Bkav® Pro SOAR

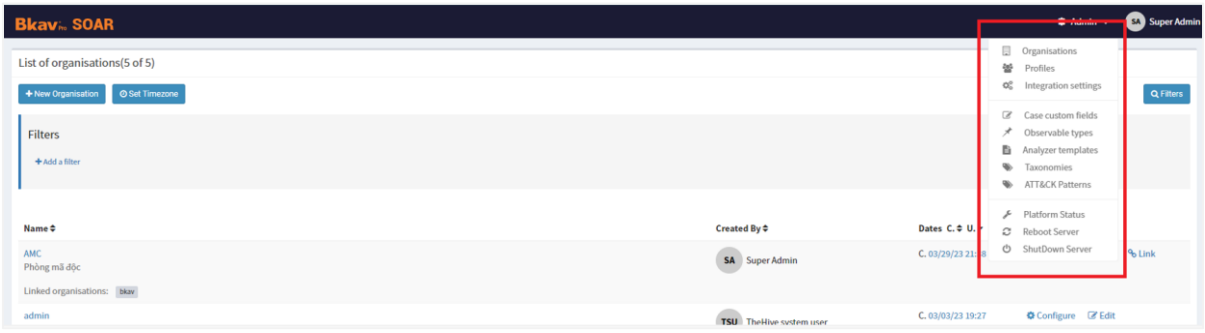
Phần mềm Điều phối, tự động hóa & phản ứng an toàn thông tin

Phần mềm Điều phối an ninh, tự động hóa và phản hồi - BkavPro Security Orchestration, Automation & Response (SOAR) cho phép cơ quan, tổ chức, doanh nghiệp thu thập dữ liệu về các mối đe dọa và hỗ trợ xử lý các sự kiện bảo mật cho đội ngũ xử lý sự cố trong SOC

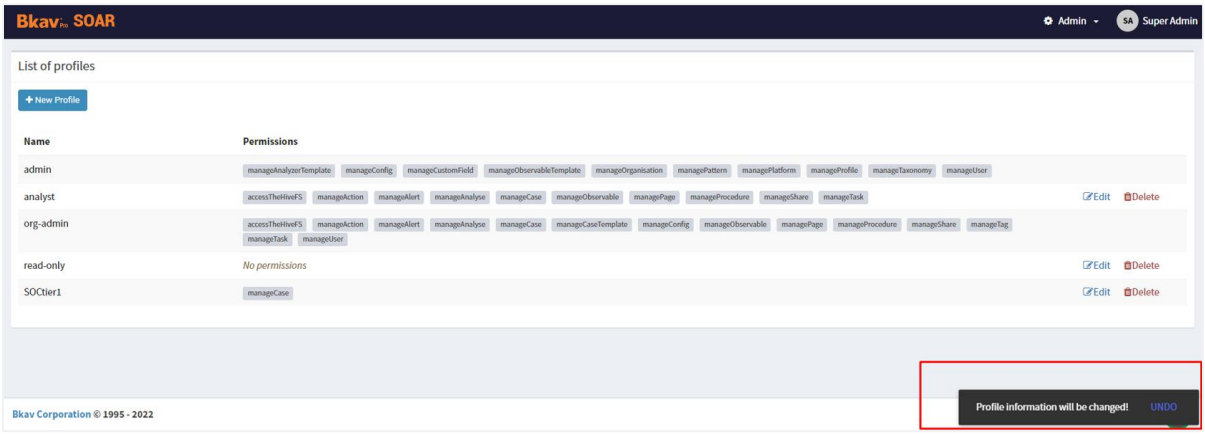
1. Quản trị hệ thống

1.1. Quản lý vận hành

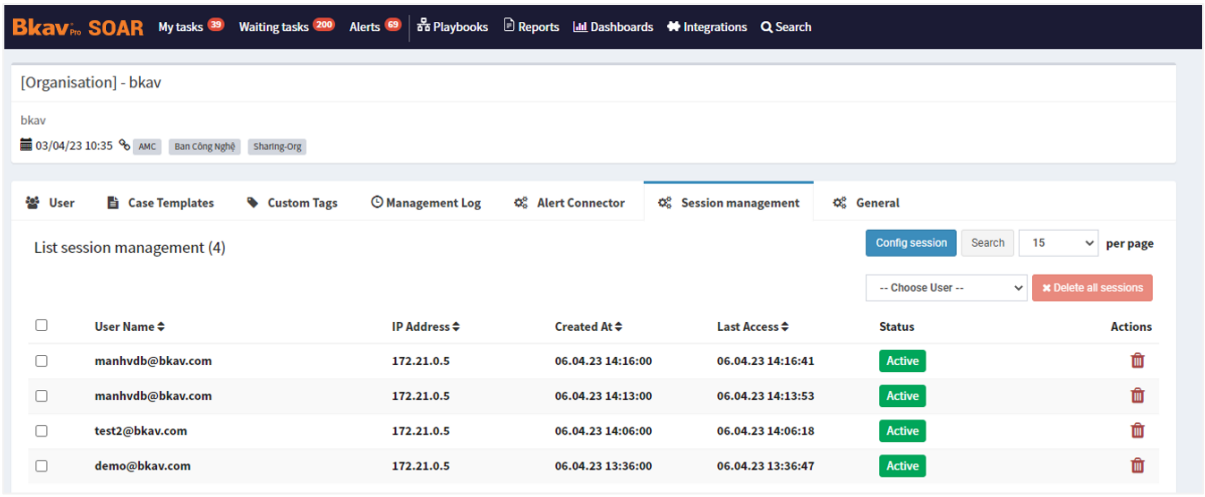
- Cho phép thiết lập, thay đổi, áp dụng và hoàn tác sự thay đổi trong cấu hình hệ thống.



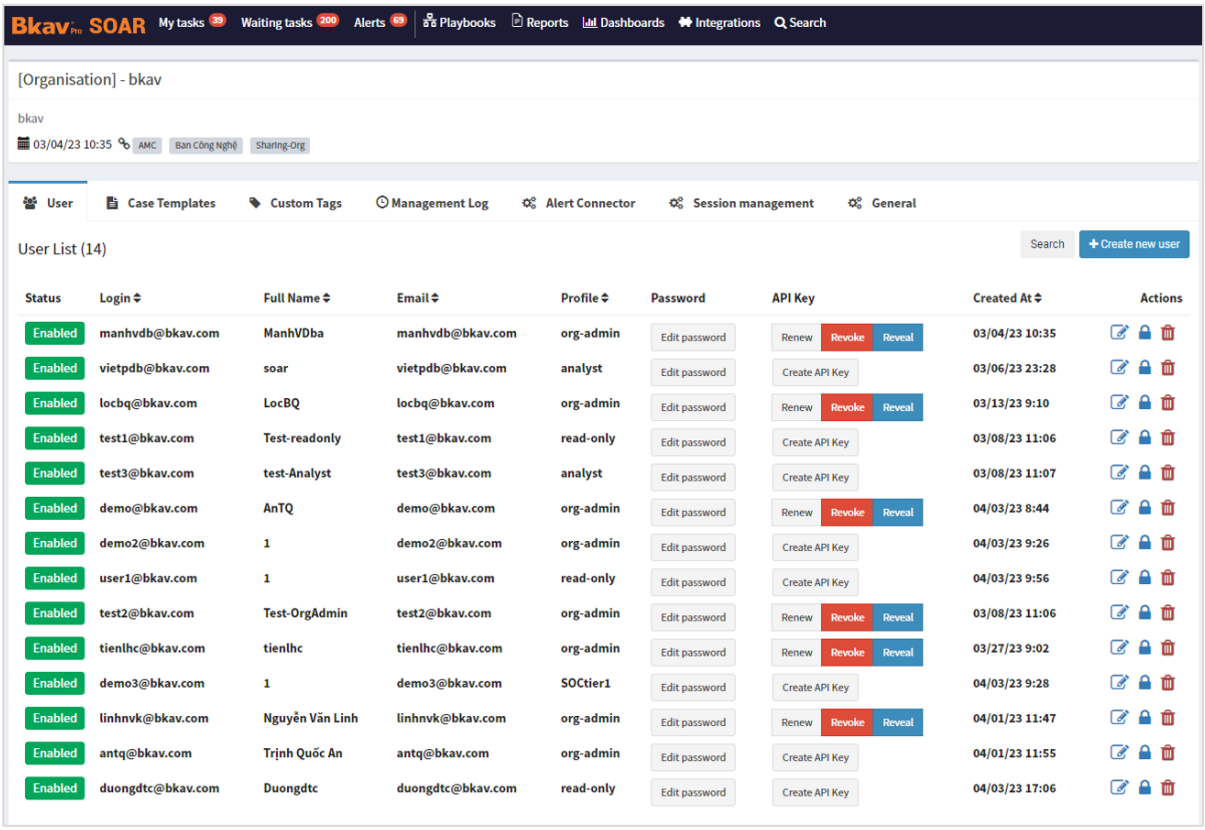
(Cấu hình hệ thống cho toàn bộ tổ chức)



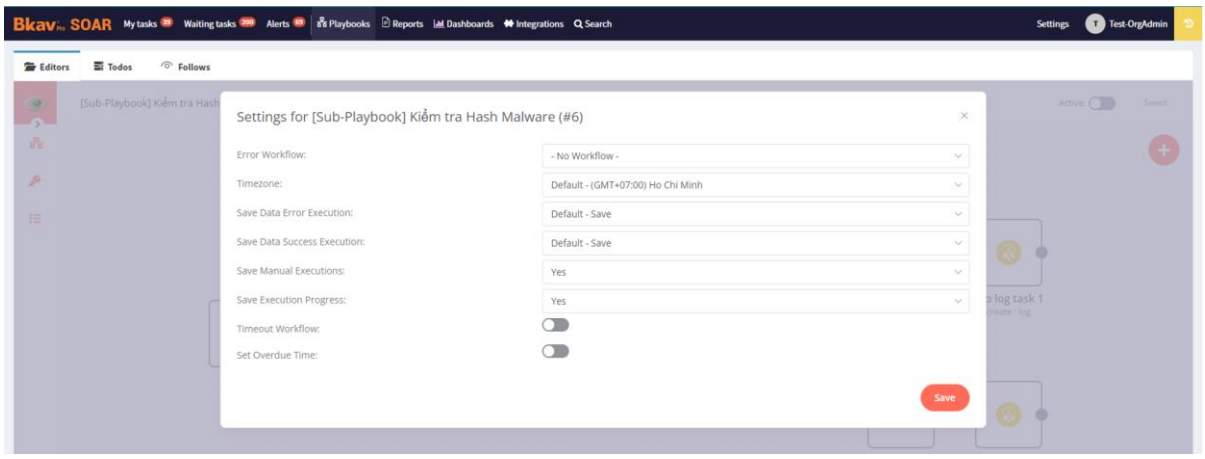
(Hoàn tác thay đổi hành động trong cấu hình)



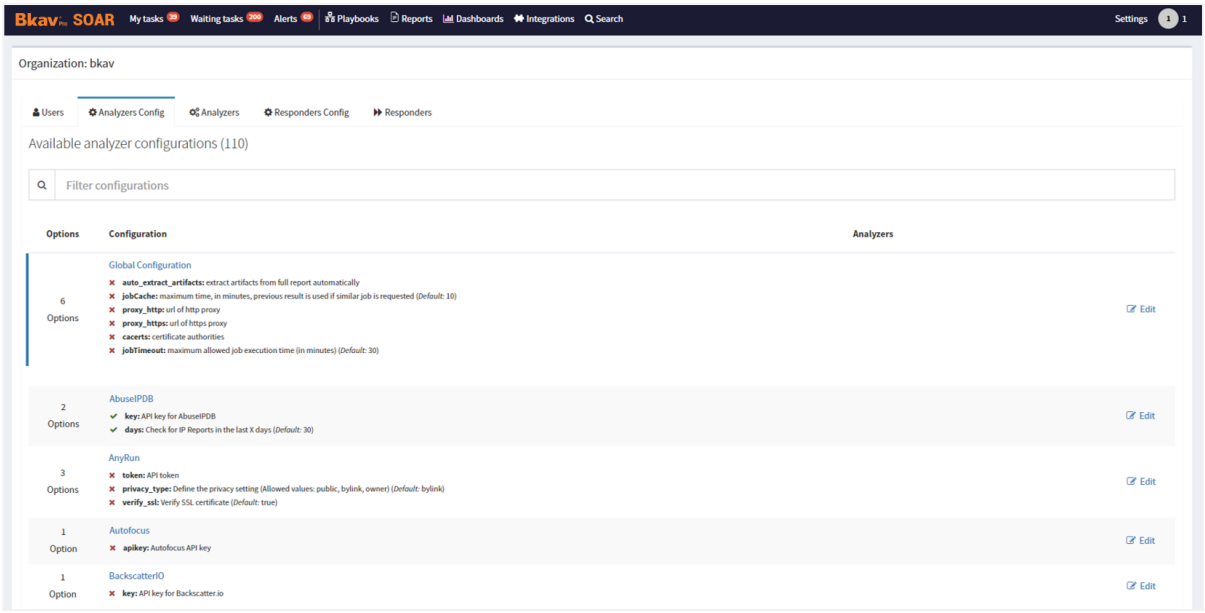
(Cấu hình quản trị truy cập)



(Cấu hình tài khoản xác thực và phân quyền người dùng)

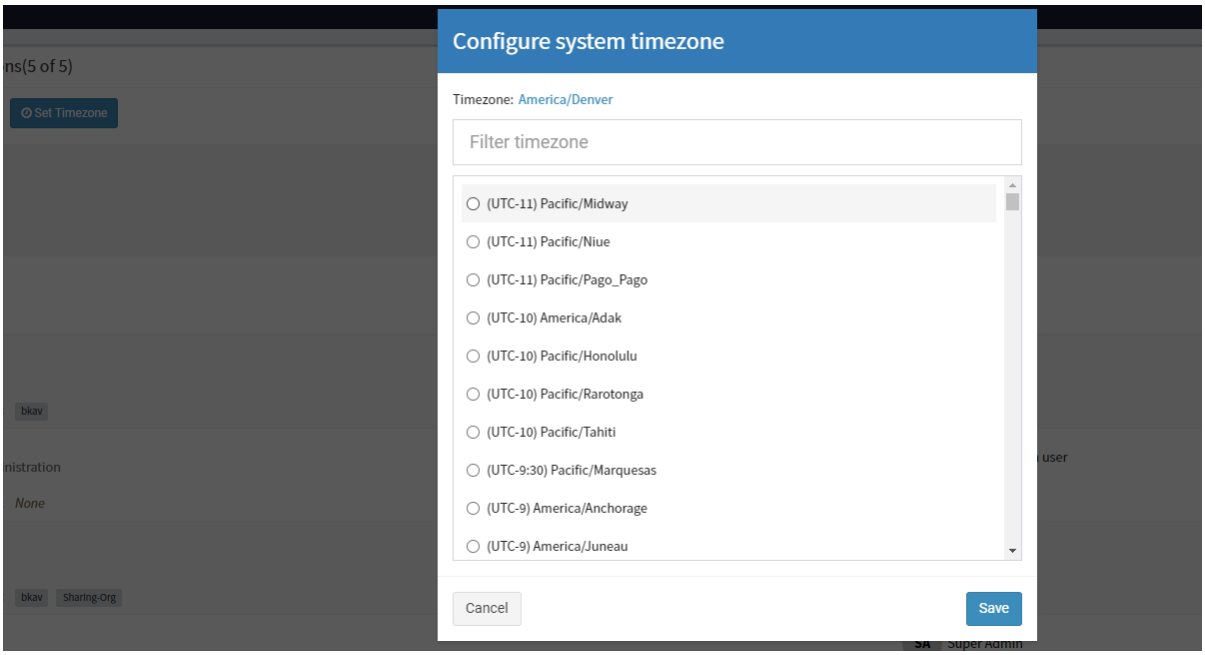


(Cấu hình kịch bản)

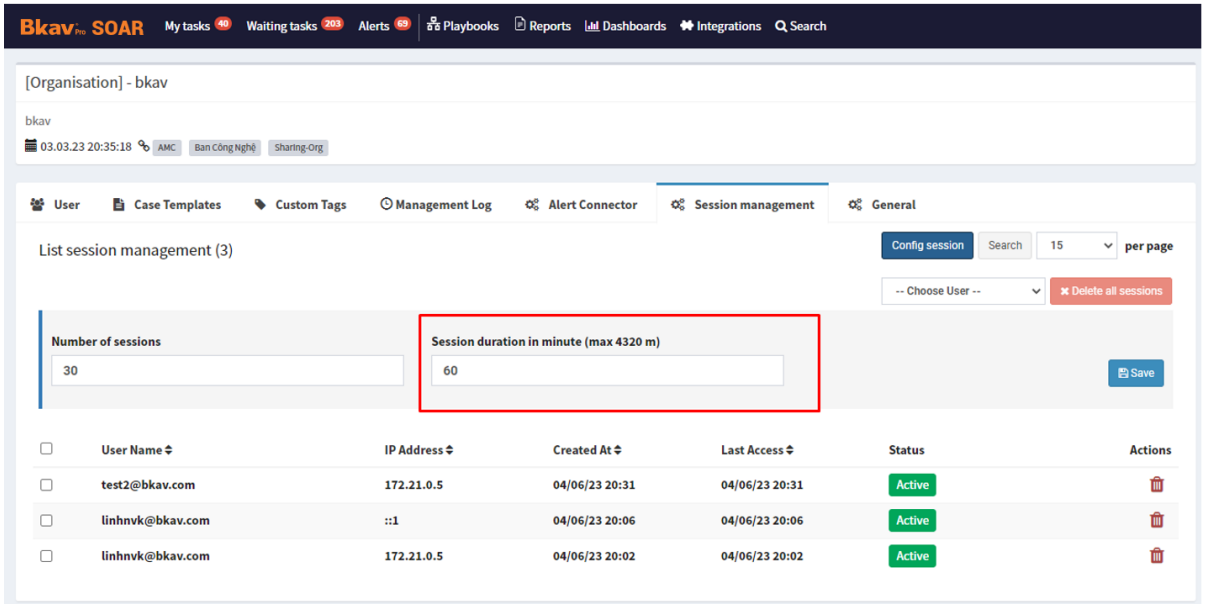


(Cấu hình thành phần tích hợp)

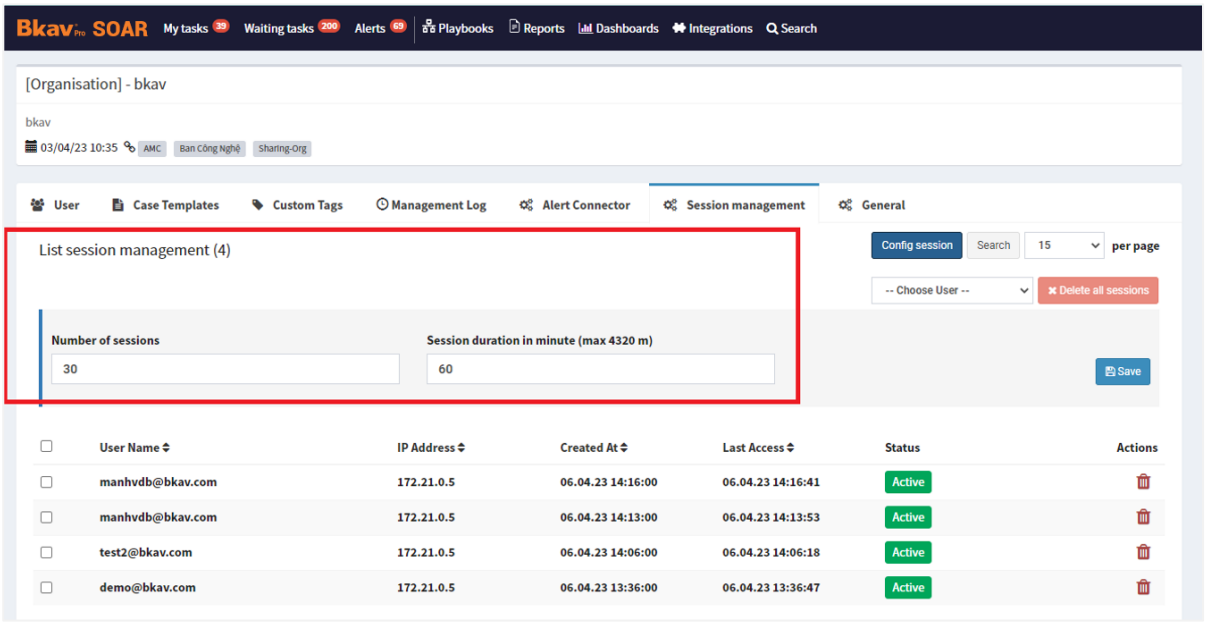
- Cho phép thay đổi thời gian hệ thống.



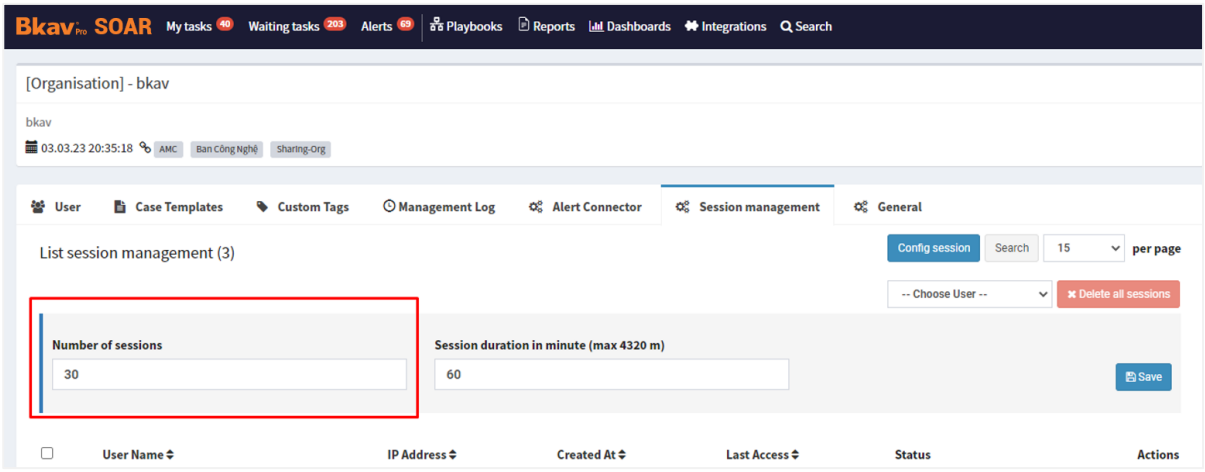
- Cho phép thay đổi thời gian duy trì phiên kết nối



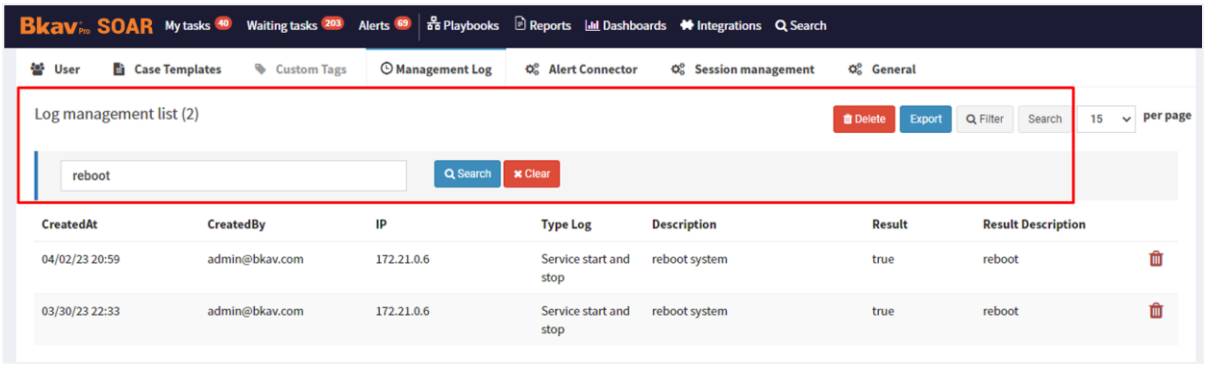
- Cho phép thiết lập, thay đổi các tham số giới hạn đối với kết nối quản trị từ xa (ví dụ: giới hạn địa chỉ IP, giới hạn số phiên kết nối quản trị từ xa đồng thời…)



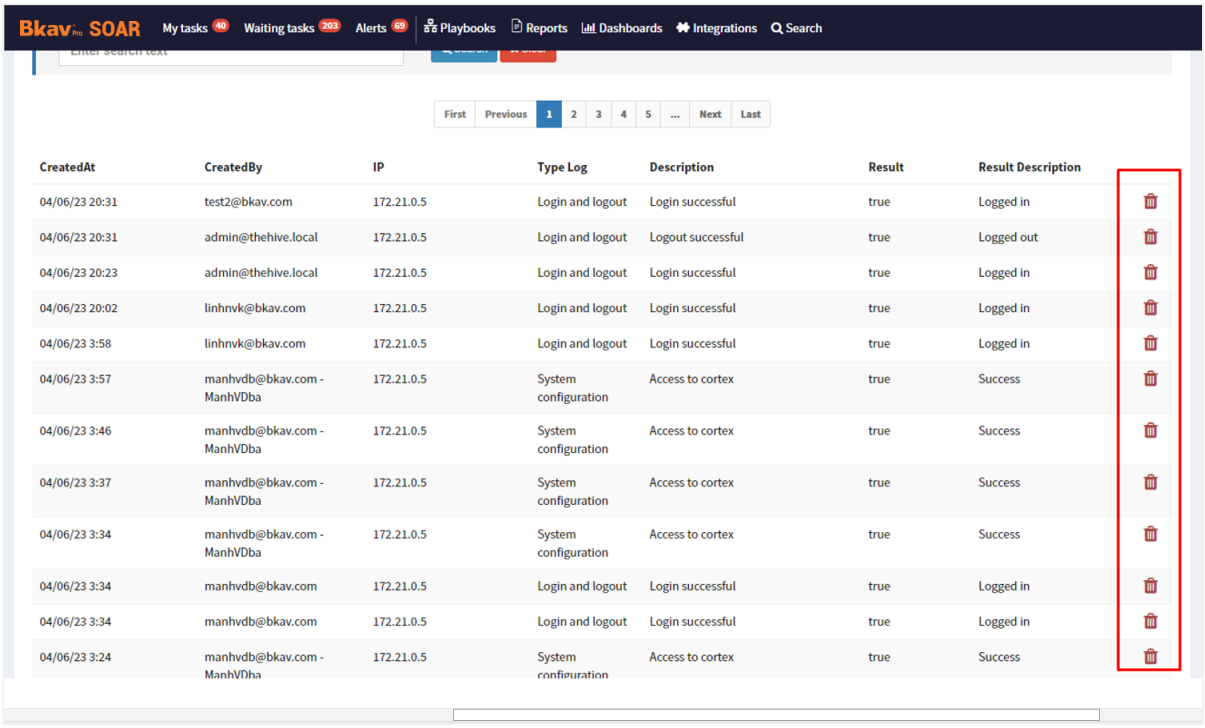
- Cho phép đăng xuất tài khoản người dùng có phiên kết nối còn hiệu lực



- Cho phép tìm kiếm dữ liệu log bằng từ khóa để xem lại



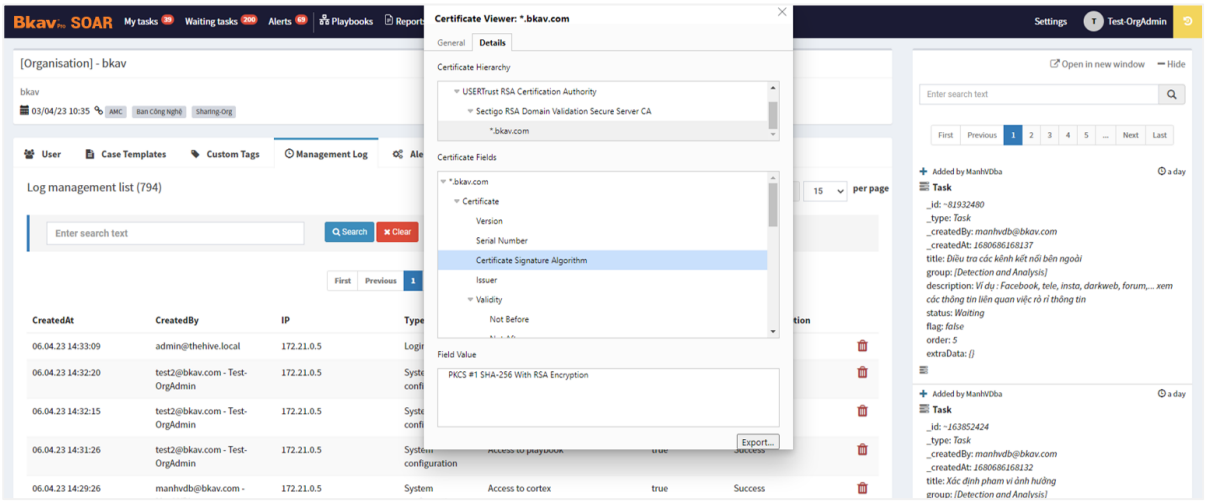
- Cho phép xóa log



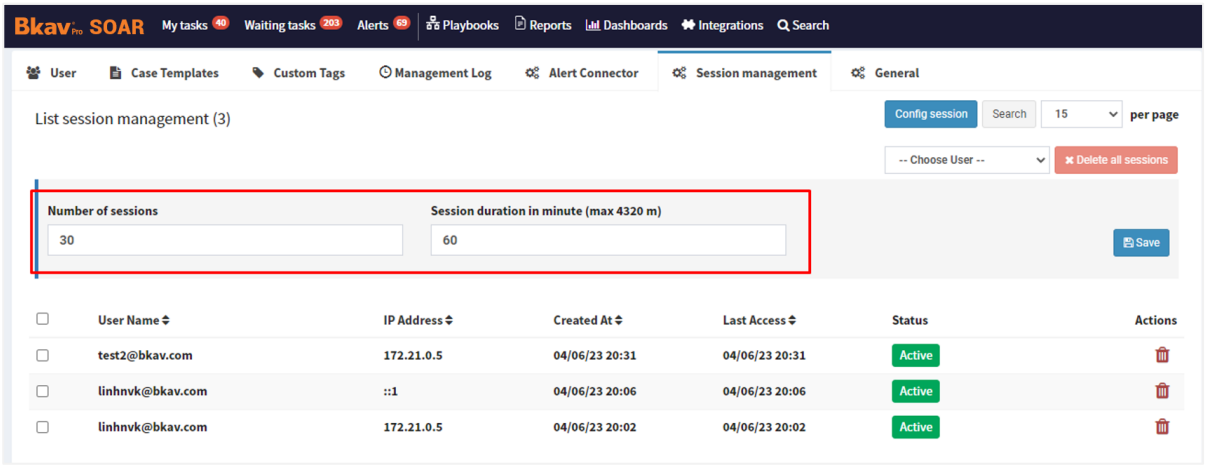
- Cho phép xem thời gian hệ thống chạy tính từ lần khởi động gần nhất

1.2. Quản trị từ xa

- Sử dụng giao thức có mã hóa TLS.

