Bkav Pro SIEM Central Engine

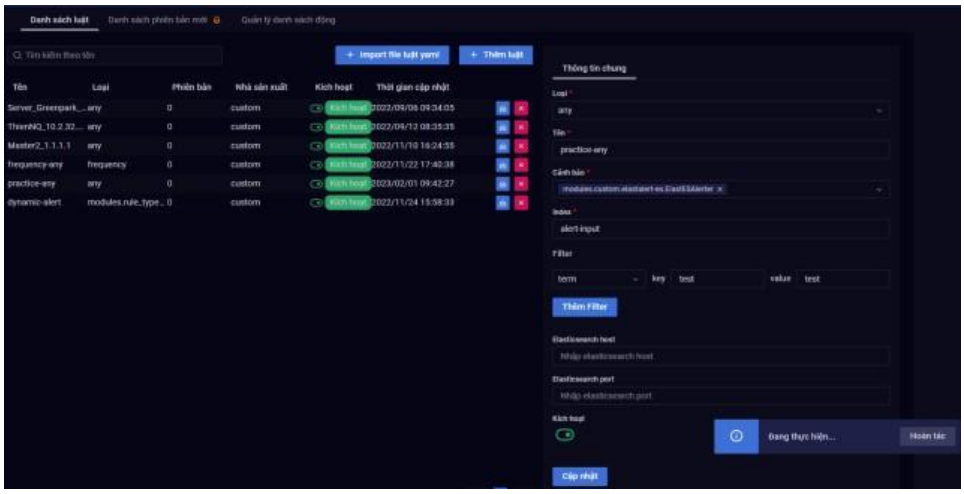
Phần mềm Quản lý và phân tích sự kiện an toàn thông tin

Bkav Pro SIEM - Hệ thống quản lý thông tin và sự kiện bảo mật thế hệ mới (NEXT GEN SIEM).

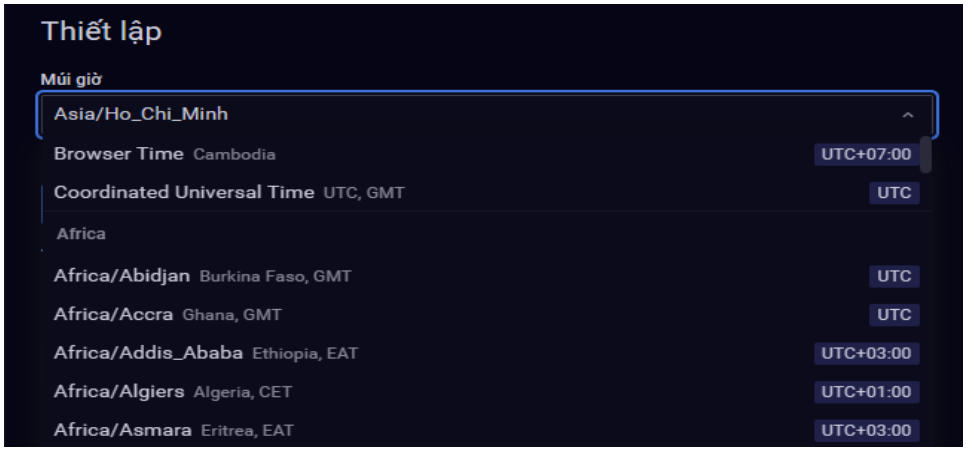
1. Quản trị hệ thống

1.1. Quản lý vận hành

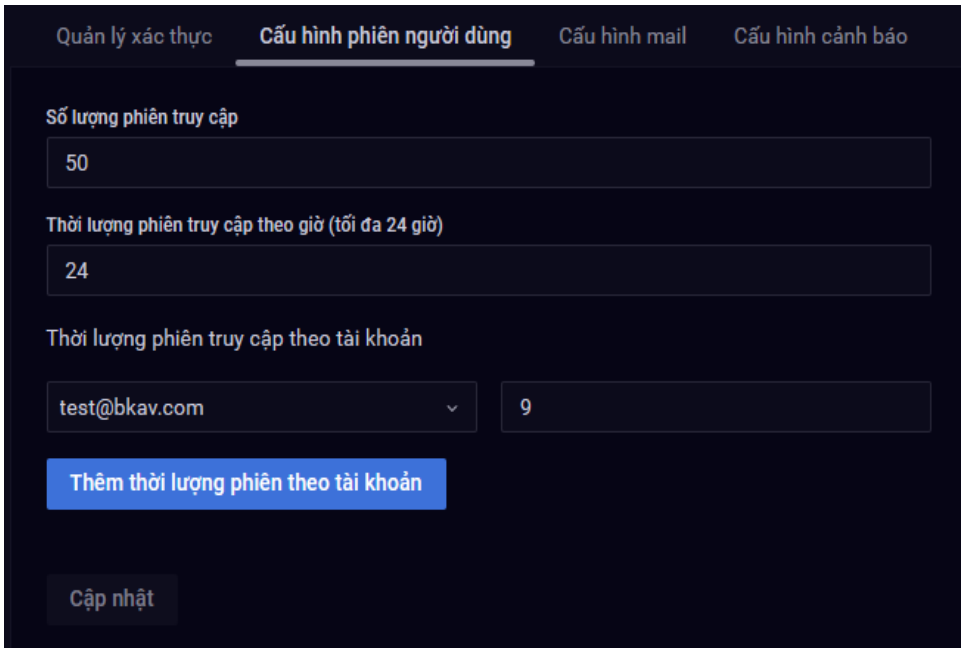
- Cho phép thiết lập, thay đổi, áp dụng và hoàn tác sự thay đổi trong cấu hình hệ thống, cấu hình quản trị từ xa, cấu hình tài khoản xác thực và phân quyền người dùng, cấu hình tập luật bảo vệ



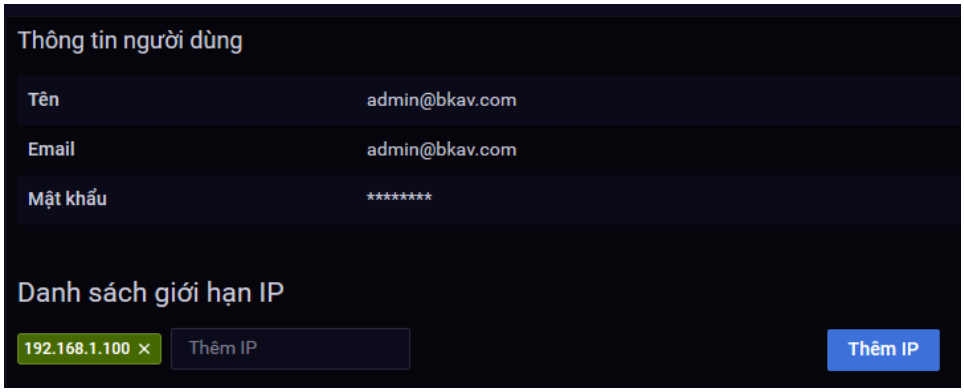
- Cho phép thay đổi thời gian hệ thống



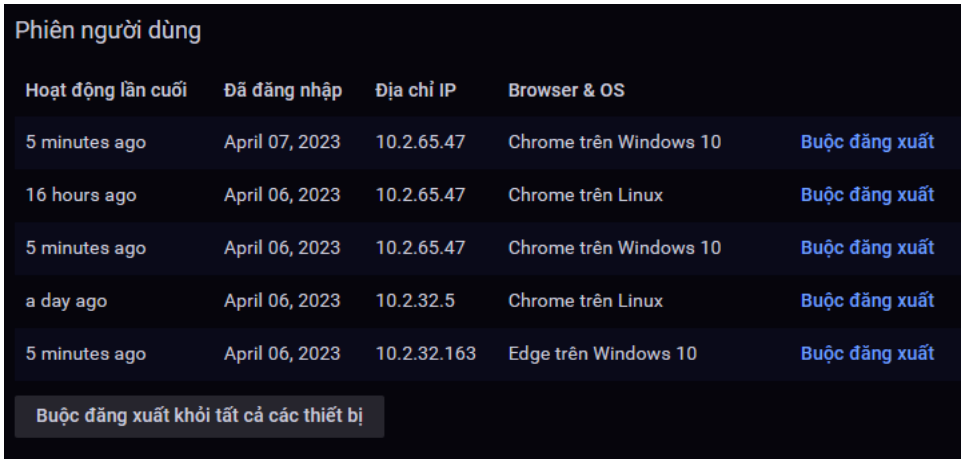
- Cho phép thay đổi thời gian duy trì phiên kết nối (giới hạn số phiên truy cập, số phiên kết nối quản trị từ xa đồng thời…)



- Cho phép thiết lập, thay đổi các tham số giới hạn đối với kết nối quản trị từ xa



