tìm kiếm và HA. Một Elasticsearch cluster single-node thường chỉ có 1 shard mỗi index và không có replica.

1. **Ưu điểm và Nhược điểm**
   1. **Ưu điểm**

Wazuh là một giải pháp giám sát an ninh mã nguồn mở, cung cấp các tính năng bảo mật mạnh mẽ và hỗ trợ các tổ chức trong việc phát hiện các mối đe dọa an ninh và tấn công vào hệ thống của họ. Tuy nhiên, như bất kỳ công nghệ nào khác, Wazuh cũng có những ưu điểm và nhược điểm riêng. Dưới đây là một số ưu điểm của Wazuh:

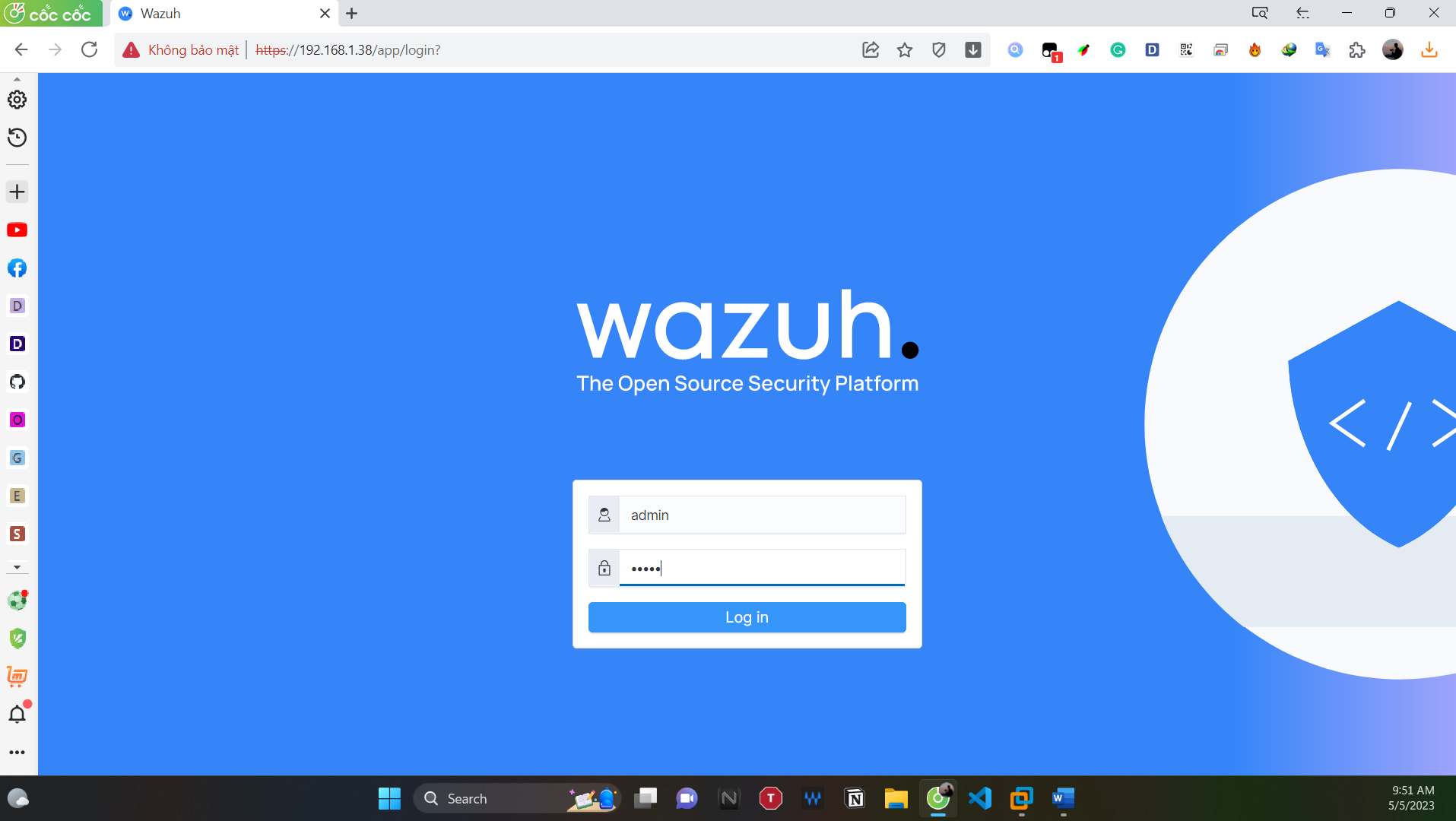
* Mã nguồn mở: Wazuh là một giải pháp mã nguồn mở, cho phép người dùng tùy chỉnh và sửa đổi các tính năng để phù hợp với yêu cầu cụ thể của họ.
* Phát hiện sớm và phản ứng nhanh: Wazuh có khả năng phát hiện các mối đe dọa và tấn công vào hệ thống một cách nhanh chóng và tự động, giúp các tổ chức có thể phản ứng kịp thời để bảo vệ hệ thống của mình.
* Tích hợp với các công cụ bảo mật khác: Wazuh có thể tích hợp với các công cụ bảo mật khác để cung cấp một hệ thống an ninh toàn diện cho tổ chức.
* Giám sát và báo cáo: Wazuh cung cấp các công cụ giám sát và báo cáo để giúp người dùng theo dõi các hoạt động an ninh của hệ thống.
  1. **Nhược điểm**
* Khó sử dụng: Wazuh là một giải pháp phức tạp và khó sử dụng đối với các người dùng không có kinh nghiệm về an ninh mạng.
* Tốn tài nguyên hệ thống: Wazuh yêu cầu một số lượng tài nguyên hệ thống khá lớn để hoạt động hiệu quả, có thể gây ảnh hưởng đến hiệu suất của hệ thống.
* Có thể xảy ra các báo động giả: Vì Wazuh sử dụng nhiều kỹ thuật phát hiện đa dạng, nó có thể tạo ra các báo động giả nếu không được cấu hình đúng.

Tóm lại, Wazuh là một giải pháp giám sát an ninh mạnh mẽ, tuy nhiên, nó cũng có những nhược điểm nhất định và có thể không phù hợp với một số tổ chức hoặc người dùng không có kinh nghiệm về an ninh mạng. Tuy nhiên, với sự tích hợp với các công cụ bảo mật khác và khả năng phát hiện sớm và phản ứng nhanh, Wazuh vẫn là một giải pháp an ninh mạng rất đáng tin cậy cho các tổ chức. Để sử dụng Wazuh hiệu quả, người dùng nên có một kiến thức cơ bản về an ninh mạng và tài nguyên hệ thống đủ mạnh để đáp ứng yêu cầu của giải pháp. Ngoài ra, cấu hình chính xác và theo dõi các báo động giả cũng là rất quan trọng để đảm bảo tính hiệu quả của Wazuh trong việc phát hiện các mối đe dọa và bảo vệ hệ thống.

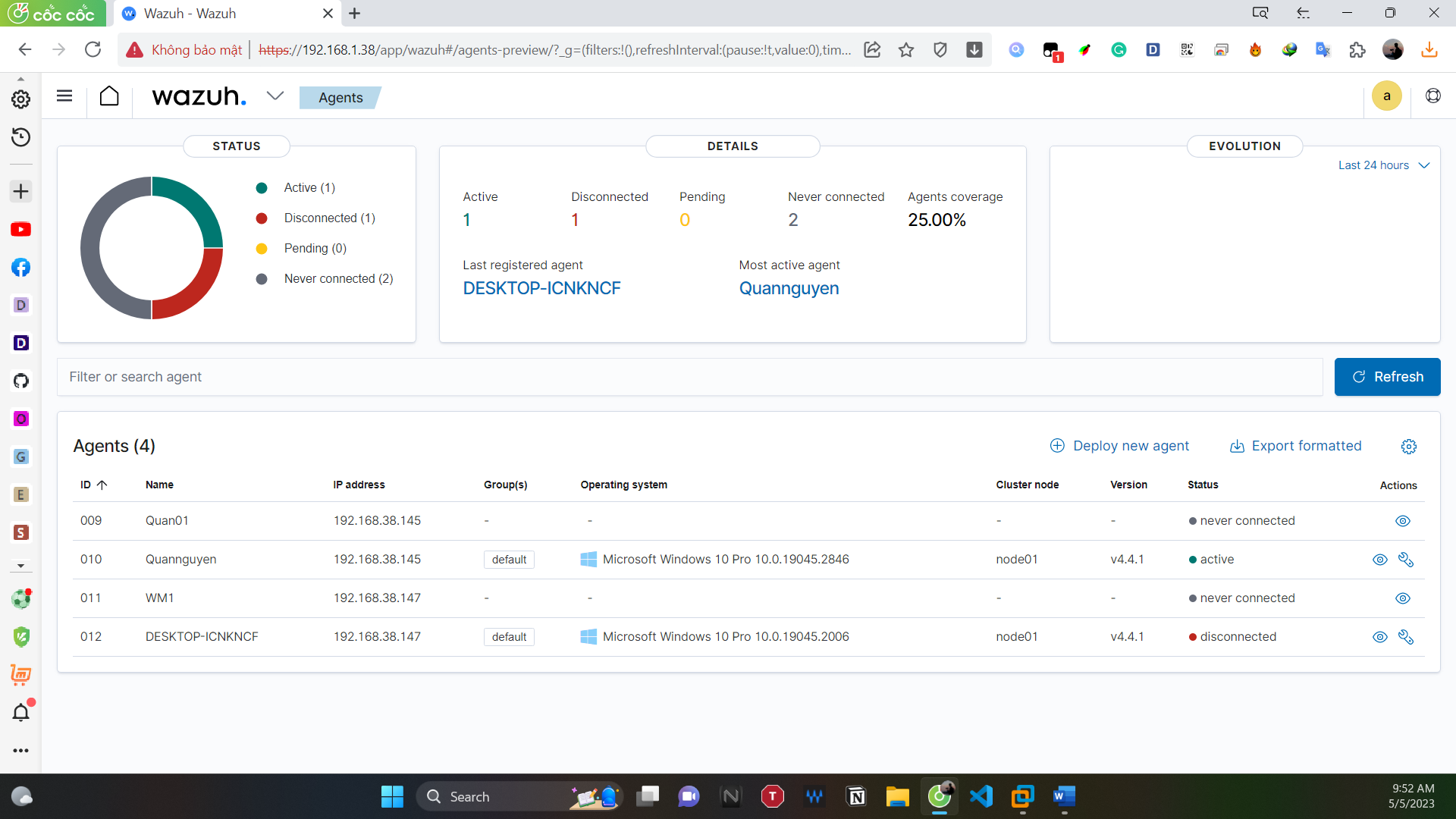
1. **Cài đặt và chạy thử**
2. **Cài đặt wazuh**