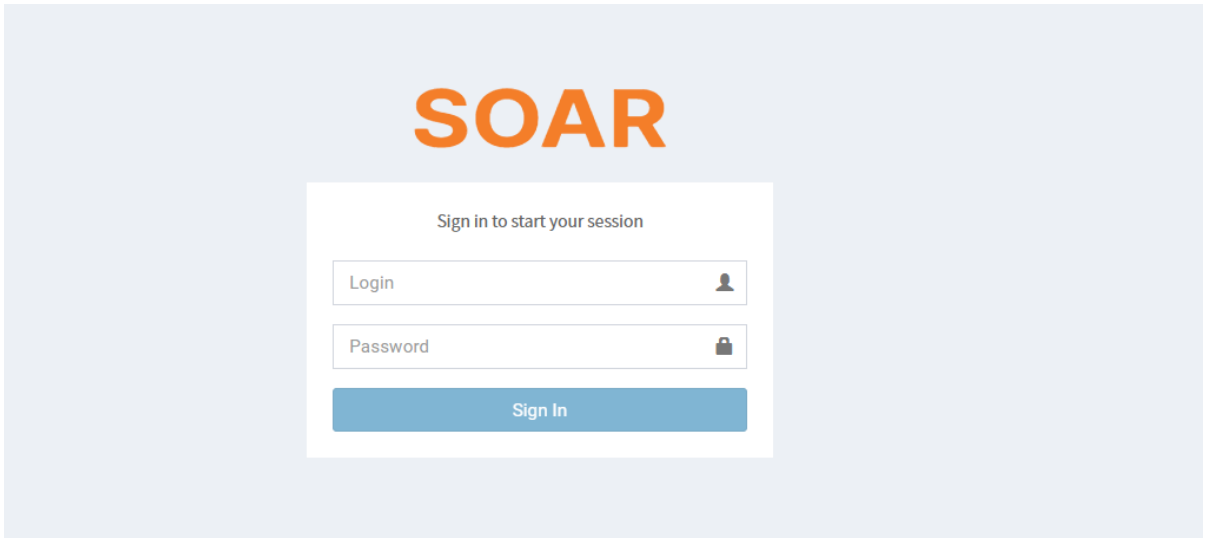


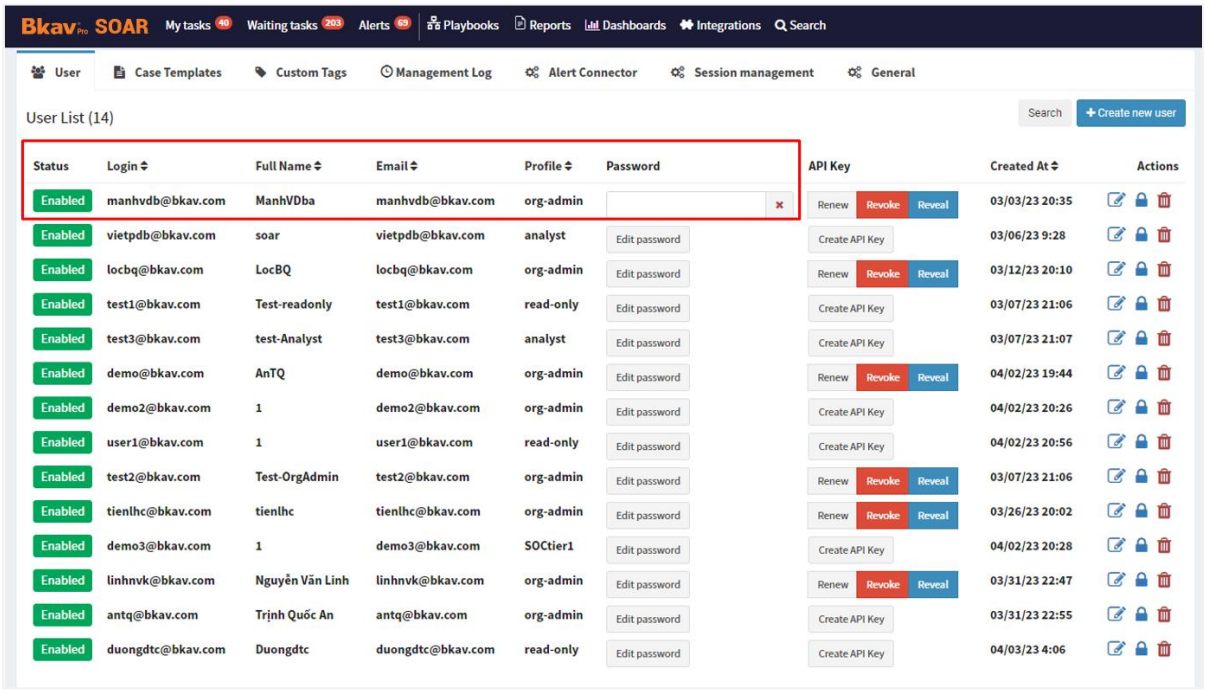
- Tự động đăng xuất tài khoản và hủy bỏ phiên kết nối quản trị từ xa khi hết thời gian duy trì phiên kết nối. Người dùng truy cập vào hệ thống khi đã sử dụng quá thời gian đã cấu hình ngưỡng thời gian 1 phiên truy cập thì sẽ tự động đăng xuất ra khỏi màn hình đăng nhập



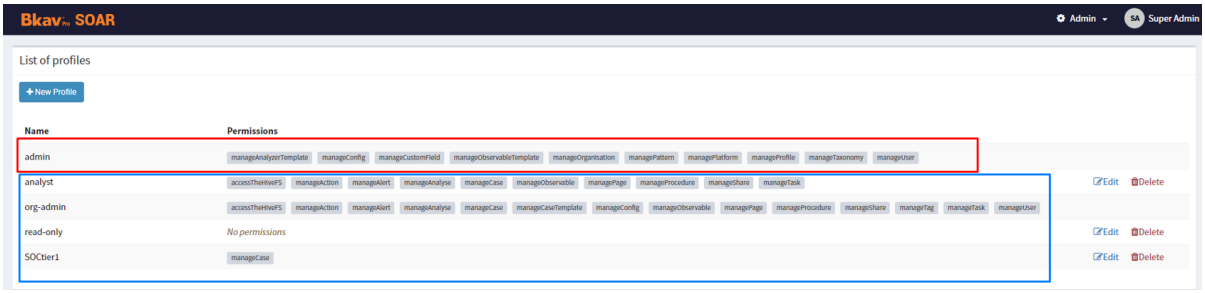
1.3. Quản lý xác thực và phân quyền

- Hỗ trợ phương thức xác thực bằng tài khoản - mật khẩu



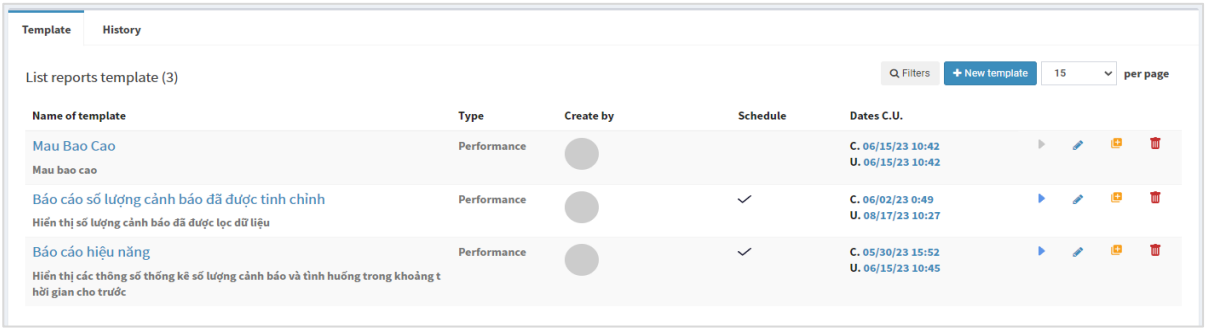


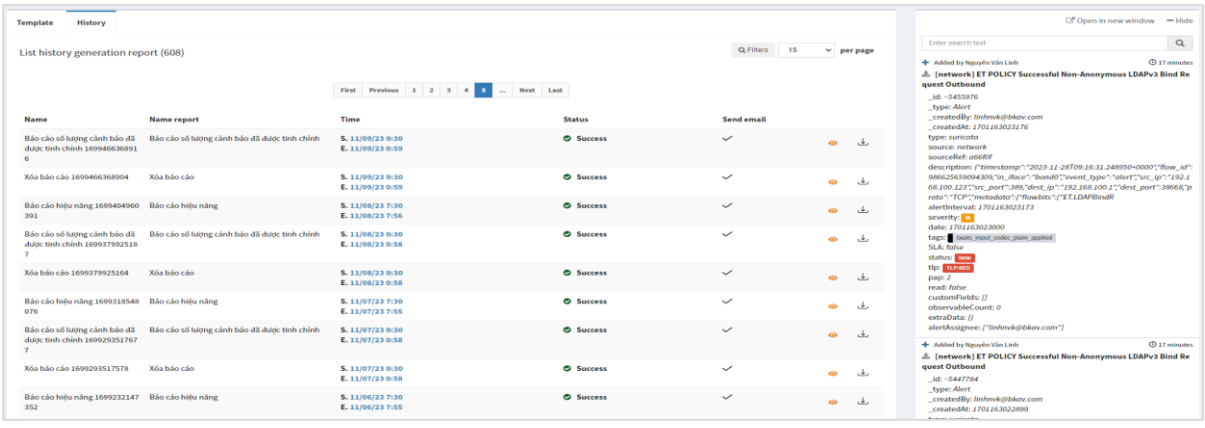
- Hỗ trợ phân nhóm tài khoản tối thiểu theo 02 nhóm là quản trị viên và người dùng thường với những quyền hạn cụ thể đối với từng nhóm
  - ✓ Hệ thống đã có tự động chia sẵn ra làm 2 nhóm và quyền hạn cụ thể của quản trị viên và người dùng hệ thống và có thể tự động tạo / tùy chỉnh các quyền hạn
  - ✓ Phần bôi màu đỏ là vai trò quản trị viên và vai trò tương ứng
  - ✓ Phần bôi màu xanh là vai trò người dùng thông thường với vai trò tương ứng

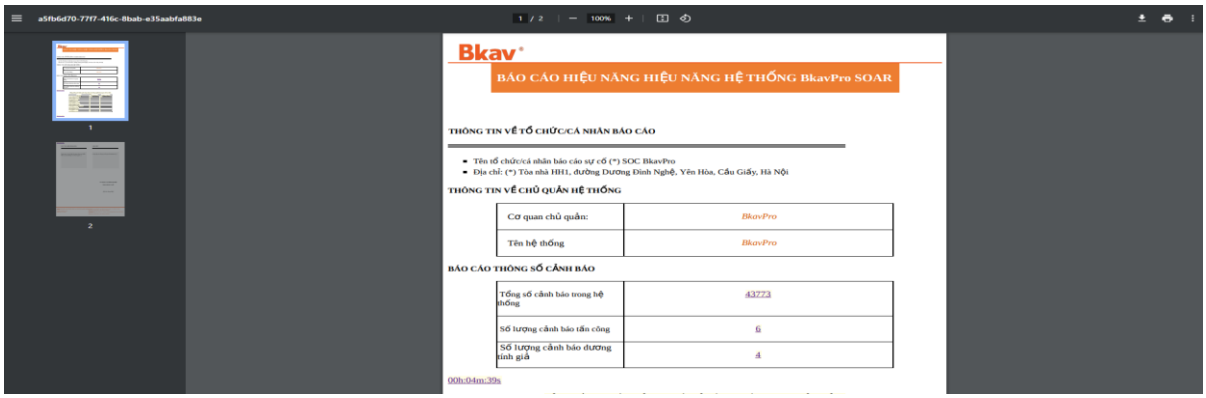


1.4. Quản lý báo cáo

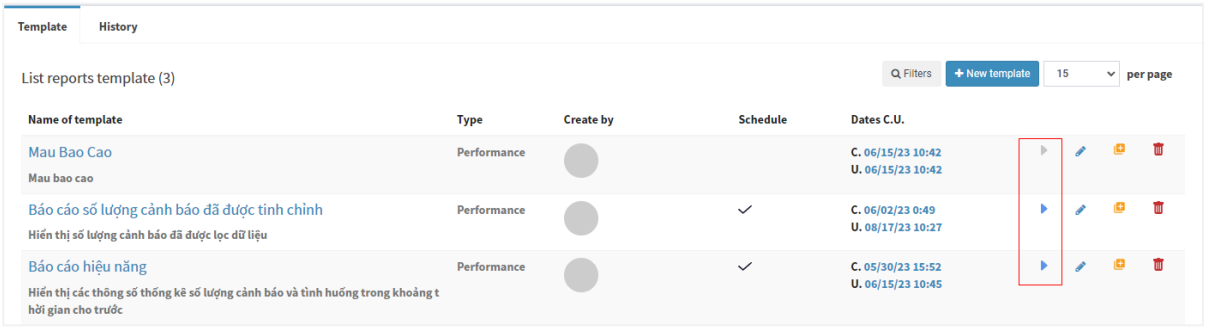
- SOAR cho phép quản lý báo cáo thông qua giao diện đồ họa đáp ứng các yêu cầu sau:.
- Cho phép tạo mới, xem lại và xóa báo cáo đã được tạo.



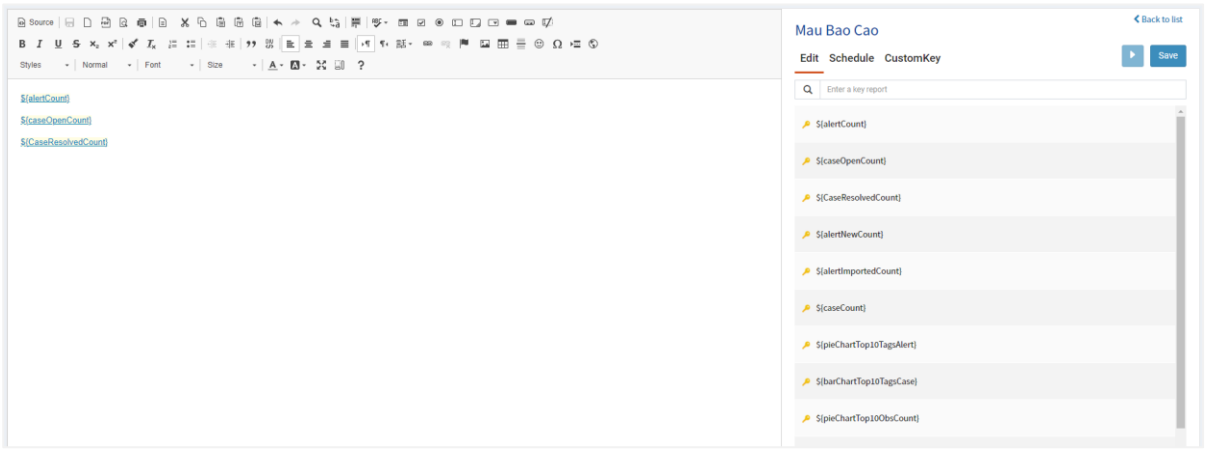




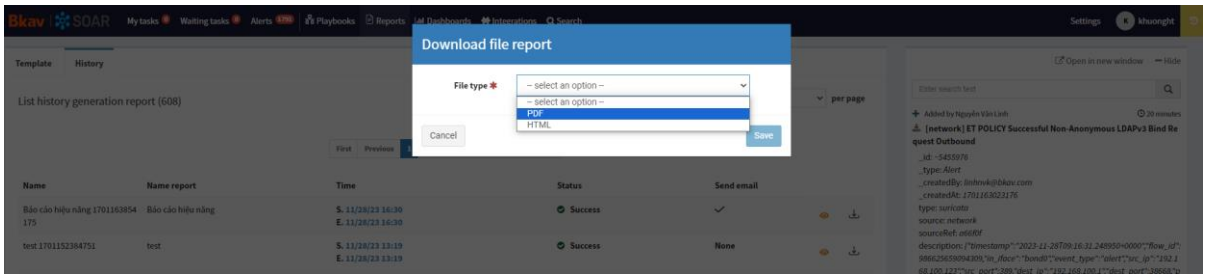
- Cho phép tạo báo cáo mới theo các mẫu báo cáo đã được định nghĩa trước.



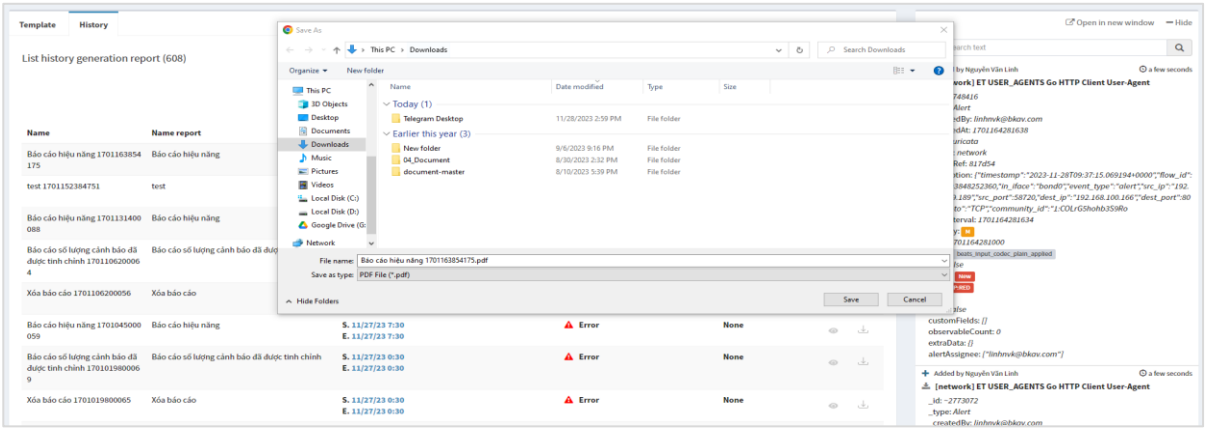
- Cho phép áp dụng các quy tắc tìm kiếm cảnh báo, sự kiện để thêm, lọc, tinh chỉnh nội dung cho báo cáo.



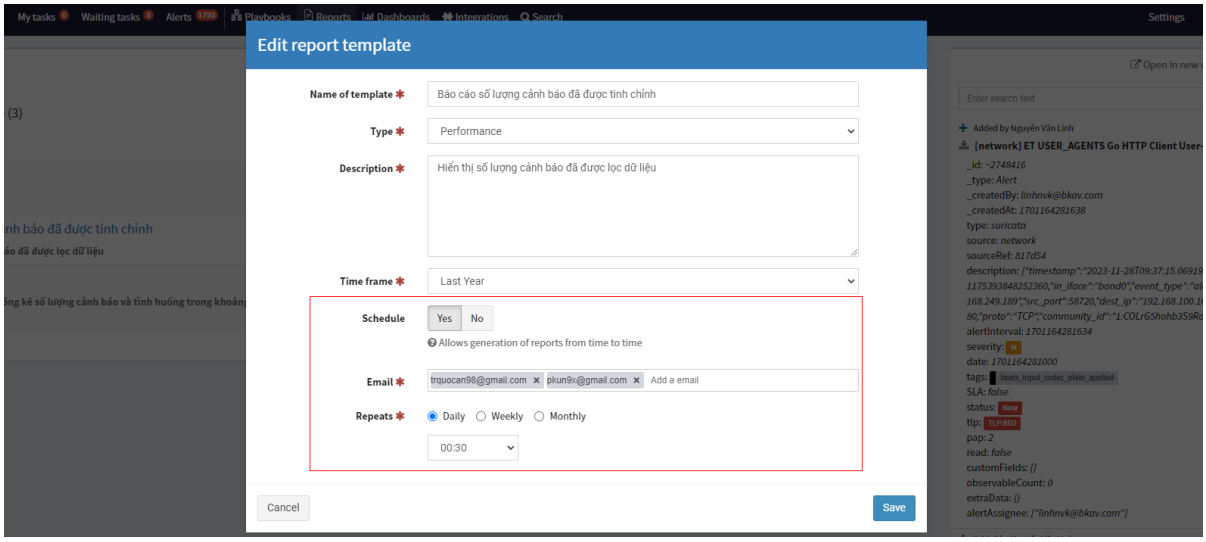
- Cho phép lựa chọn định dạng tệp tin báo cáo xuất ra các định dạng sau: PDF, HTML



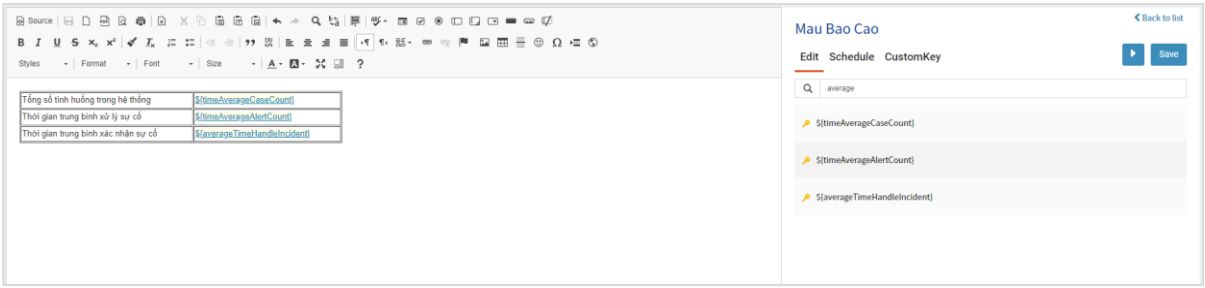
- Cho phép tải về tệp tin báo cáo đã được xuất ra;.

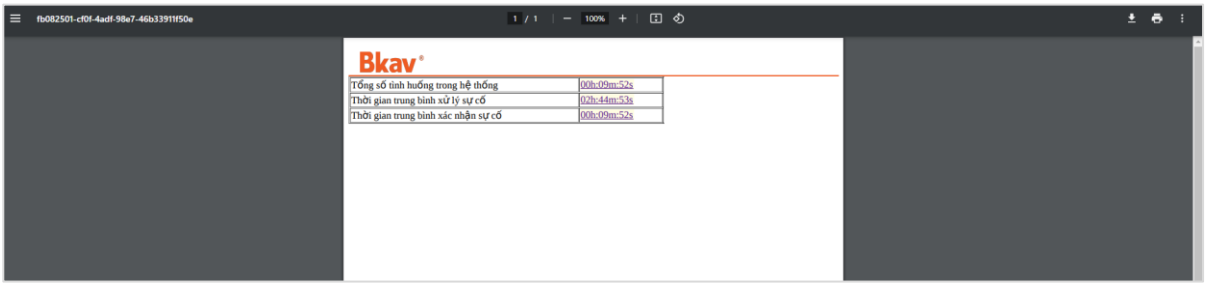


- Cho phép đặt lịch gửi báo cáo định kỳ tới email được cấu hình.



- Cho phép tạo báo cáo hiệu năng hoạt động của SOAR thông qua tối thiểu 02 thông số sau: thời gian trung bình để xác nhận một sự cố an toàn thông tin, thời gian trung bình để xử lý một sự cố an toàn thông tin kể từ lúc xác nhận.





- Cho phép tạo báo cáo hiệu quả công việc của từng người tham gia xử lý cảnh báo thông qua tối thiểu 02 thông số sau: số lượng cảnh báo được xử lý trên mỗi người, số lượng cảnh báo được xử lý đúng hạn trên mỗi người.

2. Kiểm soát lỗi

2.1. Bảo vệ cấu hình

- Trong trường hợp BkavPro SOAR phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), hệ thống vẫn đảm bảo các loại cấu hình sau mà đang được áp dụng phải được lưu lại và không bị thay đổi trong lần khởi động kế tiếp: Cấu hình hệ thống, cấu hình quản trị từ xa, cấu hình tài khoản xác thực và phân quyền người dùng, cấu hình thu thập cảnh báo, cấu hình kịch bản, cấu hình thành phần tích hợp

2.2. Bảo vệ dữ liệu log, cảnh báo, tình huống và bằng chứng

- Trong trường hợp BkavPro SOAR phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), hệ thống vẫn đảm bảo dữ liệu log, cảnh báo, tình huống và bằng chứng đã được lưu lại phải không bị thay đổi trong lần khởi động kế tiếp

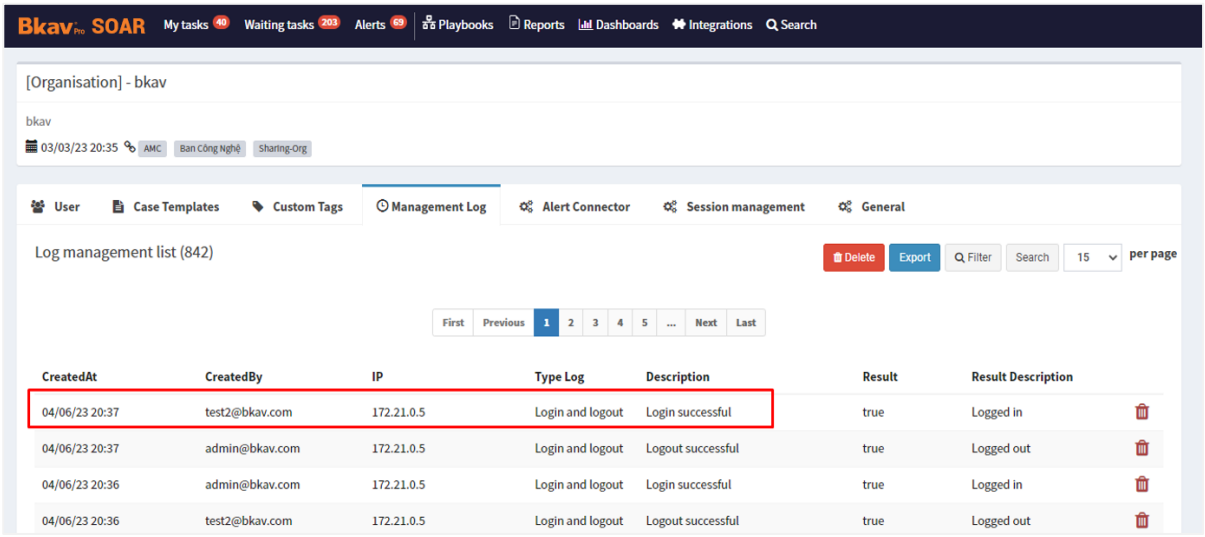
2.3. Đồng bộ thời gian hệ thống

- Trong trường hợp BkavPro SOAR phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), hệ thống đảm bảo thời gian hệ thống phải được đồng bộ tự động đến thời điểm hiện tại

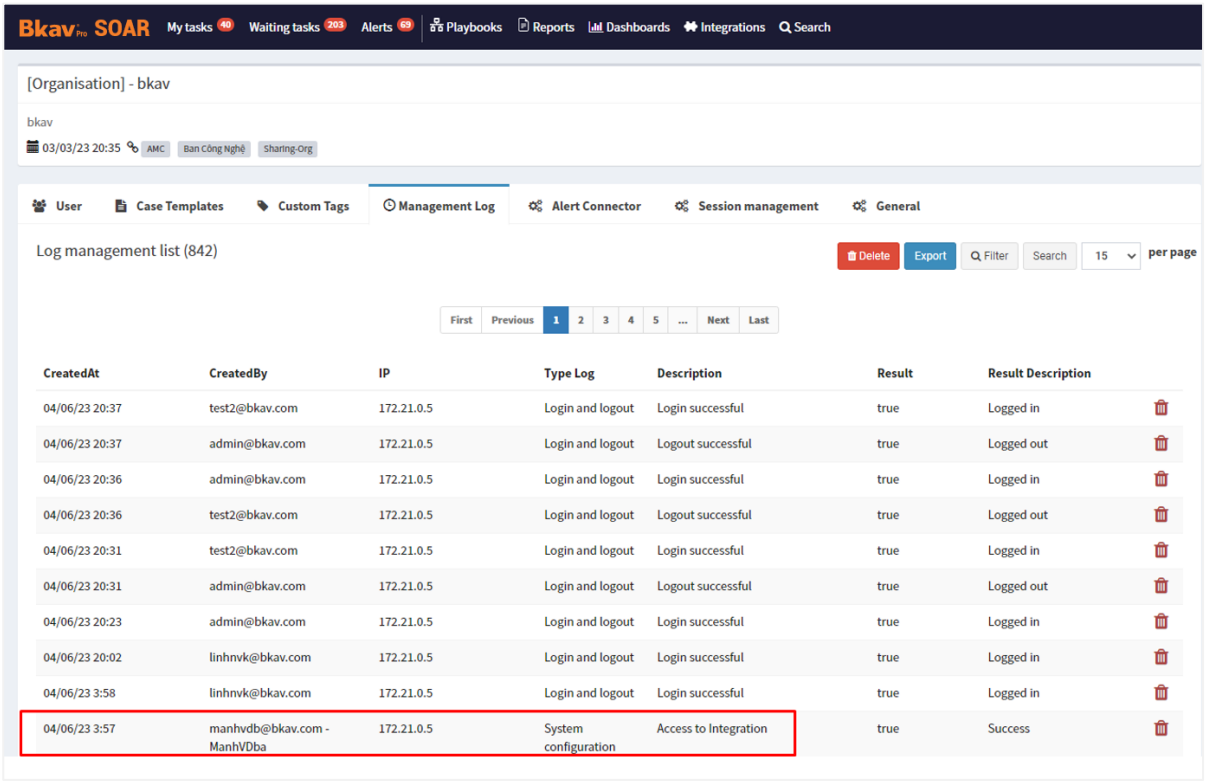
3. Chức năng về Log

3.1. Log quản trị hệ thống

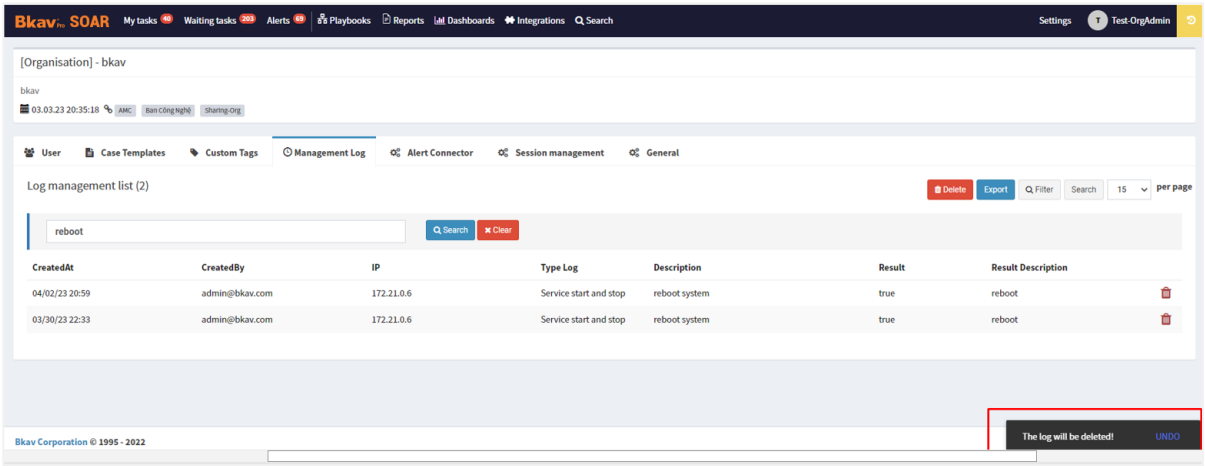
- BkavPro SOAR cho phép ghi log quản trị hệ thống về các loại sự kiện sau:
  - Đăng nhập, đăng xuất tài khoản



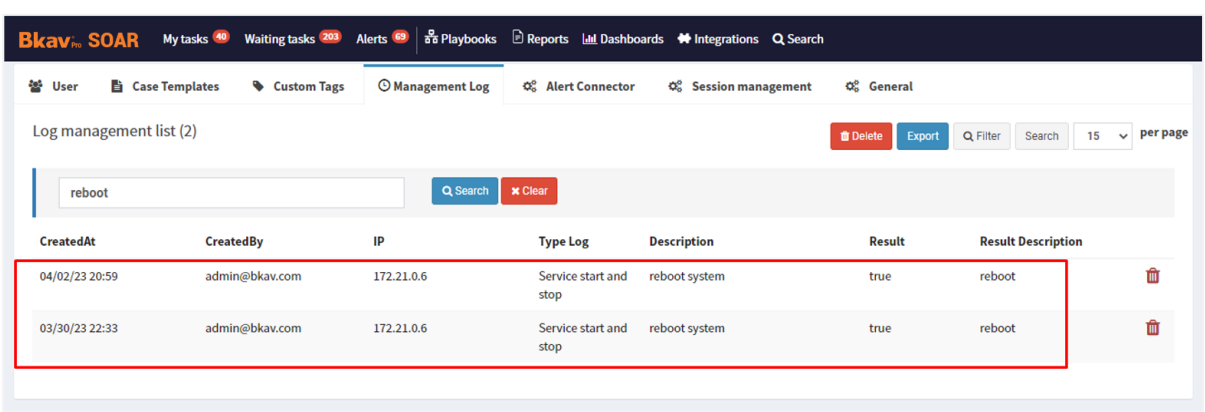
- BkavPro SOAR cho phép ghi log quản trị hệ thống về các loại sự kiện sau:
  - Xác thực trước khi cho phép truy cập vào tài nguyên, sử dụng chức năng của hệ thống