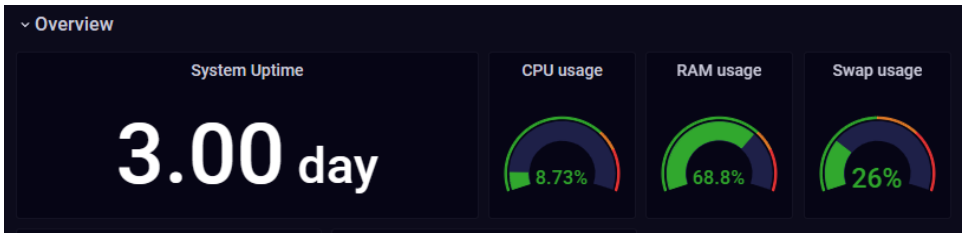
- Cho phép đăng xuất tài khoản người dùng có phiên kết nối còn hiệu lực



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

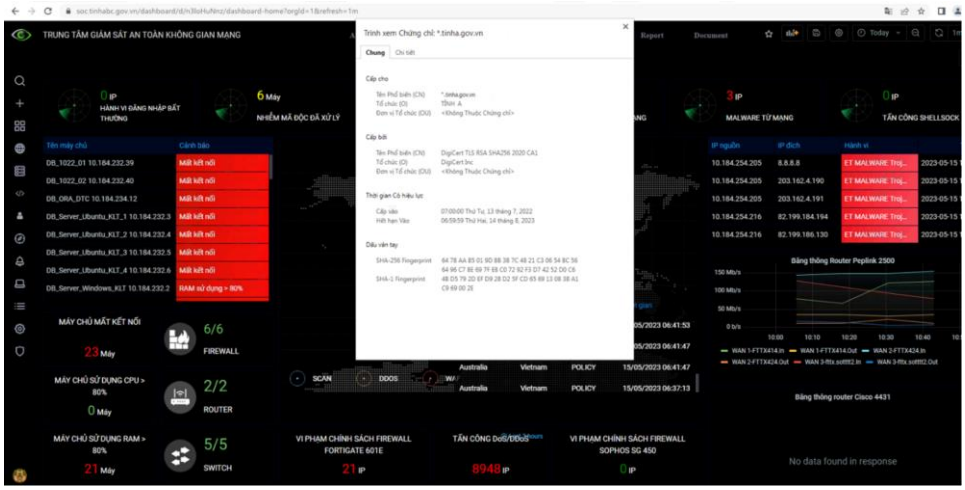
- Cho phép xóa log

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

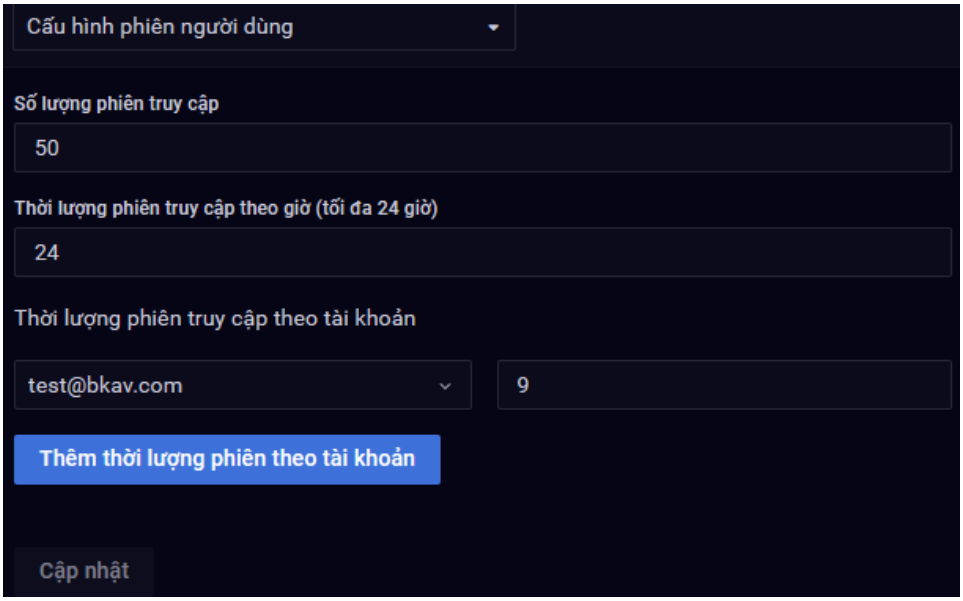


1.2. Quản lý từ xa

- Sử dụng giao thức có mã hóa TLS

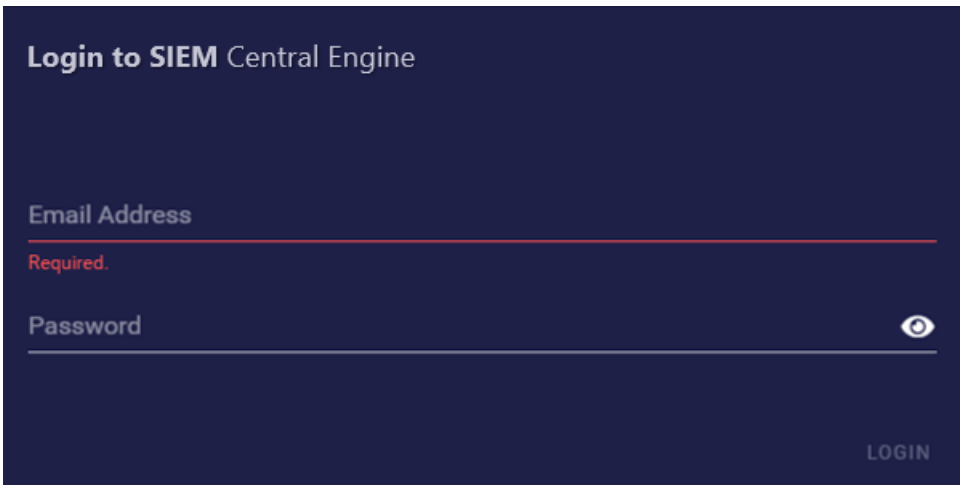


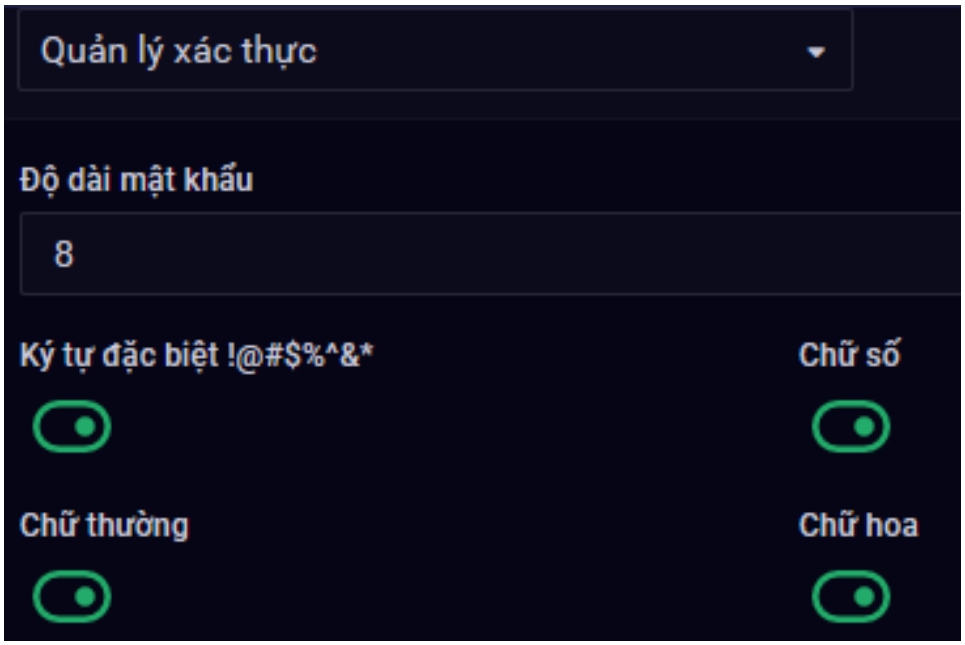
- Tự động đăng xuất tài khoản và hủy bỏ phiên kết nối quản trị từ xa khi hết thời gian duy trì phiên kết nối



1.3. Quản lý xác thực và phân quyền

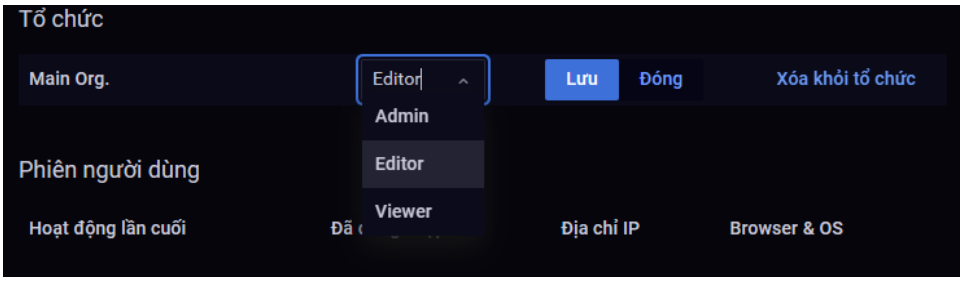
- Hỗ trợ phương thức xác thực bằng tài khoản - mật khẩu, trong đó, quản trị viên có thể thiết lập và thay đổi được độ phức tạp của mật khẩu