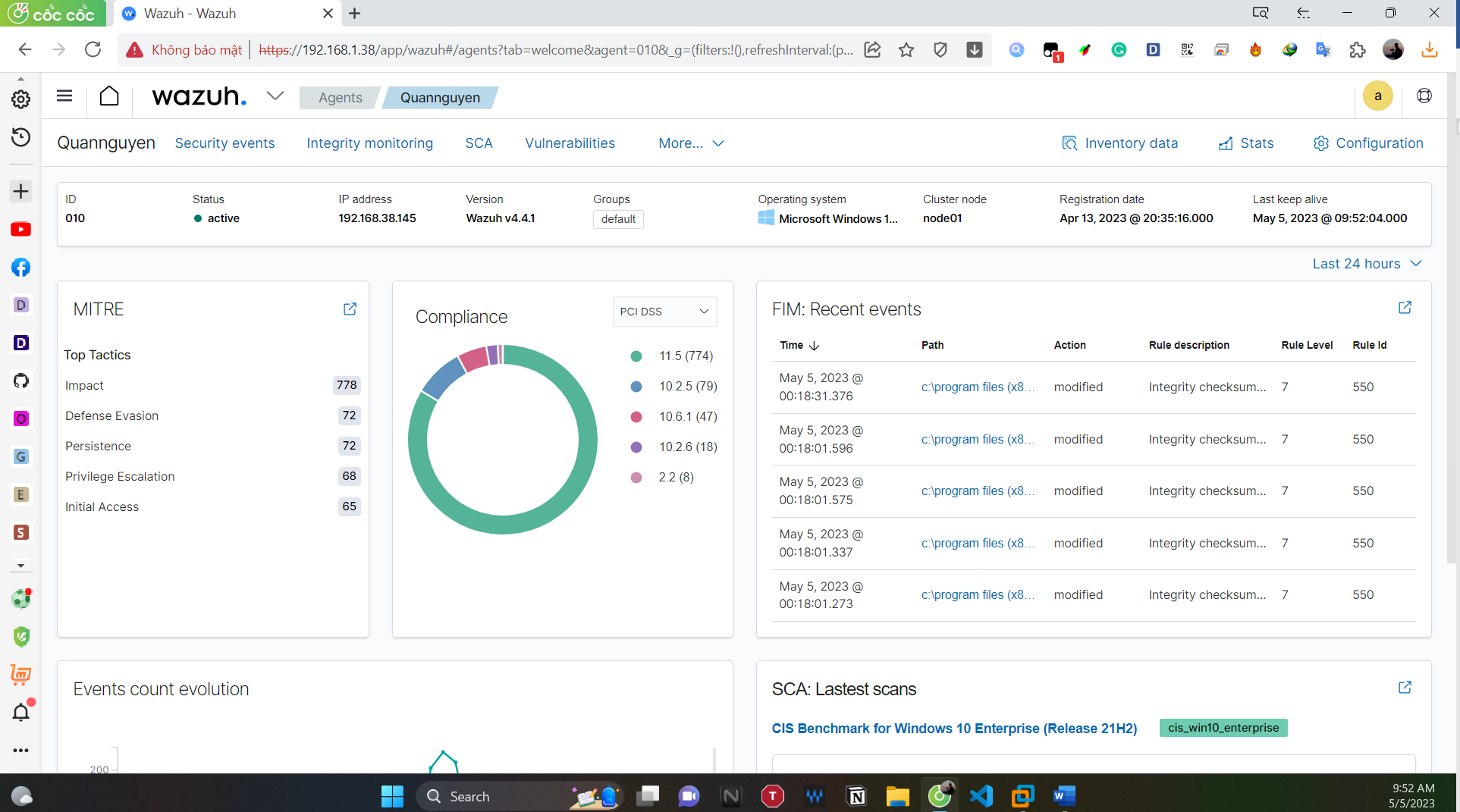
Cấu hình wazuh server trên máy ảo



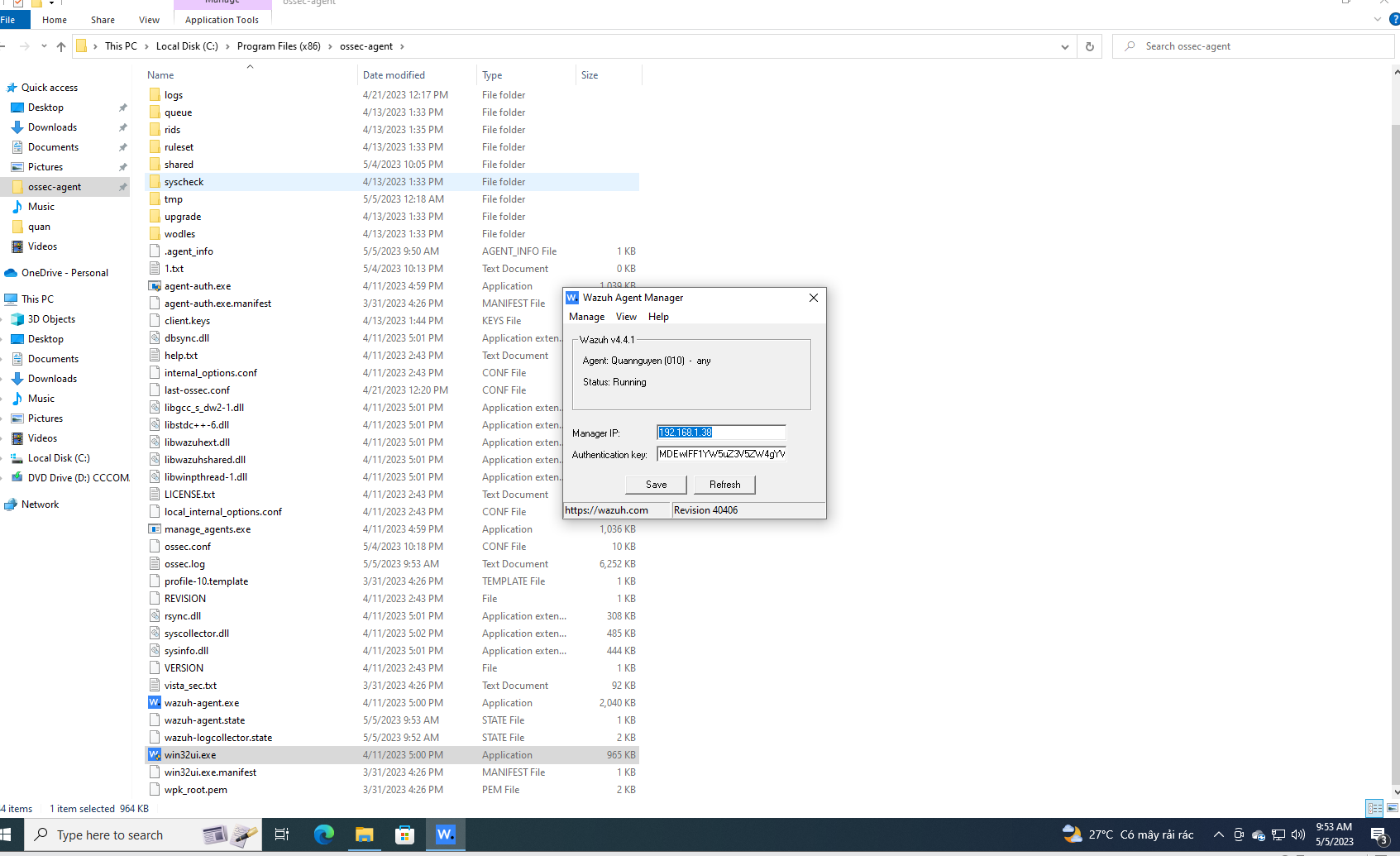
Giao diện đăng nhập



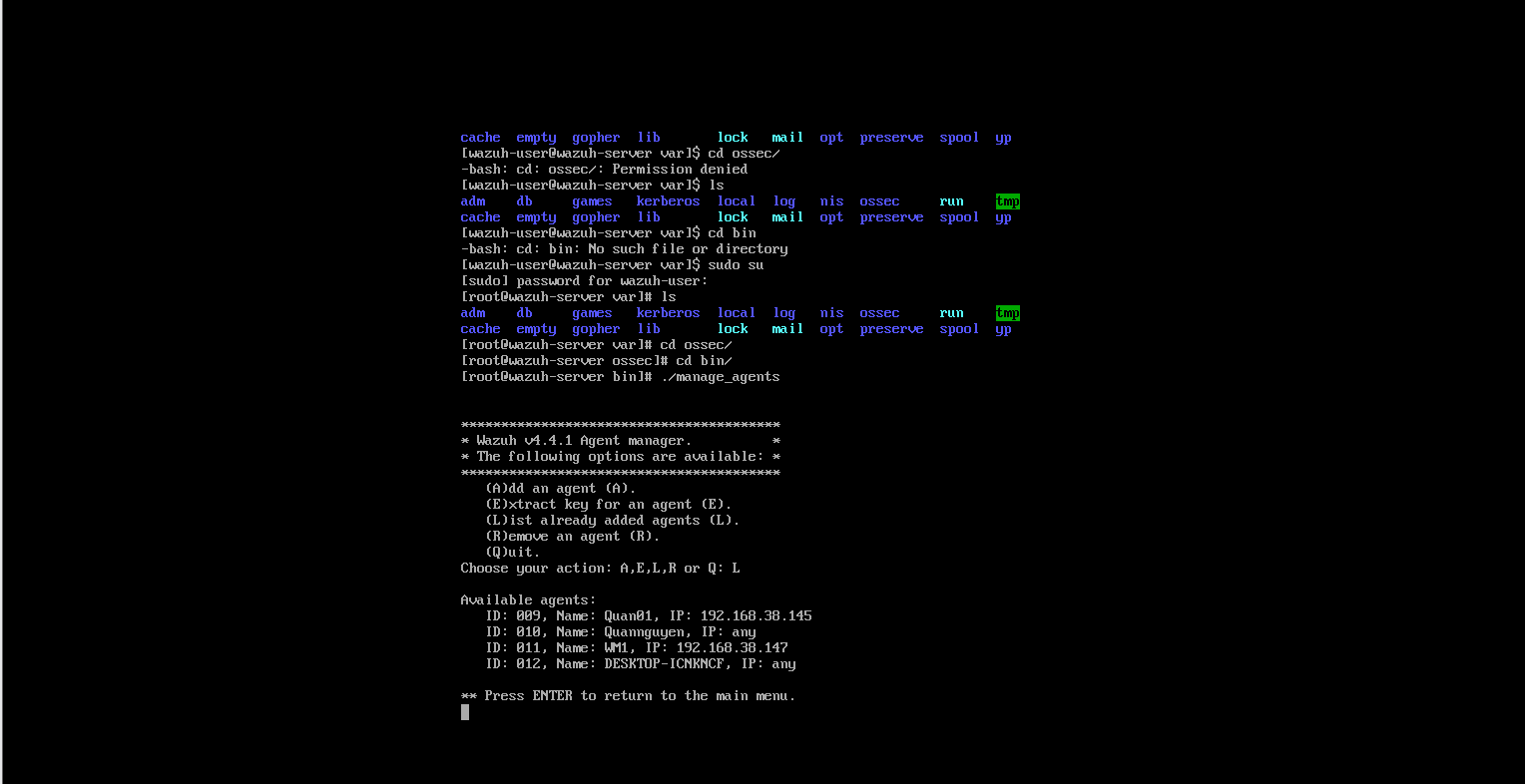
Giao diện sau khi đăng nhập



Các tab chức năng

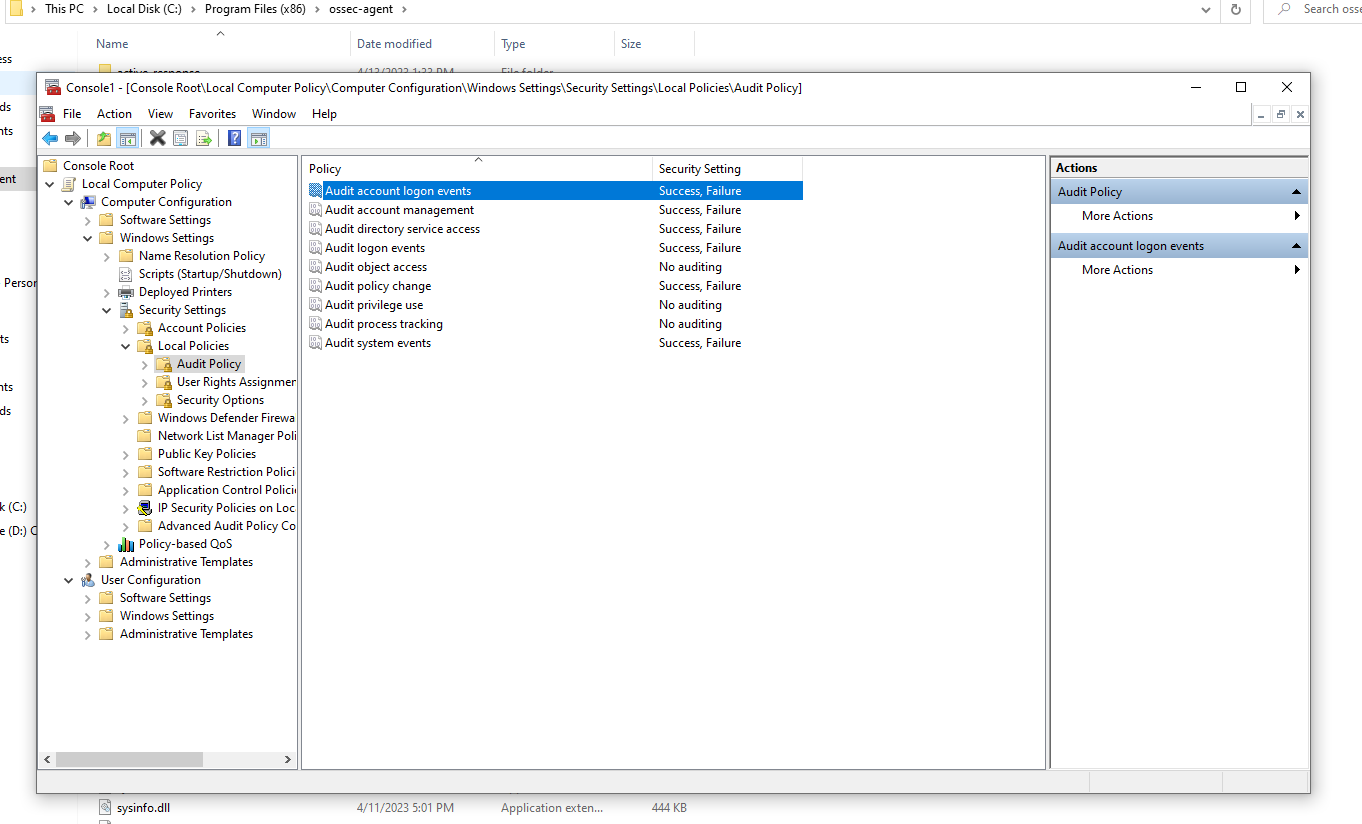