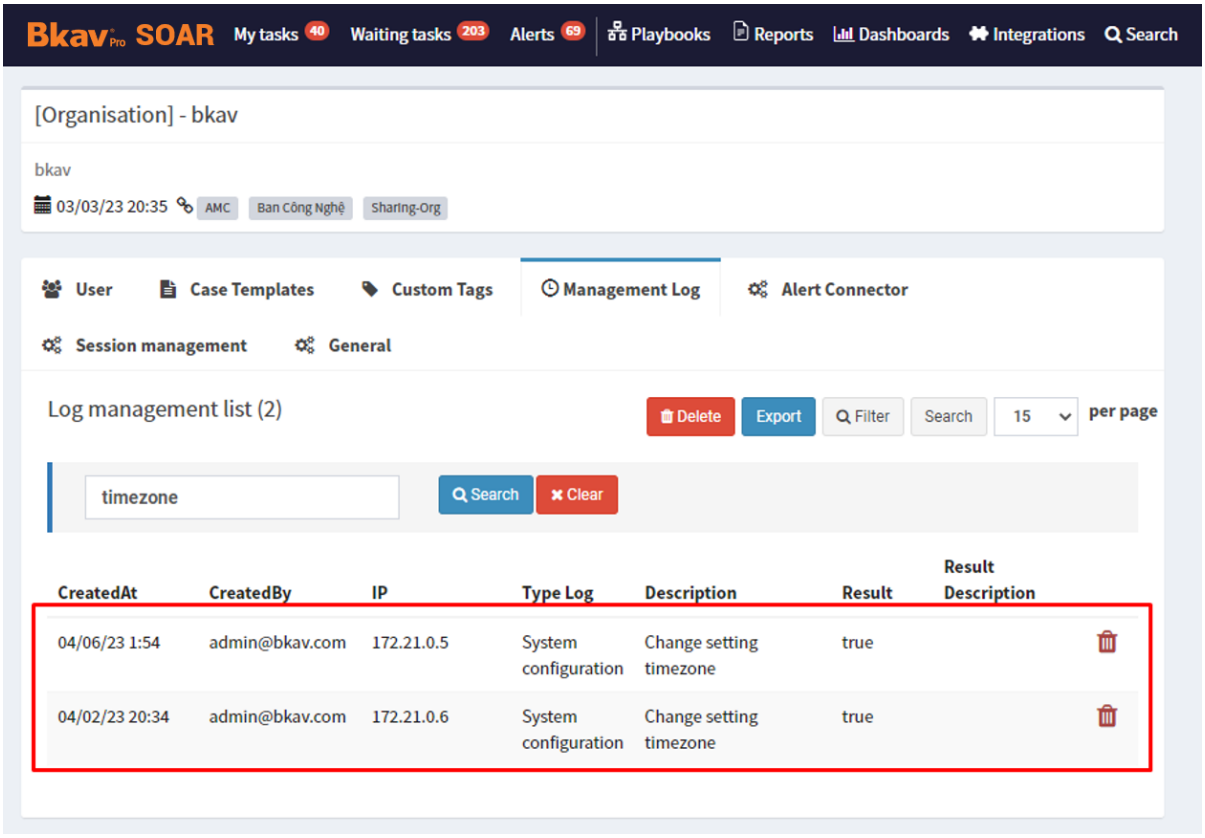
  - Áp dụng, hoàn tác sự thay đổi trong cấu hình hệ thống, cấu hình quản trị từ xa, cấu hình tài khoản xác thực và phân quyền người dùng, cấu hình thu thập cảnh báo, cấu hình kịch bản



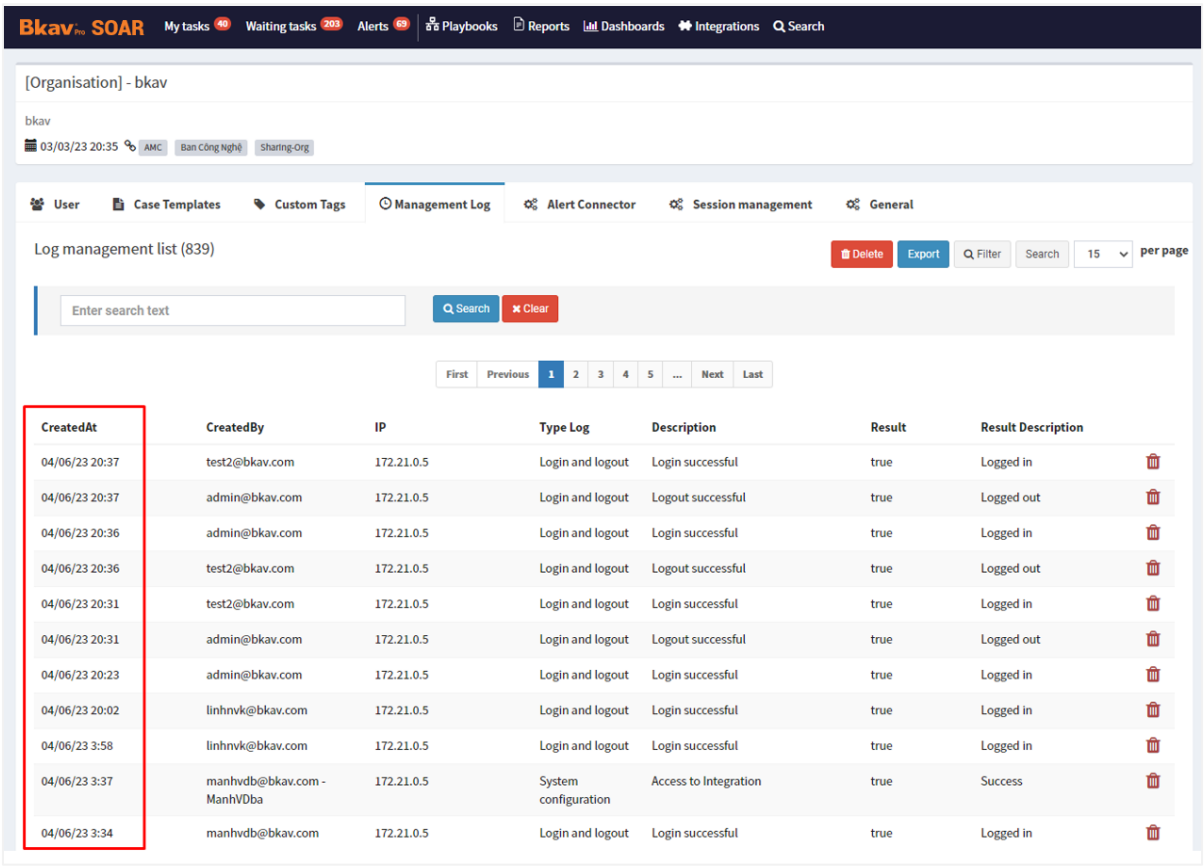
  - Kích hoạt lệnh khởi động lại, tắt hệ thống



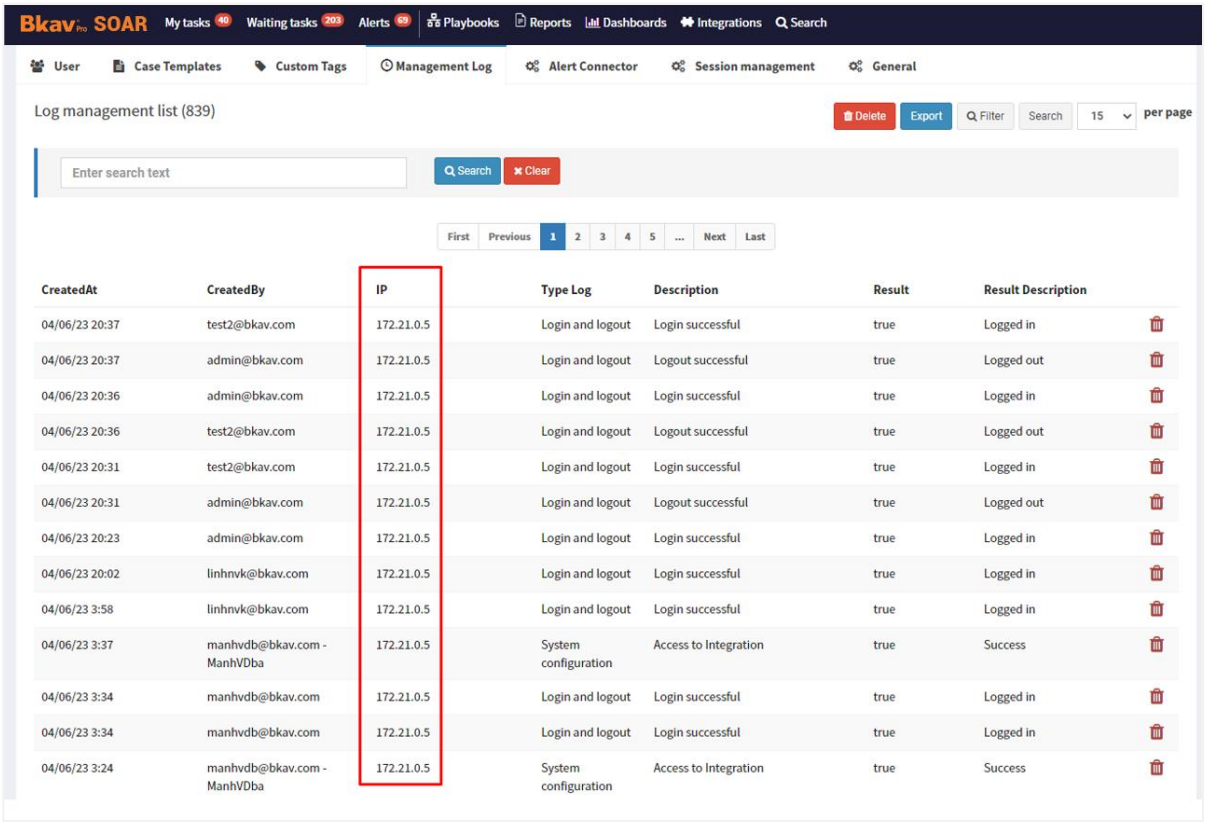
- BkavPro SOAR cho phép ghi log quản trị hệ thống về các loại sự kiện sau:
  - Thay đổi thủ công thời gian hệ thống



- BkavPro SOAR cho phép ghi log quản trị hệ thống bao gồm các trường thông tin sau:
  - Thời gian sinh log (bao gồm năm, tháng, ngày, giờ, phút và giây)

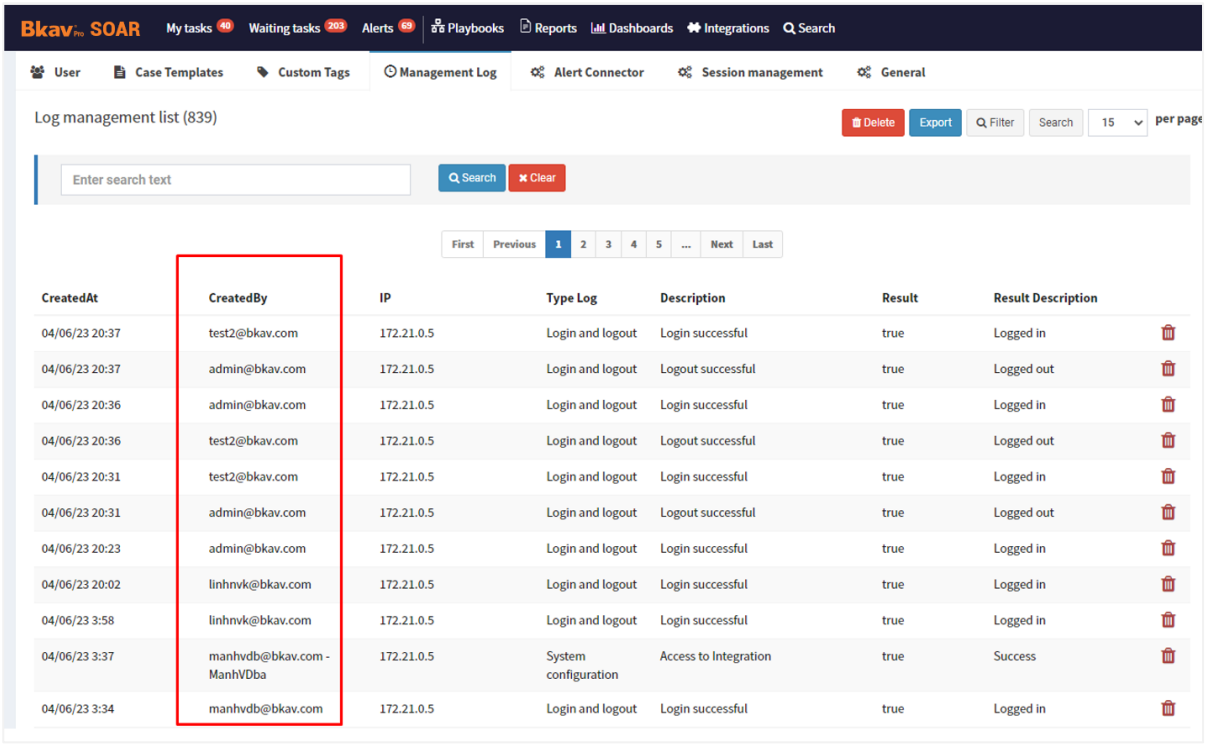


- BkavPro SOAR cho phép ghi log quản trị hệ thống bao gồm các trường thông tin sau:
  - Địa chỉ IP hoặc định danh của máy trạm



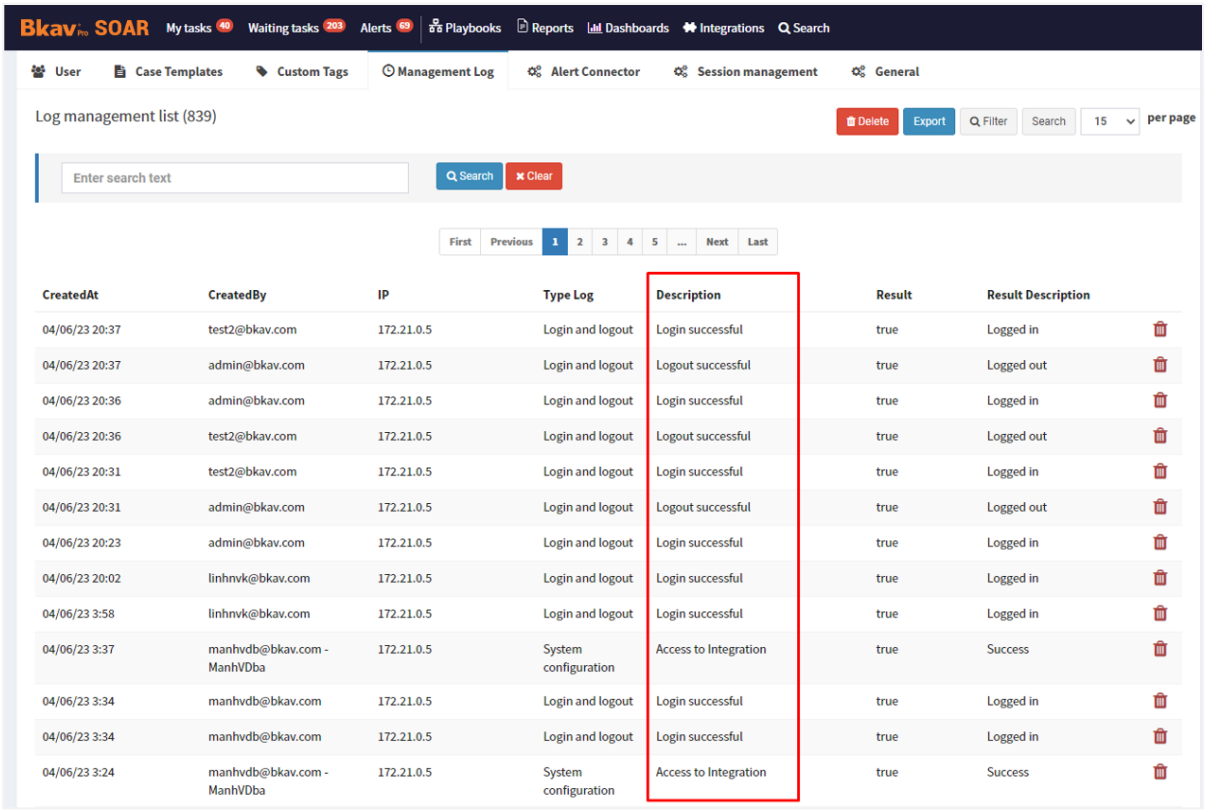
CreatedAt	CreatedBy	IP	Type Log	Description	Result	Result Description
04/06/23 20:37	test2@bkav.com	172.21.0.5	Login and logout	Login successful	true	Logged in
04/06/23 20:37	admin@bkav.com	172.21.0.5	Login and logout	Logout successful	true	Logged out
04/06/23 20:36	admin@bkav.com	172.21.0.5	Login and logout	Login successful	true	Logged in
04/06/23 20:36	test2@bkav.com	172.21.0.5	Login and logout	Logout successful	true	Logged out
04/06/23 20:31	test2@bkav.com	172.21.0.5	Login and logout	Login successful	true	Logged in
04/06/23 20:31	admin@bkav.com	172.21.0.5	Login and logout	Logout successful	true	Logged out
04/06/23 20:23	admin@bkav.com	172.21.0.5	Login and logout	Login successful	true	Logged in
04/06/23 20:02	linhnvk@bkav.com	172.21.0.5	Login and logout	Login successful	true	Logged in
04/06/23 3:58	linhnvk@bkav.com	172.21.0.5	Login and logout	Login successful	true	Logged in
04/06/23 3:37	manhvdb@bkav.com - ManhVDba	172.21.0.5	System configuration	Access to Integration	true	Success
04/06/23 3:34	manhvdb@bkav.com	172.21.0.5	Login and logout	Login successful	true	Logged in
04/06/23 3:34	manhvdb@bkav.com	172.21.0.5	Login and logout	Login successful	true	Logged in
04/06/23 3:24	manhvdb@bkav.com - ManhVDba	172.21.0.5	System configuration	Access to Integration	true	Success

  - Định danh của tác nhân (ví dụ: tài khoản người dùng, tên hệ thống…)



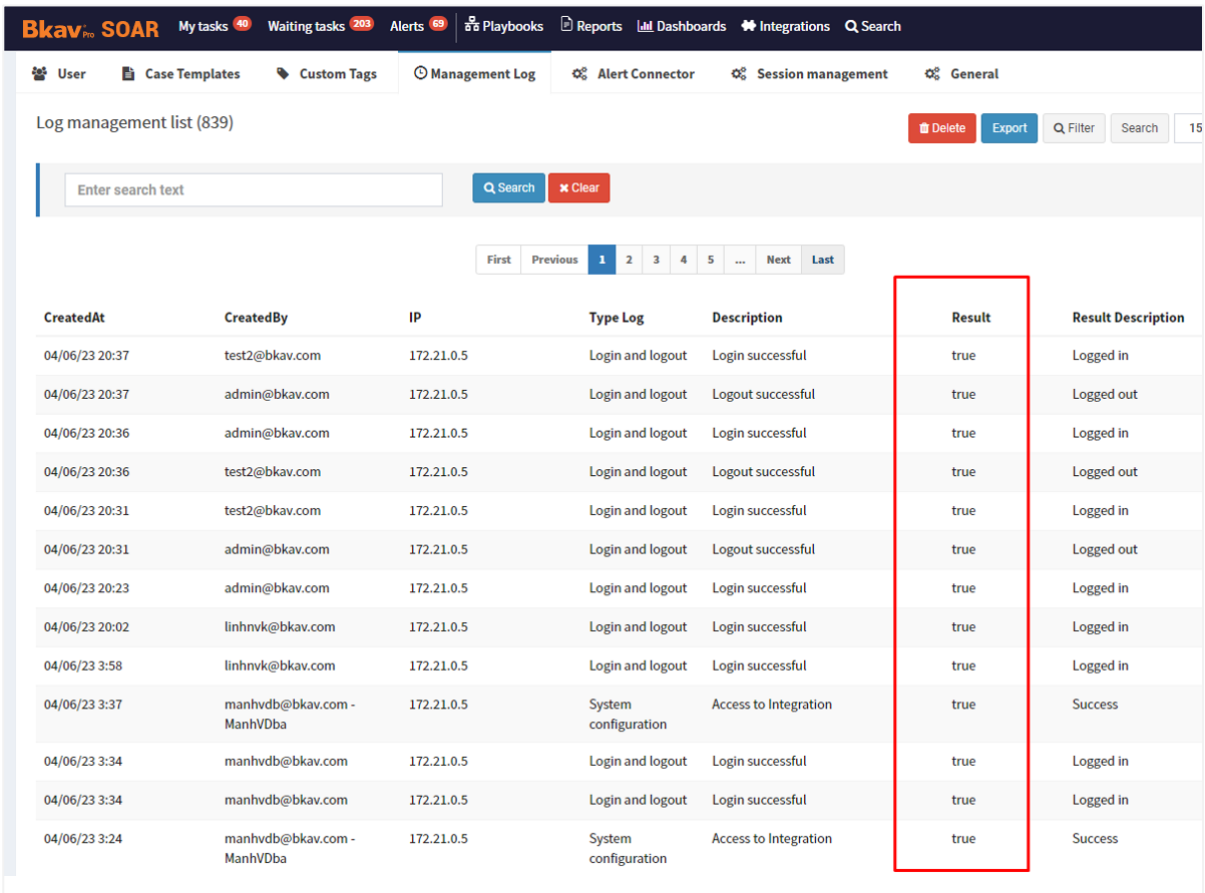
CreatedAt	CreatedBy	IP	Type Log	Description	Result	Result Description
04/06/23 20:37	test2@bkav.com	172.21.0.5	Login and logout	Login successful	true	Logged in
04/06/23 20:37	admin@bkav.com	172.21.0.5	Login and logout	Logout successful	true	Logged out
04/06/23 20:36	admin@bkav.com	172.21.0.5	Login and logout	Login successful	true	Logged in
04/06/23 20:36	test2@bkav.com	172.21.0.5	Login and logout	Logout successful	true	Logged out
04/06/23 20:31	test2@bkav.com	172.21.0.5	Login and logout	Login successful	true	Logged in
04/06/23 20:31	admin@bkav.com	172.21.0.5	Login and logout	Logout successful	true	Logged out
04/06/23 20:23	admin@bkav.com	172.21.0.5	Login and logout	Login successful	true	Logged in
04/06/23 20:02	linhnvk@bkav.com	172.21.0.5	Login and logout	Login successful	true	Logged in
04/06/23 3:58	linhnvk@bkav.com	172.21.0.5	Login and logout	Login successful	true	Logged in
04/06/23 3:37	manhvdb@bkav.com - ManhVDba	172.21.0.5	System configuration	Access to Integration	true	Success
04/06/23 3:34	manhvdb@bkav.com	172.21.0.5	Login and logout	Login successful	true	Logged in

- BkavPro SOAR cho phép ghi log quản trị hệ thống bao gồm các trường thông tin sau:
  - Thông tin về hành vi thực hiện (ví dụ: đăng nhập, đăng xuất, thêm, sửa, xóa, cập nhật, hoàn tác…)



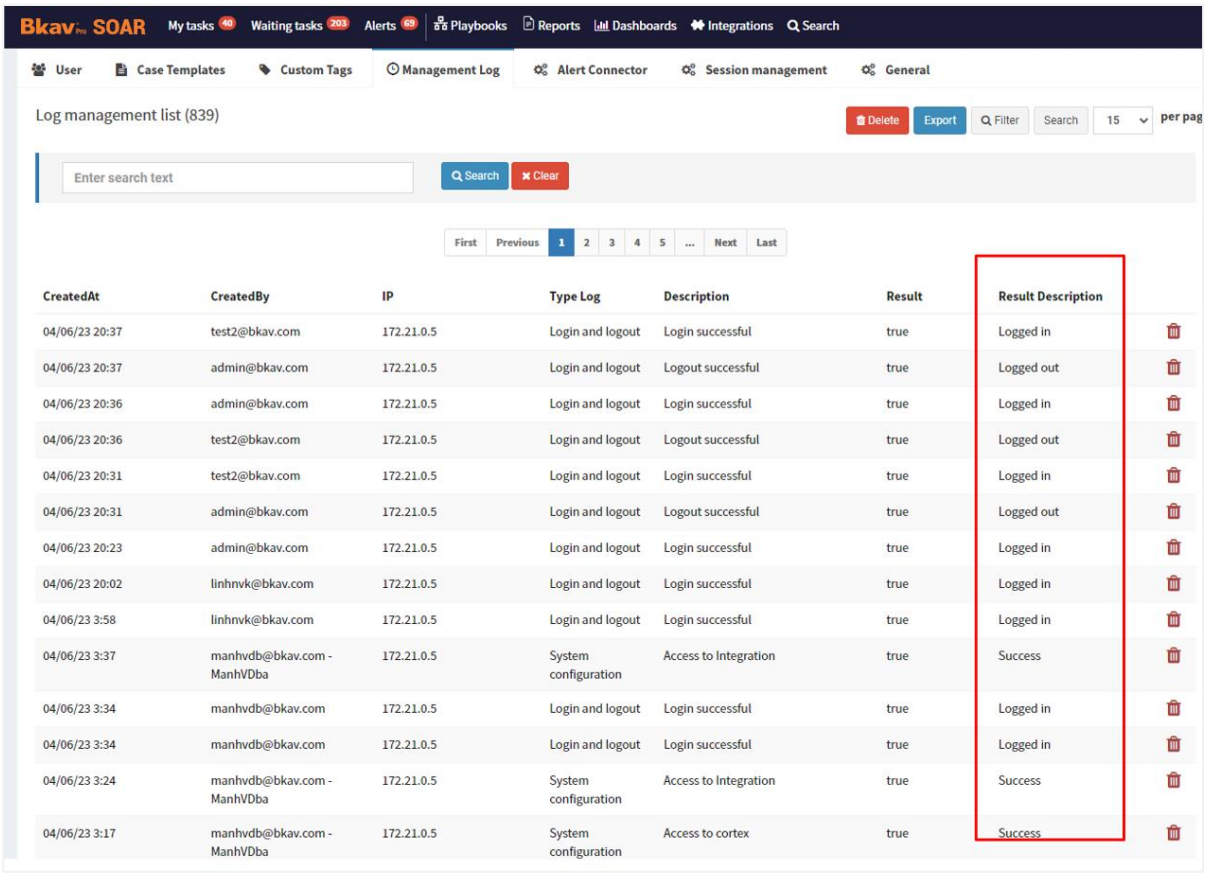
CreatedAt	CreatedBy	IP	Type Log	Description	Result	Result Description
04/06/23 20:37	test2@bkav.com	172.21.0.5	Login and logout	Login successful	true	Logged in
04/06/23 20:37	admin@bkav.com	172.21.0.5	Login and logout	Logout successful	true	Logged out
04/06/23 20:36	admin@bkav.com	172.21.0.5	Login and logout	Login successful	true	Logged in
04/06/23 20:36	test2@bkav.com	172.21.0.5	Login and logout	Logout successful	true	Logged out
04/06/23 20:31	test2@bkav.com	172.21.0.5	Login and logout	Login successful	true	Logged in
04/06/23 20:31	admin@bkav.com	172.21.0.5	Login and logout	Logout successful	true	Logged out
04/06/23 20:23	admin@bkav.com	172.21.0.5	Login and logout	Login successful	true	Logged in
04/06/23 20:02	linhnvk@bkav.com	172.21.0.5	Login and logout	Login successful	true	Logged in
04/06/23 3:58	linhnvk@bkav.com	172.21.0.5	Login and logout	Login successful	true	Logged in
04/06/23 3:37	manhvdb@bkav.com - ManhVDba	172.21.0.5	System configuration	Access to Integration	true	Success
04/06/23 3:34	manhvdb@bkav.com	172.21.0.5	Login and logout	Login successful	true	Logged in
04/06/23 3:34	manhvdb@bkav.com	172.21.0.5	Login and logout	Login successful	true	Logged in
04/06/23 3:24	manhvdb@bkav.com - ManhVDba	172.21.0.5	System configuration	Access to Integration	true	Success

  - Kết quả thực hiện hành vi (thành công hoặc thất bại)



CreatedAt	CreatedBy	IP	Type Log	Description	Result	Result Description
04/06/23 20:37	test2@bkav.com	172.21.0.5	Login and logout	Login successful	true	Logged in
04/06/23 20:37	admin@bkav.com	172.21.0.5	Login and logout	Logout successful	true	Logged out
04/06/23 20:36	admin@bkav.com	172.21.0.5	Login and logout	Login successful	true	Logged in
04/06/23 20:36	test2@bkav.com	172.21.0.5	Login and logout	Logout successful	true	Logged out
04/06/23 20:31	test2@bkav.com	172.21.0.5	Login and logout	Login successful	true	Logged in
04/06/23 20:31	admin@bkav.com	172.21.0.5	Login and logout	Logout successful	true	Logged out
04/06/23 20:23	admin@bkav.com	172.21.0.5	Login and logout	Login successful	true	Logged in
04/06/23 20:02	linhnvk@bkav.com	172.21.0.5	Login and logout	Login successful	true	Logged in
04/06/23 3:58	linhnvk@bkav.com	172.21.0.5	Login and logout	Login successful	true	Logged in
04/06/23 3:37	manhvdb@bkav.com - ManhVDba	172.21.0.5	System configuration	Access to Integration	true	Success
04/06/23 3:34	manhvdb@bkav.com	172.21.0.5	Login and logout	Login successful	true	Logged in
04/06/23 3:34	manhvdb@bkav.com	172.21.0.5	Login and logout	Login successful	true	Logged in
04/06/23 3:24	manhvdb@bkav.com - ManhVDba	172.21.0.5	System configuration	Access to Integration	true	Success

- BkavPro SOAR cho phép ghi log quản trị hệ thống bao gồm các trường thông tin sau:
  - Lý do giải trình đối với hành vi thất bại (ví dụ: không tìm thấy tài nguyên, không đủ quyền truy cập…)

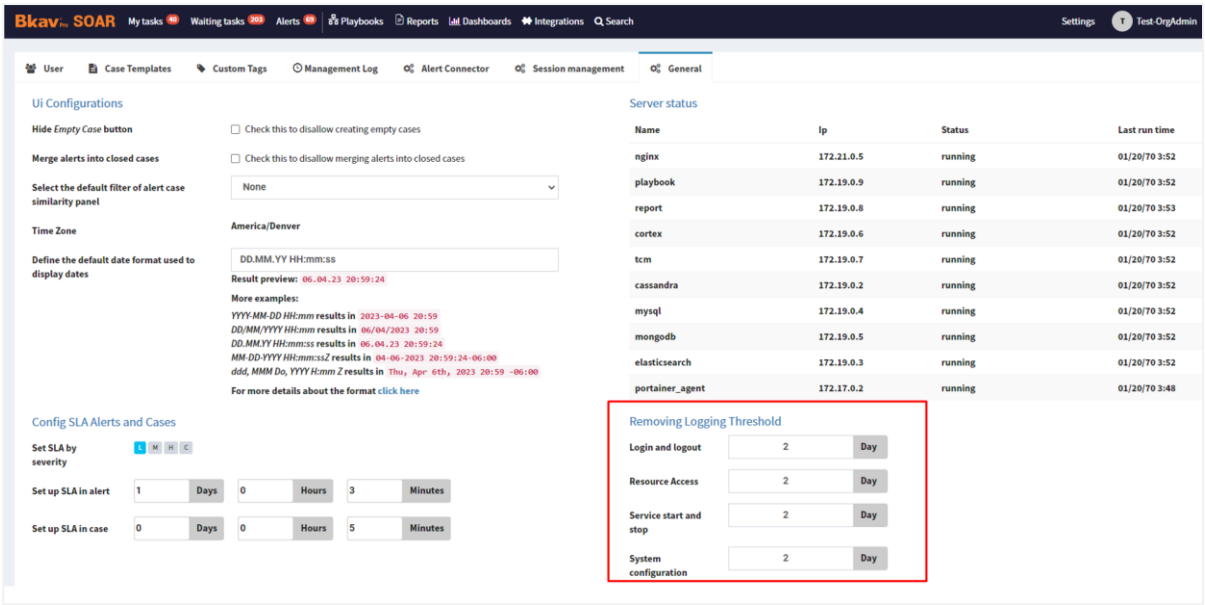


3.2. Định dạng log

- BkavPro SOAR đã thực hiện thành công việc chuẩn hóa log theo tối thiểu 01 định dạng đã được định nghĩa trước để truyền dữ liệu log cho các phần mềm quản lý, phân tích, điều tra log

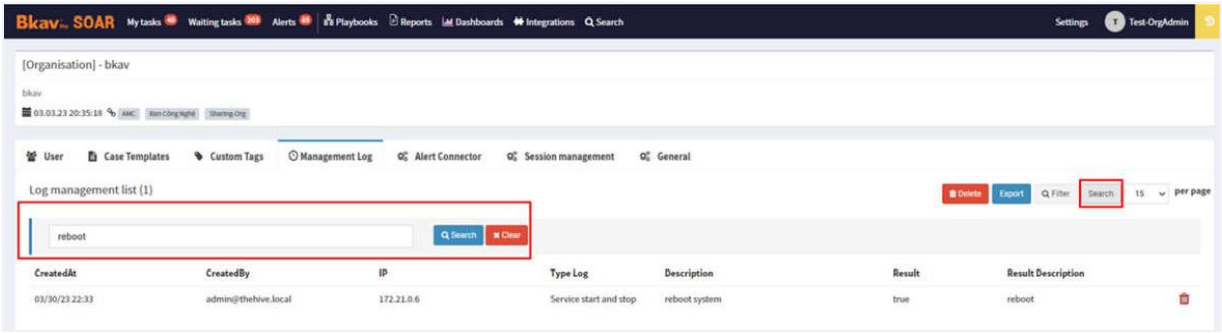
3.3. Quản lý log

- Cho phép thiết lập và cấu hình các cài đặt liên quan đến lưu trữ và hủy bỏ log (ví dụ: ngưỡng giới hạn dung lượng lưu trữ, khoảng thời gian lưu trữ…)