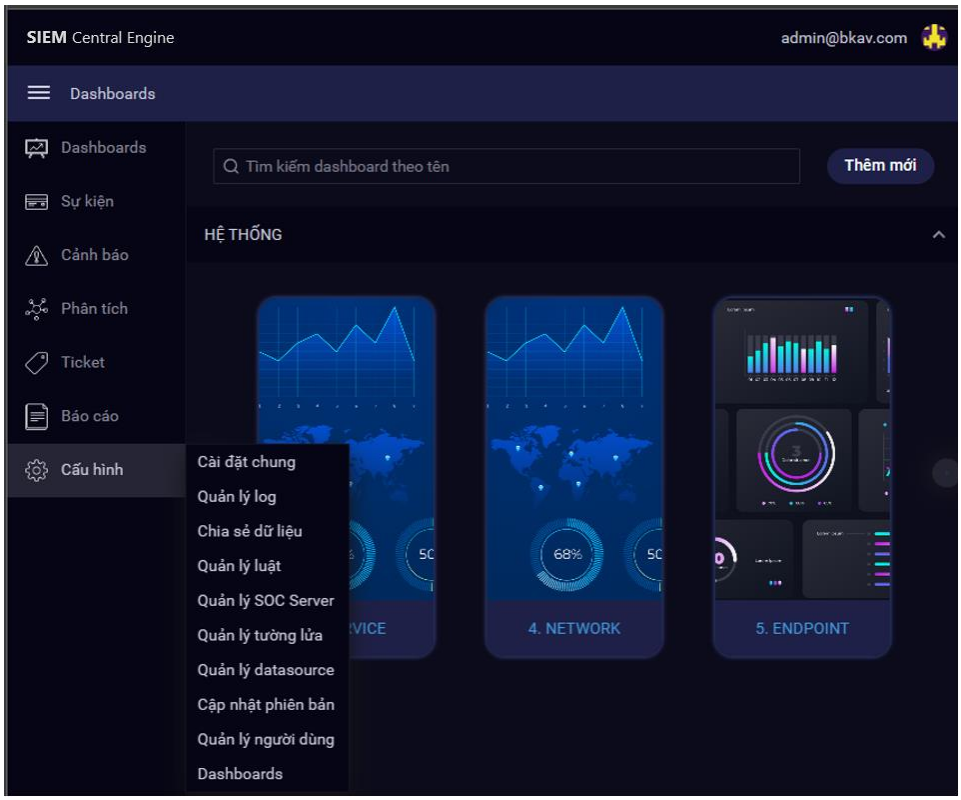


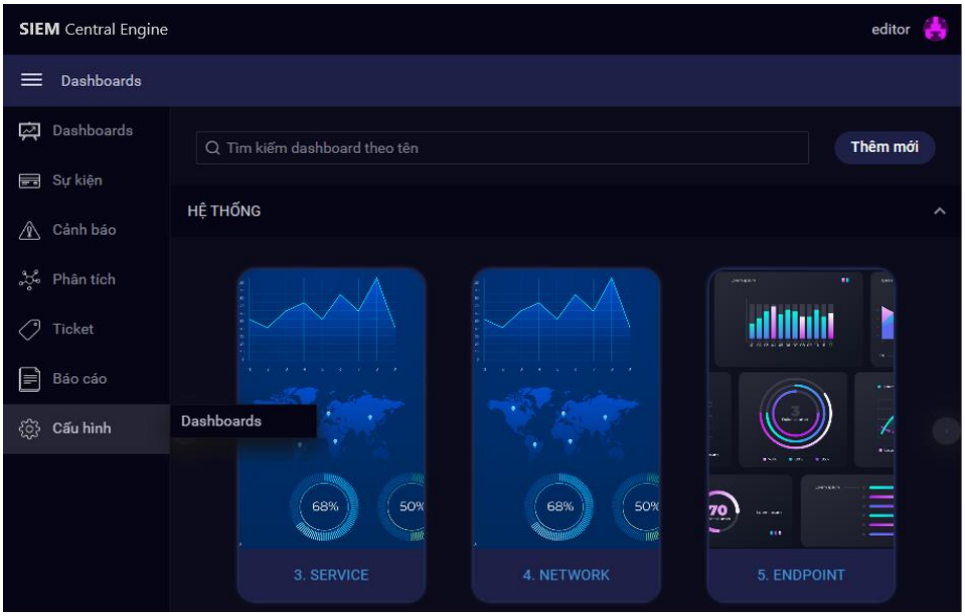


1.3. Quản lý xác thực và phân quyền (tiếp)

- Hỗ trợ phân nhóm tài khoản theo 02 nhóm là quản trị viên và người dùng thường với những quyền hạn cụ thể đối với từng nhóm

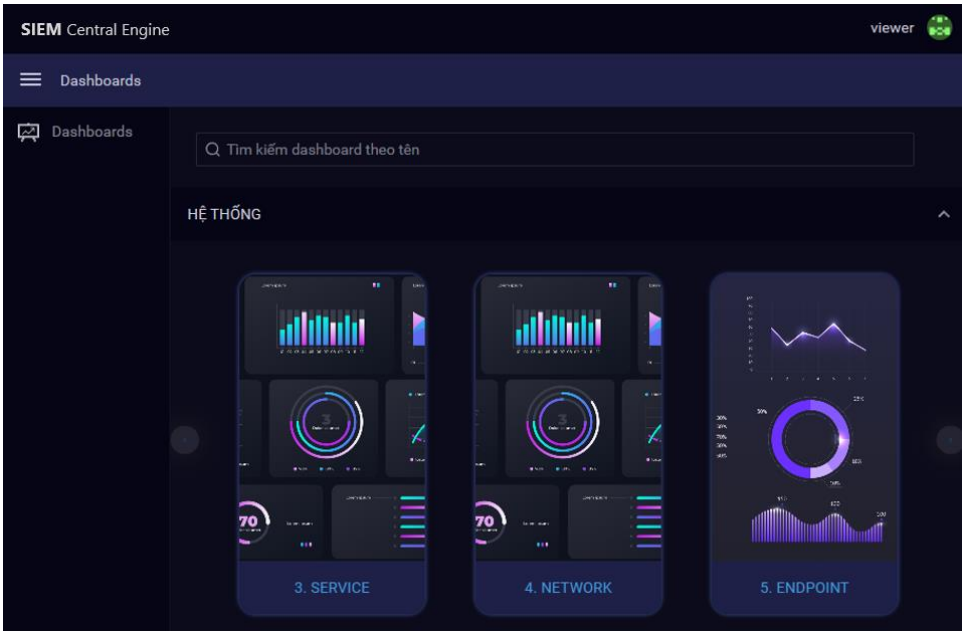






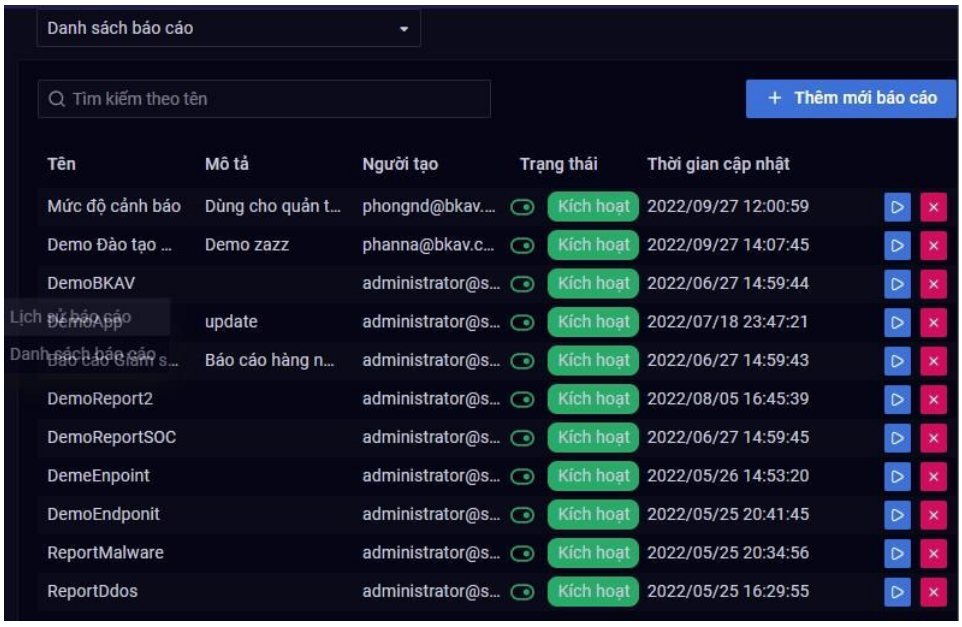
1.3. Quản lý xác thực và phân quyền (tiếp)