Cài đặt wazuh agent

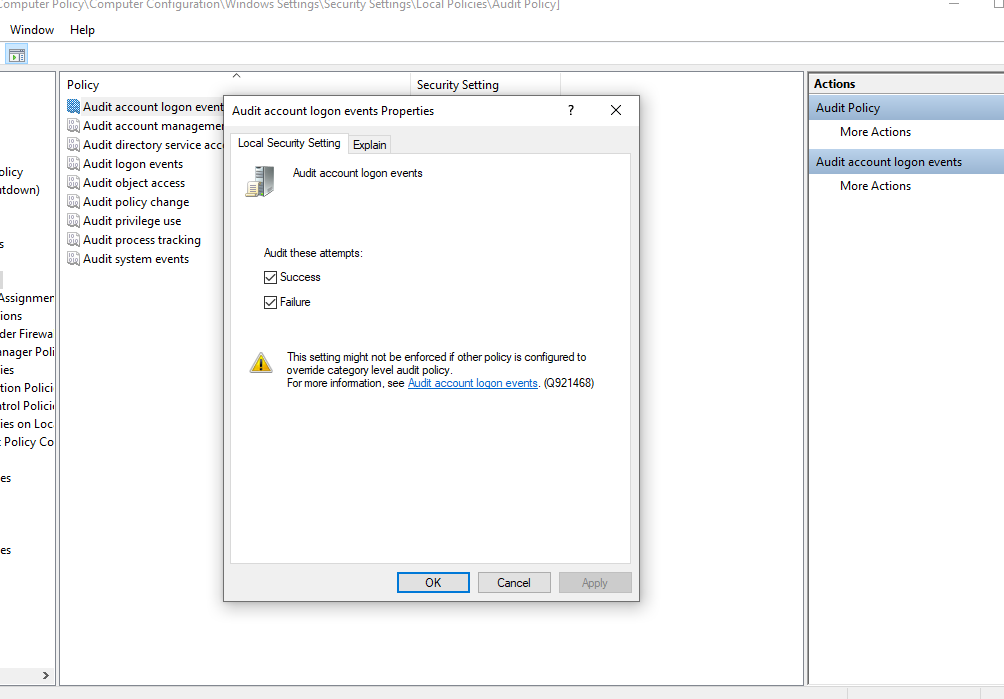


Thêm agent và tạo ssh Key cho agent

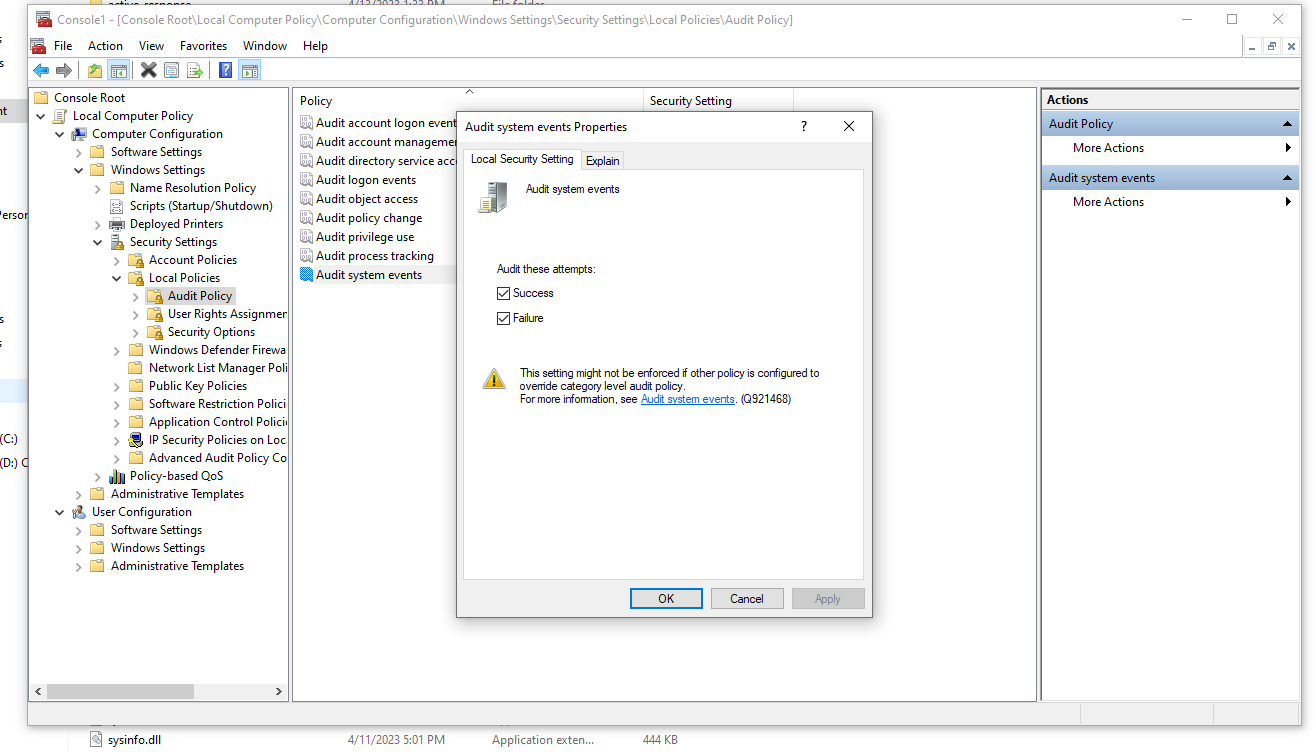
1. **Kiểm soát truy cập tài khoản**



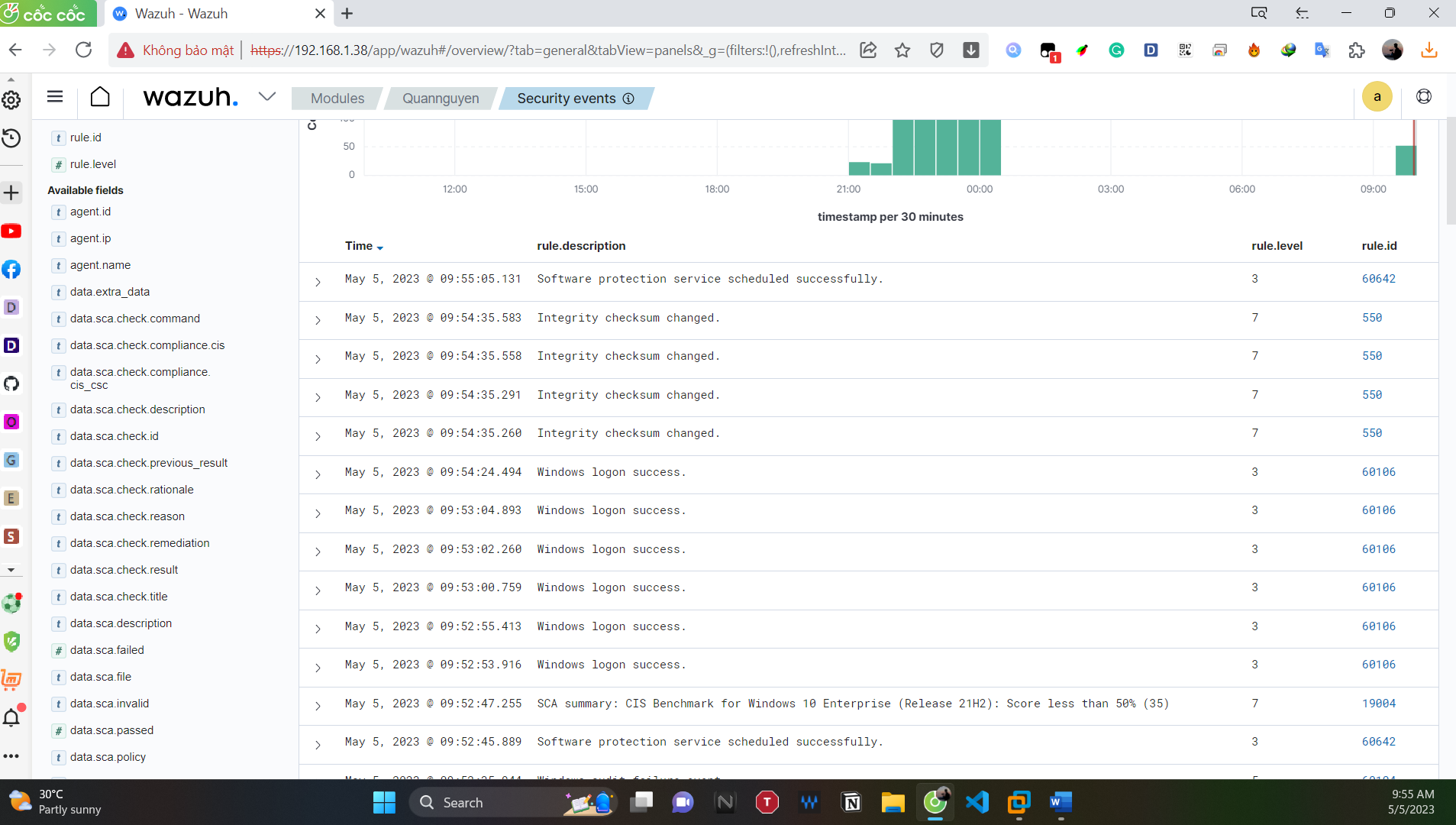
Bật tính năng cho phép theo dõi sự kiện truy cập tài khoản