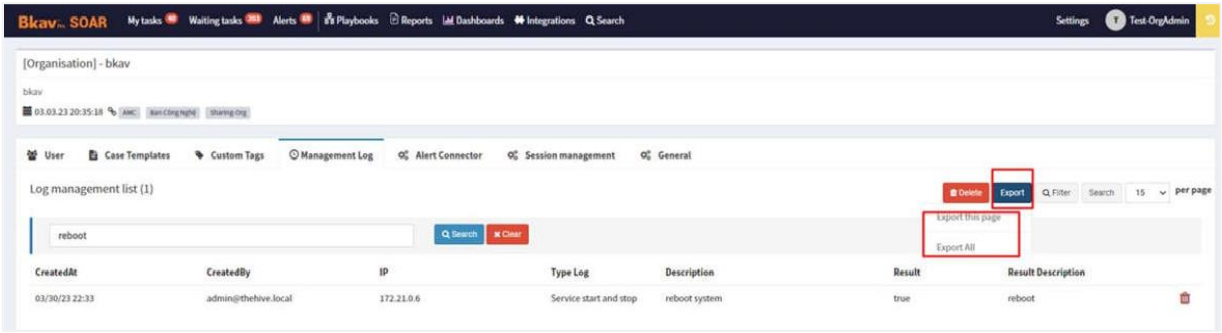


3.3. Quản lý log (tiếp)

- Cho phép tìm kiếm log theo từ khóa trên tất cả các trường thông tin bao gồm cả các trường thông tin cấp thấp hơn (nếu có)



- Cho phép xuất dữ liệu log ra để phục vụ cho việc tích hợp các dữ liệu này vào SIEM hoặc giải pháp khác về quản lý, phân tích, điều tra log



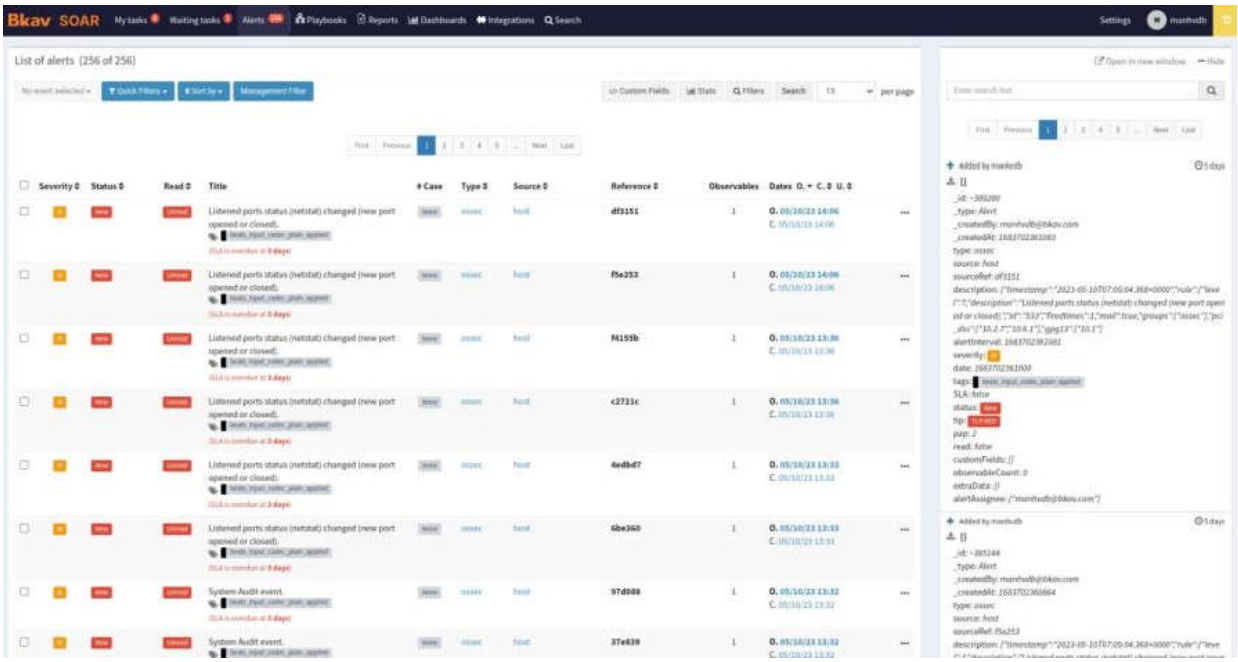
4. Hiệu năng xử lý

1. Độ trễ thời gian phản hồi các yêu cầu truy vấn dữ liệu thấp

- BkavPro SOAR đảm bảo độ trễ thời gian tìm kiếm log, cảnh báo và tình huống với độ phức tạp bất kỳ, có phản hồi trong khoảng thời gian tối đa là 01 phút

4.2. Thu thập đồng thời nhiều cảnh báo

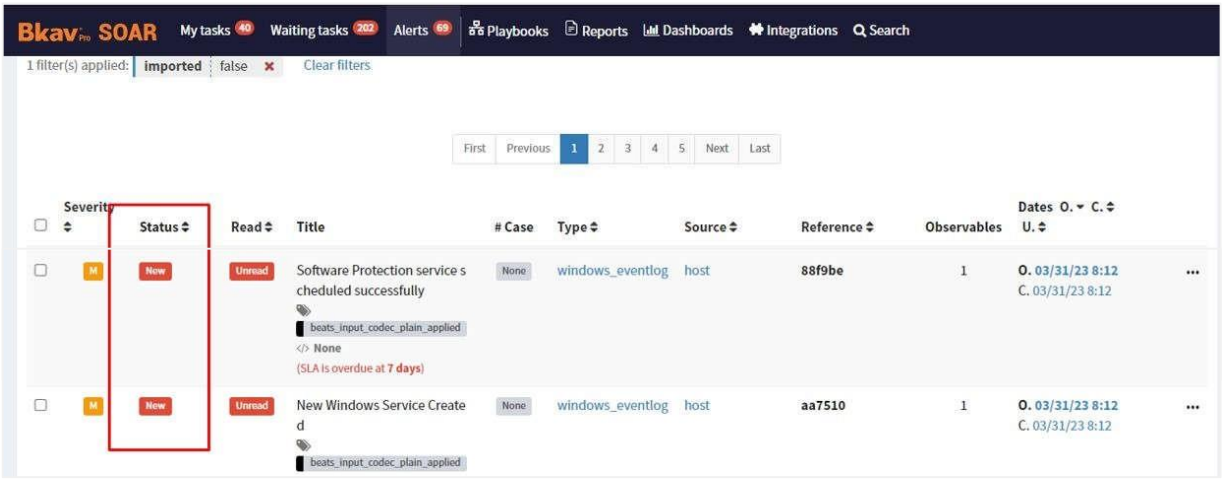
- BkavPro SOAR cho phép thu thập, xử lý và lưu trữ dữ liệu đồng thời tối thiểu 100 cảnh báo trong khoảng thời gian là 01 phút



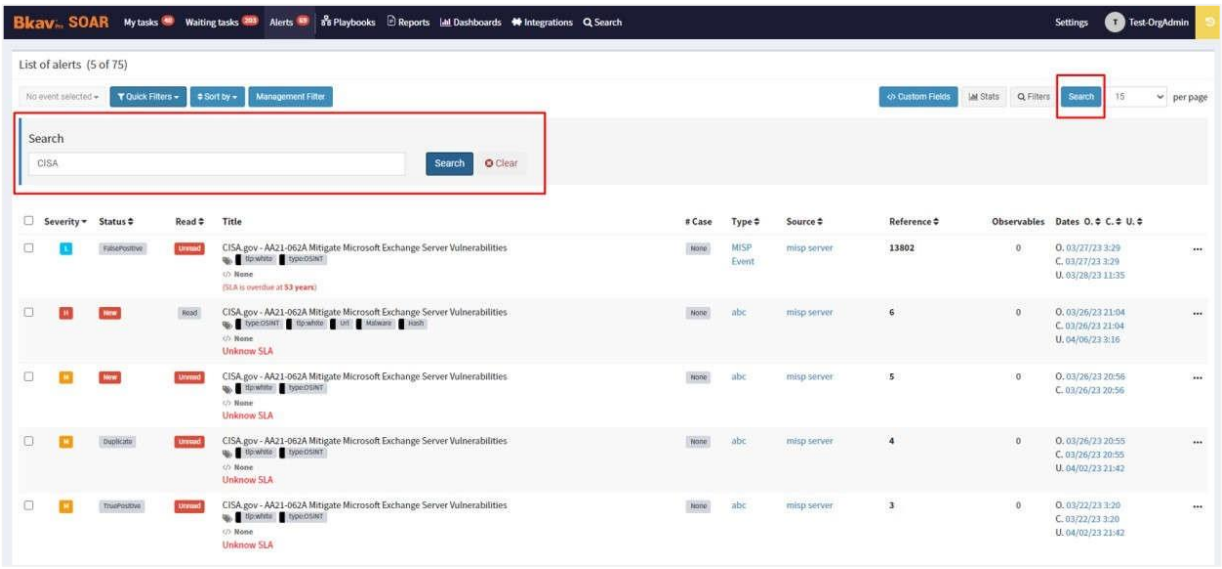
5. Chức năng điều phối xử lý và giám sát

1. Điều phối xử lý cảnh báo

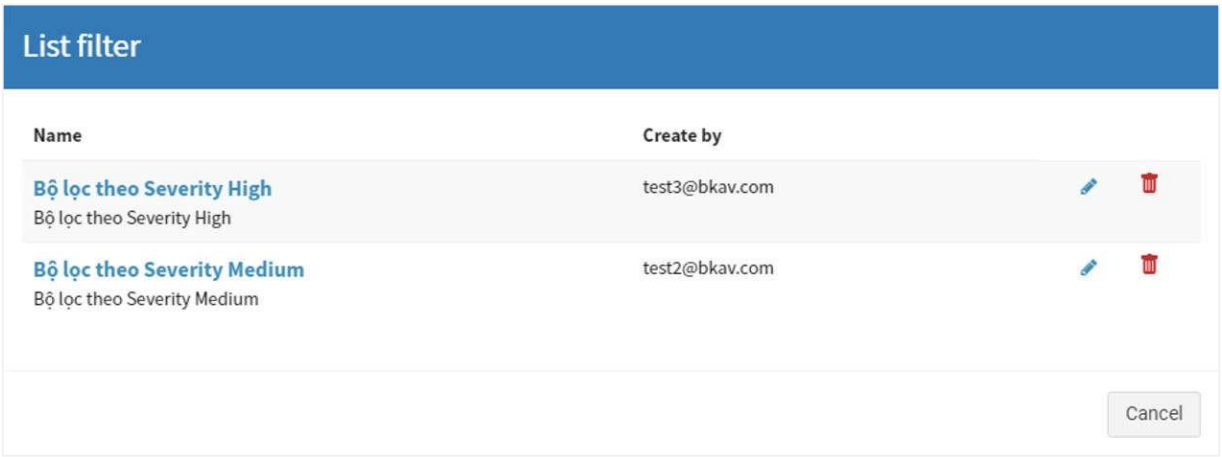
- Cho phép thiết lập cấu hình thu thập cảnh báo từ các giải pháp an toàn thông tin, công nghệ thông tin khác (ban đầu các cảnh báo được gán trạng thái là mới)



- Cho phép tìm kiếm cảnh báo theo từ khóa trên tất cả các trường thông tin của cảnh báo bao gồm cả các trường thông tin cấp thấp hơn (nếu có)

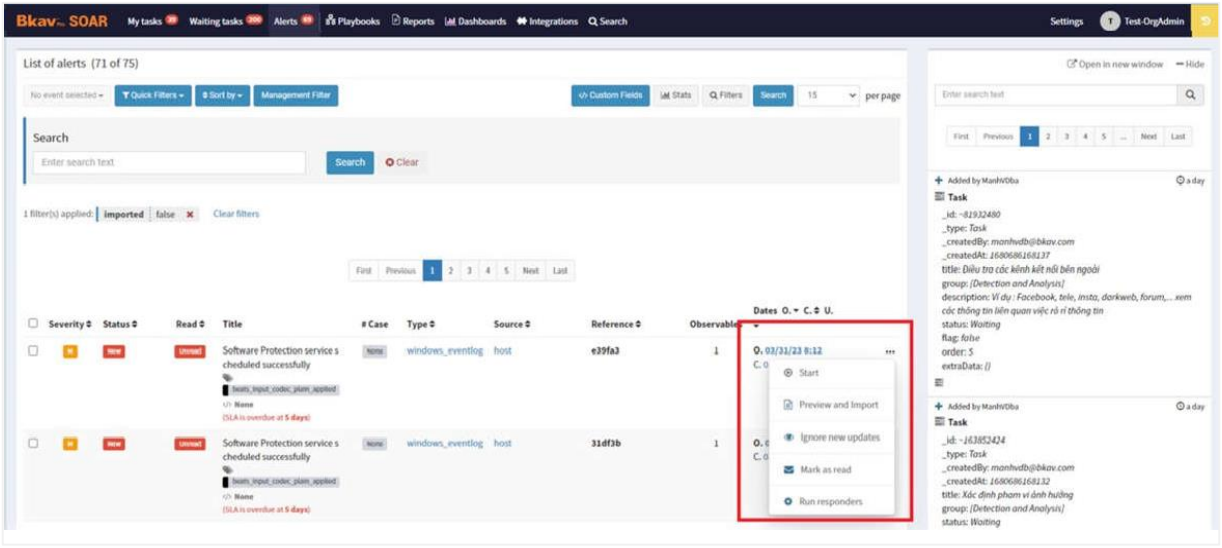


- Cho phép lưu trữ và phân nhóm cảnh báo theo các tiêu chí khác nhau (ví dụ: mức độ quan trọng của cảnh báo, nguồn gửi cảnh báo…)

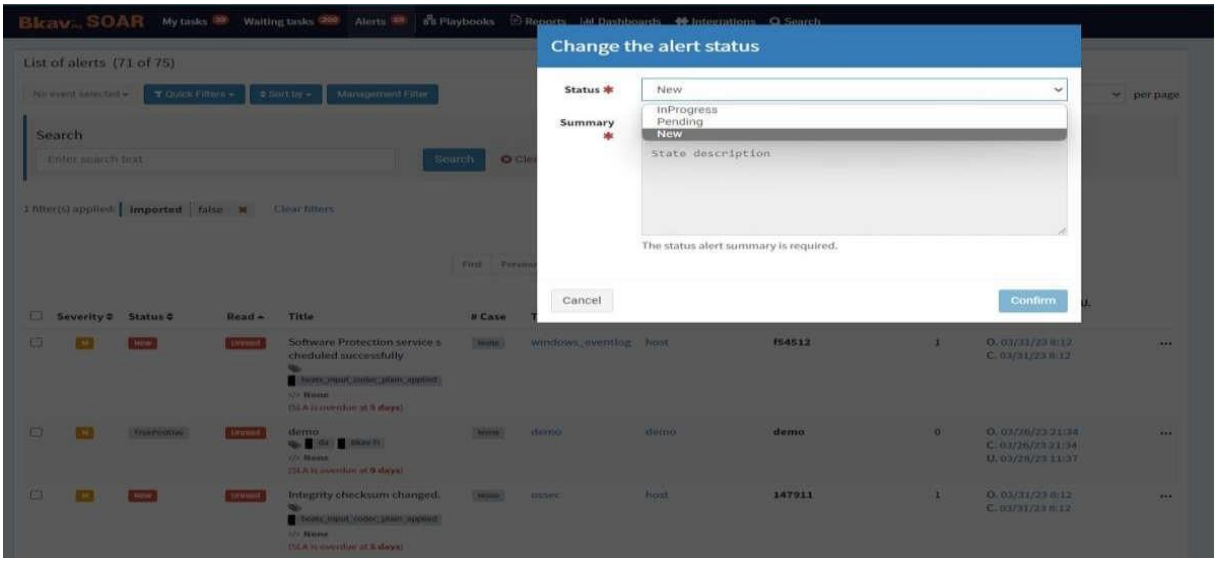


5.1. Điều phối xử lý cảnh báo (tiếp)

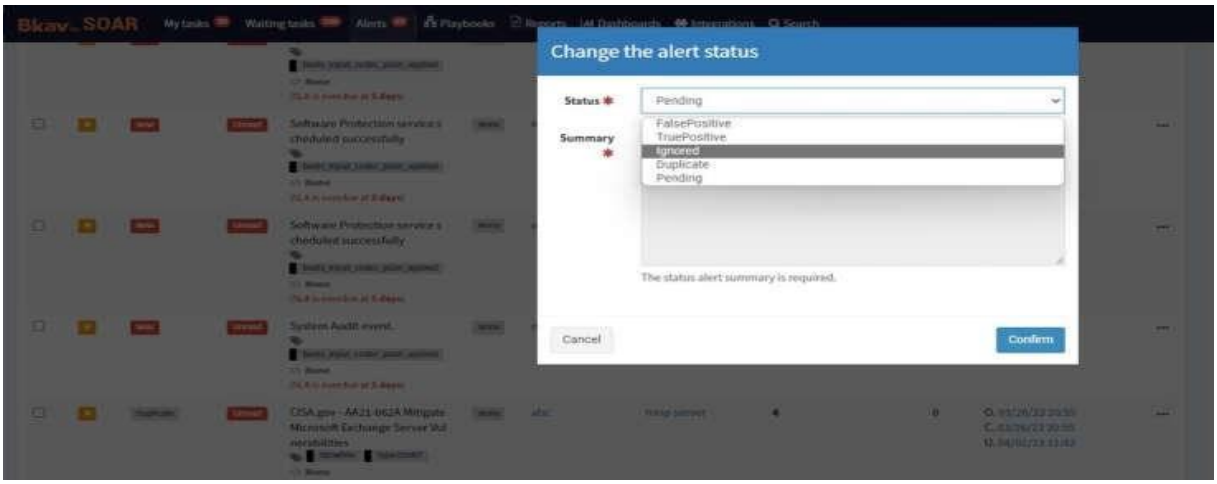
- Cho phép thực hiện xử lý cảnh báo, trong đó bao gồm tối thiểu các thao tác xử lý sau: cập nhật trạng thái xử lý, cập nhật bằng chứng thu thập được, cập nhật kết quả xử lý



- Cho phép cập nhật trạng thái xử lý cảnh báo, trong đó bao gồm tối thiểu các giá trị trạng thái xử lý sau: mới, đang xử lý, đã xửlý

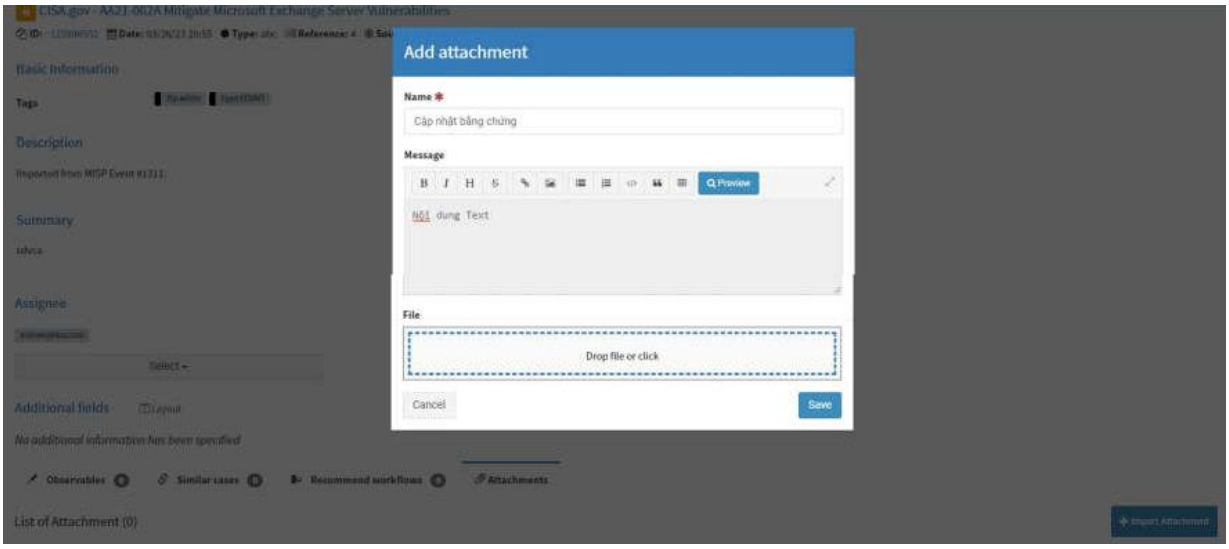


- Cho phép cập nhật kết quả xử lý cảnh báo, trong đó bao gồm tối thiểu các giá trị kết quả xử lý sau: cảnh báo thật, cảnh báo giả

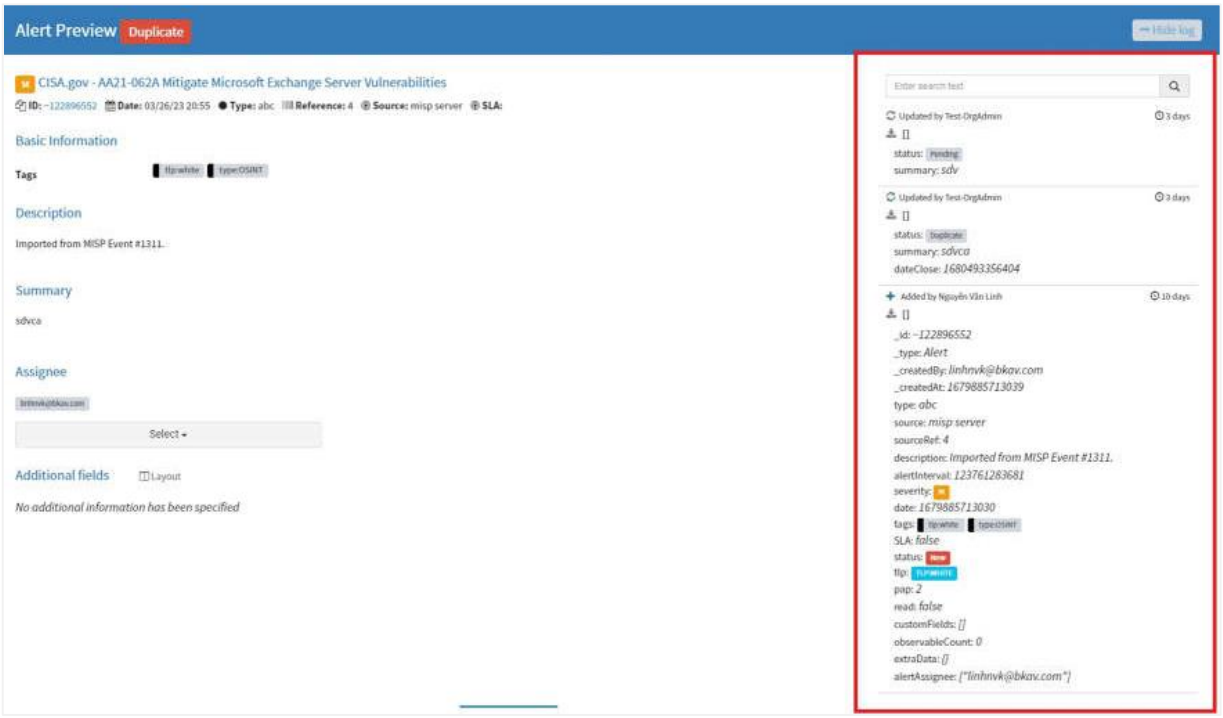


5.1. Điều phối xử lý cảnh báo (tiếp)

- Cho phép cập nhật bằng chứng thu thập được, trong đó bao gồm tối thiểu các thao tác sau: tải lên tệp tin bằng chứng, nhập nội dung text

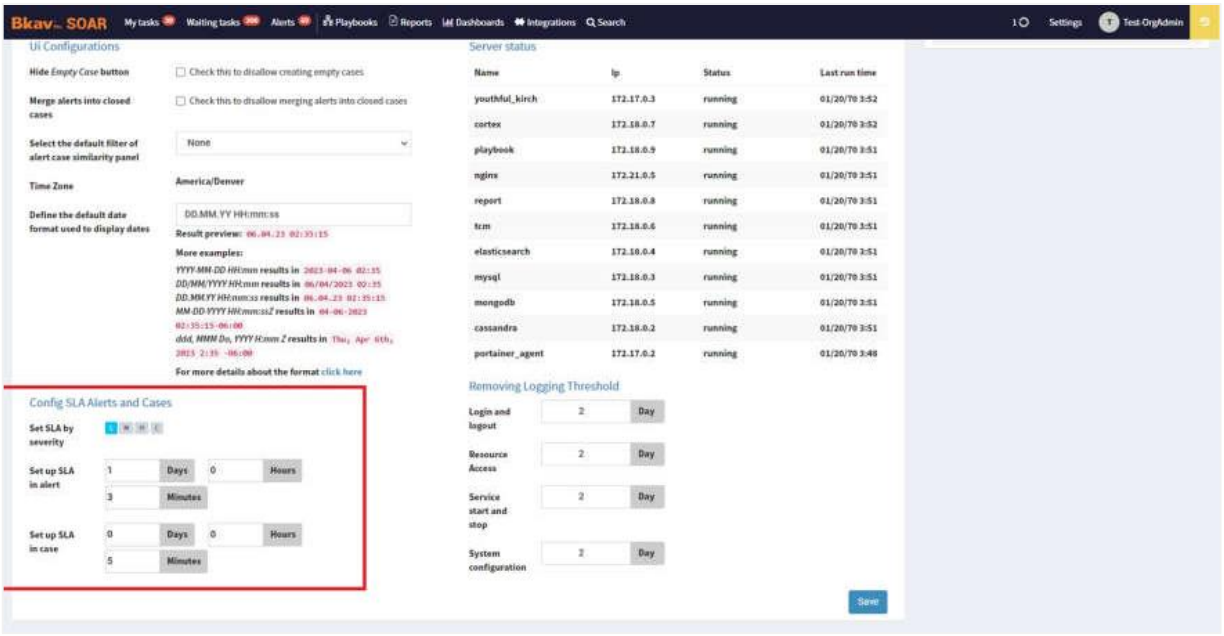


- Cho phép xem lại lịch sử xử lý cảnh báo, trong đó bao gồm tối thiểu các trường thông tin sau: thời điểm thực hiện, người thực hiện, nội dung thực hiện

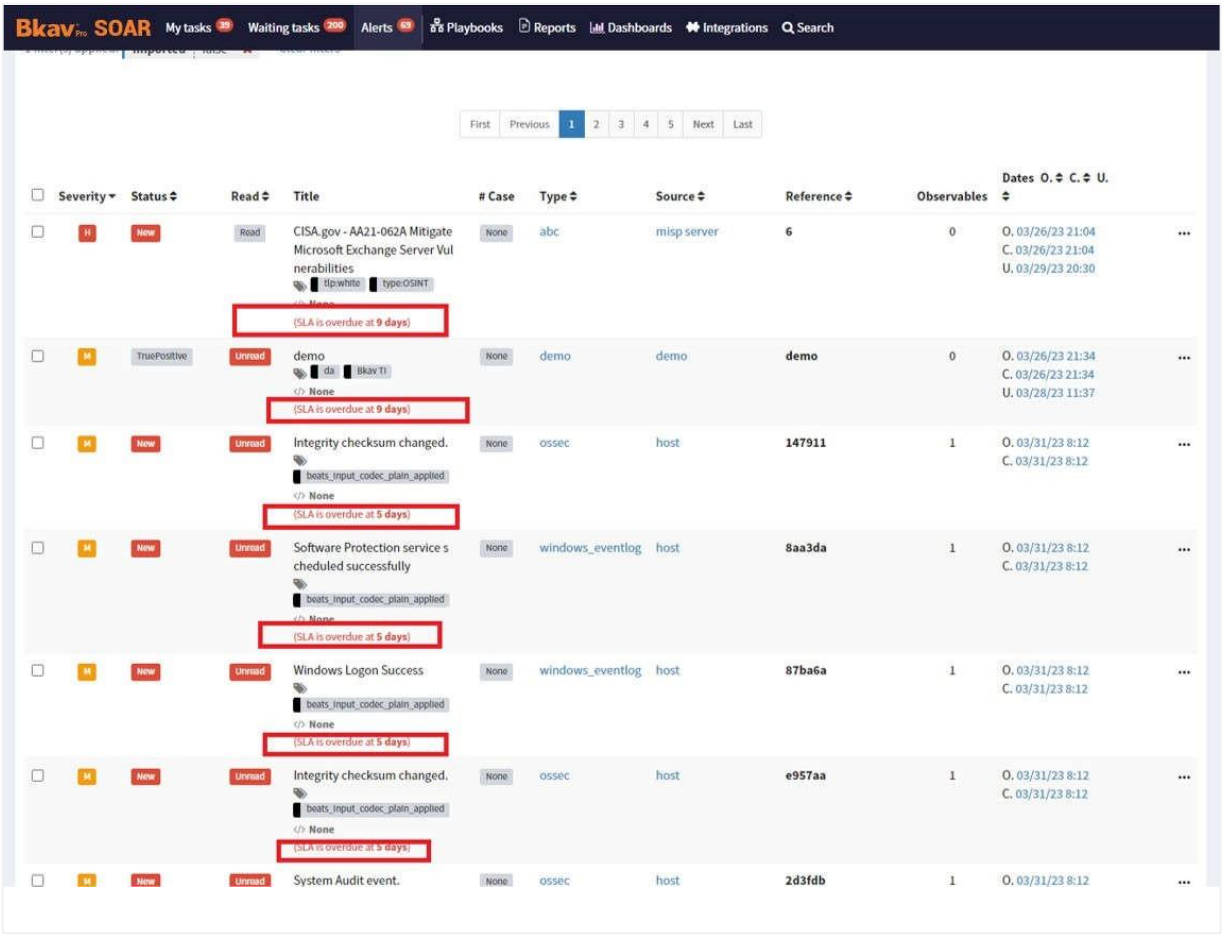


5.1. Điều phối xử lý cảnh báo (tiếp)

- Cho phép thiết lập thời hạn xử lý cảnh báo

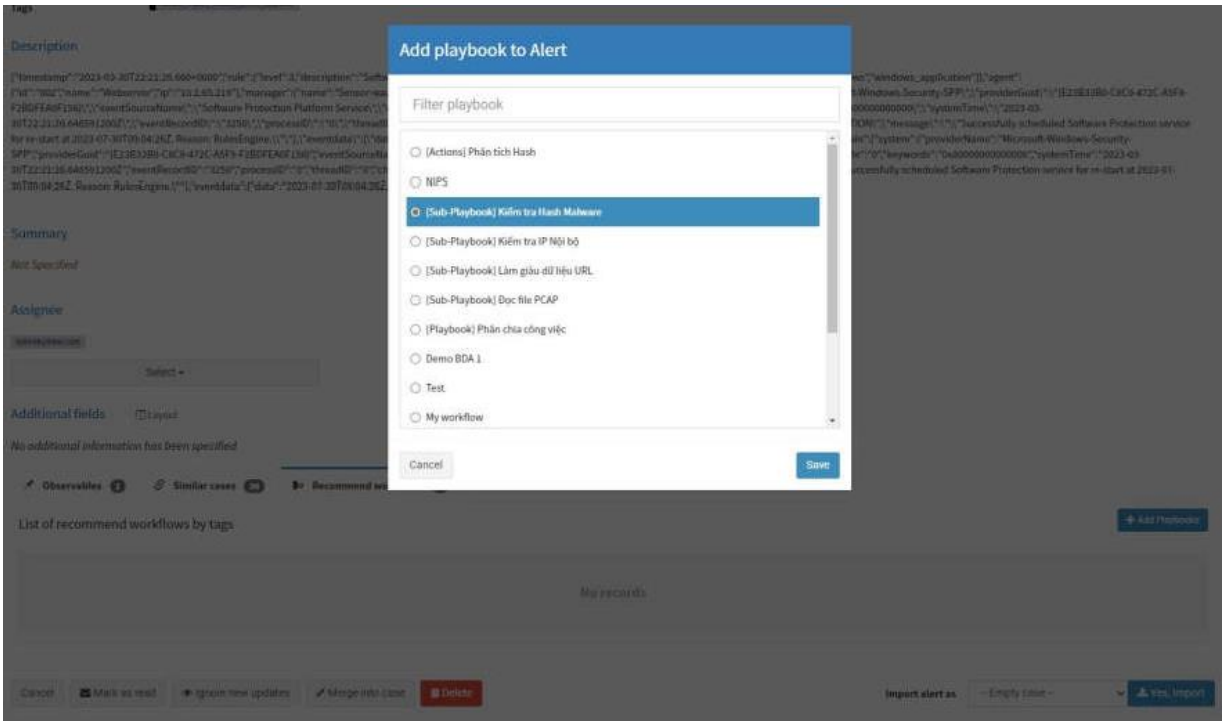


- Cho phép xác định thời gian xử lý cảnh báo có bị quá hạn hay không



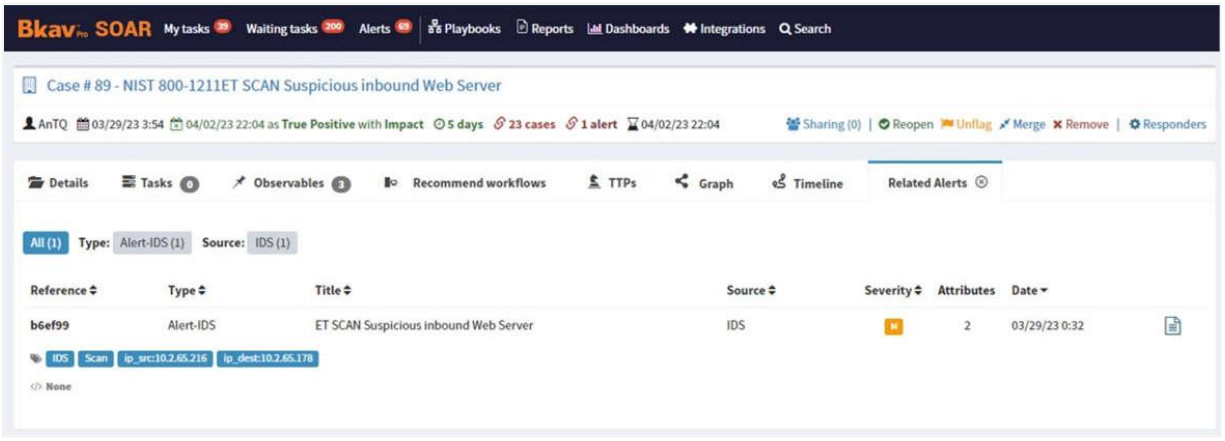
5.1. Điều phối xử lý cảnh báo (tiếp)