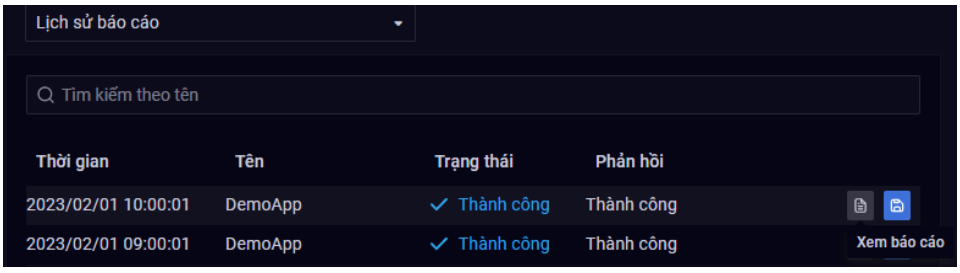
- Hỗ trợ phân nhóm tài khoản theo 02 nhóm là quản trị viên và người dùng thường với những quyền hạn cụ thể đối với từng nhóm



1.4. Quản lý báo cáo

- Cho phép tạo mới, xem lại và xóa báo cáo đã được tạo

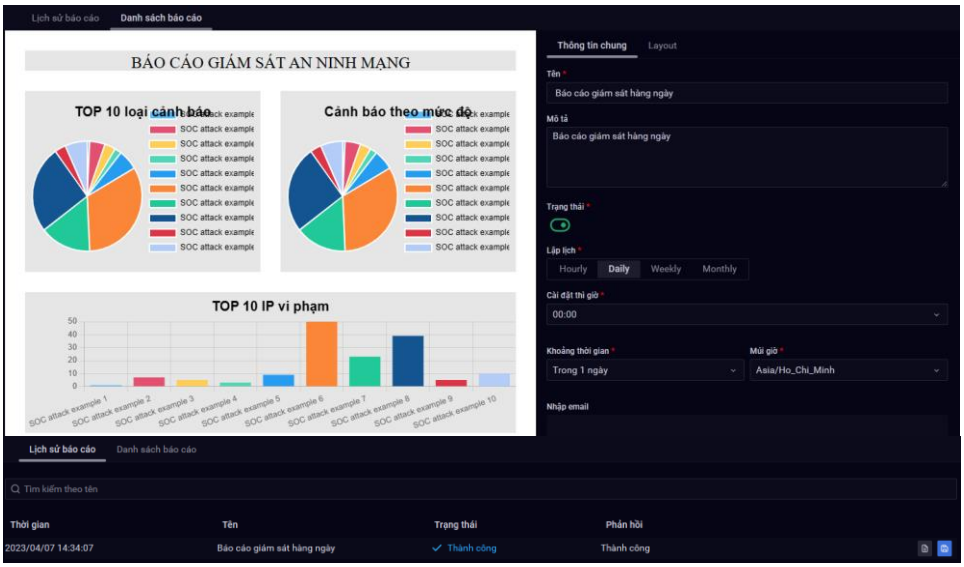




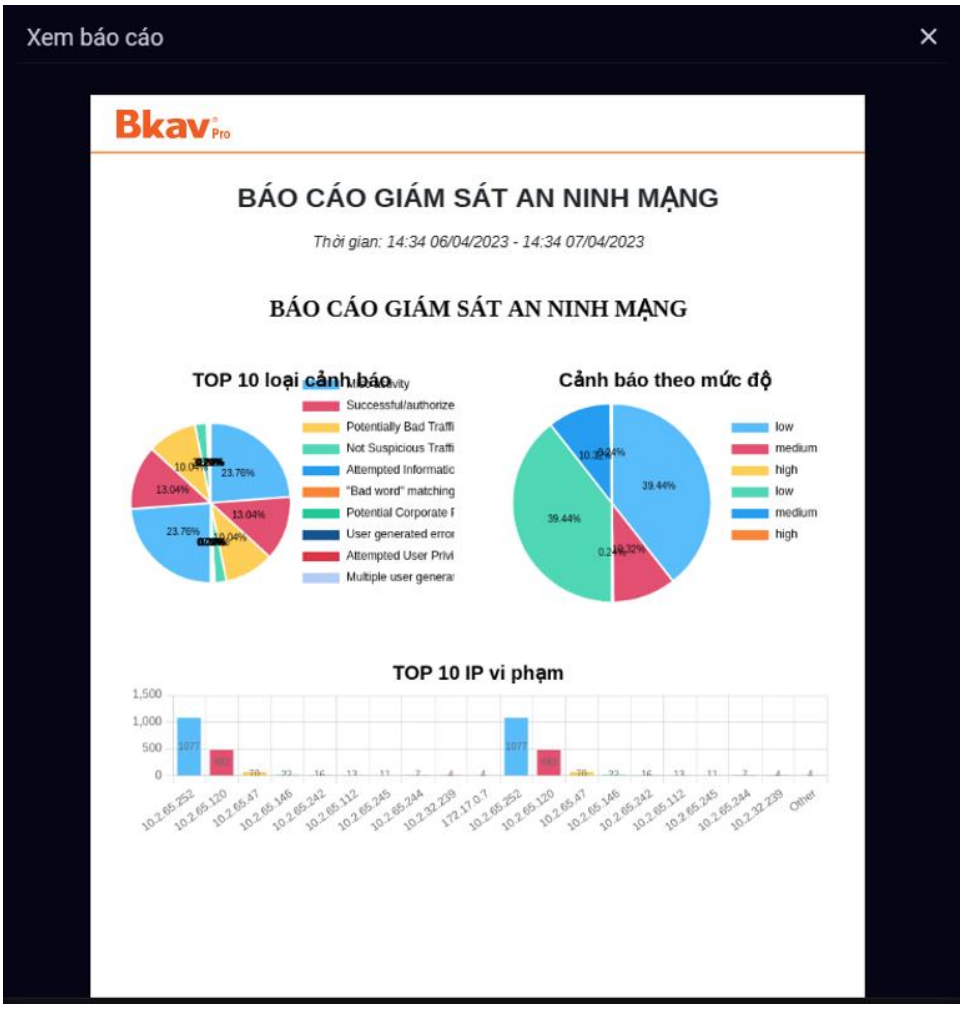
1.4. Quản lý báo cáo (tiếp)

- Cho phép tạo mới, xem lại và xóa báo cáo đã được tạo (tiếp)

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



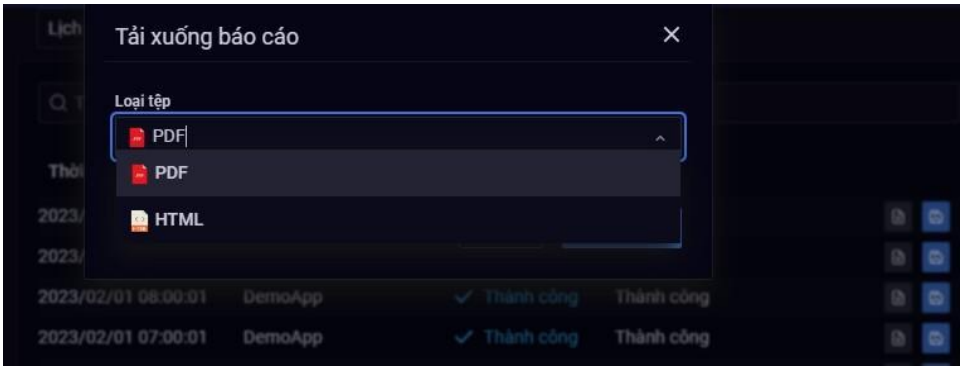
1.4. Quản lý báo cáo (tiếp)



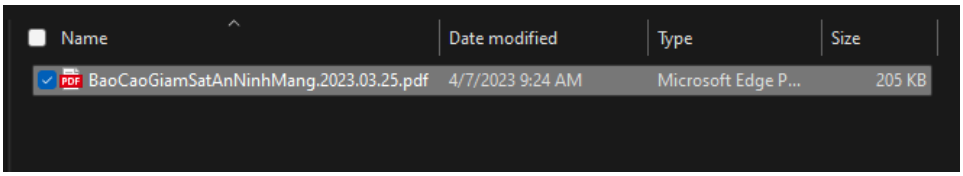
1.4. Quản lý báo cáo (tiếp)

- Cho phép áp dụng các quy tắc tìm kiếm thông tin, dữ liệu log 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