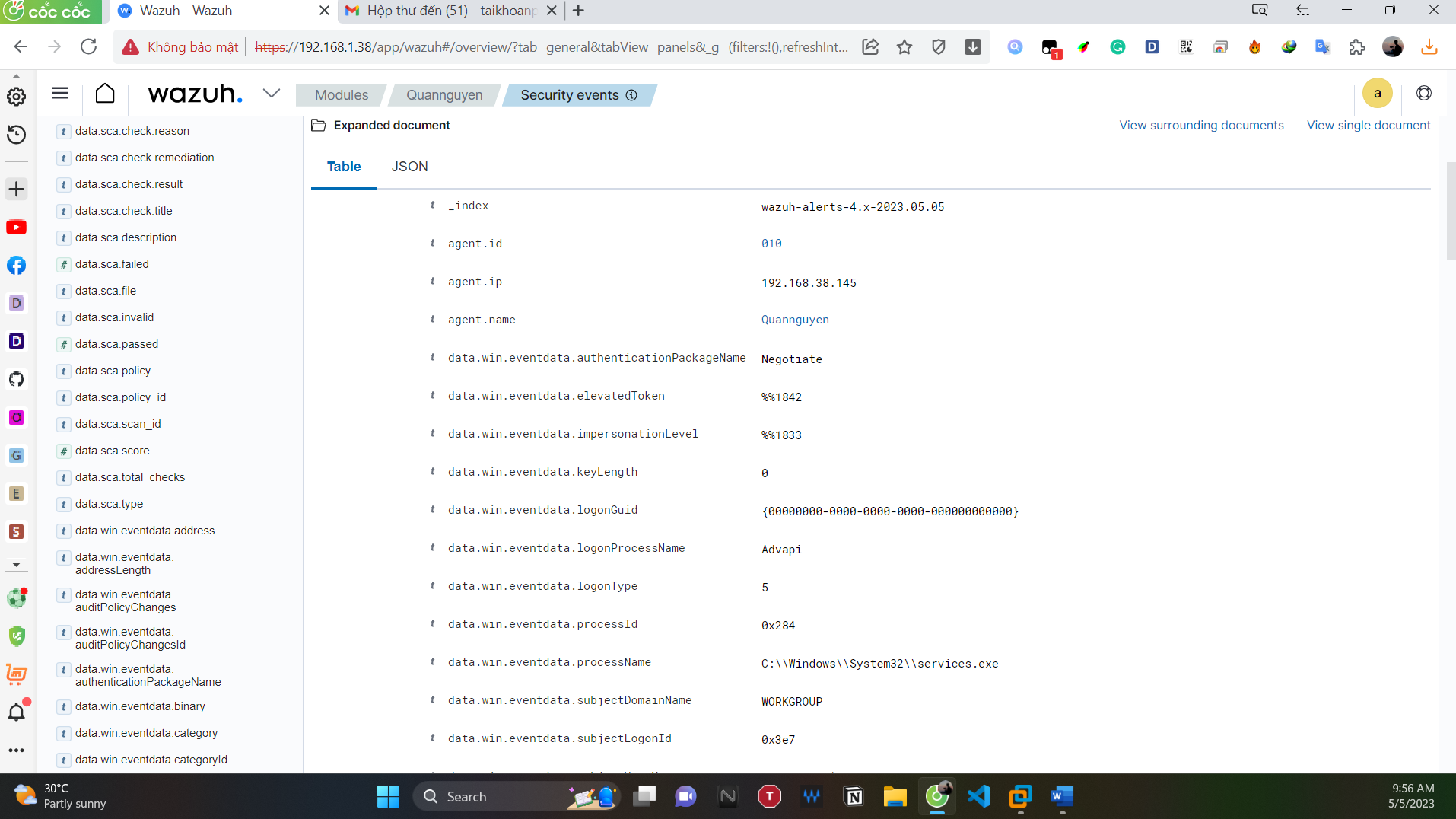
Mục xác thực đăng nhập



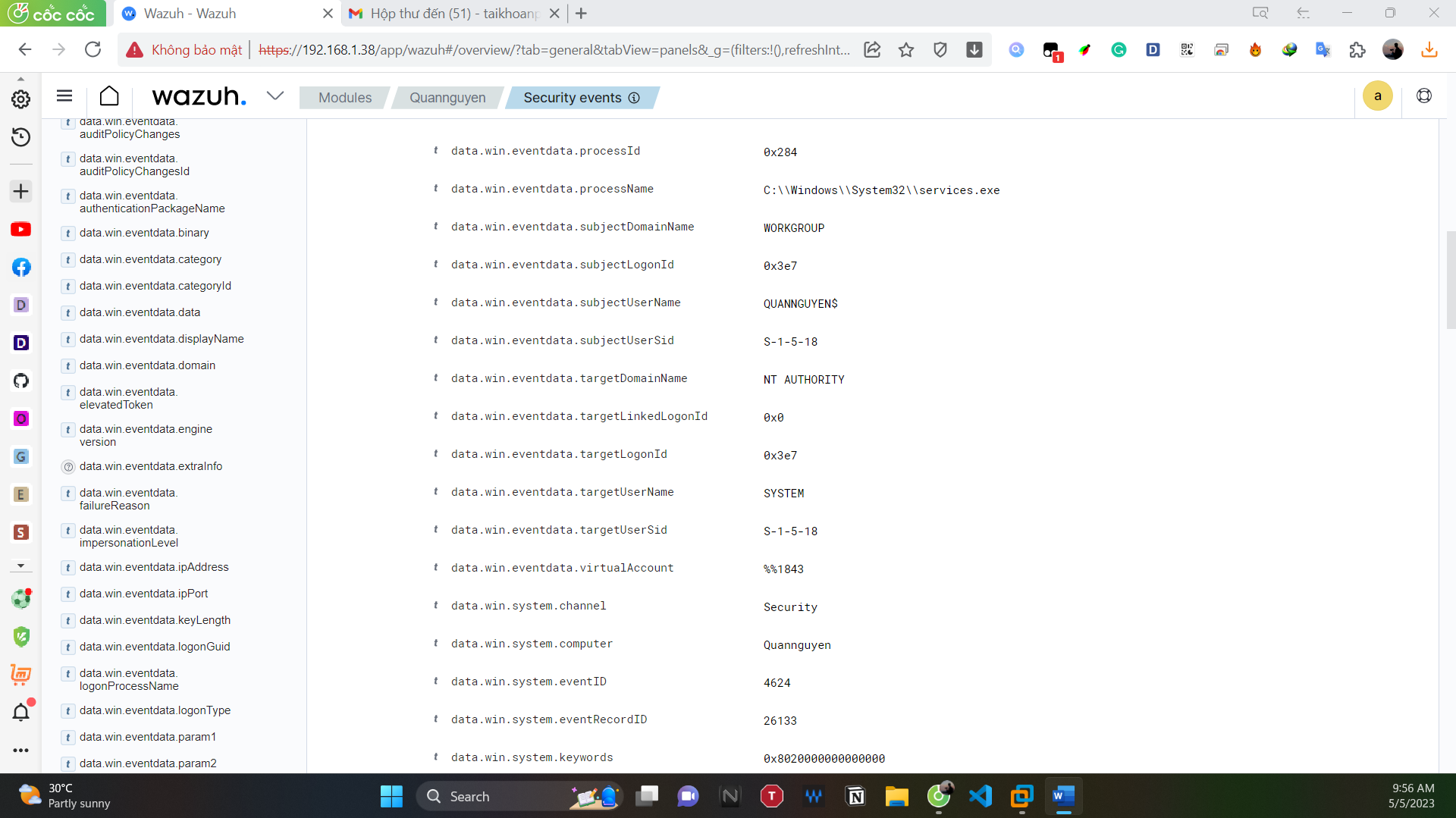
Mục bắt các sự kiện hệ thống

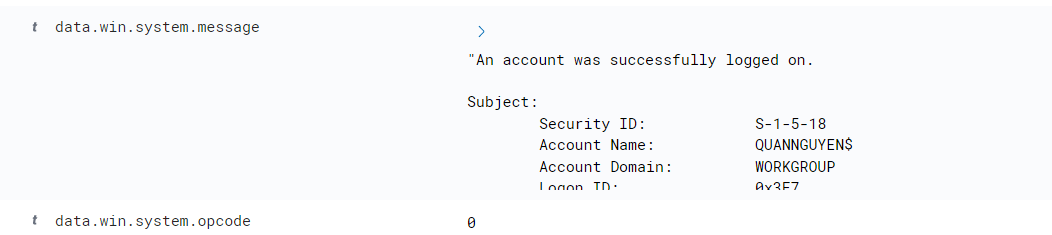


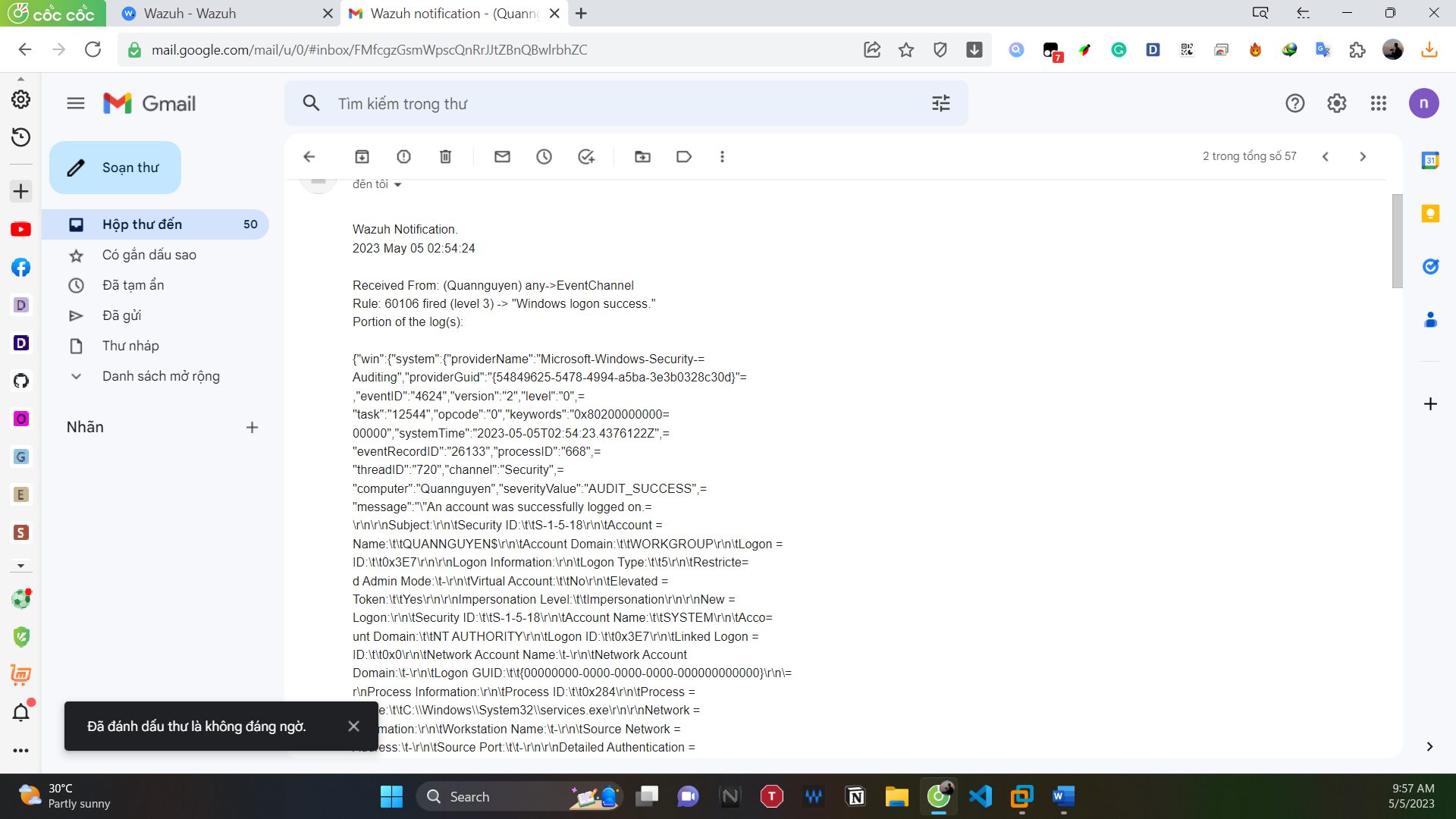
Khi đăng nhập thành công hoặc thất bạt -> wazuh server bắt được các sự kiện đã xảy ra trên máy agent