- Cho phép áp dụng thực hiện một kịch bản với cảnh báo



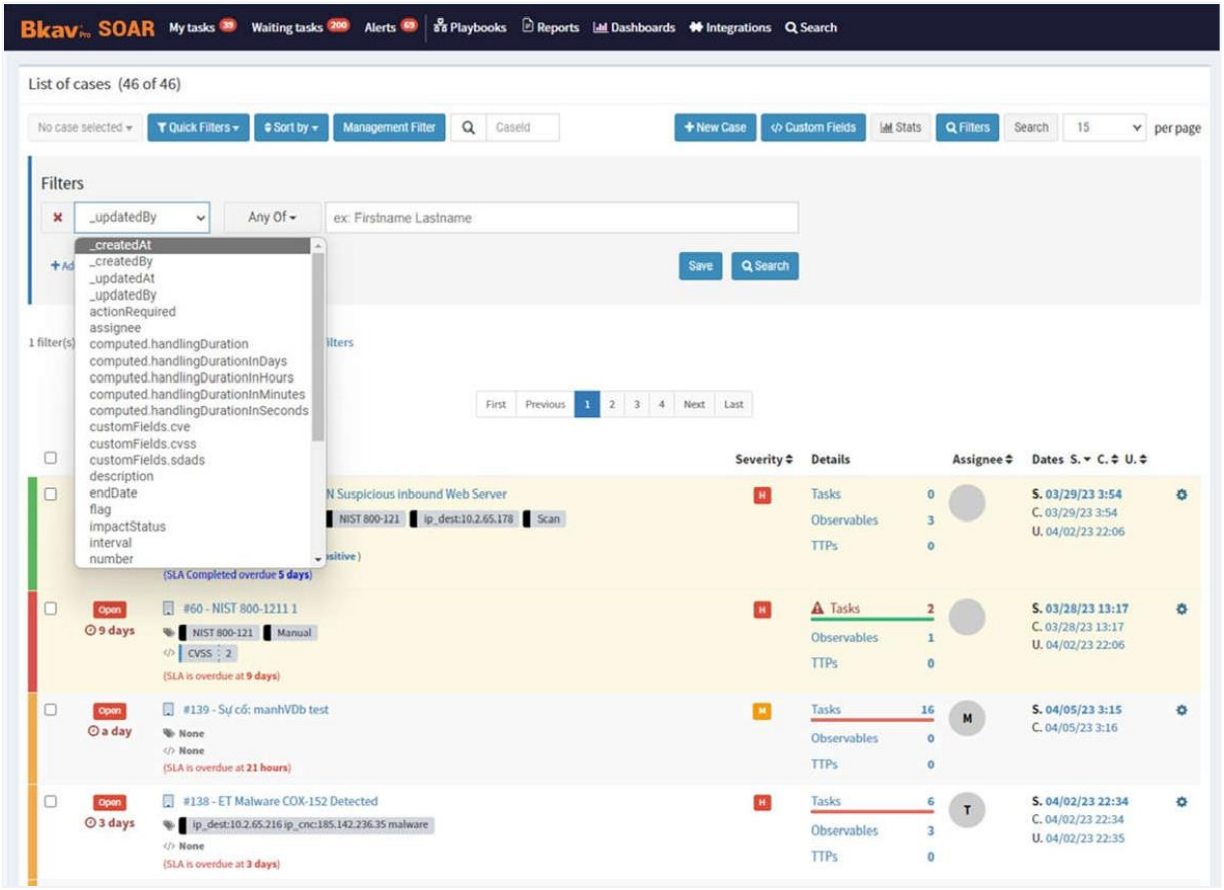
5.2. Điều phối xử lý tình huống

- Cho phép tạo một tình huống bằng việc nhóm một hoặc nhiều cảnh báo thành tình huống đó (ban đầu các tình huống được gán trạng thái là mở)

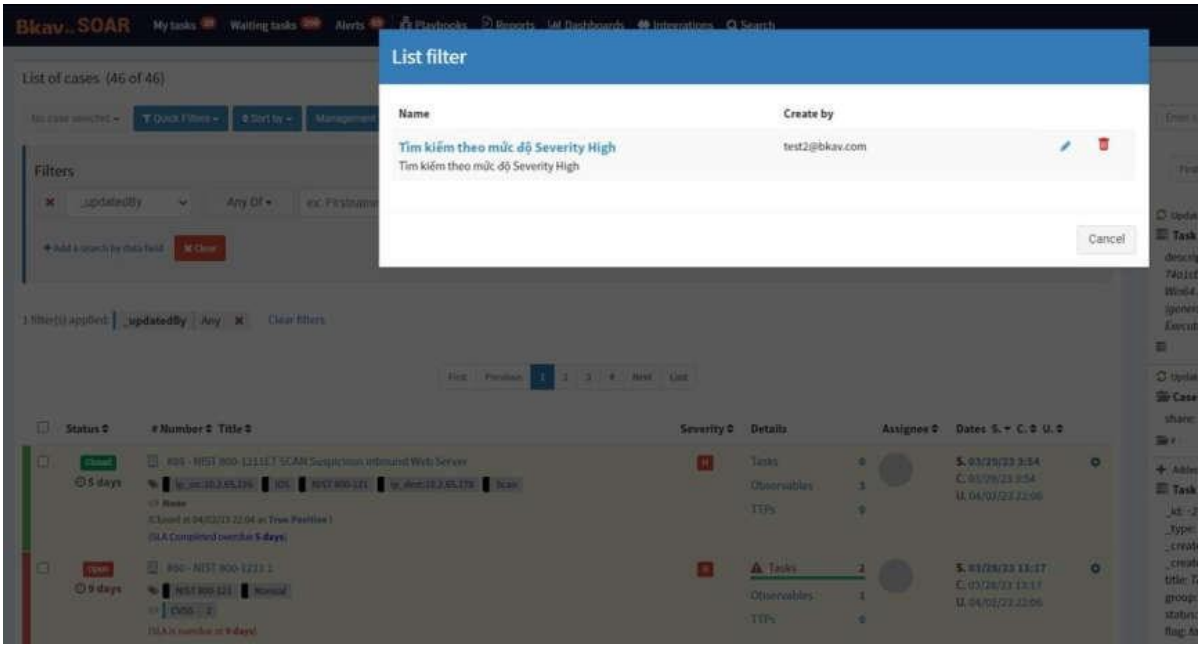


5.2. Điều phối xử lý tình huống (tiếp)

- Cho phép tìm kiếm tình huống theo từ khóa trên tất cả các trường thông tin của tình huống bao gồm cả các trường thông tin cấp thấp hơn (nếu có)

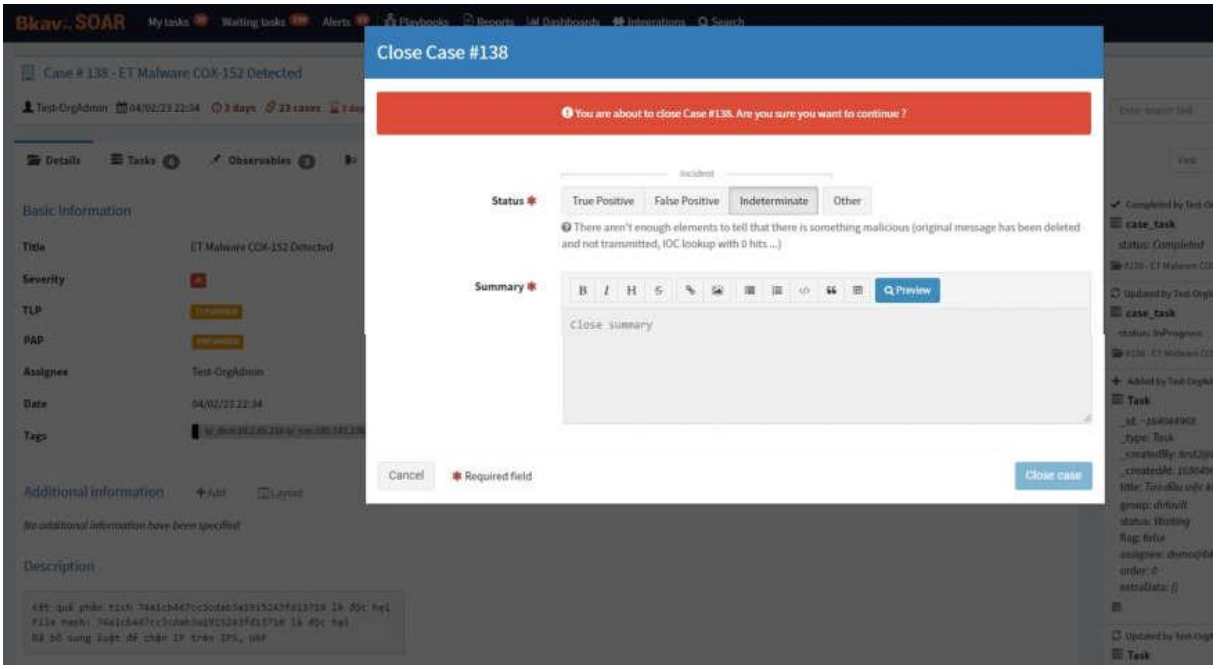


- Cho phép lưu trữ và phân nhóm tình huống theo các tiêu chí khác nhau (ví dụ: mức độ quan trọng của tình huống, nguồn tạo tình huống…)

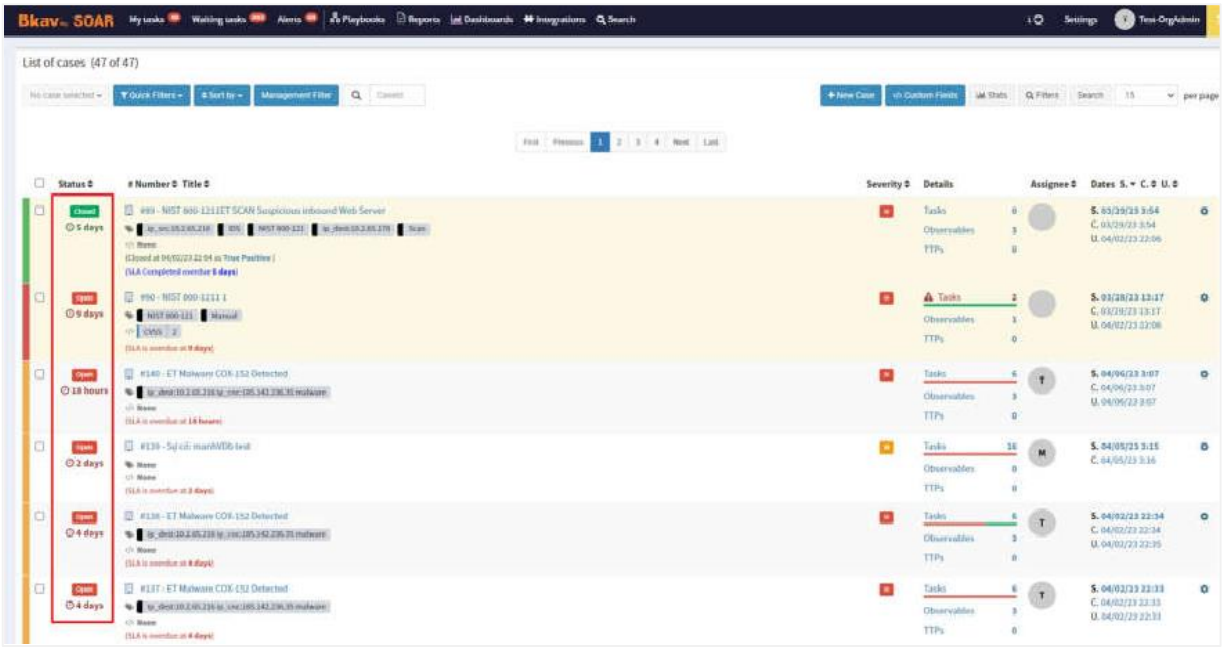


5.2. Điều phối xử lý tình huống (tiếp)

- Cho phép thực hiện xử lý tình huống, trong đó bao gồm tối thiểu các thao tác xử lý sau: cập nhật trạng thái xử lý, cập nhật kết quả xử lý

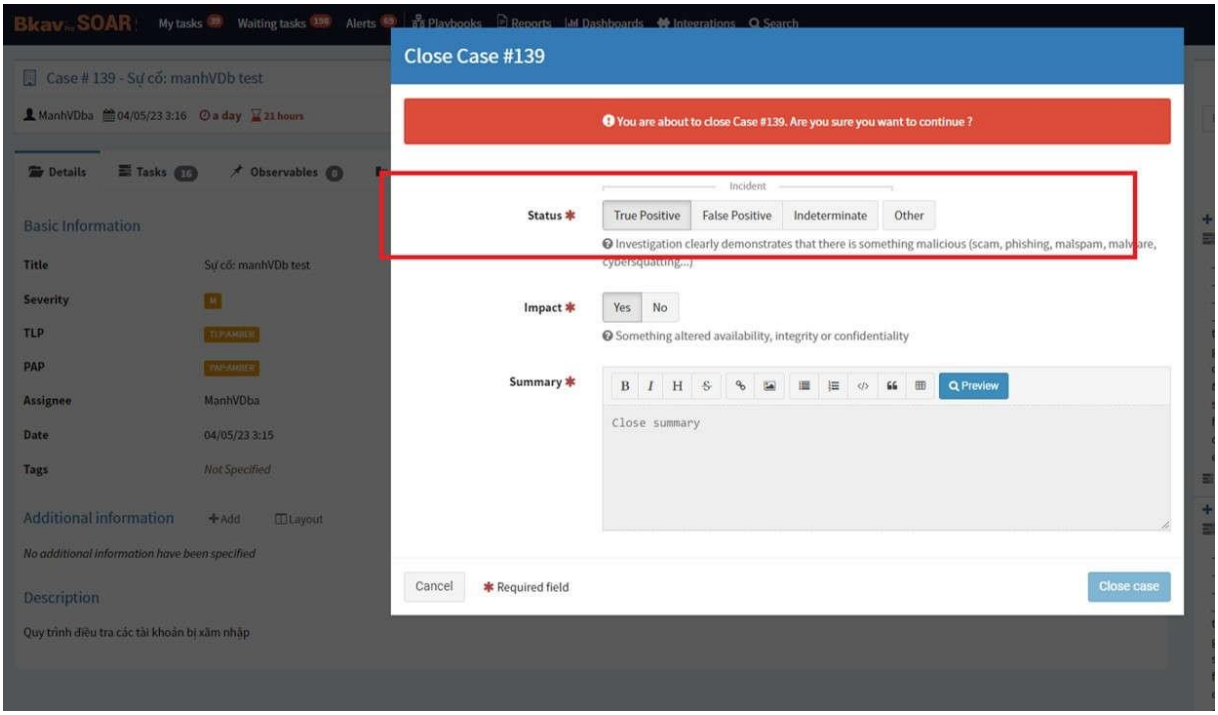


- Cho phép cập nhật trạng thái xử lý tình huống, trong đó bao gồm tối thiểu các giá trị trạng thái xử lý sau: mở, đóng

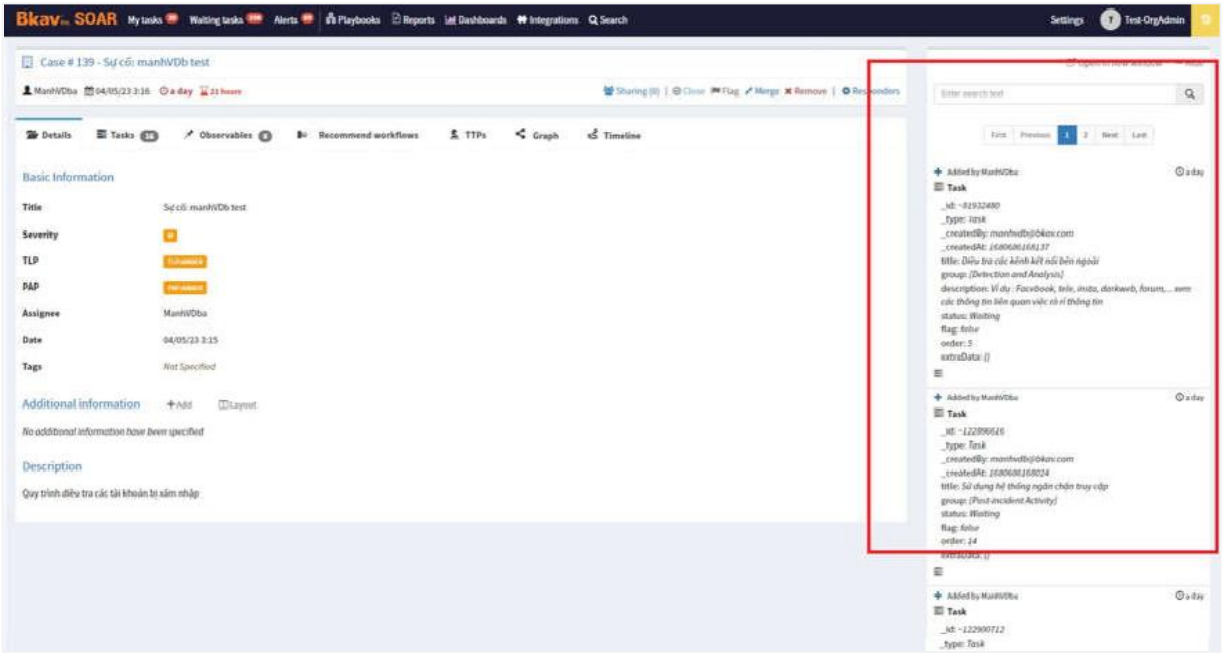


5.2. Điều phối xử lý tình huống (tiếp)

- Cho phép cập nhật kết quả xử lý tình huống, trong đó bao gồm tối thiểu các giá trị kết quả xử lý sau: phát hiện đúng, phát hiện sai

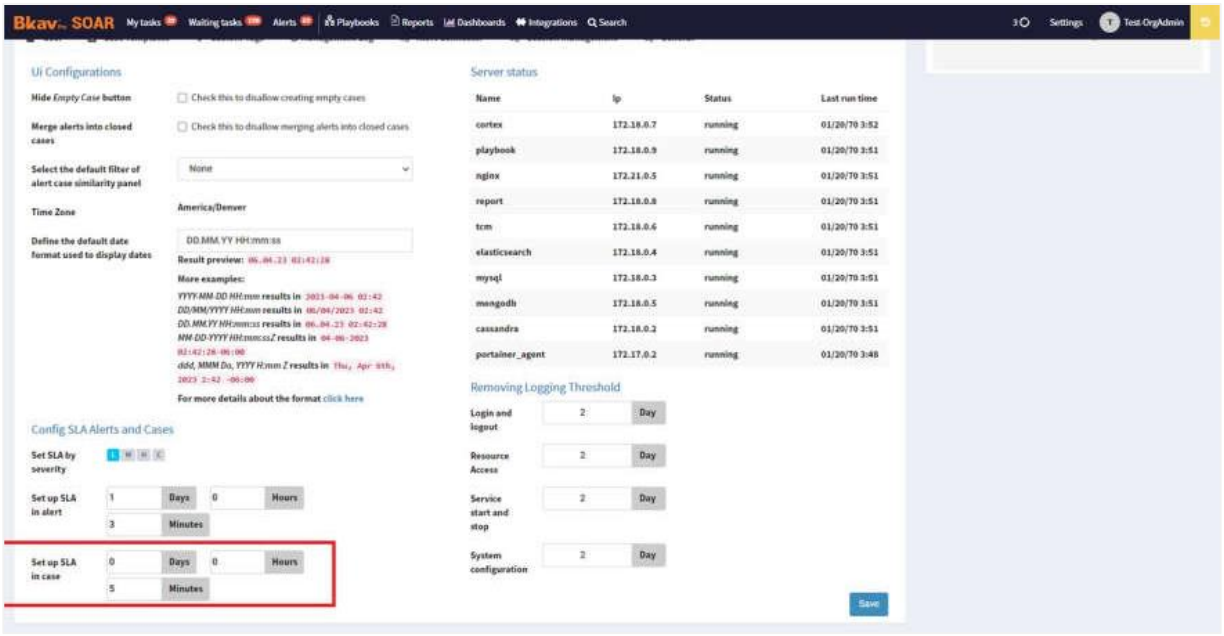


- Cho phép xem lại lịch sử xử lý tình huống, trong đó bao gồm tối thiểu các trường thông tin sau: thời điểm thực hiện, người thực hiện, nội dung thực hiện

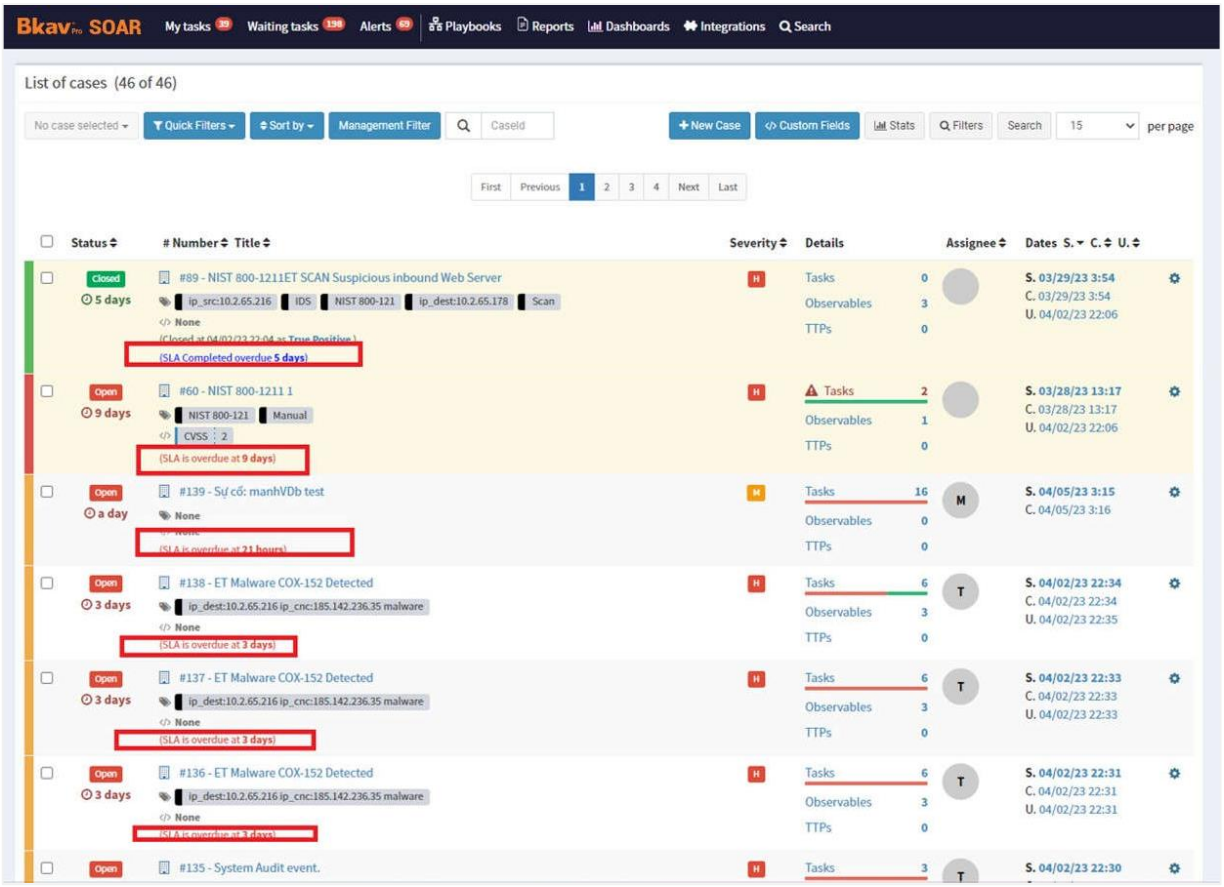


5.2. Điều phối xử lý tình huống (tiếp)

- Cho phép thiết lập thời hạn xử lý tình huống

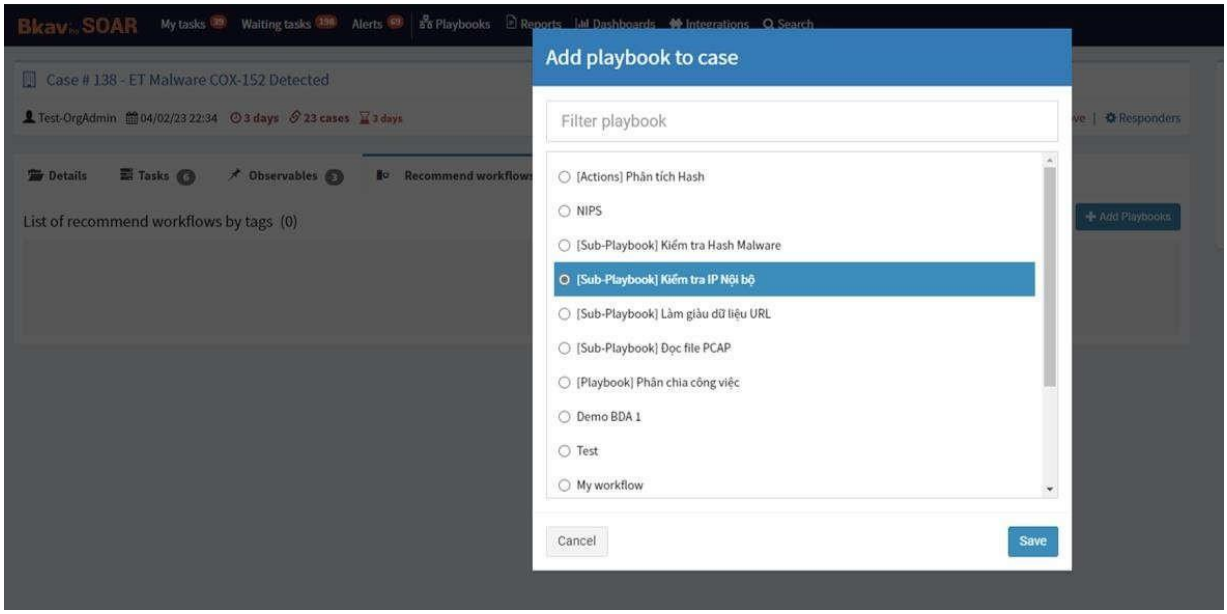


- Cho phép xác định thời gian xử lý tình huống có bị quá hạn hay không

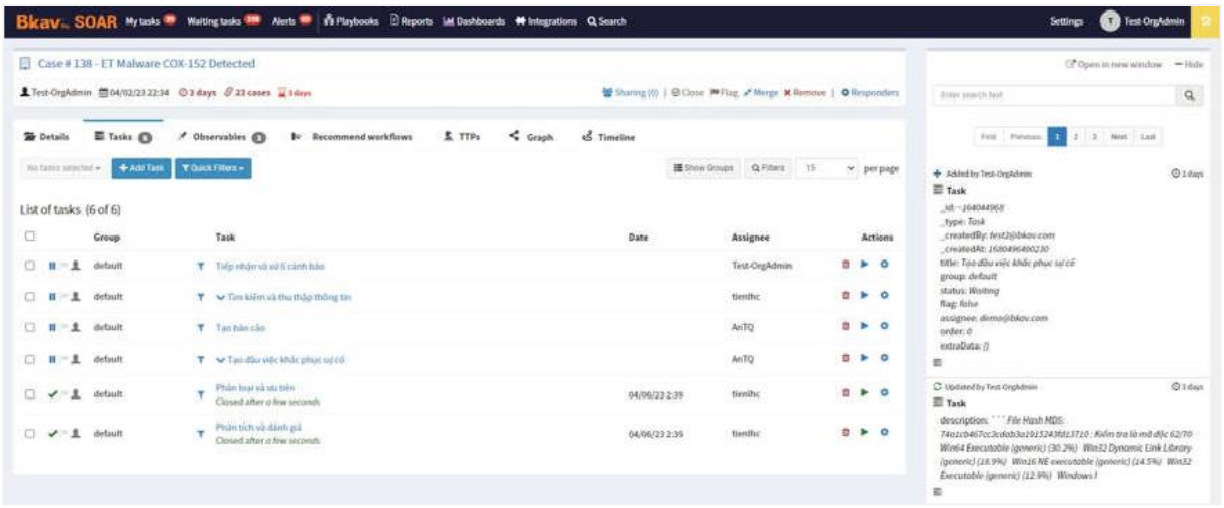


5.2. Điều phối xử lý tình huống (tiếp)

- Cho phép áp dụng thực hiện một kịch bản với tình huống

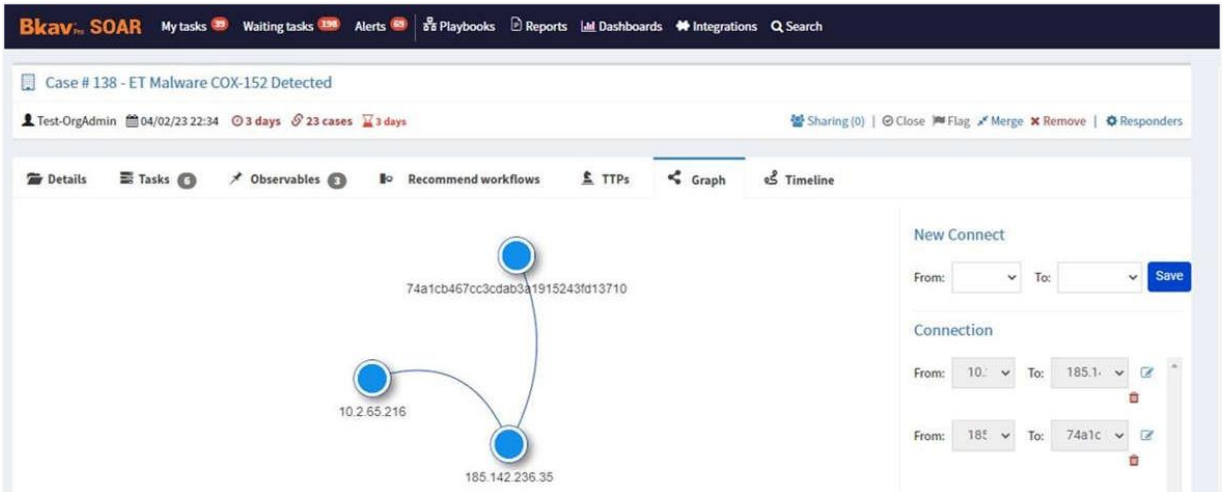


- Cho phép gán một hoặc nhiều người xử lý cho tình huống



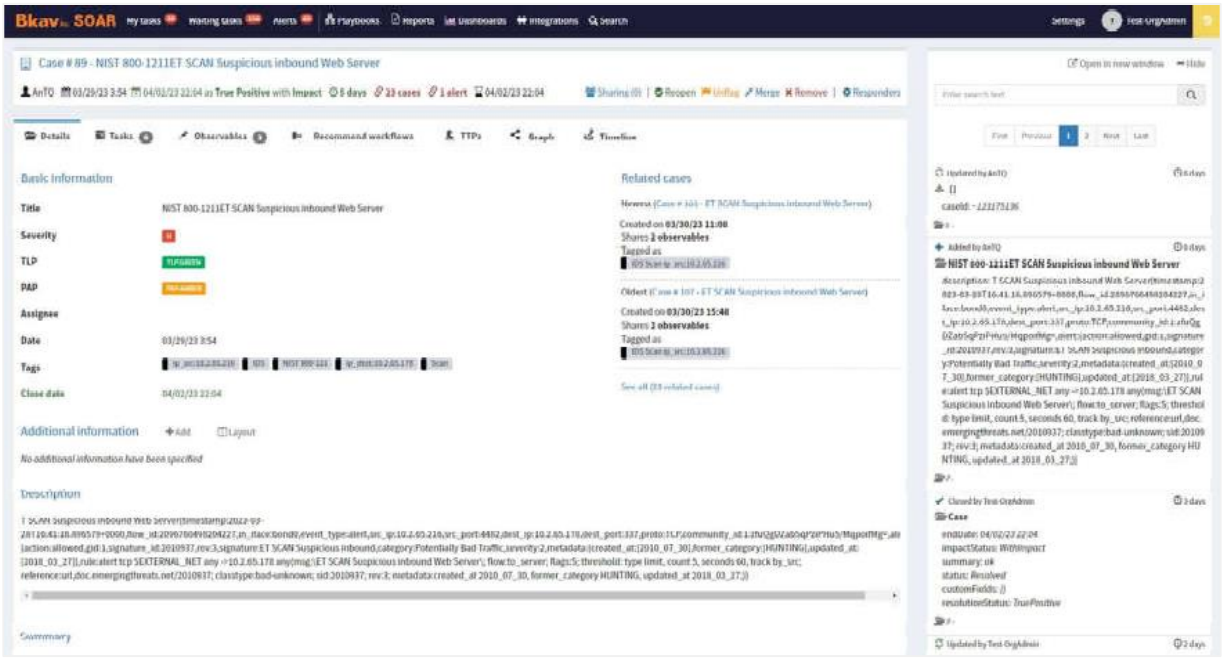
5.3. Giám sát và phân tích sự cố an toàn thông tin