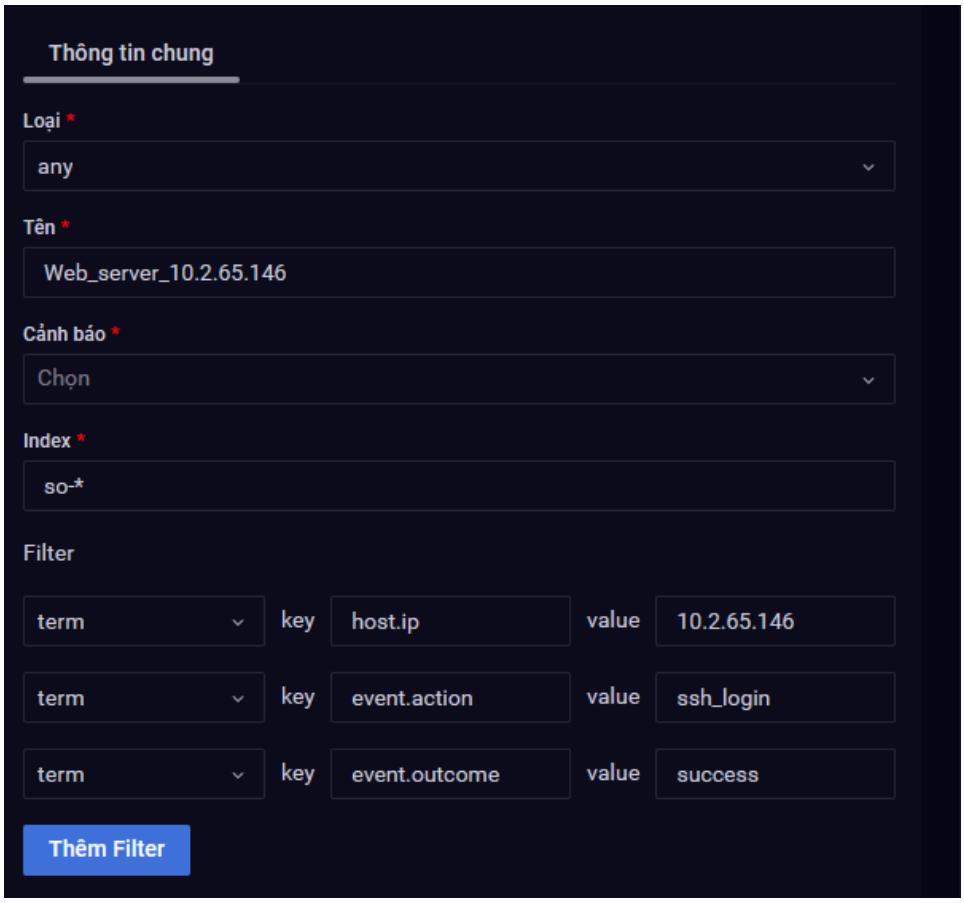


1.5. Quản lý tập luật bảo vệ

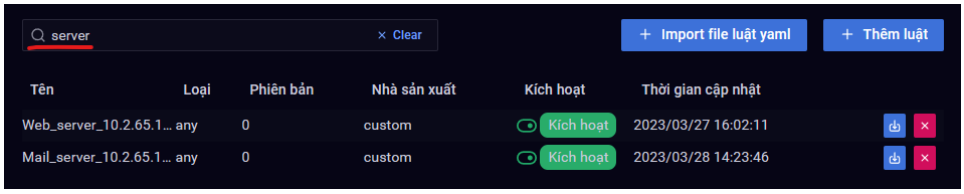
- Thêm luật mới

1.5. Quản lý tập luật bảo vệ (tiếp)

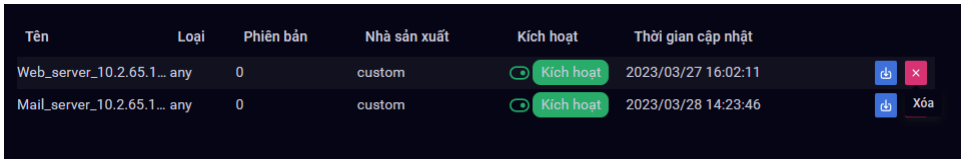
- Tinh chỉnh luật



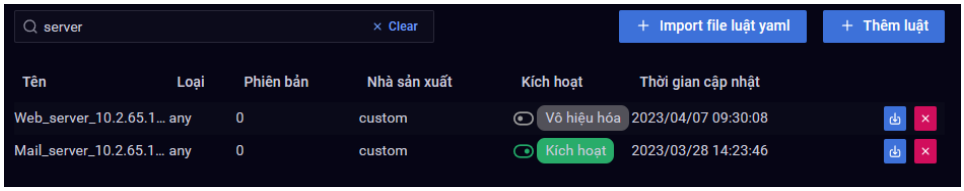
- Tìm kiếm luật



- Xóa luật

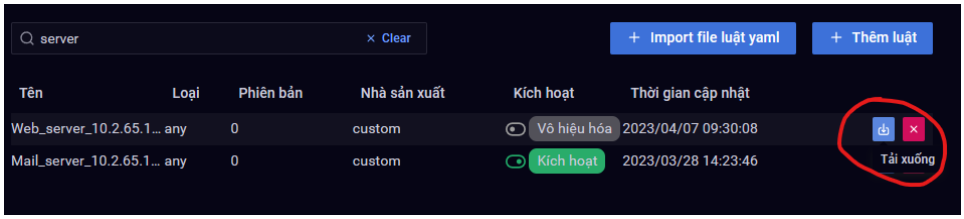


- Kích hoạt/vô hiệu hóa luật

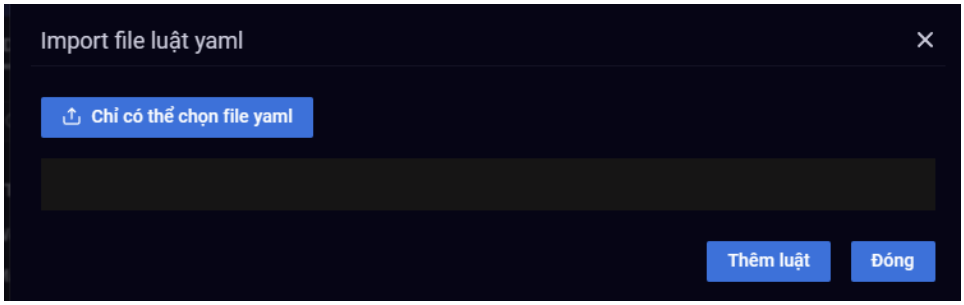


1.5. Quản lý tập luật bảo vệ (tiếp)

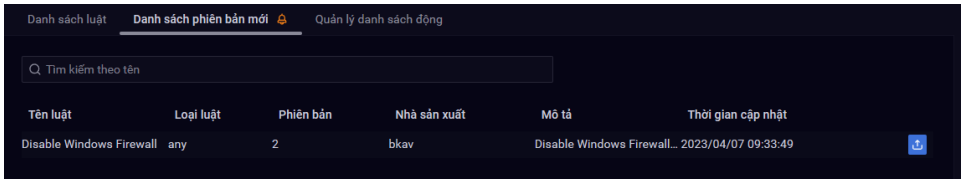
- Xuất tập luật ra tệp tin



- Khôi phục tập luật từ tệp tin



- Cập nhật tập luật được phát hành bởi nhà sản xuất

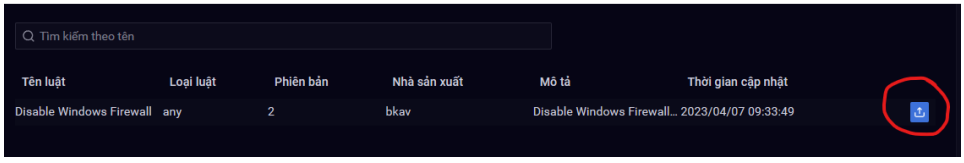


1.6. Cập nhật tập luật bảo vệ

- Cho phép tự động thông báo có bản cập nhật mới cho quản trị viên

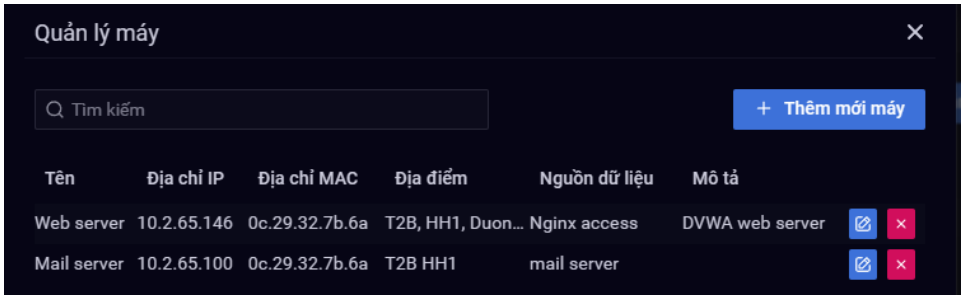
(Chuông cảnh báo xuất hiện khi có phiên bản mới của luật)

- Cho phép tải về trực tuyến và áp dụng thủ công bản cập nhật mới



1.7. Quản lý đối tượng được giám sát và nguồn gửi log

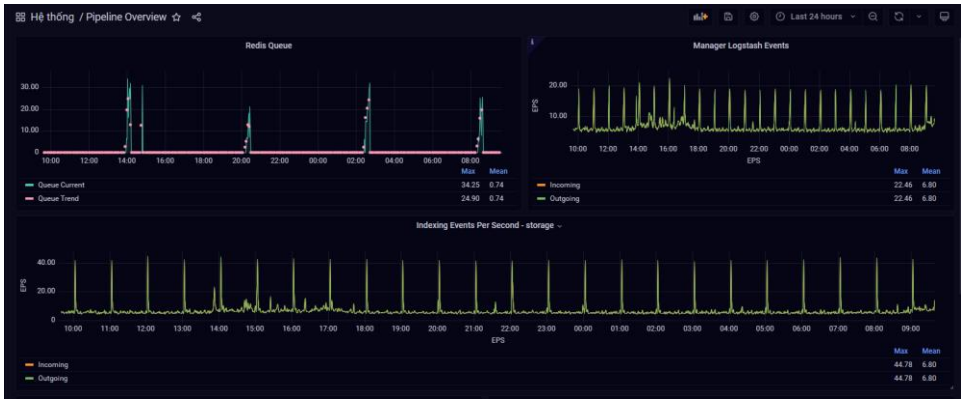
- Cho phép quản lý đối tượng được giám sát và nguồn gửi log theo các nhóm được định nghĩa bởi quản trị viên