Bản báo cáo chi tiết về sự kiện

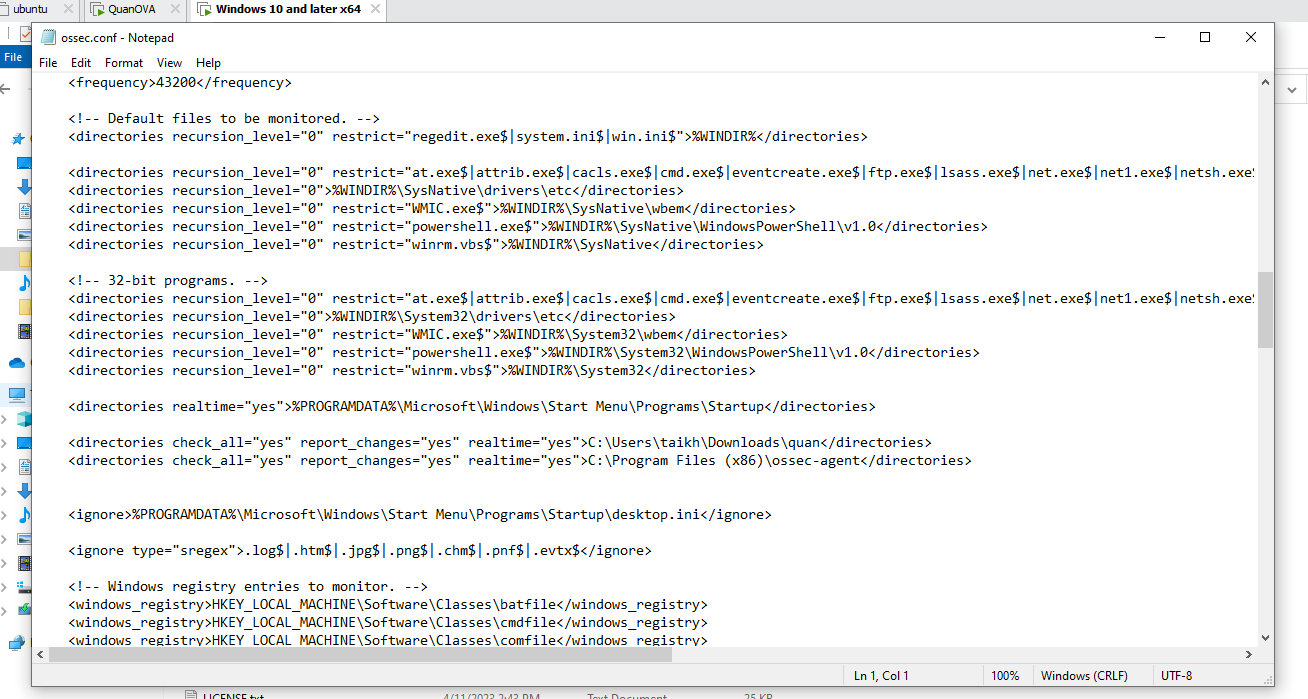


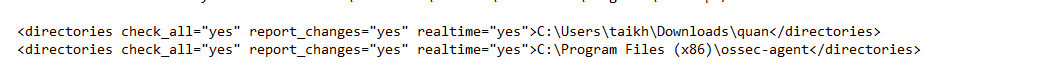




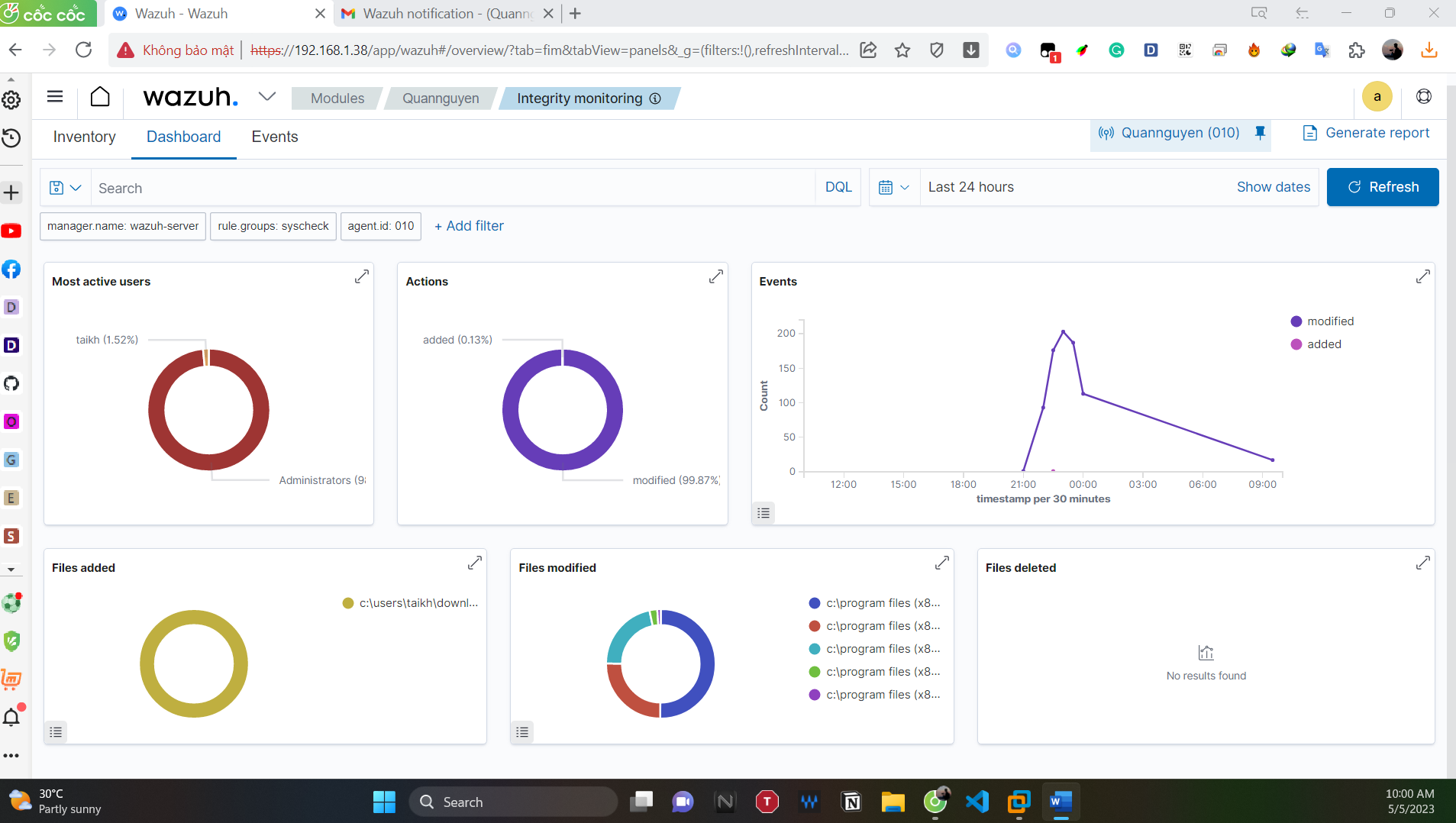
Thông báo đến email admin

1. **Kiểm soát file truy cập**

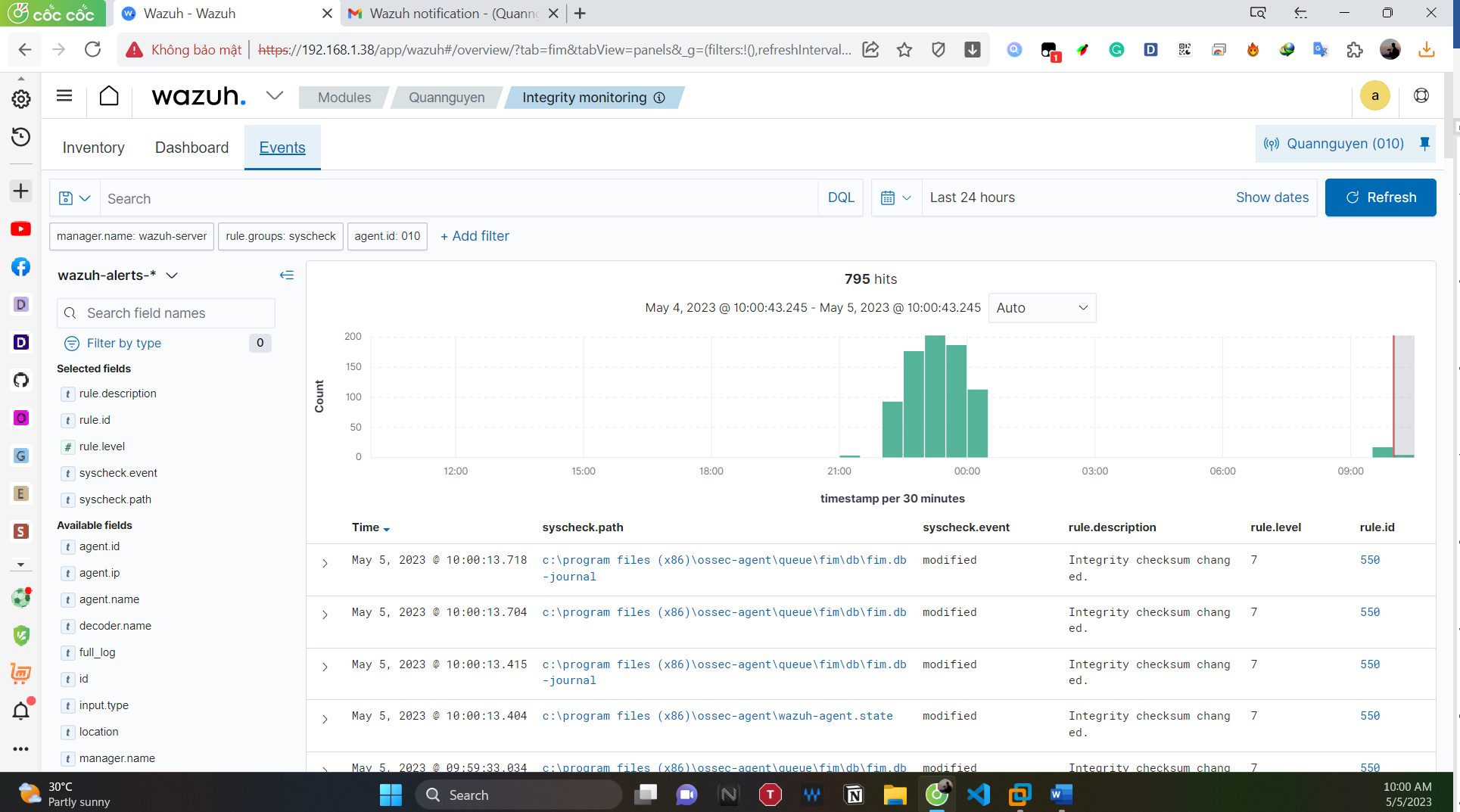


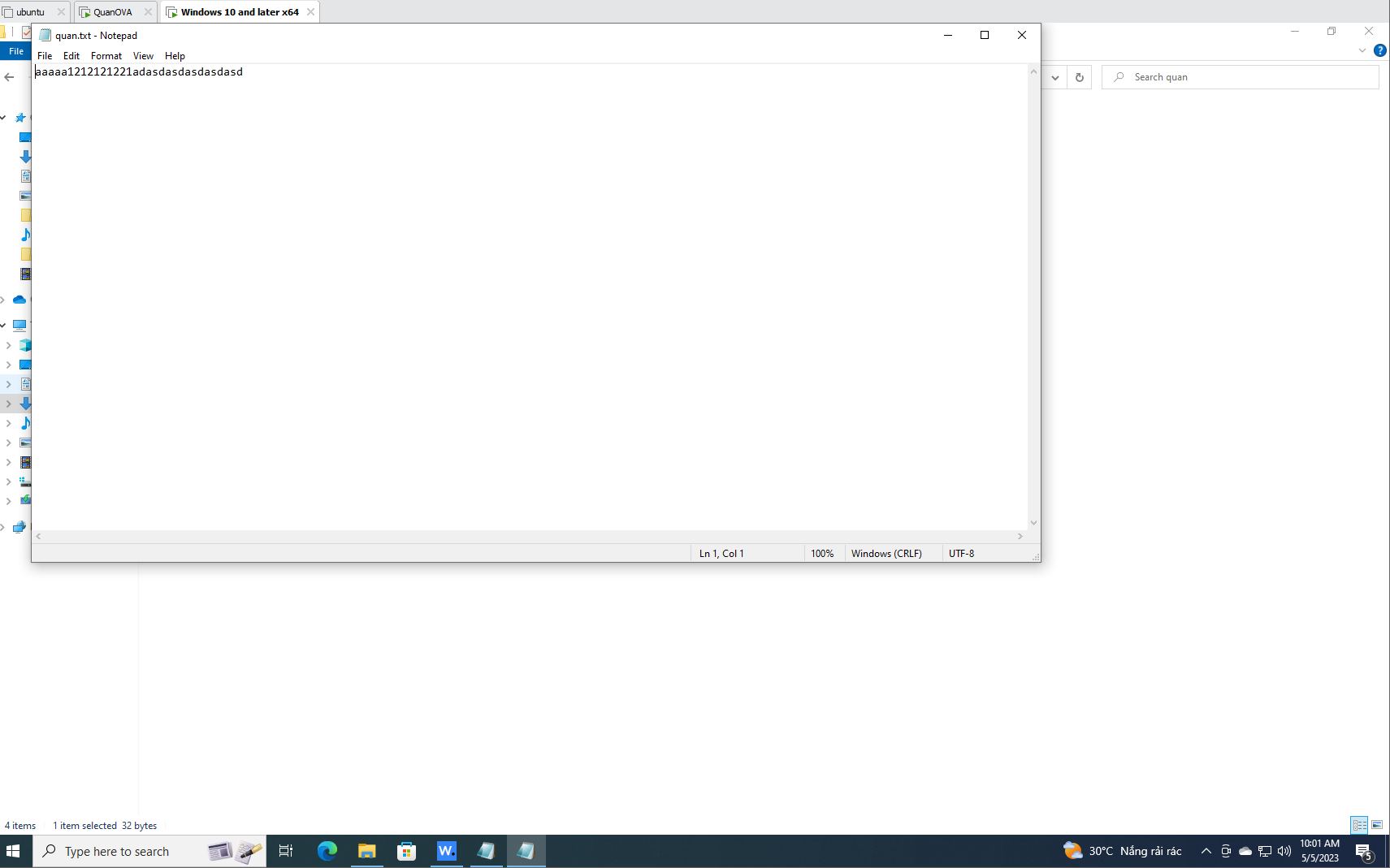


Tiến hành thêm luật cho máy agent

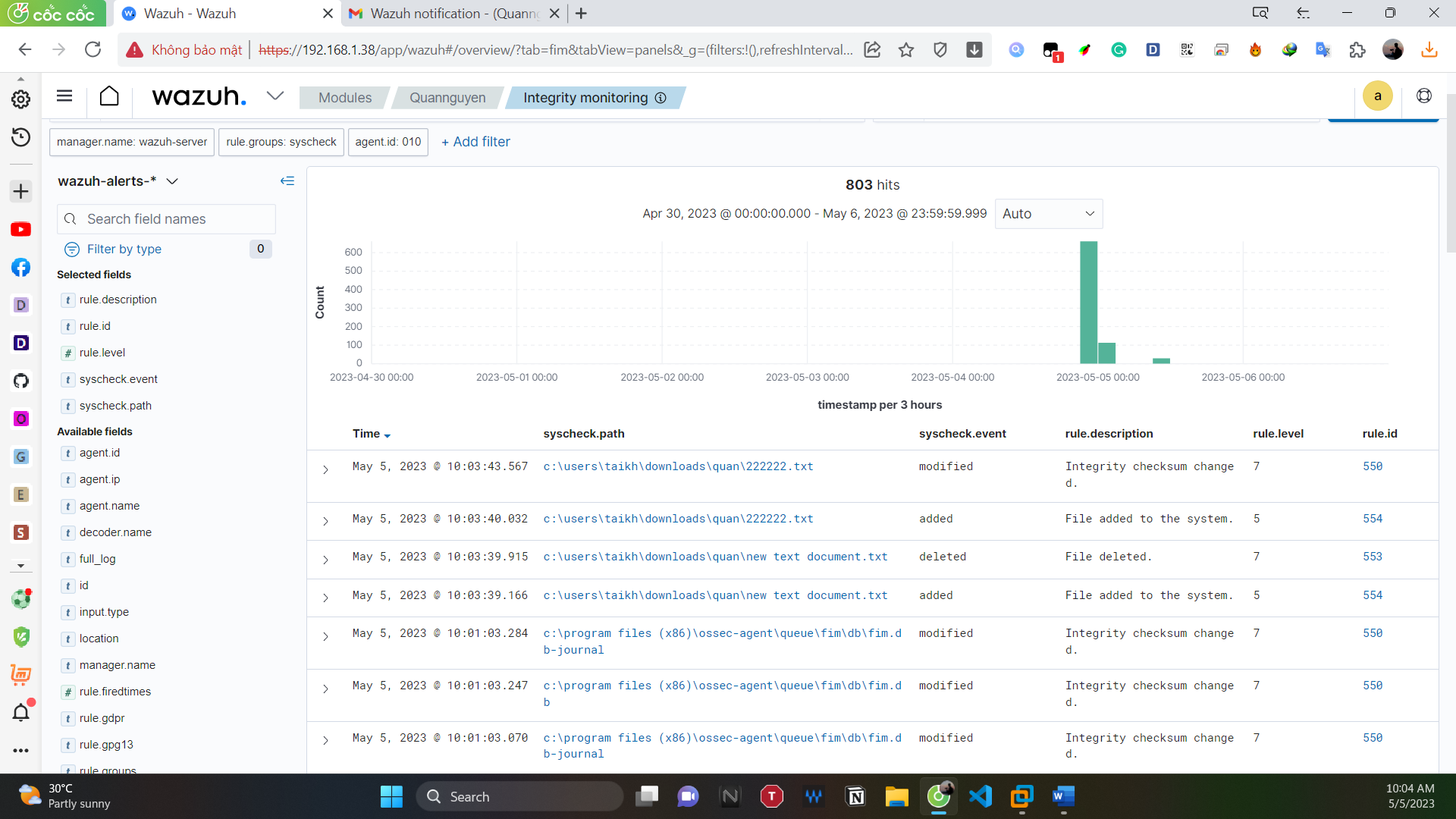


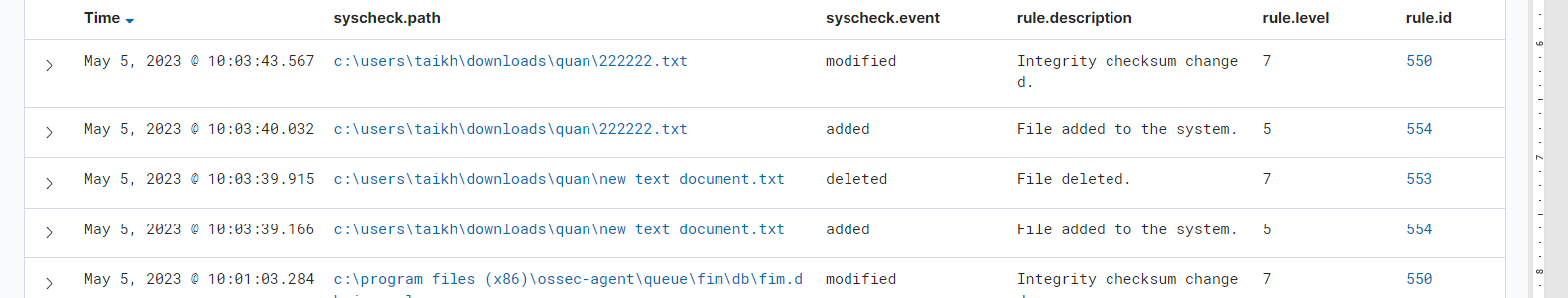
Giao diện tính năng bảo mật trên máy agent