- Cho phép hiển thị thông tin trực quan thể hiện mối liên kết giữa các đối tượng liên quan trong sự cố bằng đường đi và kèm thông tin của liên kết (nếu có), trong đó bao gồm tối thiểu các đối tượng sau: địa chỉ IP, địa chỉ email, tên miền



5.3. Giám sát và phân tích sự cố an toàn thông tin (tiếp)

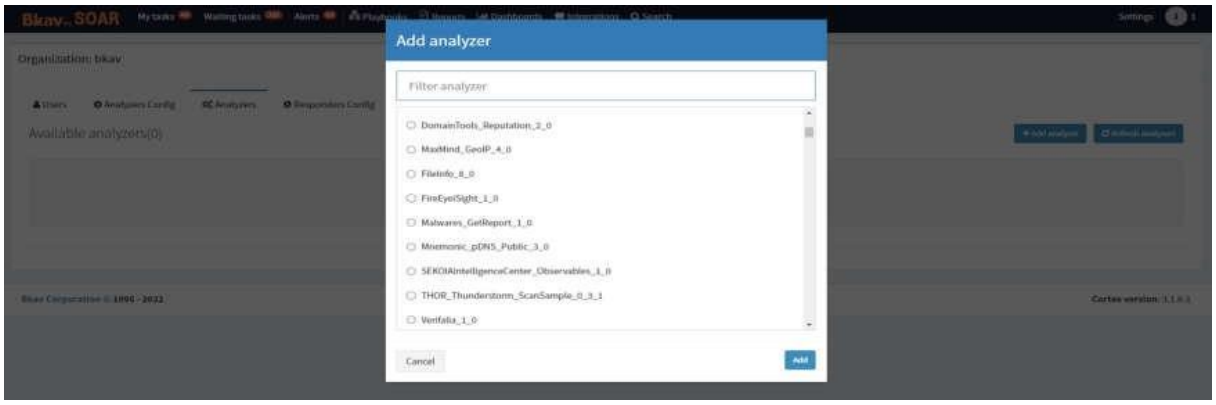
- Cho phép xem dòng thời gian của các sự kiện trong sự cố, trong đó bao gồm tối thiểu các trường thông tin sau: thời điểm xuất hiện, nội dung, các đối tượng có liên quan (nếu có), các bằng chứng thu thập được (nếu có)

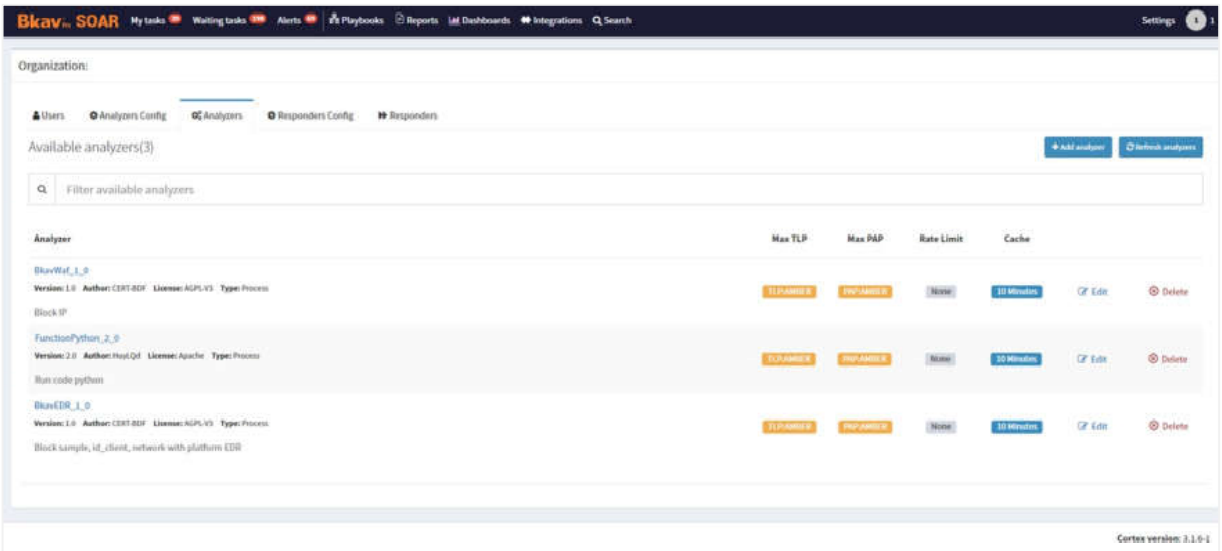


6. Chức năng tích hợp và tự động hóa

1. Quản lý thành phần tích hợp

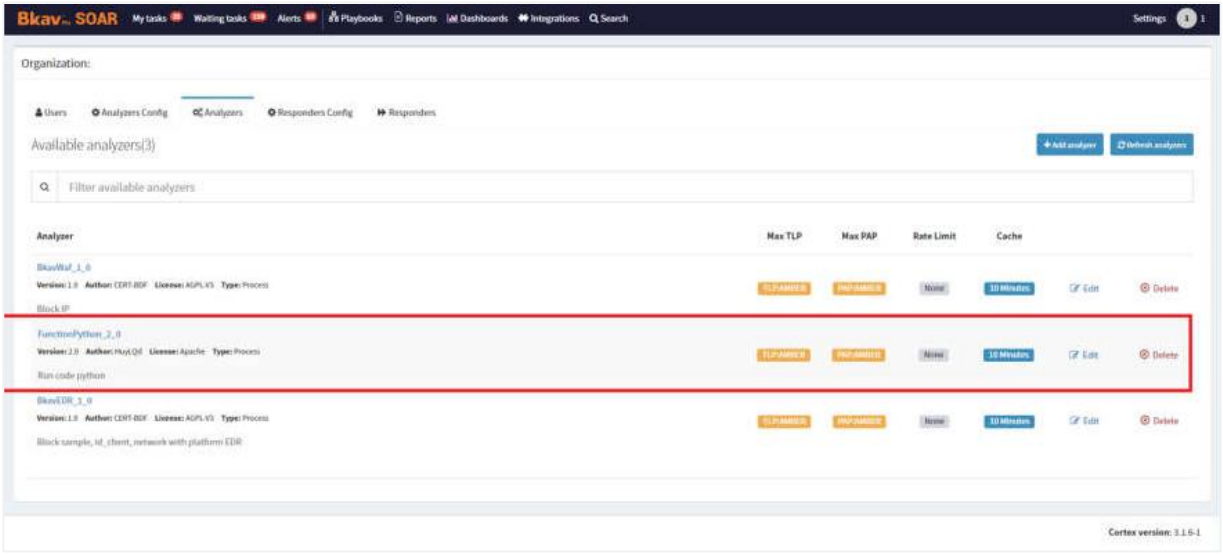
- Cho phép tạo mới, xem lại, cập nhật và xóa thành phần tích hợp đã được tạo





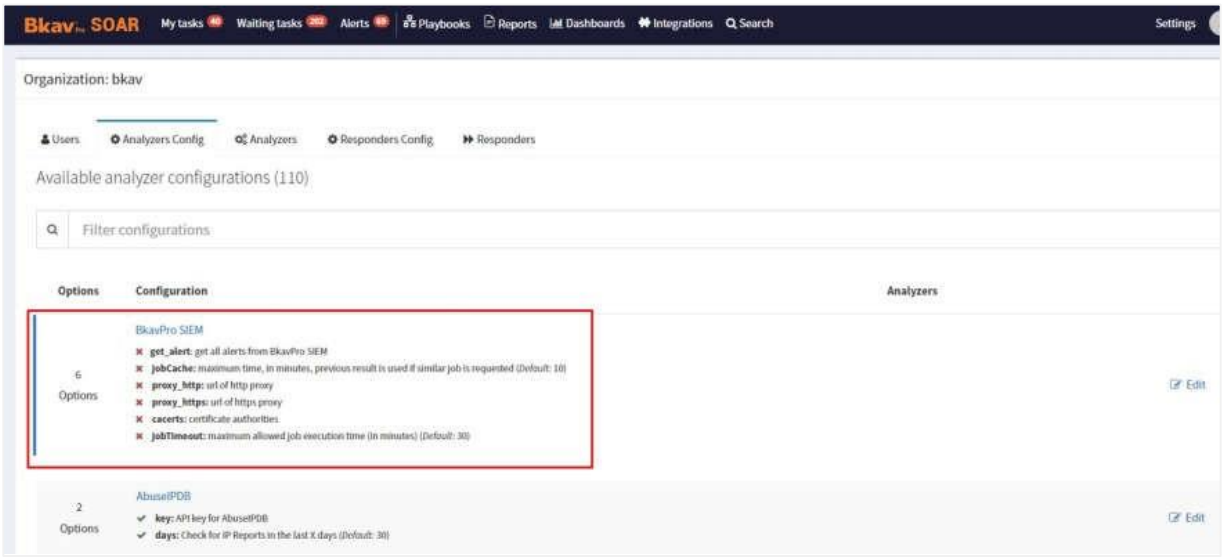
6.1. Quản lý thành phần tích hợp (tiếp)

- Cho phép phát triển thành phần tích hợp thông qua tối thiểu 01 ngôn ngữ lập trình dạng thông dịch (ví dụ: Python, Javascript…)

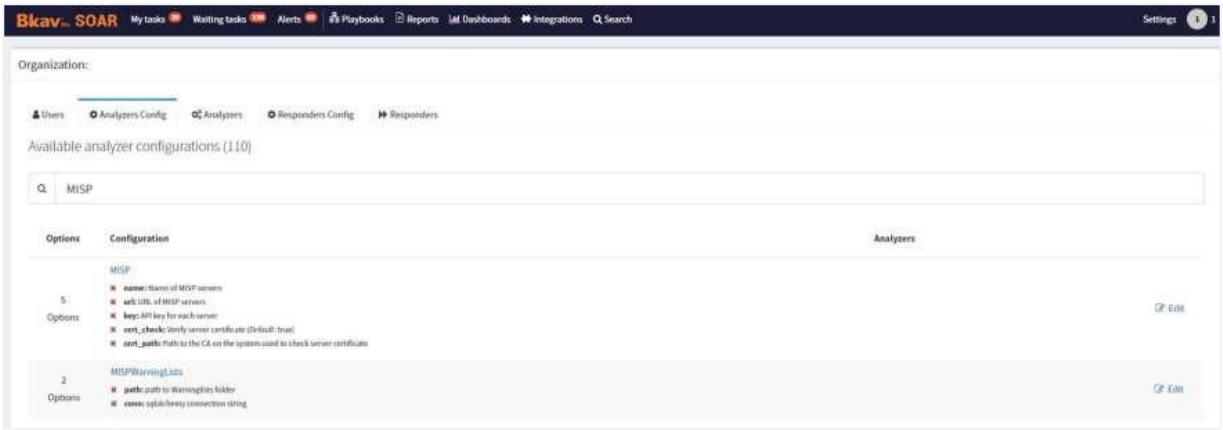


6.2. Hỗ trợ tích hợp nhiều nền tảng khác nhau

- Security Information and Event Management (SIEM) -Quản lý và phân tích sự kiện an toàn thông tin

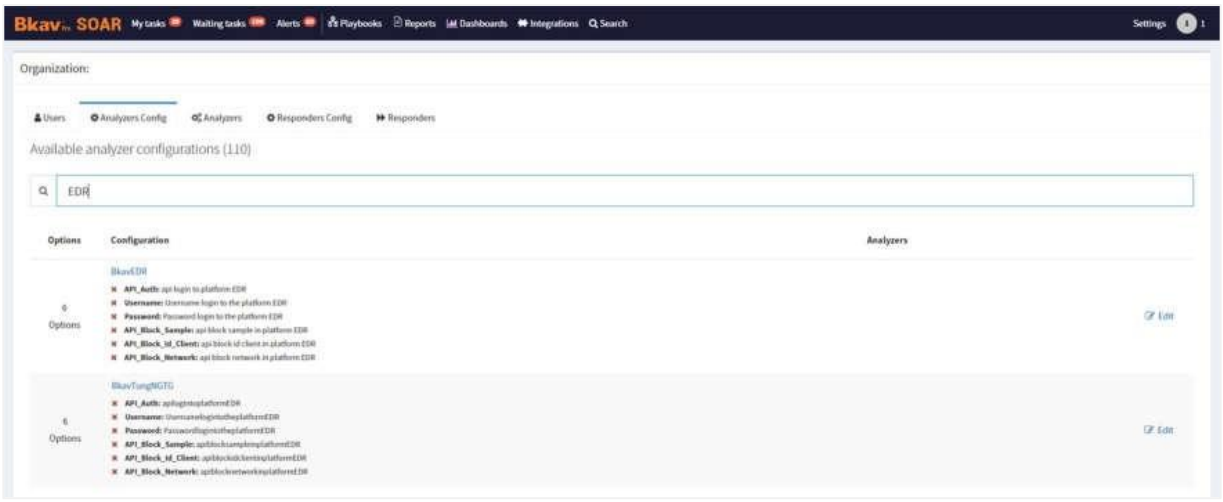


- Threat Intelligence Platform (TIP) -Nền tảng tri thức mối đe dọa an toàn thông tin

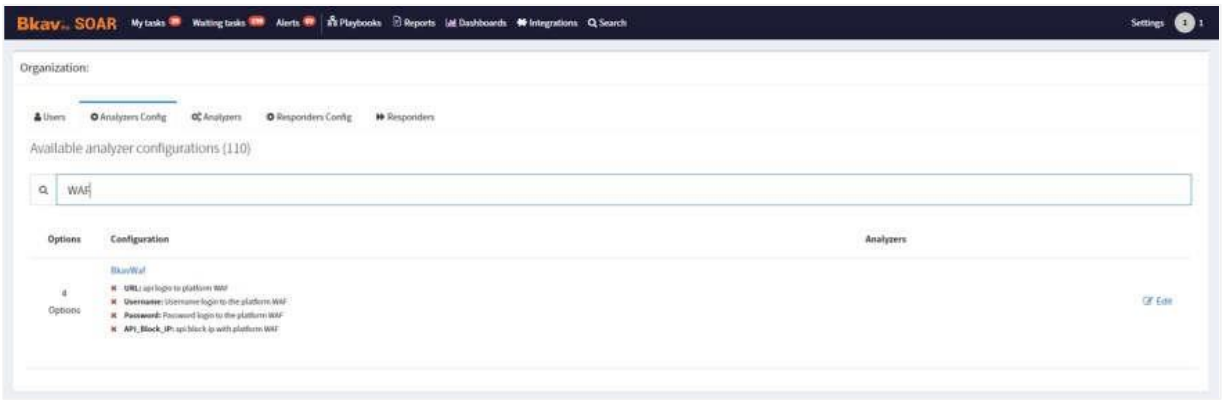


6.2. Hỗ trợ tích hợp nhiều nền tảng khác nhau (tiếp)

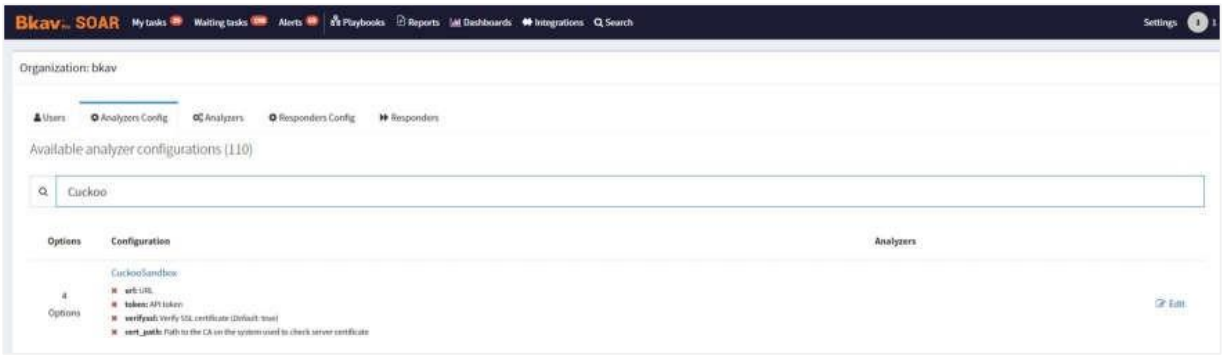
- Endpoint Security - Đảm bảo an toàn thông tin cho thiết bị đầu cuối (ví dụ: Endpoint Detection and Response (EDR) - Phát hiện và ứng phó các mối đe dọa an toàn thông tin tại thiết bị đầu cuối; Endpoint Protection Platform (EPP)- Nền tảng bảo vệ thiết bị đầu cuối…)



- Network Security - Đảm bảo an toàn thông tin mạng (ví dụ: Network-based Intrusion Prevention System (NIPS) - Phòng, chống xâm nhập lớp mạng; Web Application Firewall (WAF) - Tường lửa ứng dụng web…)

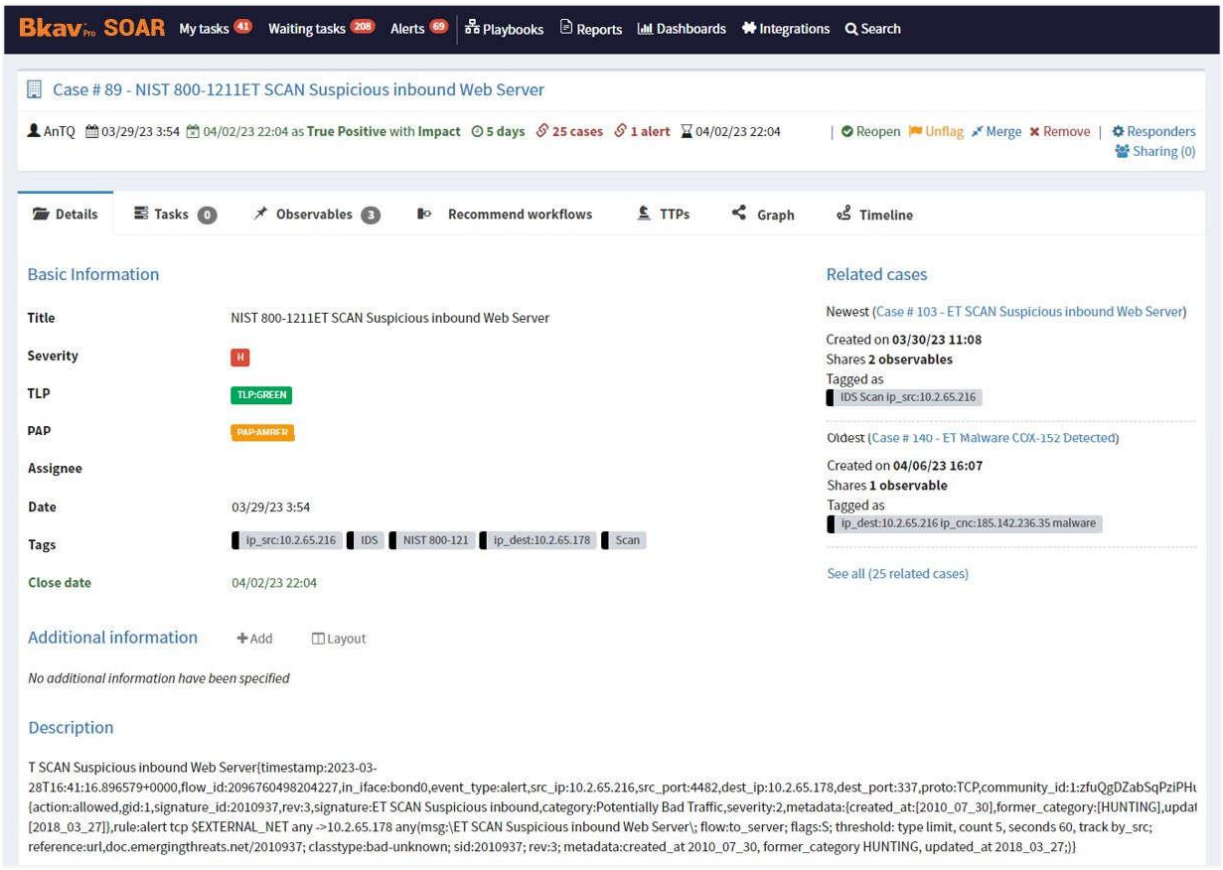


- Malware Analysis -Phân tích mã độc



6.2. Hỗ trợ tích hợp nhiều nền tảng khác nhau (tiếp)

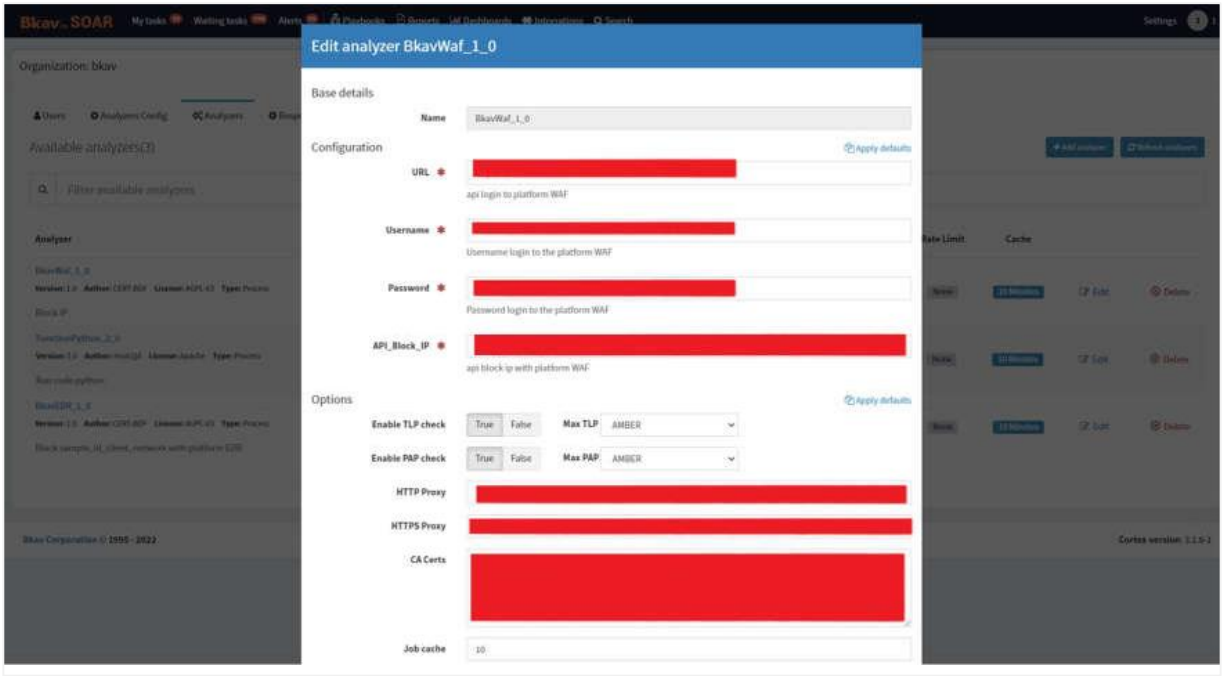
- Ticketing System -Quản lý các yêu cầu cần giải quyết: Hệ thống đã tích hợp hệ thống Ticket trong phần Case và Alert



- Identity and Access Management (IAM) -Quản lý định danh và truy cập: Hệ thống đã tích hợp sẵn trong nền tảng chạy hệ thống SOAR

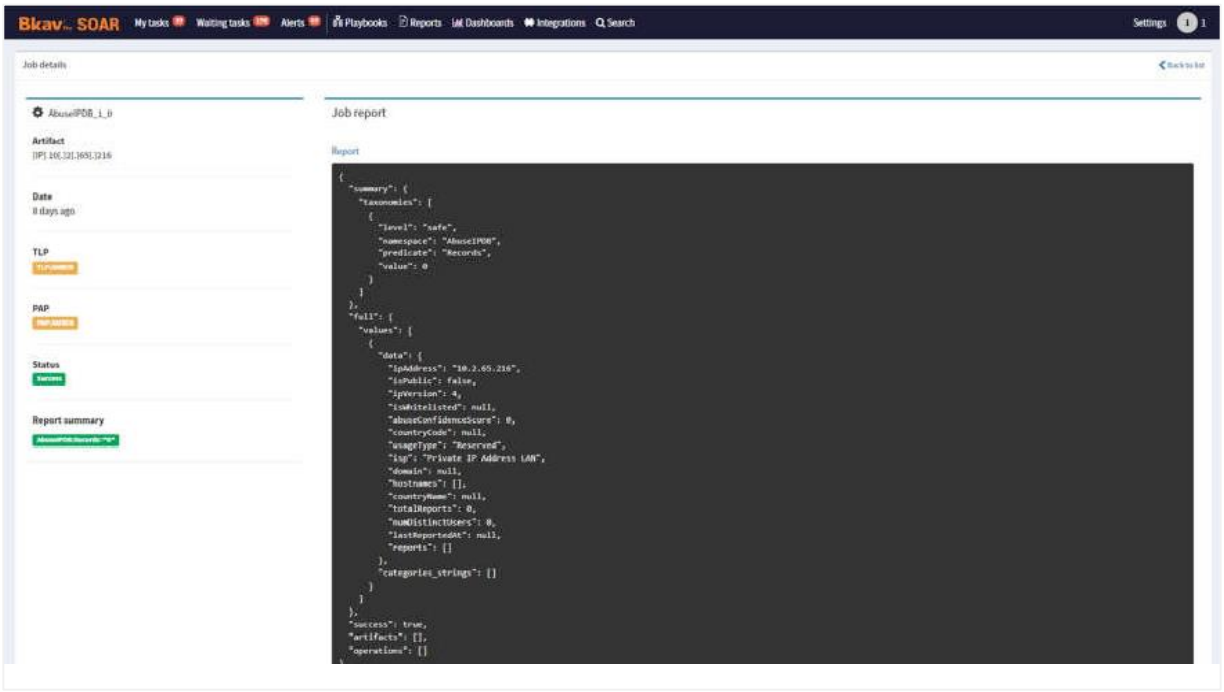
6.3. Hỗ trợ tích hợp nhiều API

- BkavPro SOAR đã thực hiện thành công thiết lập cấu hình một hoặc nhiều API trên các thành phần tích hợp để ứng dụng nhiều nhất có thể các chức năng, tính năng mà nền tảng tích hợp cung cấp

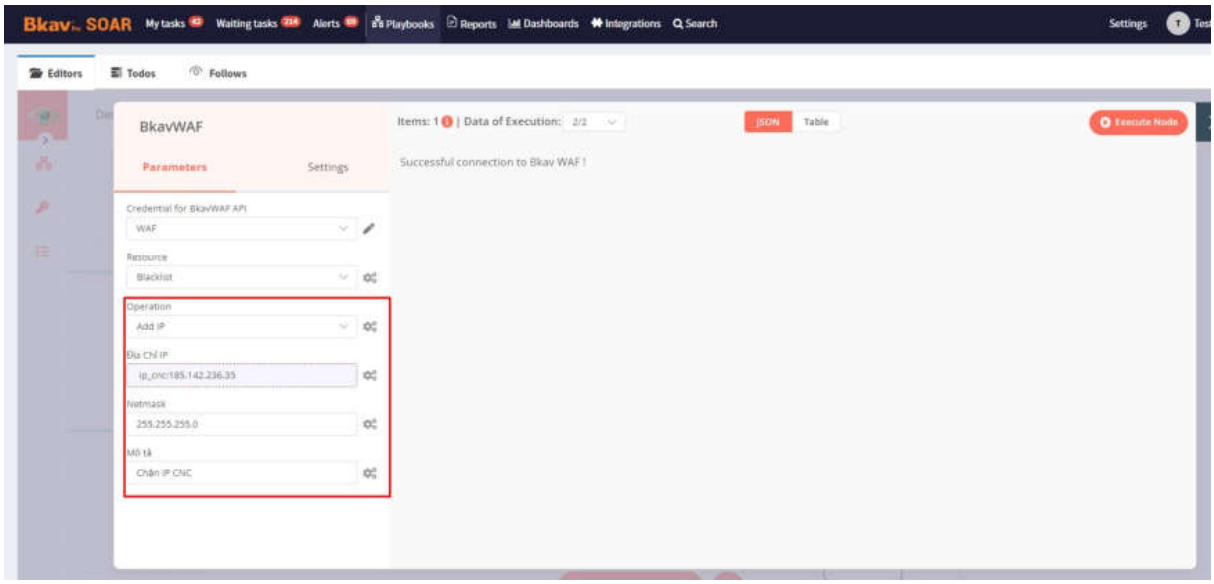


6.4. Hỗ trợ tích hợp API theo hai chiều

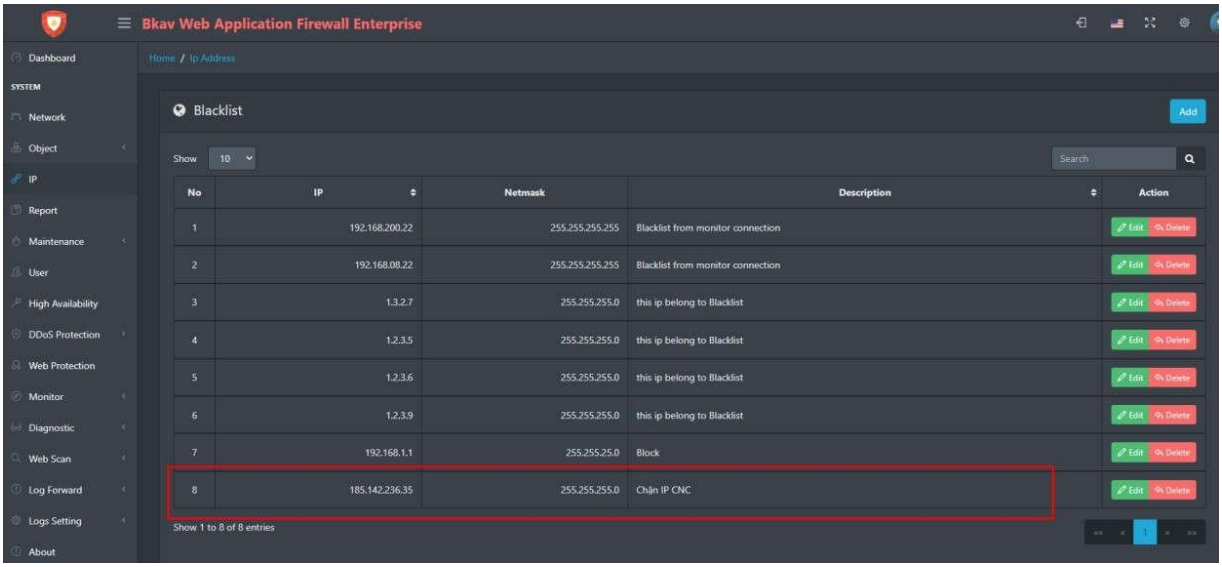
- BkavPro SOAR đã thực hiện thành công truy vấn dữ liệu từ nền tảng tích hợp để làm giàu thông tin cho các dữ liệu được xử lý và lưu trữ trên SOAR