1.7. Quản lý đối tượng được giám sát và nguồn gửi log (tiếp)

- Cho phép quản lý đối tượng được giám sát và nguồn gửi log theo địa chỉ vật lý, địa chỉ mạng và vị trí địa lý

- Quản lý và giám sát tập trung các thành phần tích hợp bên trong: Receiver, Parser, Indexer, Storage, Correlator

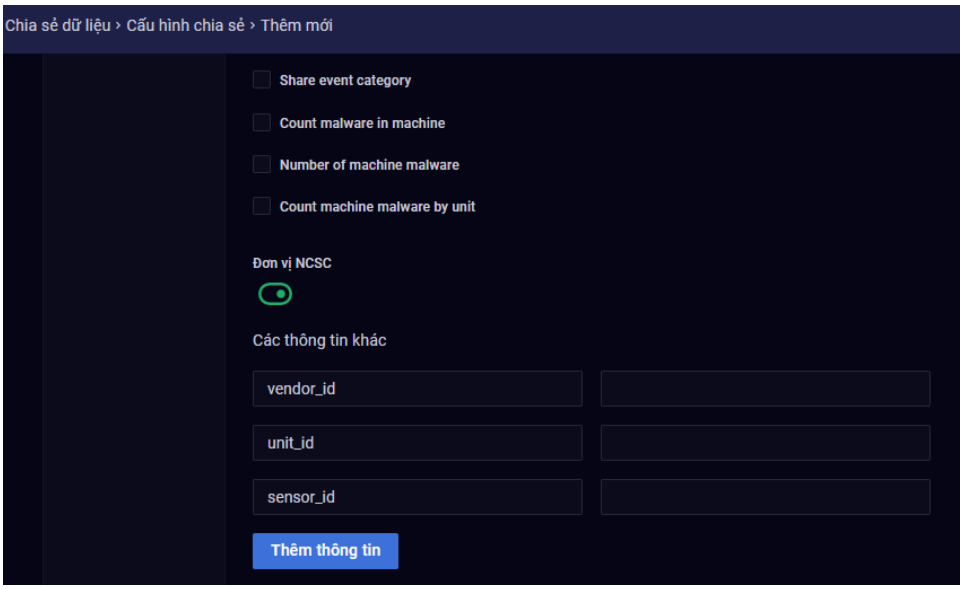


1.8. Chia sẻ dữ liệu

- Hệ thống giám sát an toàn không gian mạng quốc gia Việt Nam

1.8. Chia sẻ dữ liệu (tiếp)

- Hệ thống giám sát an toàn không gian mạng quốc gia Việt Nam



2. Khả năng kiểm soát lỗi

2.1. Bảo vệ cấu hình

- Trong trường hợp phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), đảm bảo các loại cấu hình sau mà đang được áp dụng được lưu lại và không bị thay đổi trong lần khởi động kế tiếp:
  - ✓ Cấu hình hệ thống: Cấu hình hệ thống không bị thay đổi khi hệ thống được khởi động lại.
  - ✓ Cấu hình quản trị từ xa: Cấu hình hệ thống không bị thay đổi khi hệ thống được khởi động lại.
  - ✓ Cấu hình tài khoản xác thực và phân quyền người dùng: Cấu hình hệ thống không bị thay đổi khi hệ thống được khởi động lại.
  - ✓ Cấu hình tập luật bảo vệ: Cấu hình hệ thống không bị thay đổi khi hệ thống được khởi động lại.

2.2. Bảo vệ dữ liệu log

- Trong trường hợp phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), đảm bảo dữ liệu log đã được lưu lại không bị thay đổi trong lần khởi động kế tiếp.

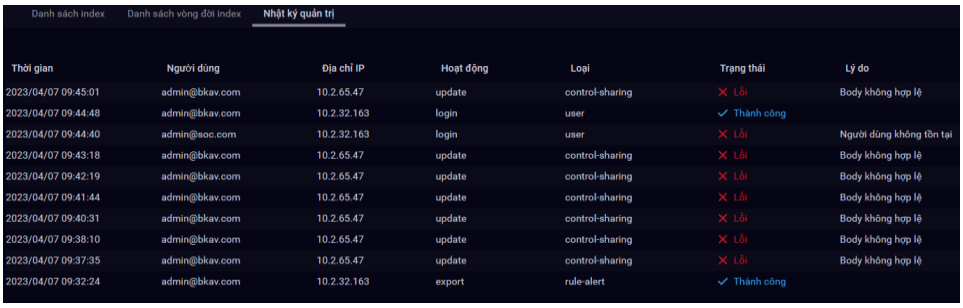
2.3. Đồng bộ thời gian hệ thống

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

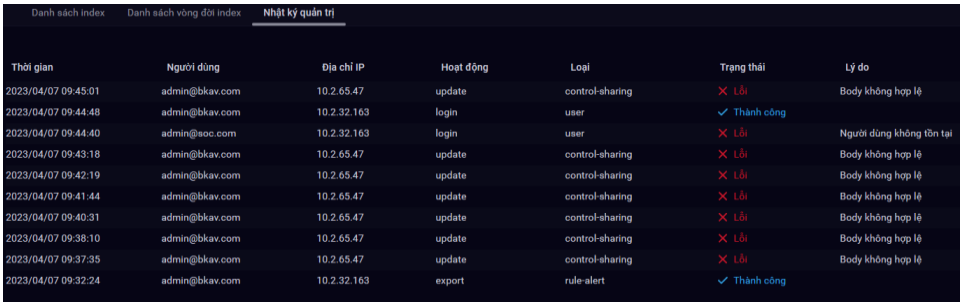
3. Chức năng về log

3.1. Log quản trị hệ thống

- Cho phép ghi log quản trị hệ thống về các loại sự kiện sau: Đăng nhập, đăng xuất tài khoản; 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 tập luật bảo vệ; Kích hoạt lệnh khởi động lại, tắt hệ thống; Thay đổi thủ công thời gian hệ thống

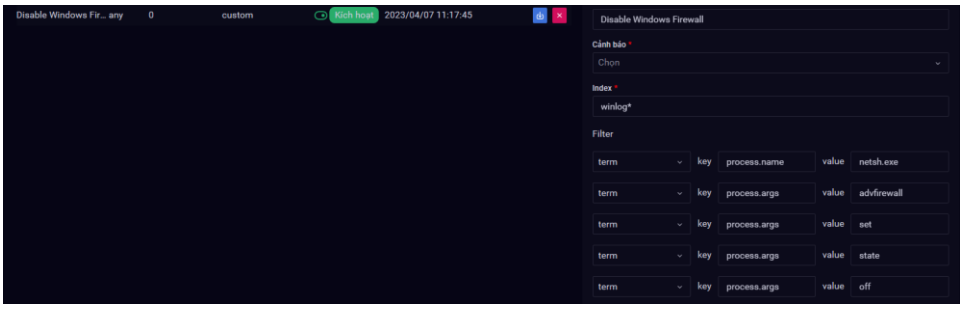


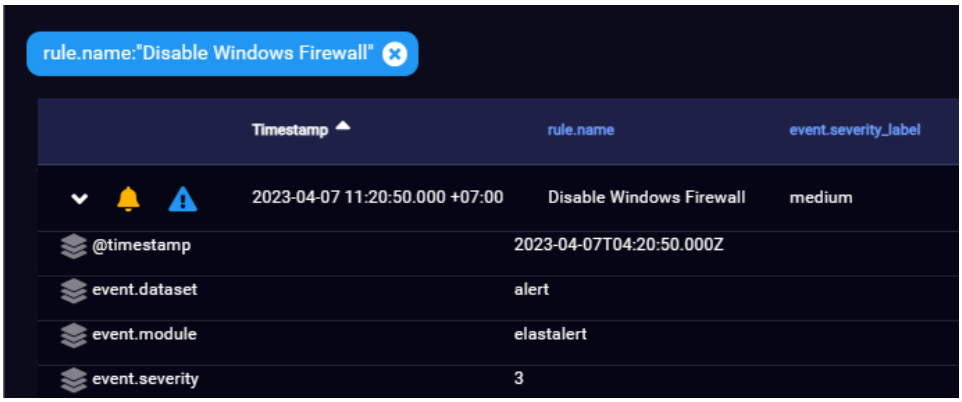
- Cho phép ghi log quản trị hệ thống có các trường thông tin sau: Thời gian sinh log (bao gồm năm, tháng, ngày, giờ, phút và giây); Địa chỉ IP hoặc định danh của máy; Định danh của tác nhân; Thông tin về hành vi thực hiện; Kết quả thực hiện hành vi (thành công hoặc thất bại); Lý do giải trình đối với hành vi thất bại