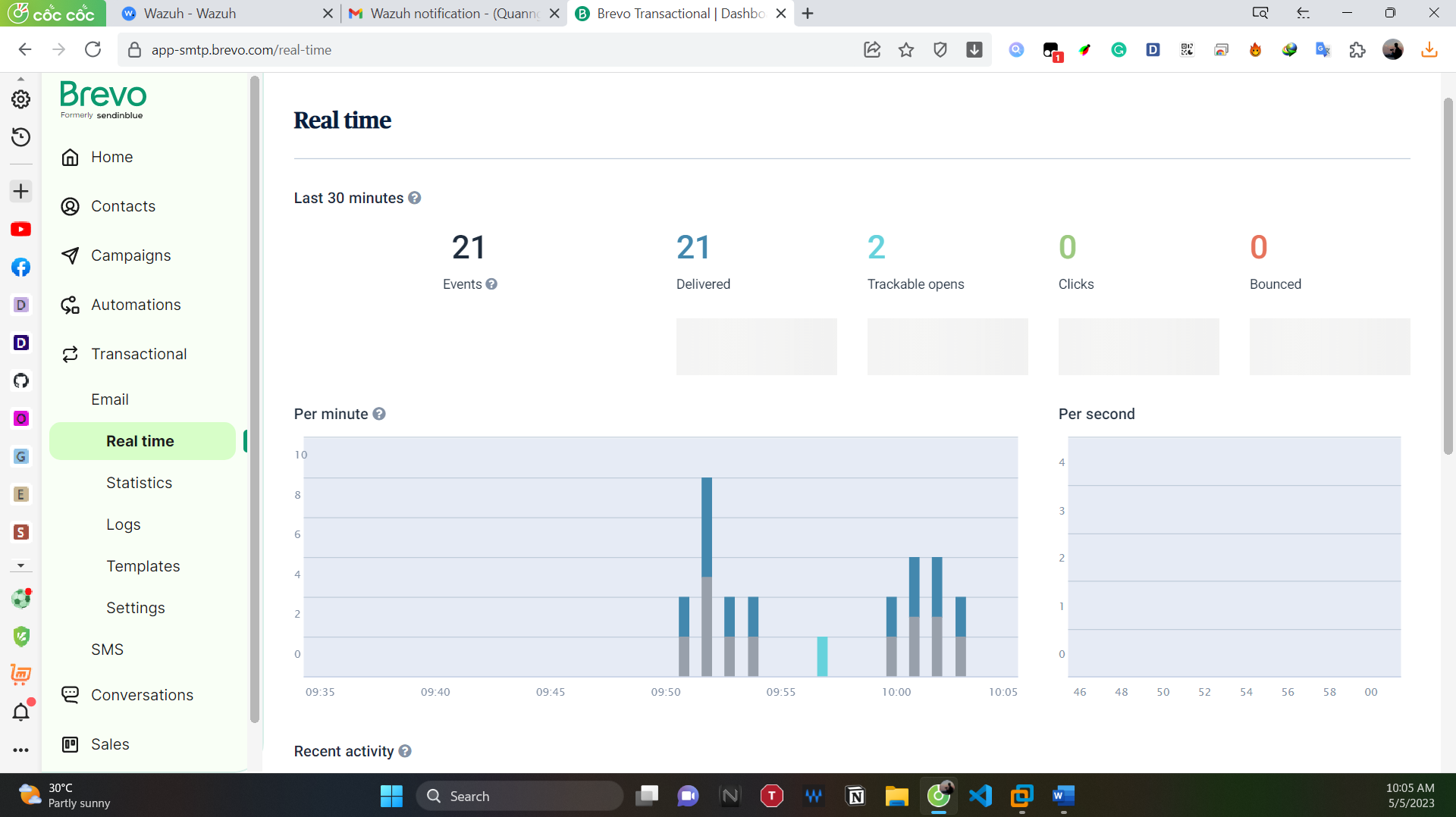
Tạo file và sửa xóa file trên máy agent



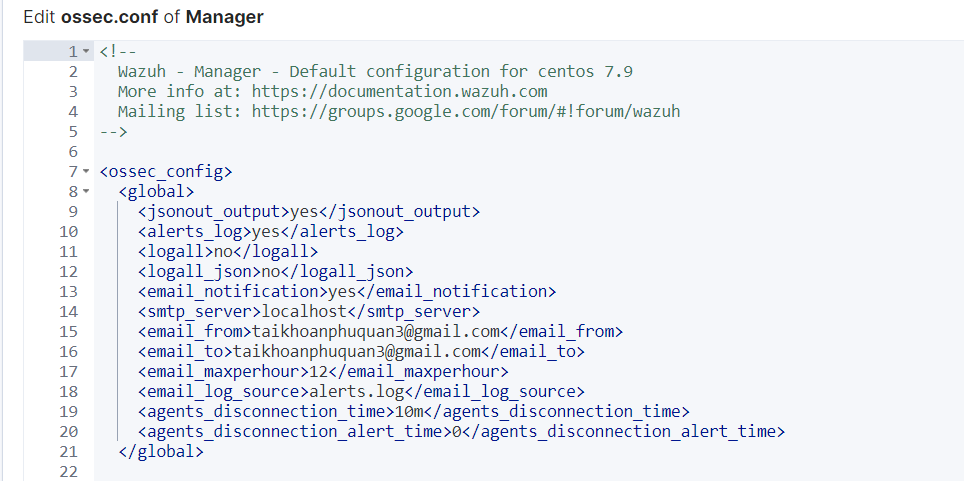


Các hành động đã được nhật kí ghi lại

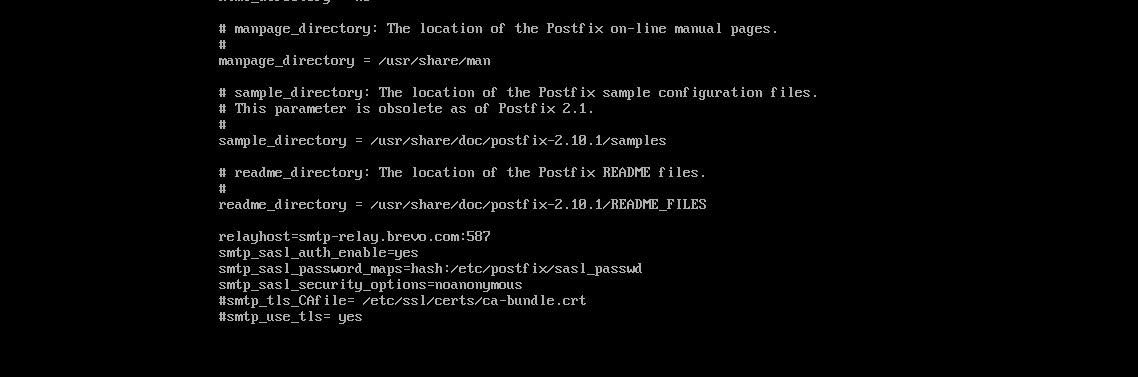
1. **Gửi cảnh báo qua email**

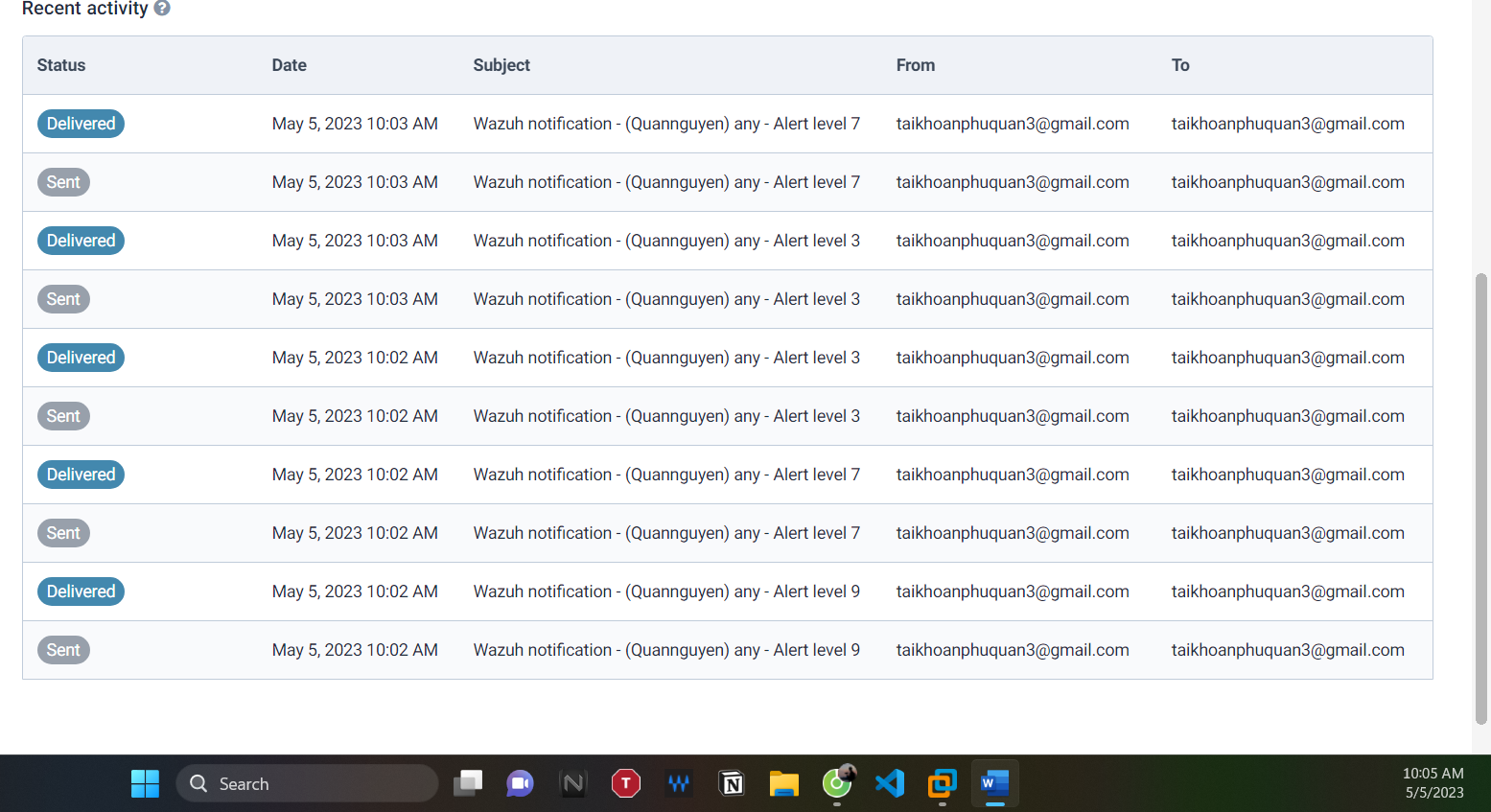


Đăng kí 1 smtp để gửi email