- BkavPro SOAR đã thực thi lệnh tác động đến nền tảng tích hợp để thực hiện việc ứng phó sự kiện, cố an toàn thông tin



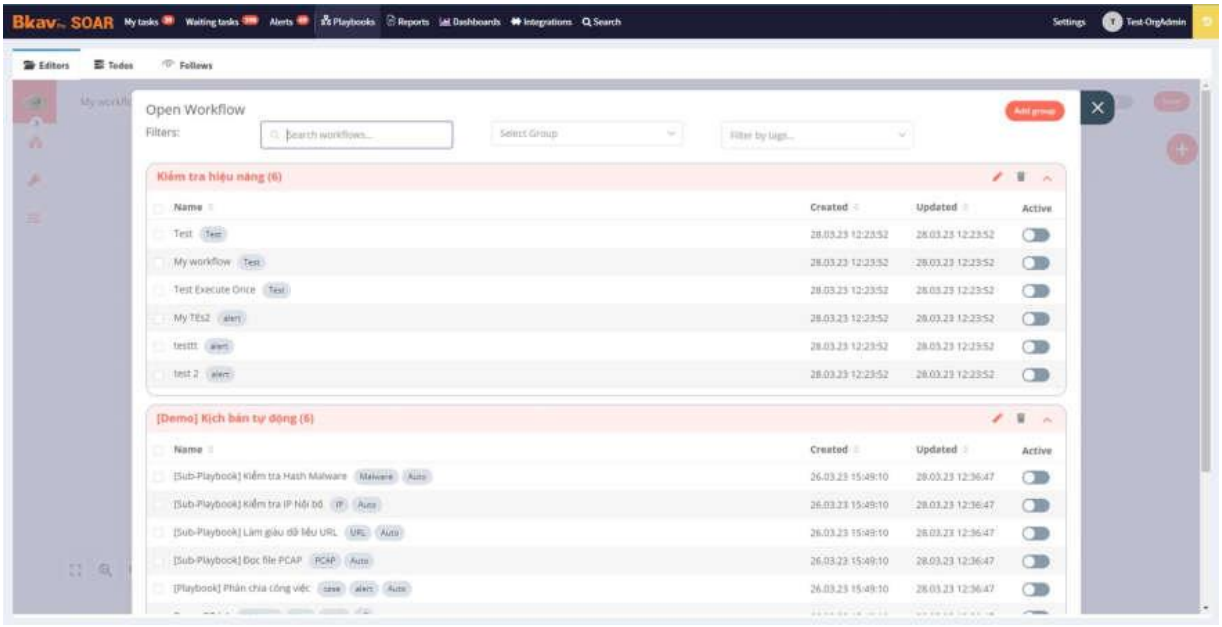
(Thực thi kết nối đến sản phẩm Bkav WAF và truyền nội dung thông tin)



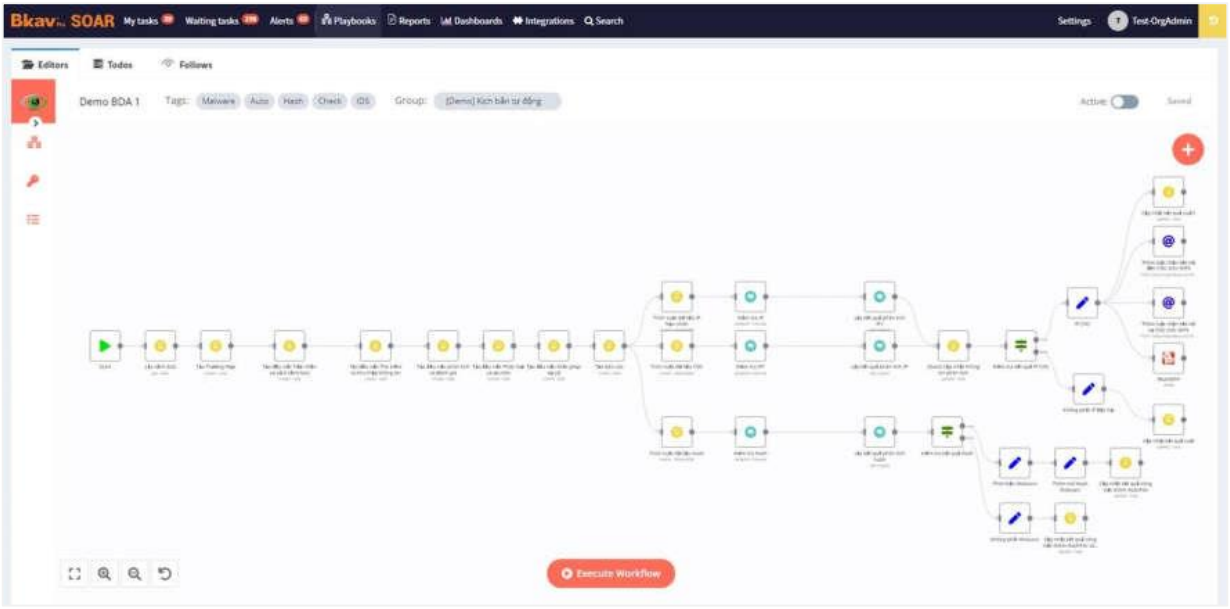
(Kết nối và truyền tự động dữ liệu từ BkavPro SOAR truyền sang BWAF)

6.5. Quản lý kịch bản

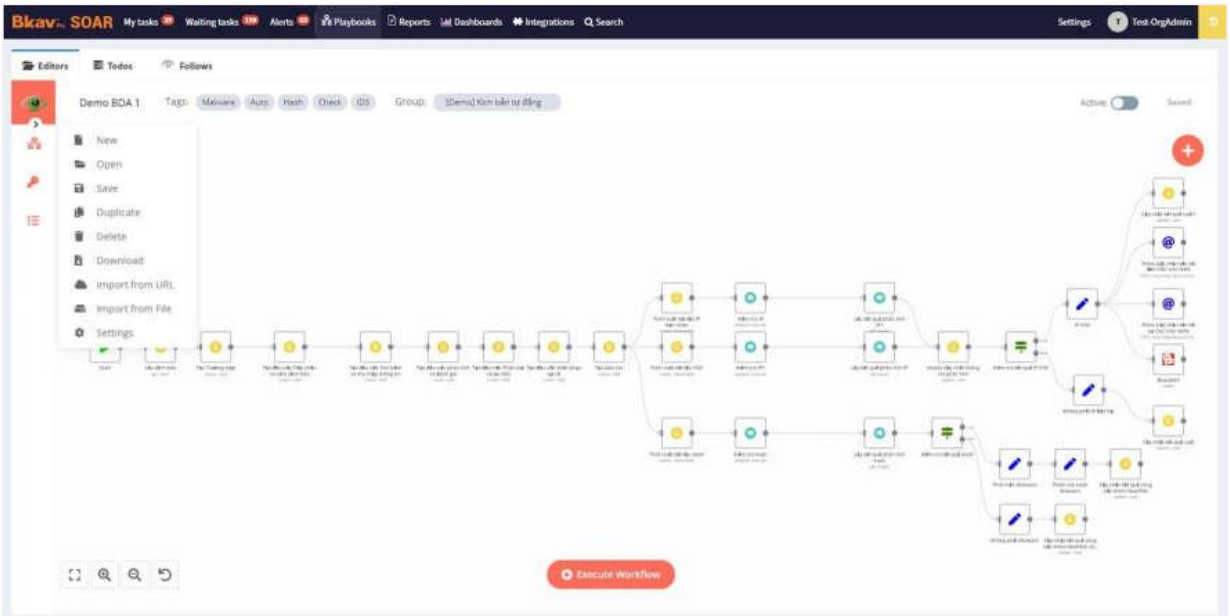
- Cho phép tạo mới, xem lại, cập nhật và xóa kịch bản đã đượctạo



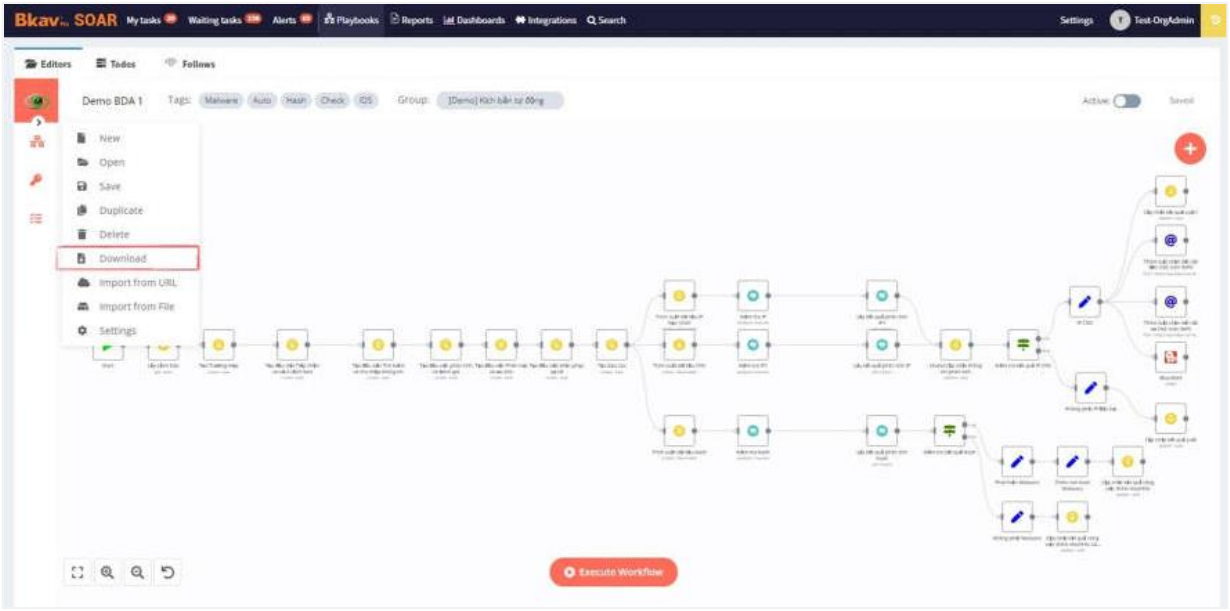
- Cho phép xây dựng kịch bản với tối thiểu các thành phần sau: khối thực thi, đường đi giữa các khối, điều kiện rẽ nhánh



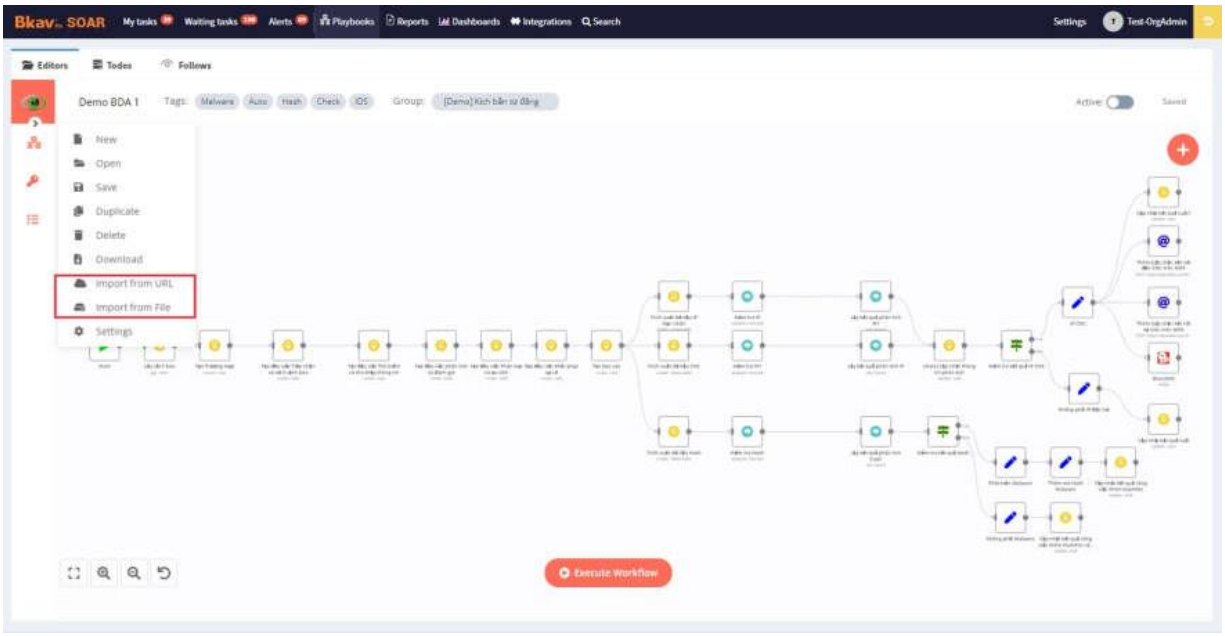
- BkavPro đã thực hiện thành công việc xây dựng kịch bản thông qua tối thiểu các thao tác sau để tương tác với loại thành phần trên: tạo mới, xem lại, cập nhật, xóa



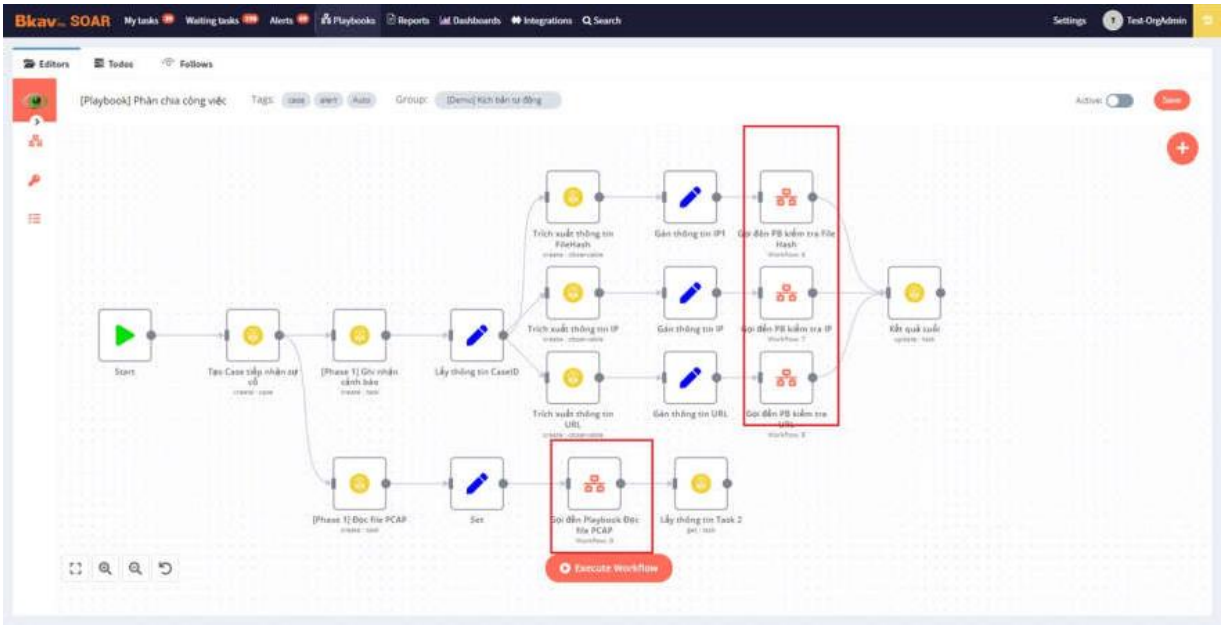
- Cho phép xuất một kịch bản ra tệp tin và tải về tệp tin đãxuất



- Cho phép tải lên tệp tin chứa một kịch bản và nhập kịch bản từ tệp tin đó

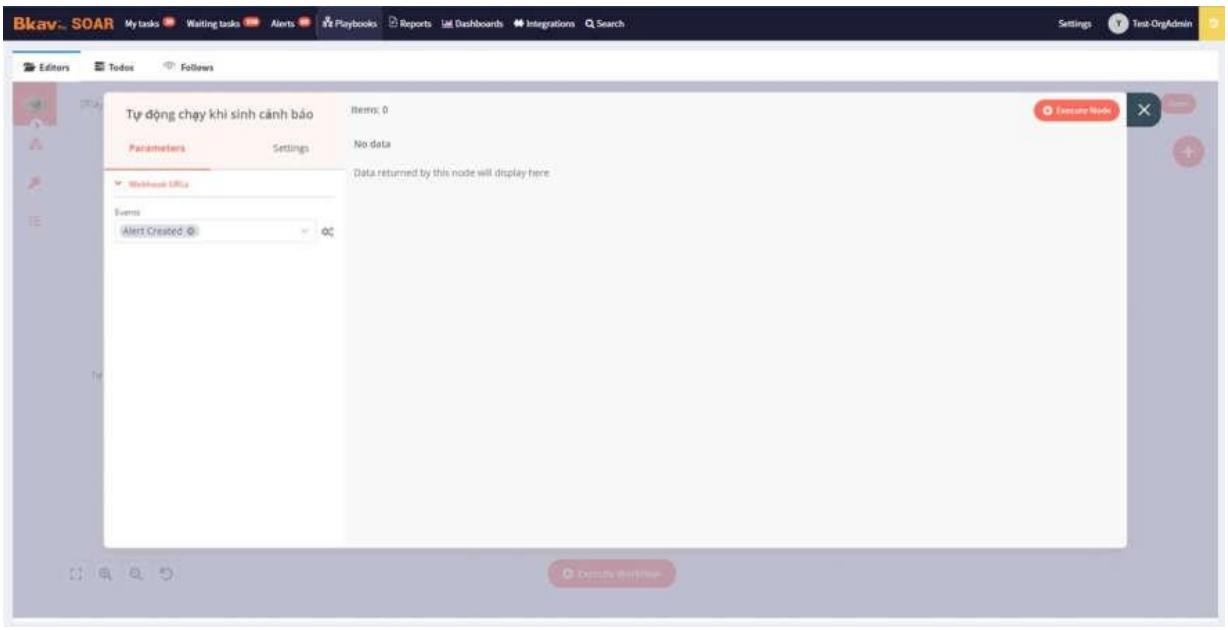


- Cho phép đưa một kịch bản đã được xây dựng trước đó vào một kịchbản

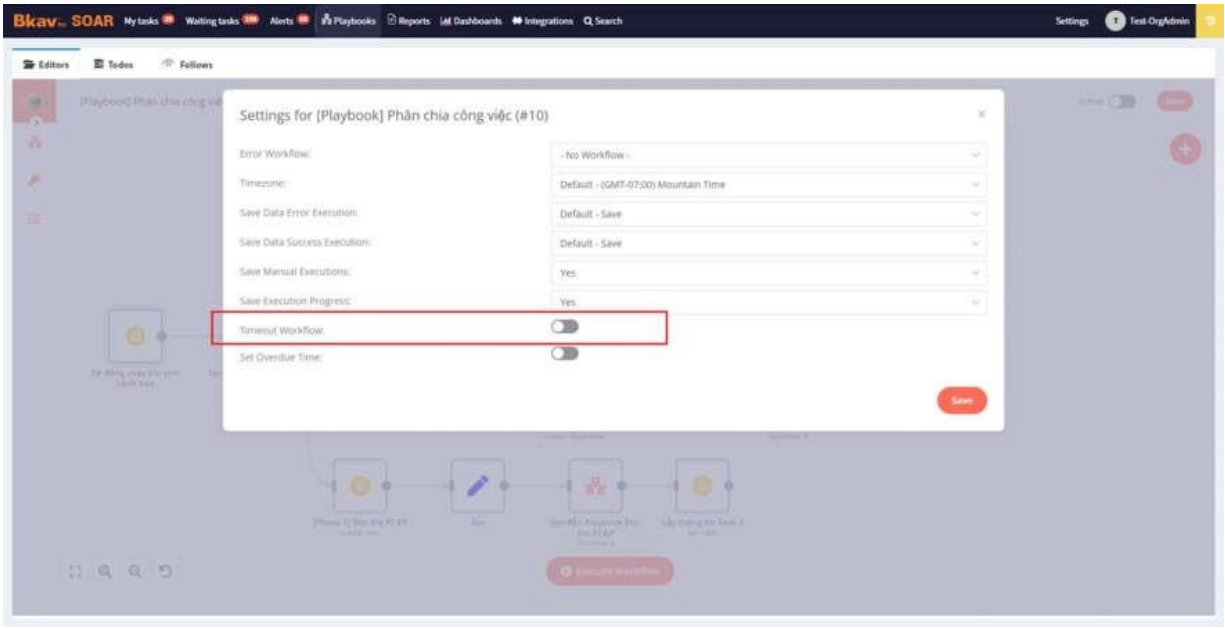


6.6. Hỗ trợ thực hiện kịch bản tự động

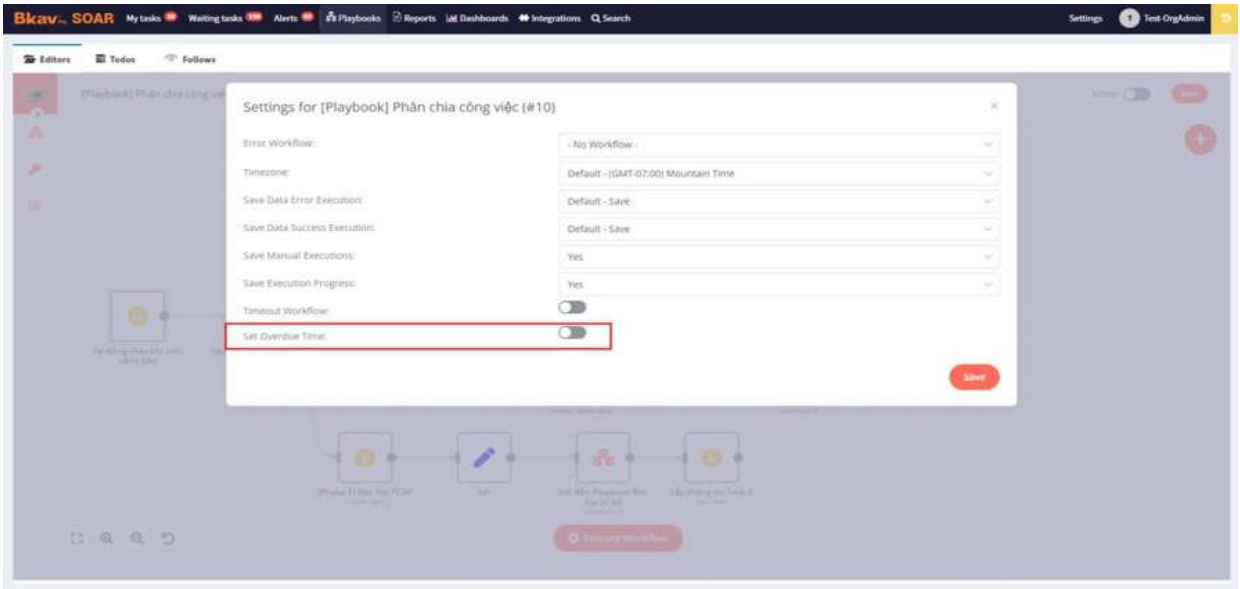
- Cho phép cấu hình kịch bản dựa theo các điều kiện, quy tắc tìm kiếm cảnh báo, tình huống để thực hiện tất cả các bước trong kịch bản mà không cần con người tương tác



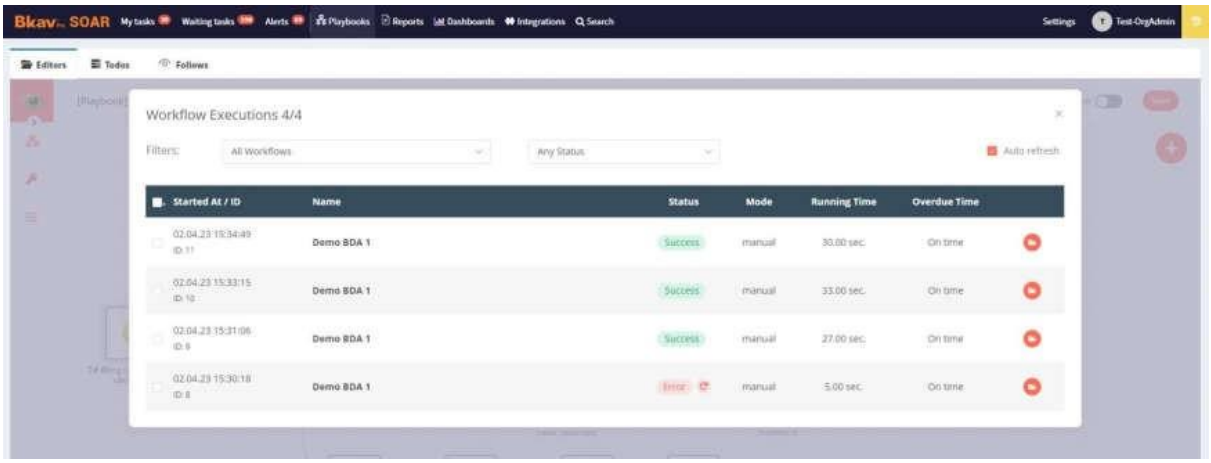
- Cho phép thiết lập thời hạn thực hiện kịch bản

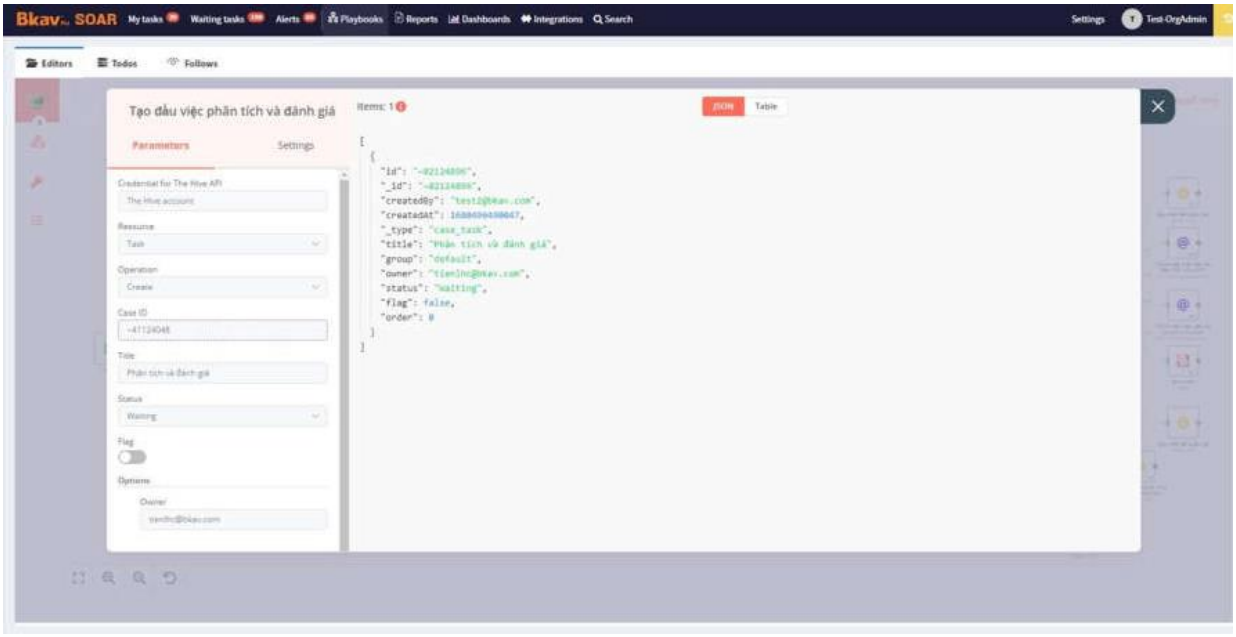


- Cho phép xác định thời gian thực hiện kịch bản có bị quá hạn hay không



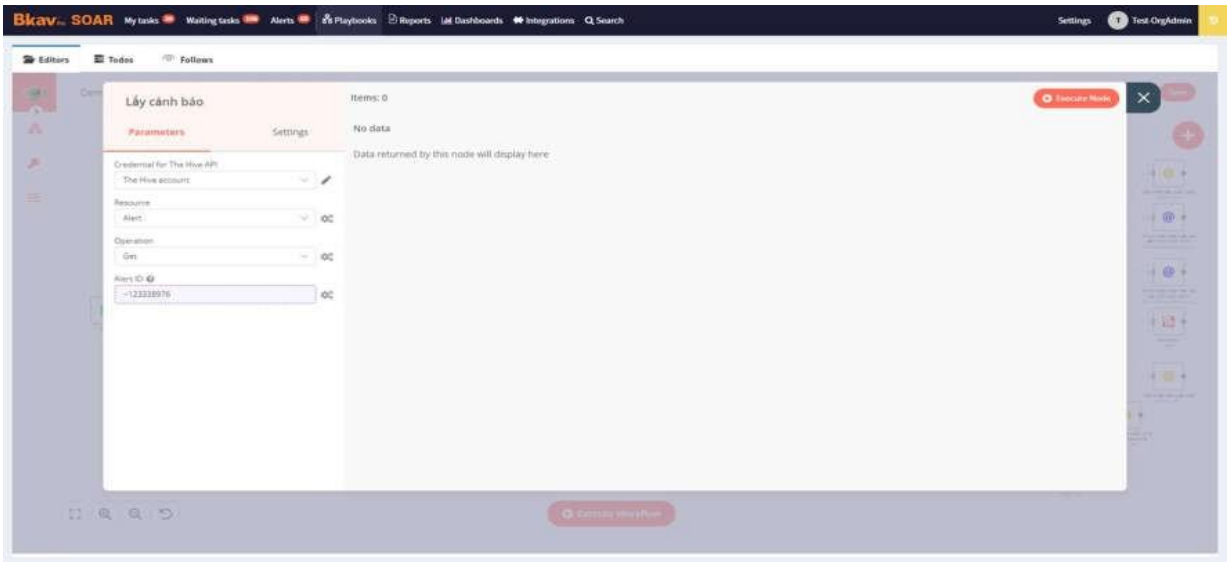
- Cho phép xem lại lịch sử thực hiện của từng bước trong kịch bản, trong đó bao gồm tối thiểu các trường thông tin sau: tập dữ liệu đầu vào, tập dữ liệu đầu ra, thời điểm bắt đầu thực hiện, thời điểm kết thúc thực hiện, trạng thái thực hiện (thành công hoặc thấtbại)



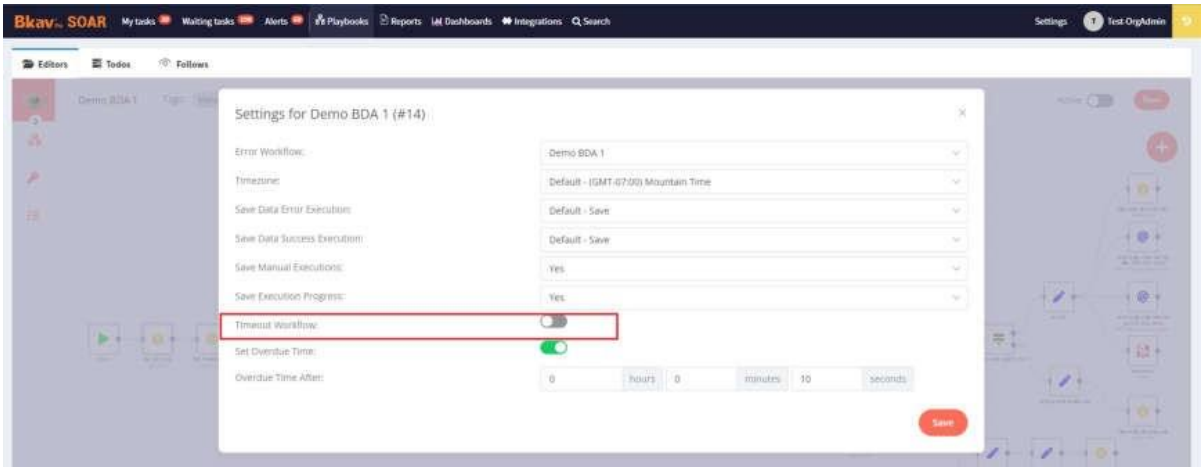


6.7. Hỗ trợ thực hiện kịch bản bán tự động

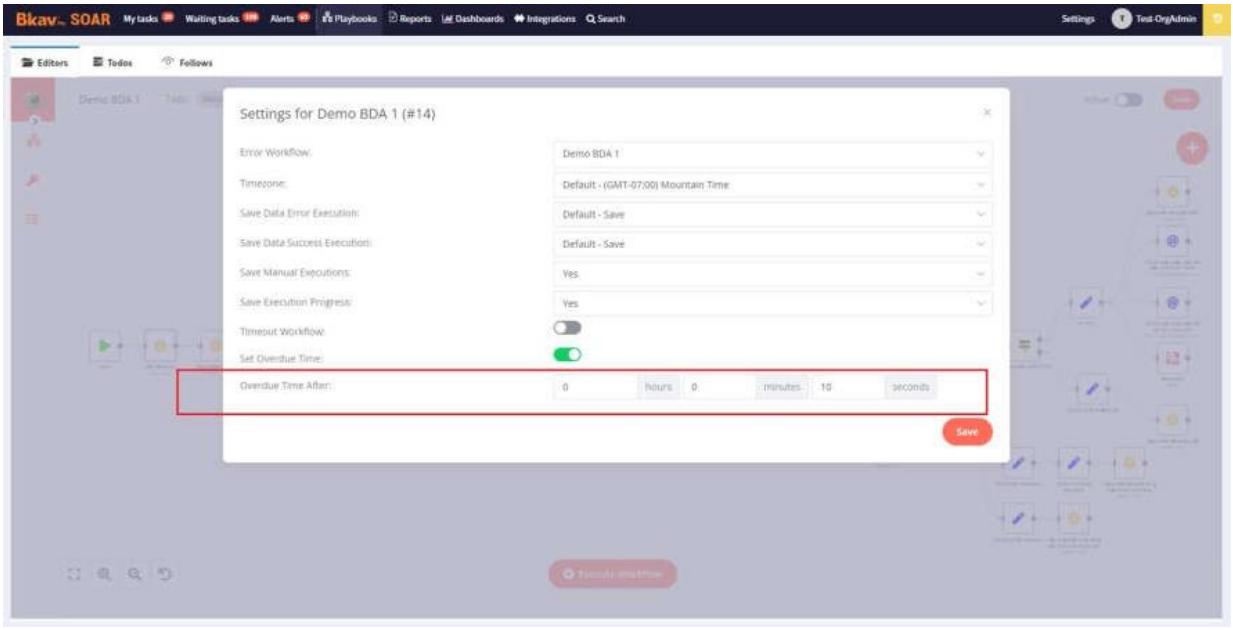
- Cho phép thực hiện kịch bản dựa vào dữ liệu người dùng đưa vào, thông qua một hoặc một số các thao tác sau: nhập giá trị (số hoặc chuỗi ký tự), chọn một hoặc một số trong các giá trị có sẵn, tải lên tệp tin, thiết lập thời điểm bắt đầu tự động thực hiện, thiết lập thời hạn thựchiện