3.2. Log cảnh báo

- Cho phép ghi log cảnh báo được sinh ra bởi việc thực thi tập luật bảo vệ





3.3. Định dạng log

- Cho phép 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

```
Mar 12 01:18:58 10.10.8.254 date=2023-03-27 time=08:18:57 devname="YBI-EXT-FW02"
devid="FGT2KETB19900873" eventtime=1647047937724295741 tz="+0700" logid="0001000014" type="traffic"
subtype="local" level="notice" vd="root" srcip=fe80::2413:5cef:69aa:62cd srcport=53639 srcintf="port25"
srcintfrole="wan" dstip=ff02::c dstport=1900 dstintf="unknown0" dstintfrole="undefined"
sessionid=5154713 proto=17 action="deny" policyid=0 policytype="local-in-policy6" service="udp/1900"
trandisp="noop" app="udp/1900" duration=0 sentbyte=0 rcvdbyte=0 sentpkt=0 rcvdpkt=0 appcat="unscanned"
Mar 12 01:19:04 10.10.8.254 date=2023-03-27 time=08:19:03 devname="YBI-EXT-FW02"
devid="FGT2KETB19900873" eventtime=1647047943757528647 tz="+0700" logid="0001000014" type="traffic"
subtype="local" level="notice" vd="root" srcip=fe80::2413:5cef:69aa:62cd srcport=53639 srcintf="port25"
srcintfrole="wan" dstip=ff02::c dstport=1900 dstintf="unknown0" dstintfrole="undefined"
sessionid=5154784 proto=17 action="deny" policyid=0 policytype="local-in-policy6" service="udp/1900"
trandisp="noop" app="udp/1900" duration=0 sentbyte=0 rcvdbyte=0 sentpkt=0 rcvdpkt=0 appcat="unscanned"
Mar 12 01:19:07 10.10.8.254 date=2023-03-27 time=08:19:06 devname="YBI-EXT-FW02"
devid="FGT2KETB19900873" eventtime=1647047947165767570 tz="+0700" logid="0001000014" type="traffic"
subtype="local" level="notice" vd="root" srcip=fe80::2d85:ad84:a2bb:4888 srcport=53307 srcintf="port25"
srcintfrole="wan" dstip=ff02::1:3 dstport=5355 dstintf="unknown0" dstintfrole="undefined"
sessionid=5154842 proto=17 action="deny" policyid=0 policytype="local-in-policy6" service="udp/5355"
trandisp="noop" app="udp/5355" duration=0 sentbyte=0 rcvdbyte=0 sentpkt=0 rcvdpkt=0 appcat="unscanned"
```

(Log thô)

observer.type	observer.vendor	related.ip	rule.category	rule.id	rule.ruleset	sort	source.bytes	source.ip
firewall	Fortinet	["fe80::62ab:67…	unscanned	0	local-in-policy6	[1679879987000,…	0	fe80::62ab:67ff:fecf…
firewall	Fortinet	["fe80::62ab:67…	unscanned	0	local-in-policy6	[1679879987000,…	0	fe80::62ab:67ff:fecf…
firewall	Fortinet	["fe80::62ab:67…	unscanned	0	local-in-policy6	[1679879987000,…	0	fe80::62ab:67ff:fecf…
firewall	Fortinet	["fe80::62ab:67…	unscanned	0	local-in-policy6	[1679879987000,…	0	fe80::62ab:67ff:fecf…
firewall	Fortinet	["fe80::b990:ce…	unscanned	0	local-in-policy6	[1679879965000,…	0	fe80::b990:ce22:c3f…

destination.ip	destination.packets	destination.port	event.action	event.category	event.code
ff02::fb	0	5353	deny	["network"]	1000014
ff02::fb	0	5353	deny	["network"]	1000014
ff02::fb	0	5353	deny	["network"]	1000014
ff02::fb	0	5353	deny	["network"]	1000014
ff02::fb	0	5353	deny	["network"]	1000014

(Log sau khi chuẩn hóa)

3.4. Quản lý log

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

```
21    log_size_limit: 46 # GB
22    node_route_type: 'hot'
```

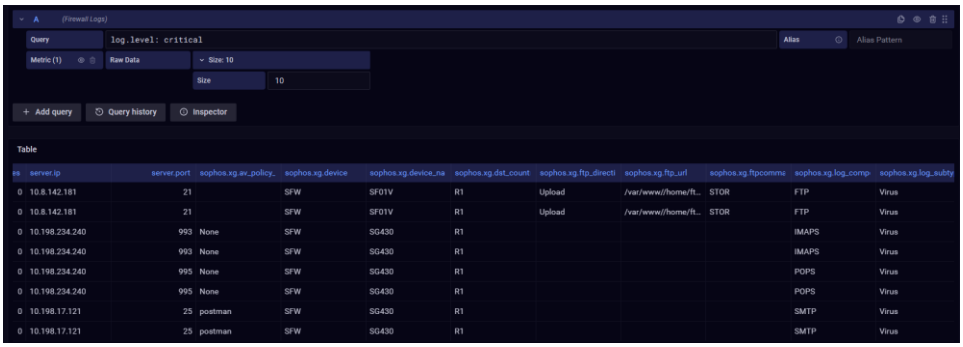
(Ngưỡng giới hạn dung lượng lưu trữ log)

Index	Warm	Đóng	Xóa	Trạng thái
so-firewall	7	30	365	Đã được quản lý
so-zeek	7	45	365	Đã được quản lý
so-osquery	4	35	365	Đã được quản lý
so-syslog	7	6	9	Đã được quản lý
so-strelka	7	6	30	Đã được quản lý
so-ossec	7	30	365	Đã được quản lý

(Ngưỡng thời gian lưu trữ log)

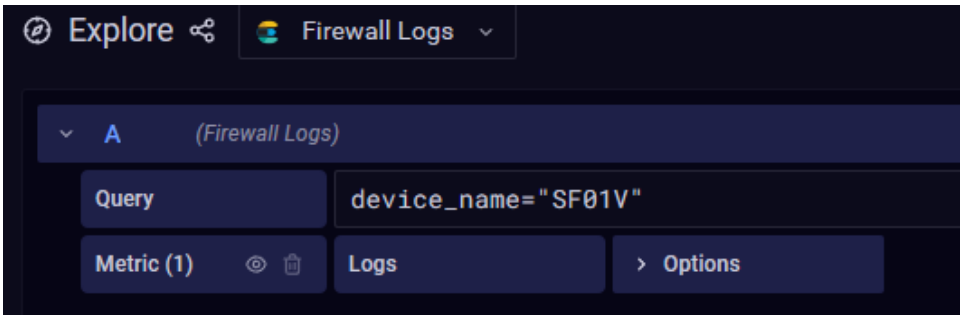
3.4. Quản lý log (tiếp)

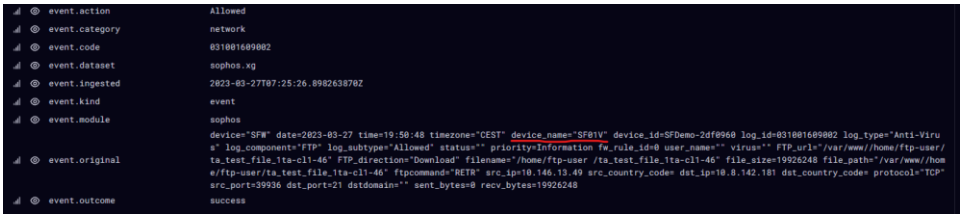
- Cho phép tìm kiếm log theo từ khóa trên tất cả các trường thông tin bao gồm cả các trường thông tin cấp thấp hơn (nếu có)



- Cho phép phân nhóm log thành các nhóm sự kiện theo các tiêu chí khác nhau

- Cho phép truy xuất dữ liệu thô của log thông qua kết quả tìm kiếm và cảnh báo





3.4. Quản lý log (tiếp)

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

3.5. Cách thức tiếp cận log

Cho phép tiếp nhận log gửi từ Collector thông qua các cách thức sau:

- Tiếp nhận log qua kết nối UDP

```
input {
  udp {
    port => "5045"
  }
}
```

- Tiếp nhận log qua kết nối TCP không mã hóa

```
input {
  tcp {
    port => "5045"
  }
}
```