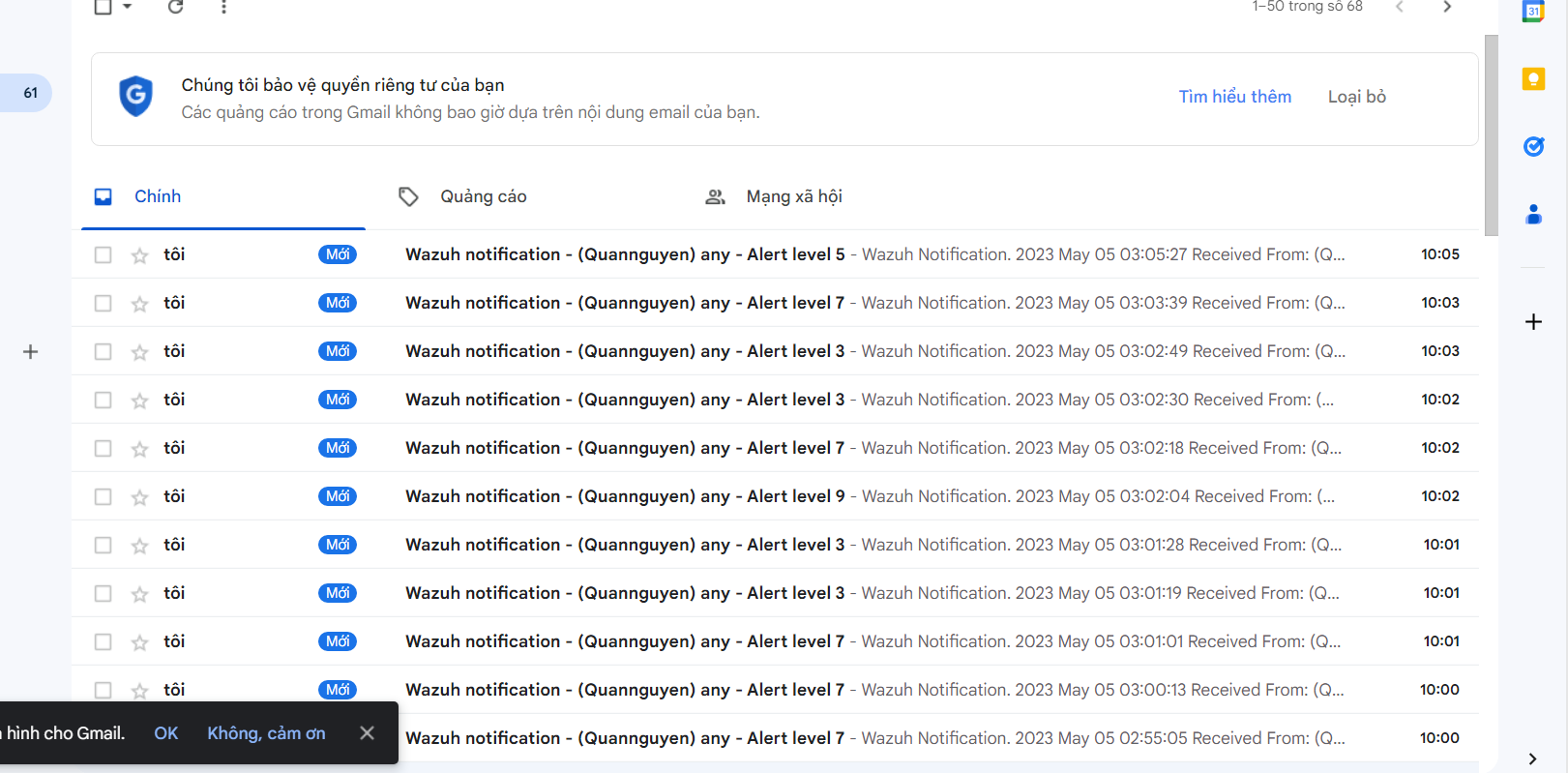


Thêm luật cho wazuh



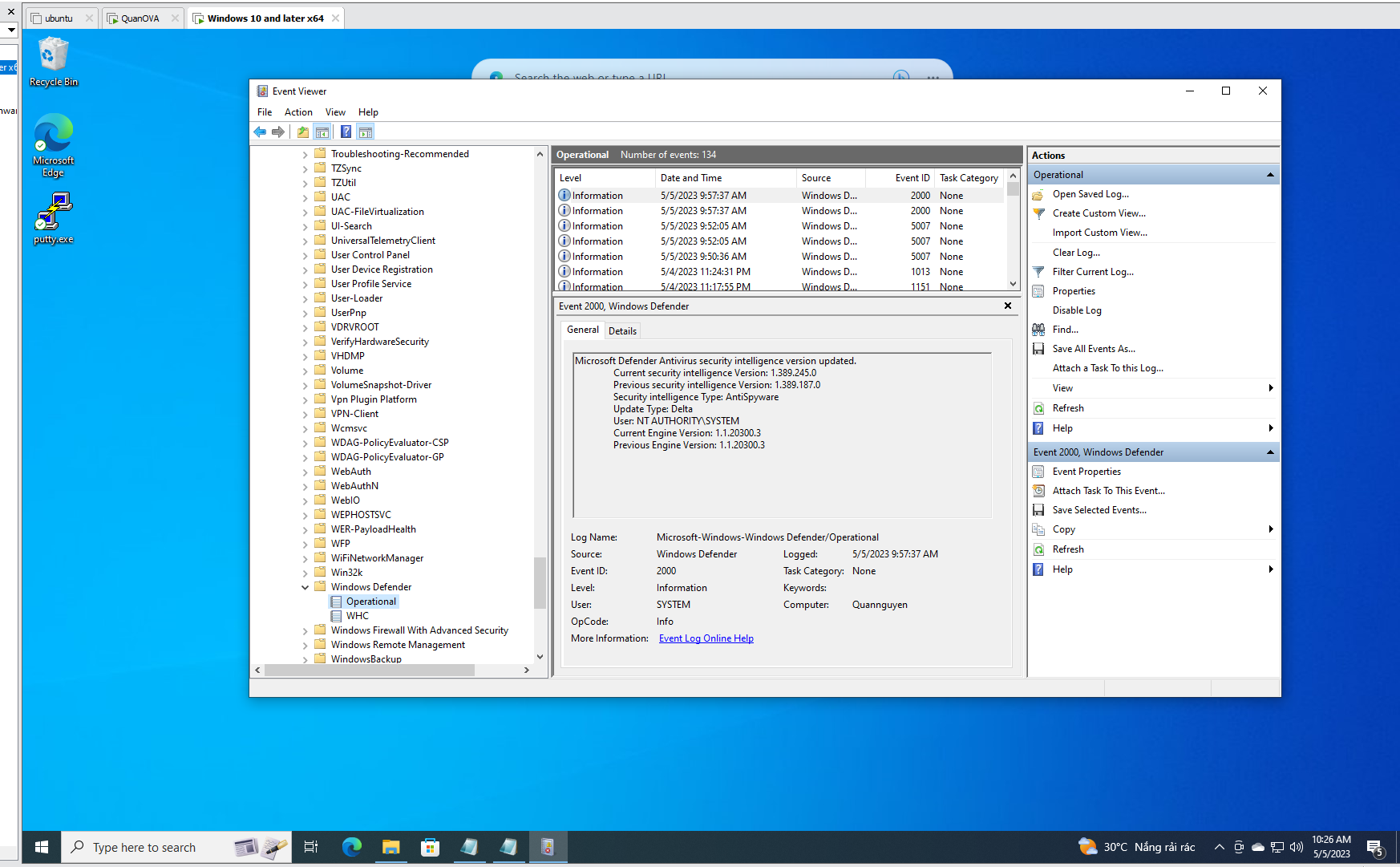


Cài đặt máy chủ email

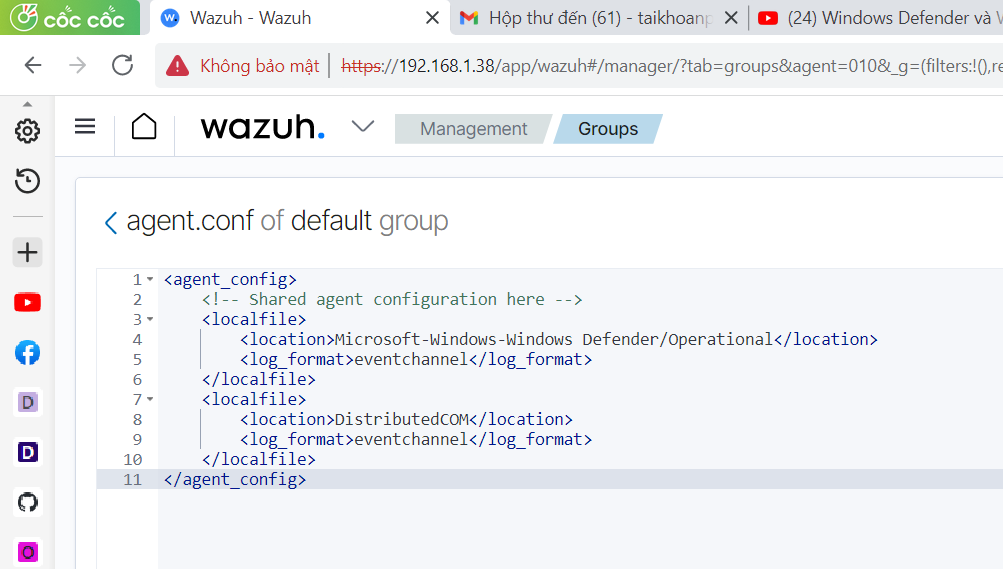


Các email đã được gửi qua smtp

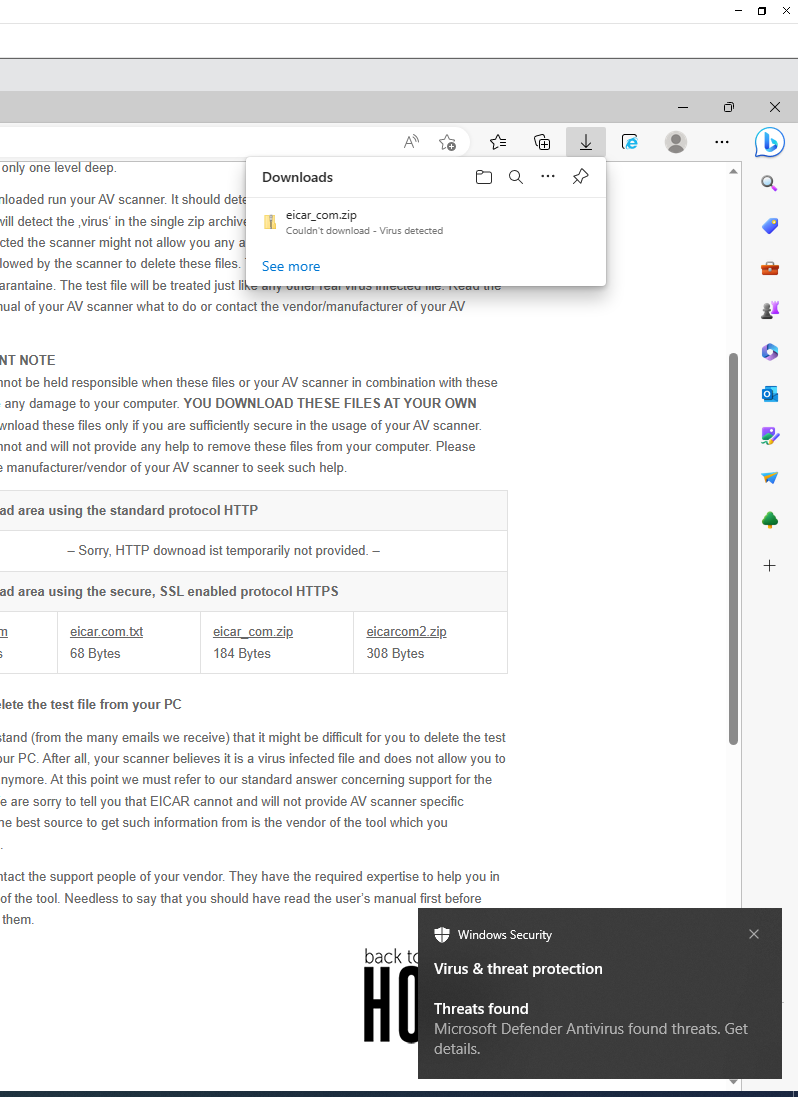
1. **Chuyển tiếp nhật ký Windows Defender sang Wazuh**