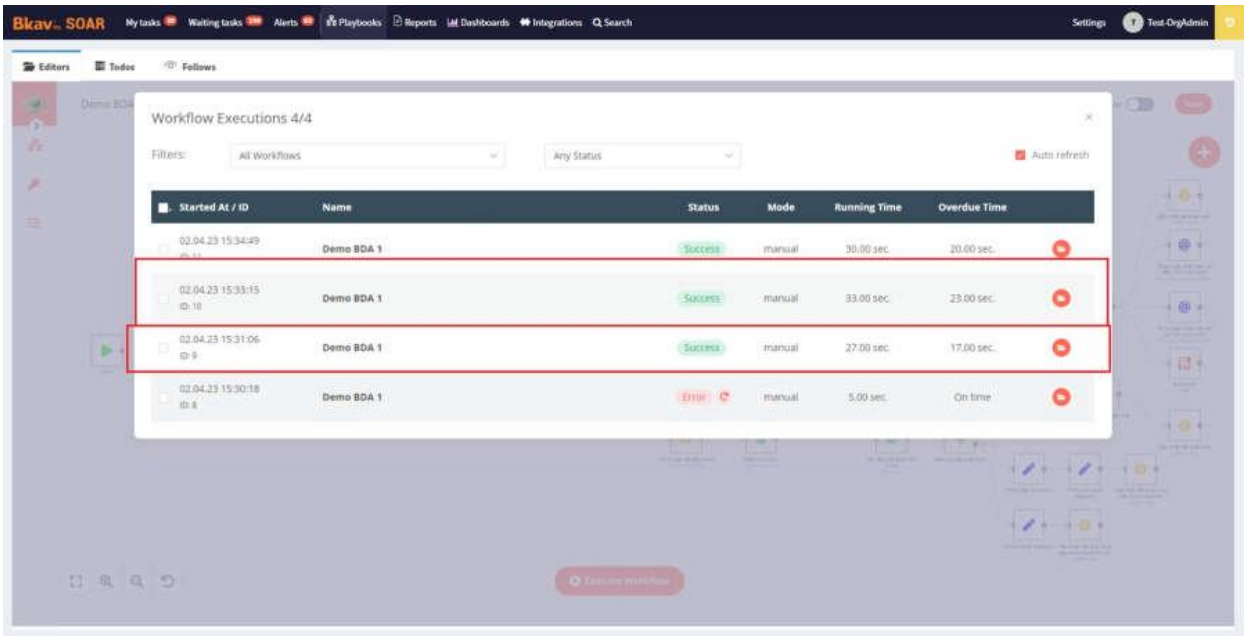
- Cho phép thiết lập thời hạn thực hiện kịch bản



- Cho phép xác định thời gian thực hiện kịch bản và từng bước trong kịch bản có bị quá hạn hay không

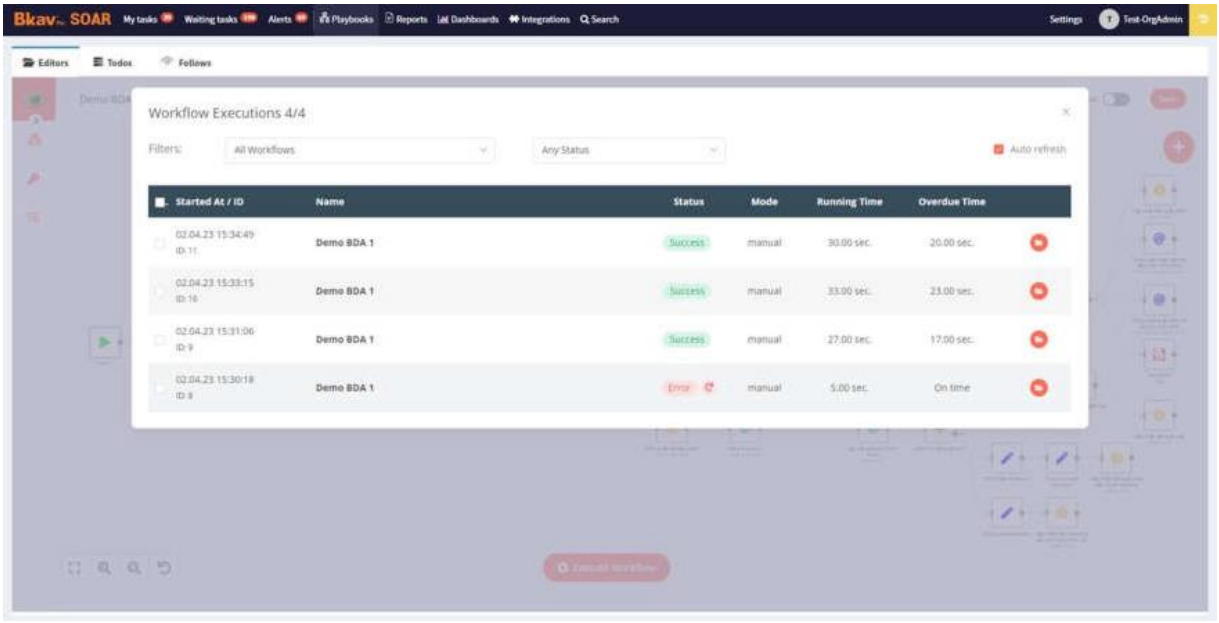


(Cấu hình thời gian xác định quá hạn)

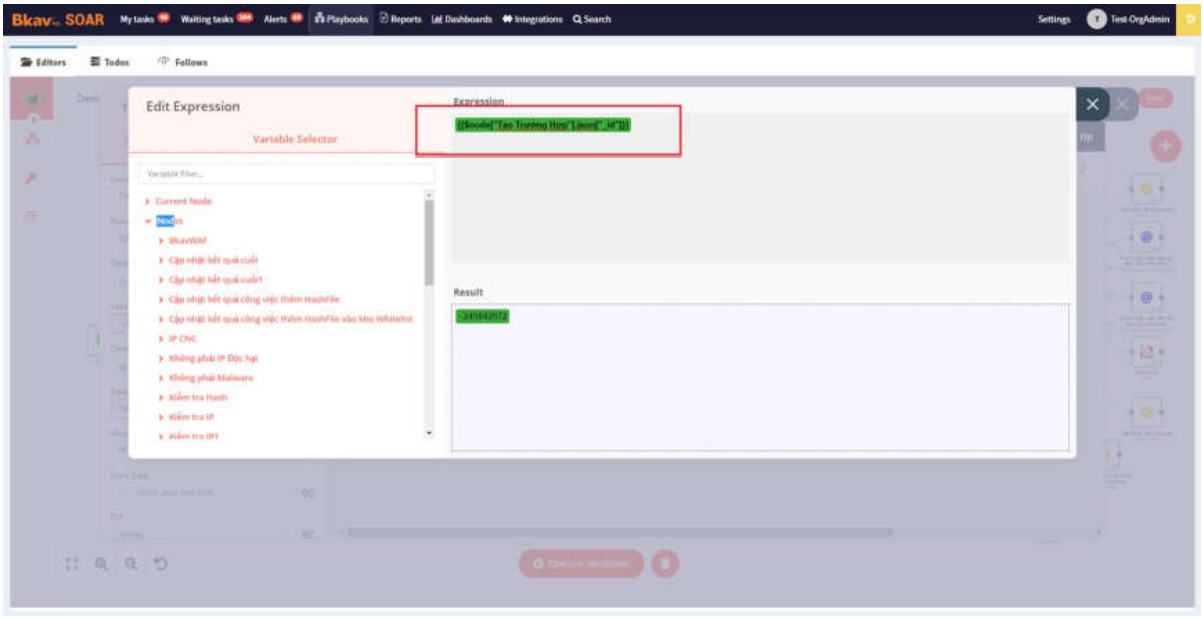


(Thời gian quá hạn -Overdue time)

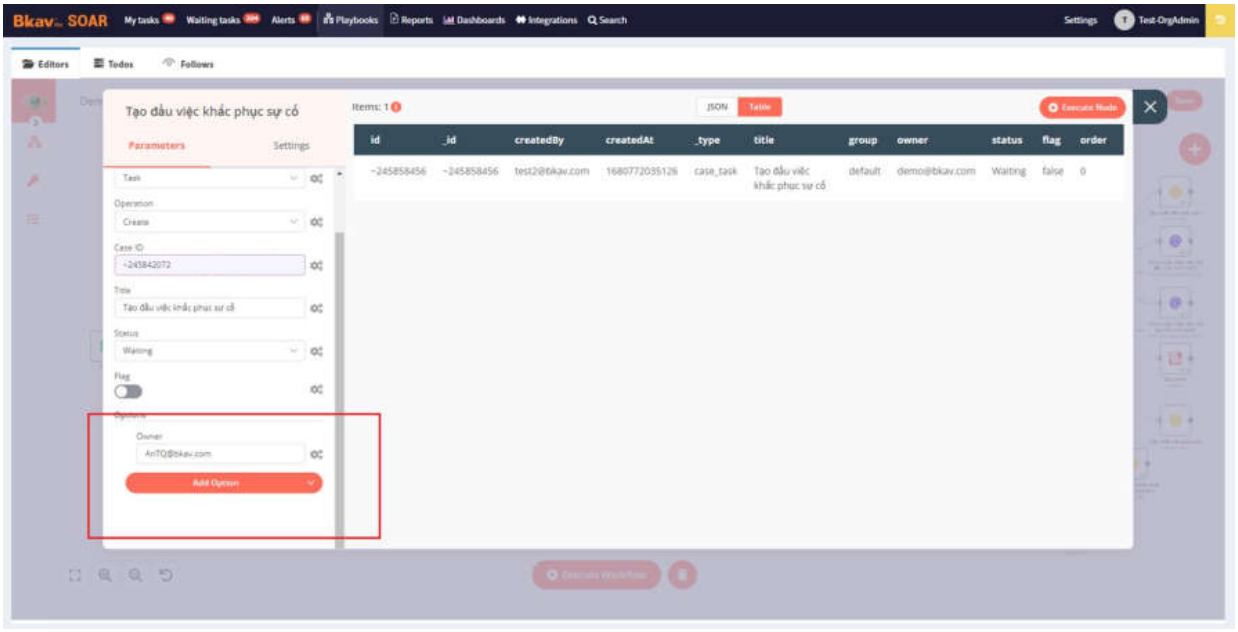
- Cho phép xem lại lịch sử thực hiện của từng bước trong kịch bản, trong đó bao gồm tối thiểu các trường thông tin sau: tập dữ liệu đầu vào, tập dữ liệu đầu ra, thời điểm bắt đầu thực hiện, thời điểm kết thúc thực hiện, trạng thái thực hiện (thành công hoặc thất bại), tài khoản người dùng có tương tác



- Cho phép sử dụng kết quả thực hiện của bước trước đó làm dữ liệu đầu vào cho bước tiếp theo trong kịch bản



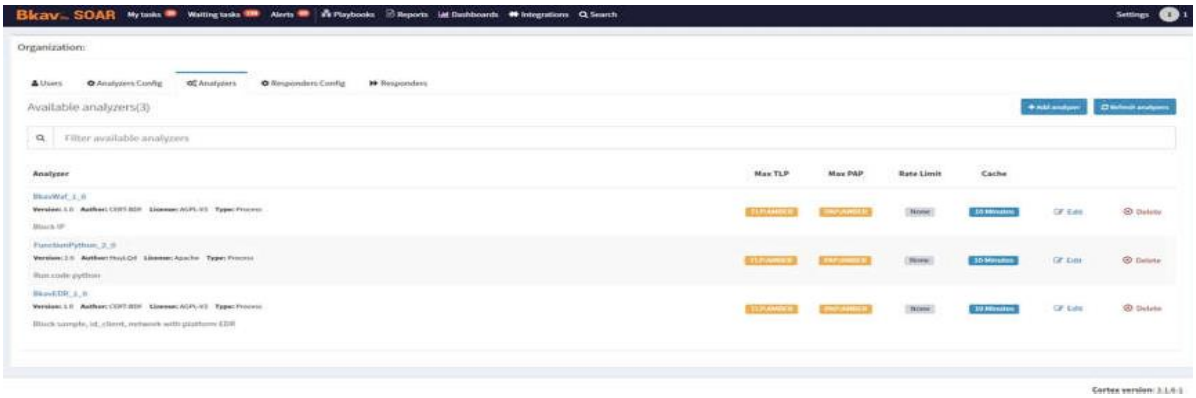
- Cho phép gán một hoặc nhiều người tương tác cho những bước trong kịch bản cần con người tương tác

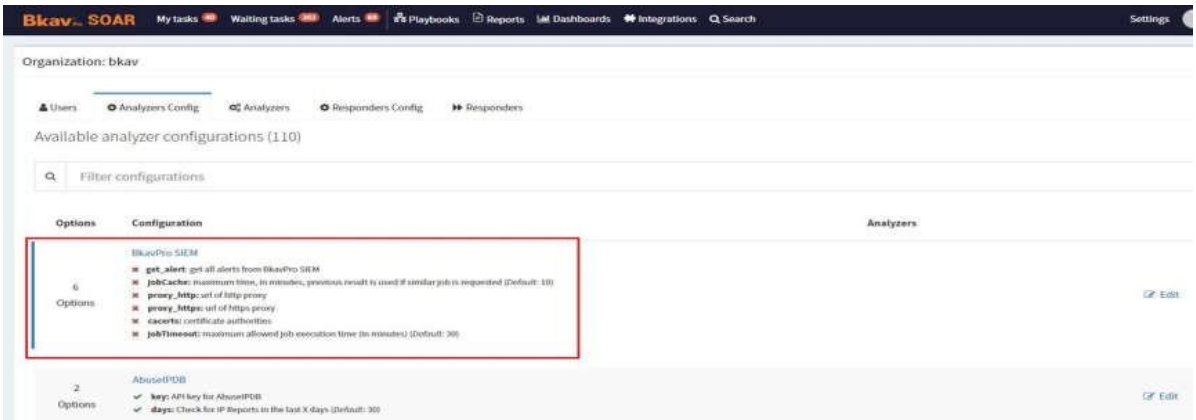


7. Chức năng khác

- **Hỗ trợ tích hợp các giải pháp bảo mật: Tích hợp các công cụ bảo mật khác nhau dễ dàng tìm kiếm thông tin, đánh giá mức độ và tương quan các sự kiện có liên quan đến sự cố cần điều tra**

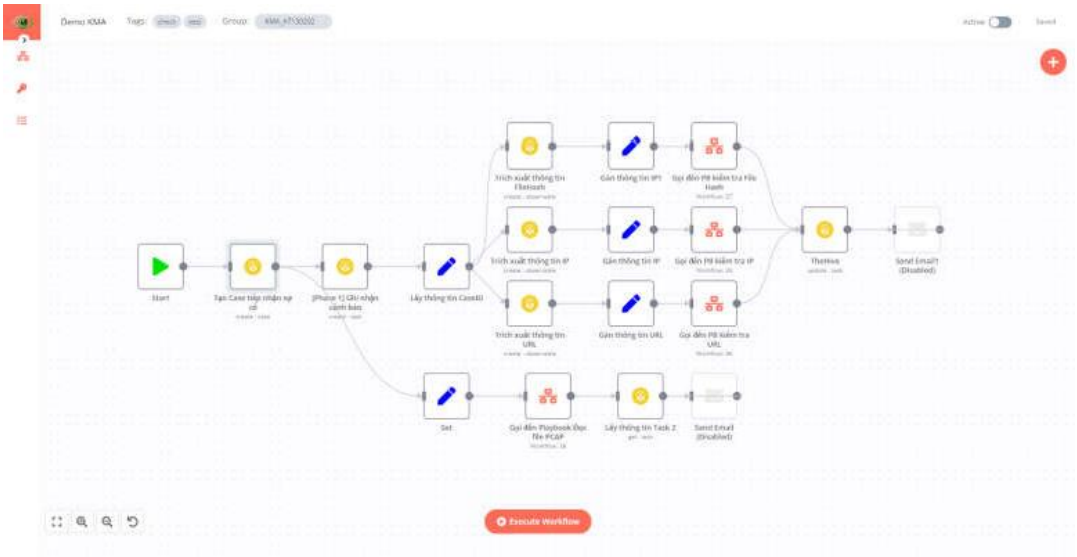
  BkavPro SOAR đã thành công tích hợp với các giải pháp bảo mật nội bộ của Bkav phát triển bao gồm: BTI (BkavPro Threat Intelligence), BkavPro EDR (BkavPro Endpoint Detection and Response), BkavPro WAF (BkavPro Web Application Firewall), BIF (BkavPro Firewall), BkavPro NIPS (BkavPro Network Intrusion and Protection System), BkavPro SIEM (BkavPro Security Informations and Events Management). Ngoài ra, còn tích hợp đến các công cụ đã được tích hợp sẵn như: Sandbox, VirusTotal, AbuseIDp, OpenCTI, MISP...





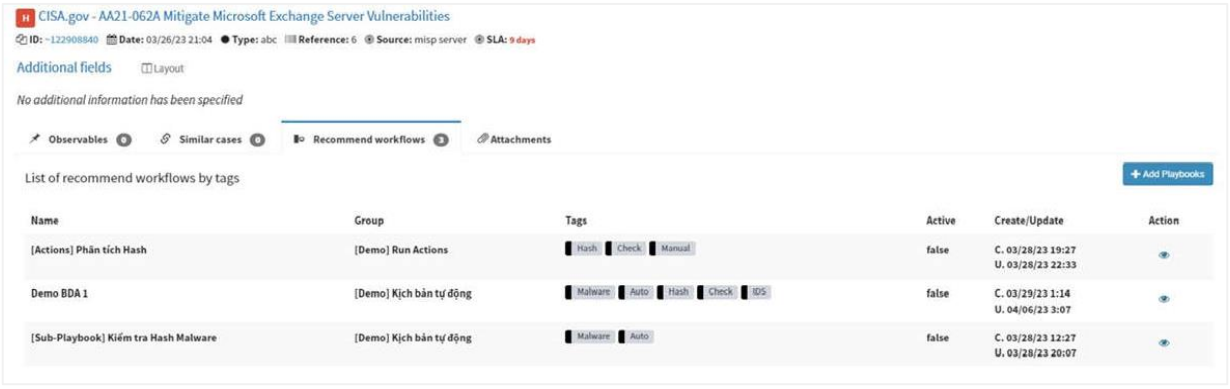
7. Chức năng khác (tiếp)

Quy trình xử lý tự động:



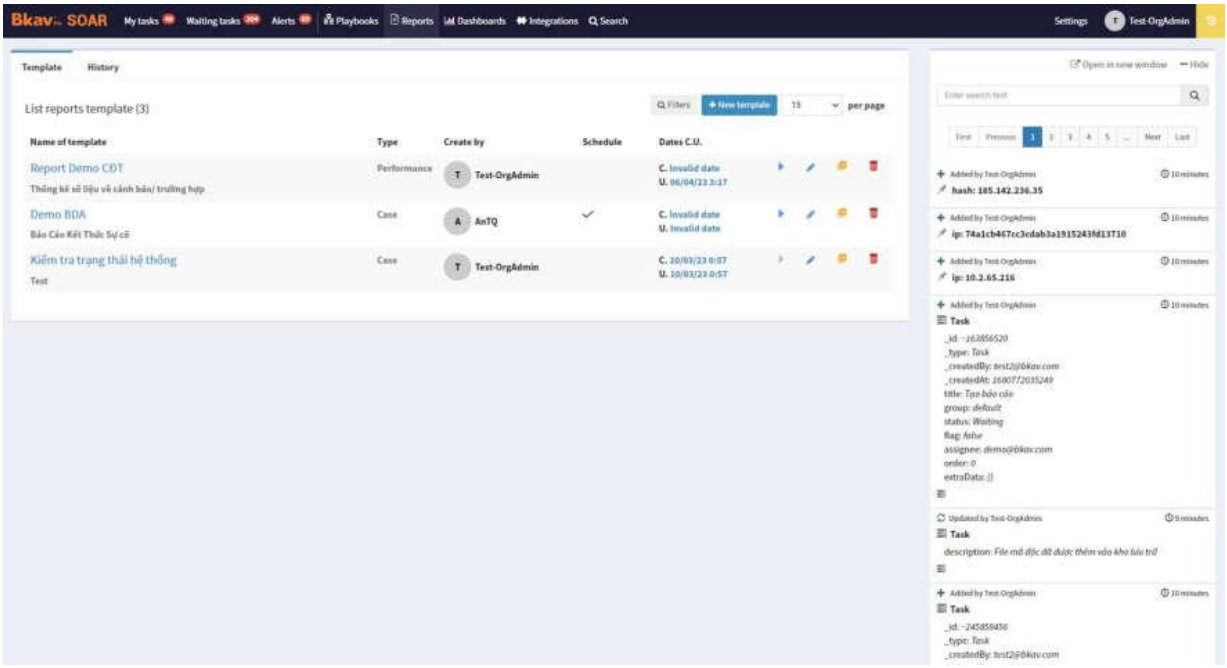
- **Cung cấp các kịch bản xử lý sự cố và các thông tin liên quan cần thiết để ứng phó các cuộc tấn công phức tạp. Playbook sẽ tự động đưa ra các kịch bản khi kiểm tra thấy các thông tin có trong cảnh báo hay sự kiện về cuộc tấn công diễn ra khớp với các điều kiện của dạng tấn công đó**

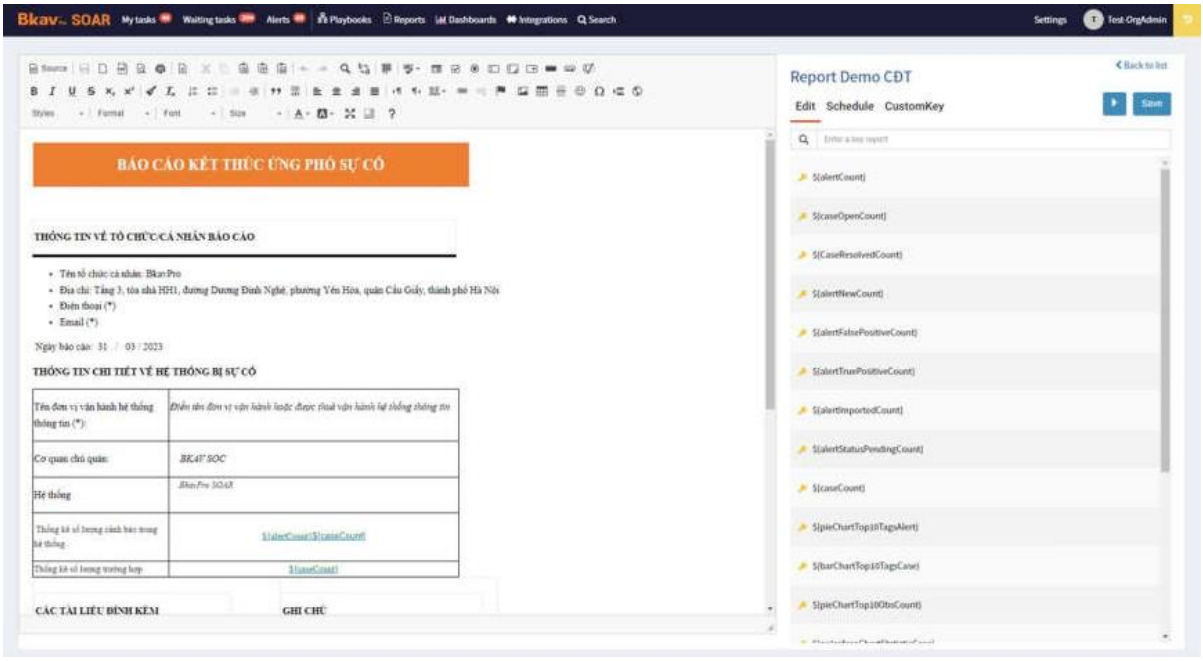
  BkavPro SOAR cung cấp các kịch bản Playbook và thông tin liên quan cần thiết để ứng phó sự cố thông qua việc đối xứng dữ liệu thông qua các thẻ tag, thông tin được cập nhật. Các kịch bản sẽ được tự động gợi ý theo các trường dữ liệu cho trước và người dùng có thể thêm các kịch bản Playbook để xử lí tùy thuộc theo nhu cầu của công việc



7. Chức năng khác (tiếp)

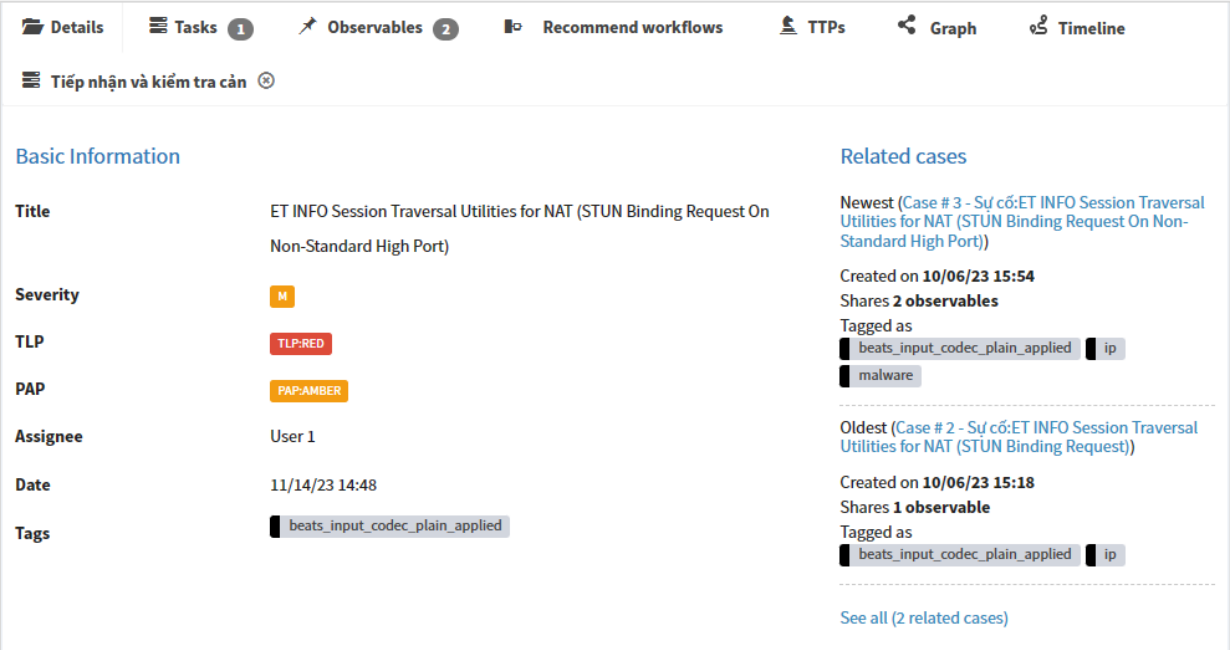
- **Xuất báo cáo: Hỗ trợ các mẫu báo cáo chung hoặc có thể tùy chỉnh báo cáo phù hợp với yêu cầu của tổ chức**

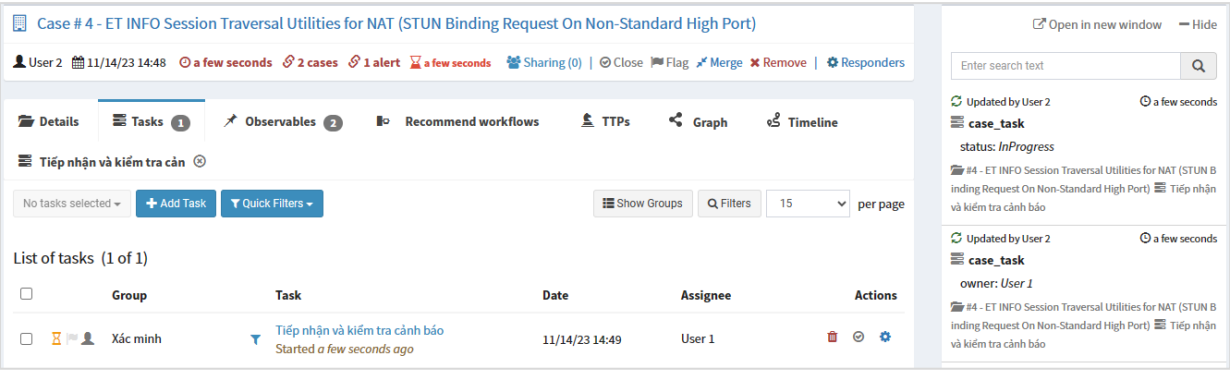


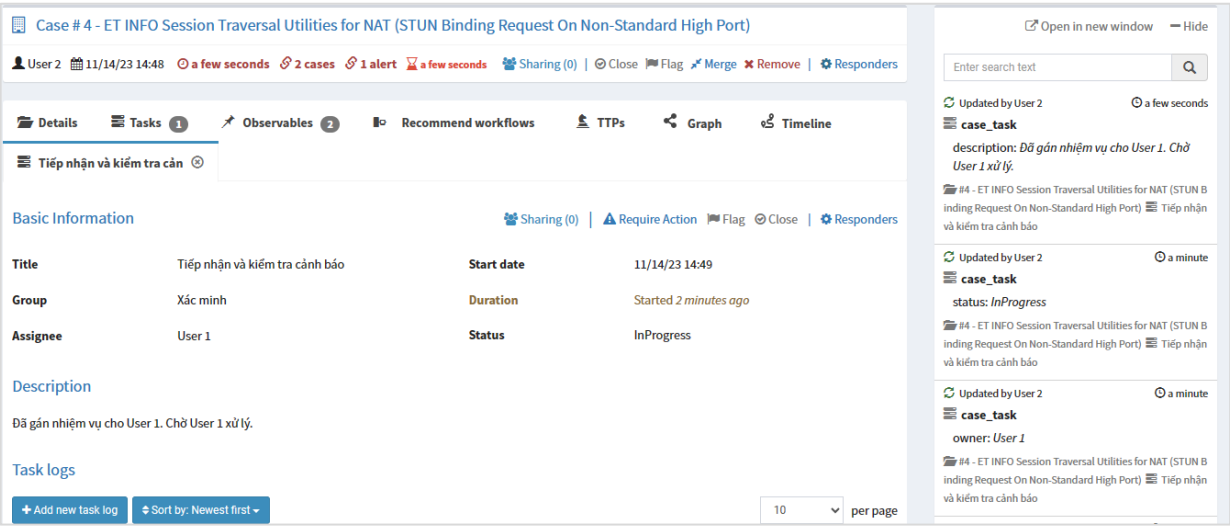


7. Chức năng khác (tiếp)

- **Incident Management:** Tạo ra các ticket, gán cho người vận hành xử lý. Theo dõi tiến độ xử lý của ticket.







Giấy phép sử dụng

Bản quyền sử dụng vĩnh viễn, thời gian hỗ trợ: Tối thiểu 02 năm

Hiệu năng xử lý: Tối thiểu 50 GB/ngày