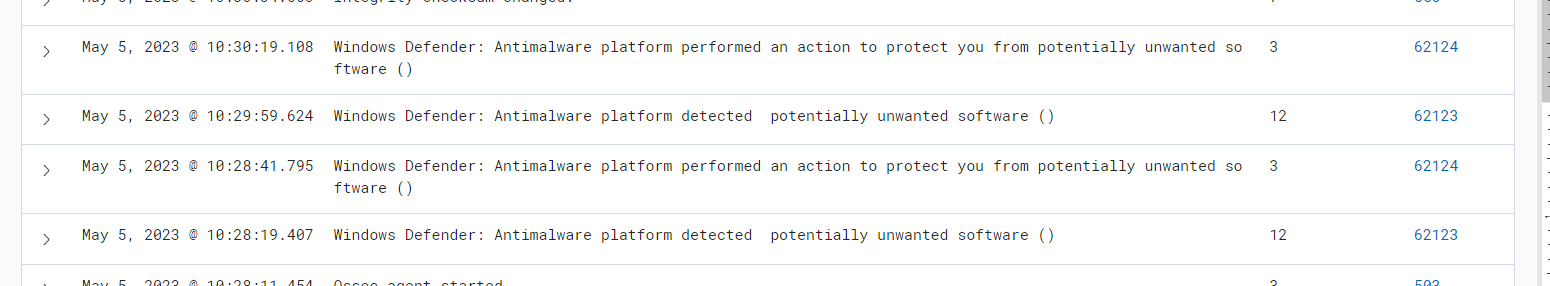
Sự kiện của Windows Defender



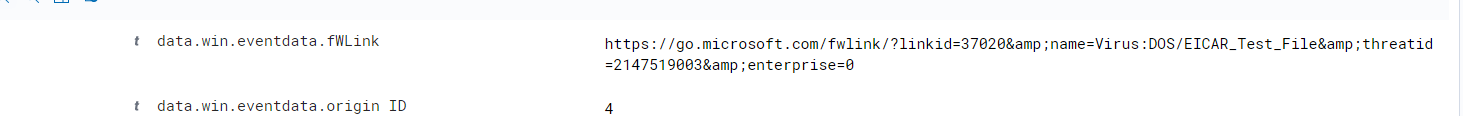
Áp luật vào Wazuh

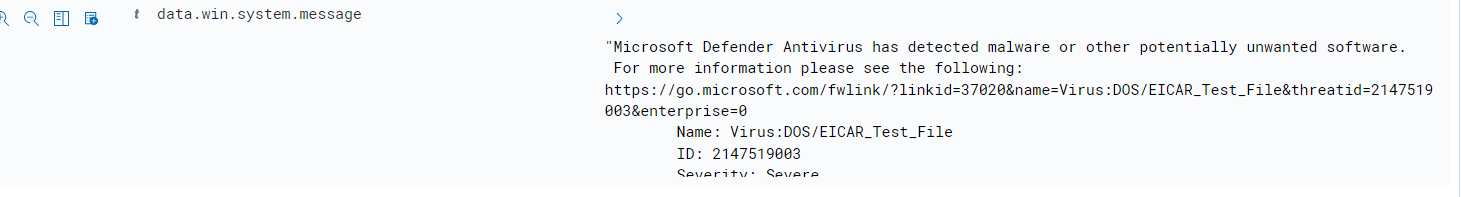


Tải một mã độc bất kì



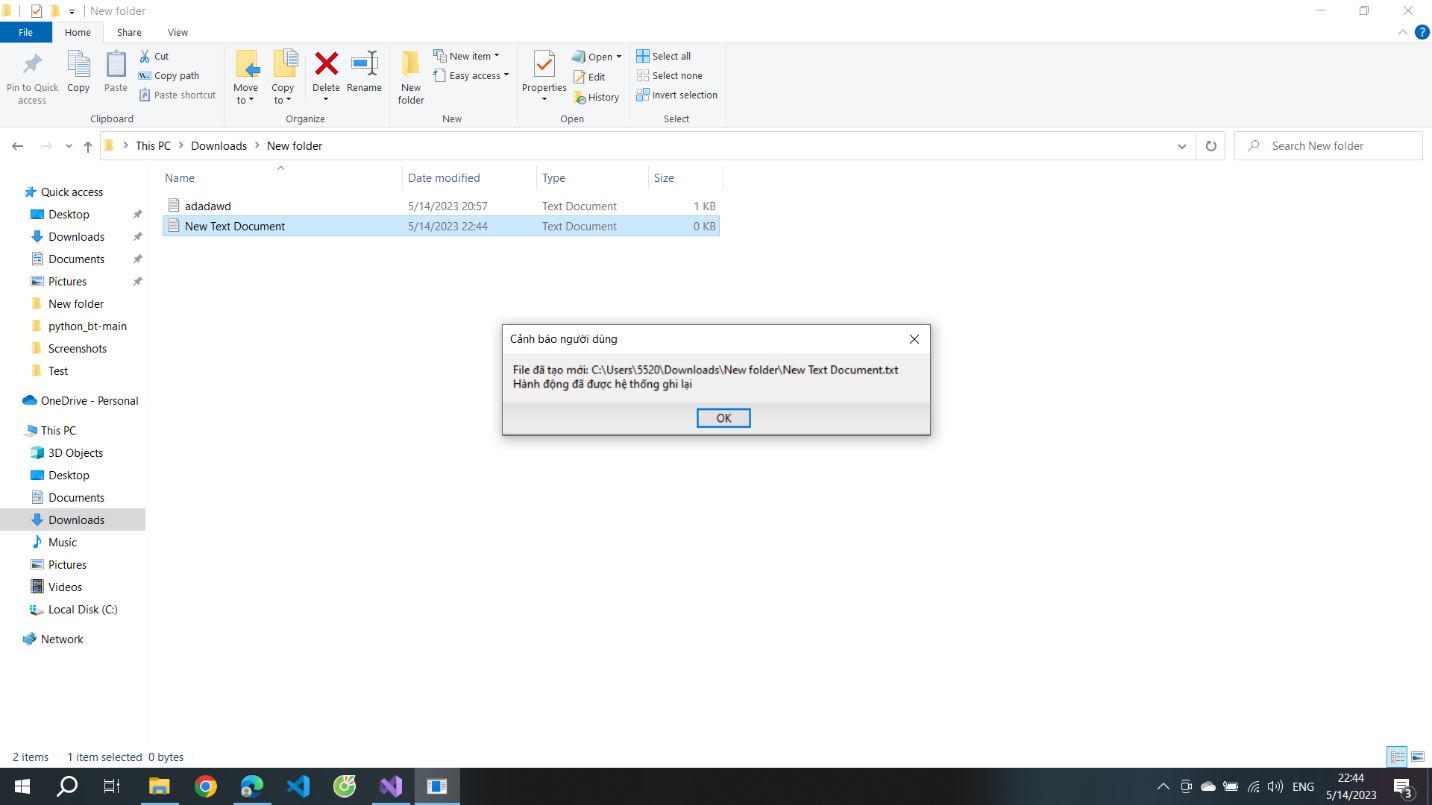
Bản log sự kiện của Windows Defender



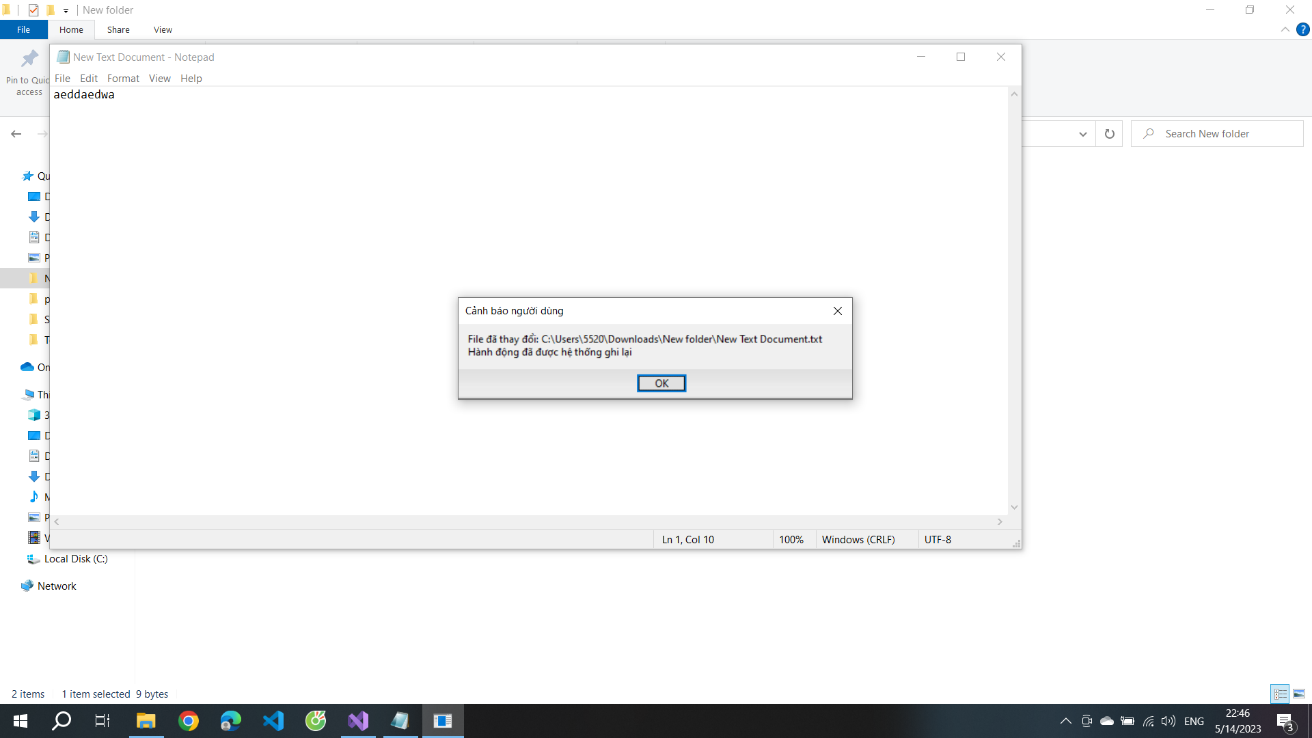


Thông tin chi tiết

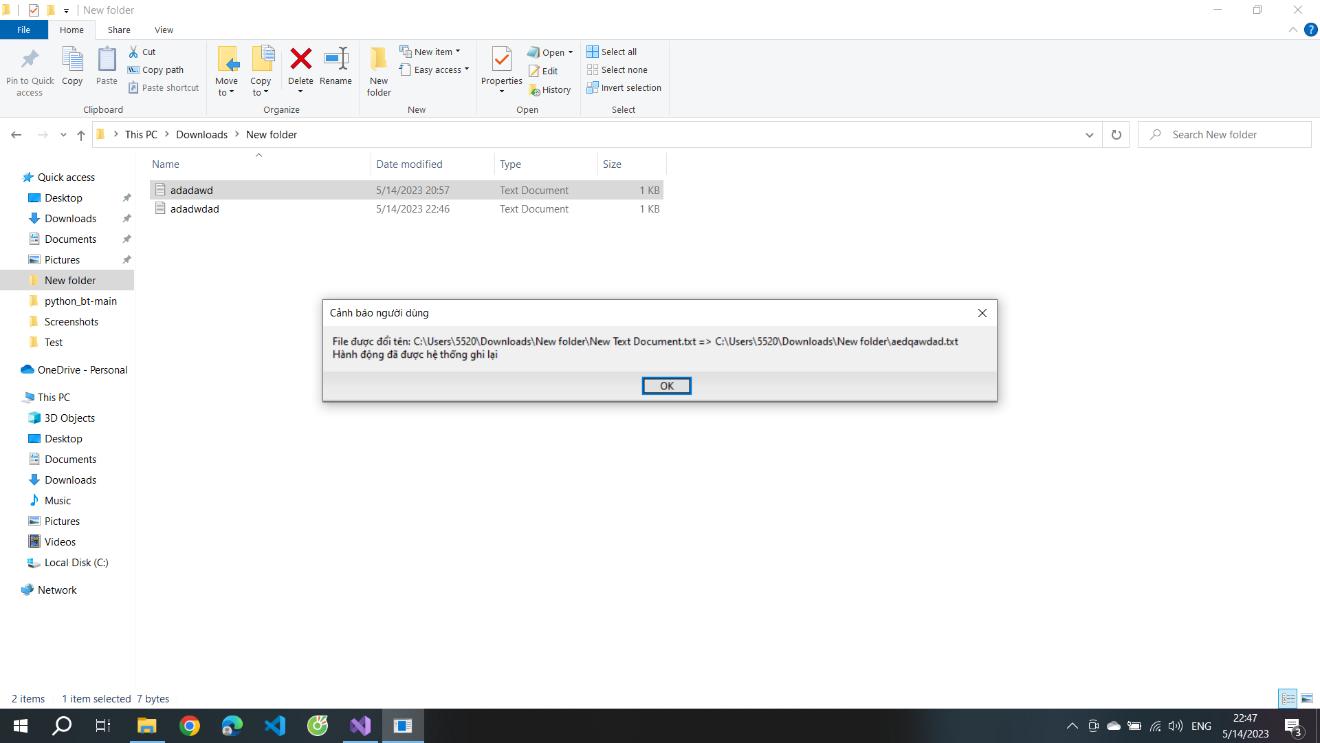
1. **Cảnh báo tại máy Agent**

****

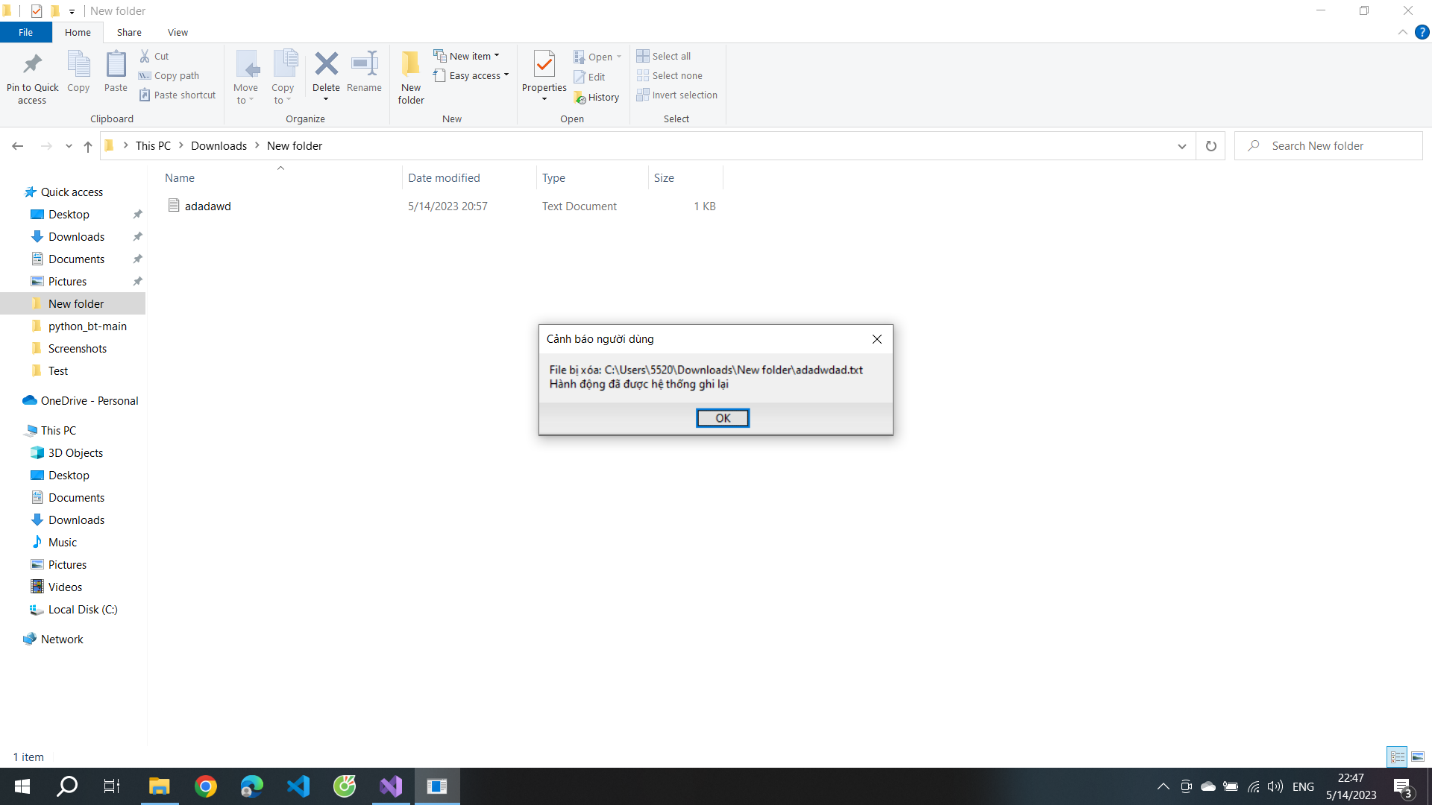
Cảnh báo tạo mới file

****

Cảnh báo file bị thay đổi

****

Cảnh báo sửa tên file

****

Cảnh báo xóa file

1. **TỔNG KẾT**

Wazuh là một giải pháp an ninh mở và miễn phí được phát triển dựa trên nền tảng Elastic Stack. Nó cung cấp các tính năng để giám sát và phát hiện các mối đe dọa an ninh trong môi trường máy chủ và ứng dụng.

Một trong những ưu điểm của Wazuh là nó cung cấp một giao diện web đơn giản và dễ sử dụng để quản lý và xử lý cảnh báo an ninh. Nó cũng hỗ trợ nhiều ngôn ngữ lập trình để phát triển các tính năng tùy chỉnh.

Wazuh cũng có khả năng tích hợp với các công cụ an ninh phổ biến khác như Snort và Suricata để tăng cường khả năng phát hiện.

Tuy nhiên, điểm yếu của Wazuh là quá trình triển khai và cấu hình có thể phức tạp, đặc biệt đối với những người không quen thuộc với các công nghệ an ninh. Ngoài ra, Wazuh cũng có thể tiêu tốn tài nguyên hệ thống khá lớn, do đó nó có thể không phù hợp với các môi trường có tài nguyên hạn chế.

1. **TÀI LIỆU THAM KHẢO**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | [1] | [Wazuh · The Open Source Security Platform](https://wazuh.com/) | | [2] | [DLP là gì? Cách hoạt động và lợi ích của DLP | BKHOST](https://bkhost.vn/blog/dlp-data-loss-prevention/) | | [3] | [ghichep-SOC/ghichep-overview-wazuh.md at master · hocchudong/ghichep-SOC (github.com)](https://github.com/hocchudong/ghichep-SOC/blob/master/ghichep-wazuh/ghichep-overview-wazuh.md) | |