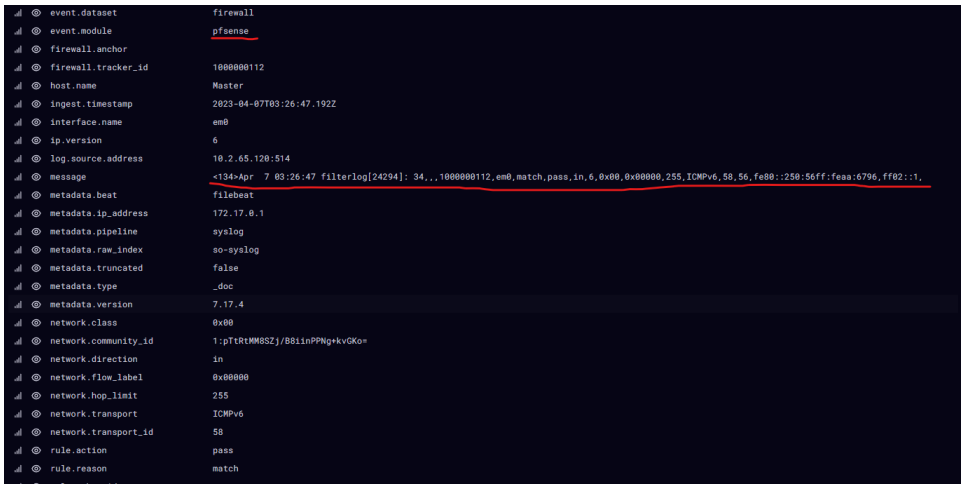
- Tiếp nhận log qua kết nối TCP có mã hóa như TLS

```
input {
  tcp {
    port => "5046"
    ssl_enable => true
    ssl_cert => "/etc/pki/tls/myCA/server_crt.pem"
    ssl_key => "/etc/pki/tls/myCA/server_key.pem"
    ssl_cacert => "/etc/pki/tls/myCA/cacert.pem"
  }
}
```

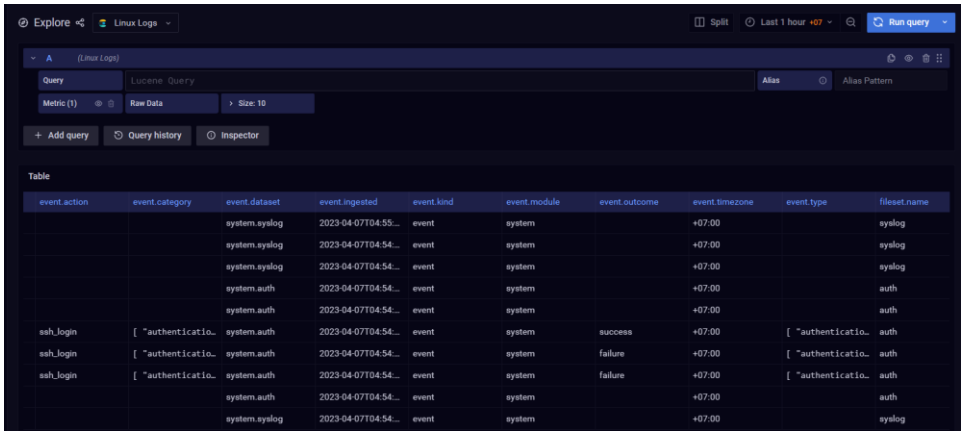
3.6. Chuẩn hóa log

Cho phép tiếp nhận và chuẩn hóa log gửi từ Collector theo tối thiểu 10 loại log khác nhau:

- Chuẩn hóa được log theo các định dạng tệp tin các định dạng bao gồm: SYSLOG, JSON, CSV, CEF, NETFLOW

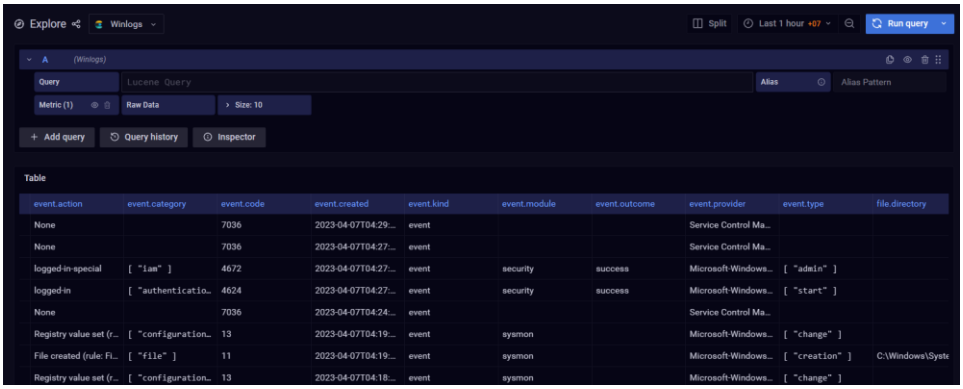


- Chuẩn hóa được log của hệ điều hành Windows và Unix



3.6. Chuẩn hóa log (tiếp)

- Chuẩn hóa được log của hệ điều hành Windows và Unix



- Chuẩn hóa được log của các loại tường lửa khác nhau như là: Pfsence, Barracuda, Fortinet, Checkpoint, Sophos, Cisco, Palo Alto Networks, Juniper SRX Firewalls

- Chuẩn hóa được log của các loại thiết bị mạng khác nhau như là: Juniper, TP-Link, Cisco, DrayTek

3.6. Chuẩn hóa log (tiếp)

- Chuẩn hóa được log của các loại thiết bị mạng khác nhau như là: Juniper, TP-Link, Cisco, DrayTek (tiếp)

event.module	highlight	message	sort	source.ip	source.mac	source.port
draytek		Local User (MAC=0...	[1678333917000,...	192.168.10.12	0C-C4-7A-C8-B6-2F	
draytek		Local User (MAC=0...	[1678333916000,...	192.168.10.12	0C-C4-7A-C8-B6-2F	
draytek		Local User (MAC=0...	[1678333916000,...	192.168.10.12	0C-C4-7A-C8-B6-2F	
draytek		Local User (MAC=0...	[1678333915000,...	192.168.10.12	0C-C4-7A-C8-B6-2F	25575
draytek		Local User (MAC=0...	[1678333915000,...	192.168.10.12	0C-C4-7A-C8-B6-2F	
draytek		Local User (MAC=0...	[1678333915000,...	192.168.10.12	0C-C4-7A-C8-B6-2F	
draytek		Local User (MAC=0...	[1678333914000,...	192.168.10.12	0C-C4-7A-C8-B6-2F	
draytek		Local User (MAC=0...	[1678333914000,...	192.168.10.12	0C-C4-7A-C8-B6-2F	
draytek		Local User (MAC=0...	[1678333913000,...	192.168.10.12	0C-C4-7A-C8-B6-2F	
draytek		Local User (MAC=0...	[1678333913000,...	192.168.10.12	0C-C4-7A-C8-B6-2F	26571

cisco.ios.facility	event.code	event.dataset	event.module	event.severity	highlight	log.original	message
SYS	CONFIG_I	ios	cisco	5		00:00:48: %SYS-5-C...	Configured from co...
SYS	CONFIG_I	ios	cisco	5		00:00:48: %SYS-5-C...	Configured from co...
LINEPROTO	UPDOWN	ios	cisco	5		00:00:48: %LINEPR...	Line protocol on Int...
LINEPROTO	UPDOWN	ios	cisco	5		00:00:48: %LINEPR...	Line protocol on Int...
LINK	UPDOWN	ios	cisco	3		00:00:47: %LINK-3-...	Interface GigabitEth...
LINK	UPDOWN	ios	cisco	3		00:00:47: %LINK-3-...	Interface GigabitEth...
LINK	UPDOWN	ios	cisco	3		00:00:46: %LINK-3-...	Interface Port-chan...

3.7. Đồng bộ hóa thời gian log

- Cho phép đồng bộ hóa thời điểm log được tiếp nhận tại Receiver và thời điểm log được thu thập tại Collector dựa trên cài đặt về múi giờ đã được thiết lập.

3.8. Lưu trữ log dưới dạng dữ liệu thô

- Cho phép lưu trữ tất cả log dưới dạng dữ liệu thô bất kể có thể phân tích cú pháp được hay không. Dữ liệu thô được lưu trữ nguyên bản trong database dưới dạng một trường dữ liệu cho dù được phân tích hay không. Người dùng có thể tìm kiếm toàn văn trên trường dữ liệu này.

_index	so-cisco
_source	[object Object]
_type	_doc
cisco.ios.facility	SYS
event.code	CONFIG_I
event.dataset	ios
event.module	cisco
event.severity	5
log.original	00:00:48: %SYS-5-CONFIG_I: Configured from console by ijbrown on vty0 (172.25.1.1)
message	Configured from console by ijbrown on vty0 (172.25.1.1)
sort	1679474533337,6

3.9. Làm giàu thông tin

- Cho phép làm giàu thông tin cho log (phân giải chuỗi ký tự định danh thành tên tài khoản người dùng; tọa độ, vị trí địa lý cho địa chỉ IP public; lưu lại thời gian sinh log theo múi giờ cục bộ tại máy)

Tên máy	IP	Đơn vị	Mã độc	Tên máy	IP	Đơn vị	Lỗ hổng
tranquang-pc-71mdd	127.0.0.1	so tttt	w32.xfileusb.worm	zqc9vuemdplri7r-02579	192.168.1.41	so nnptnt	ms15-034
tranquang-pc-71mdd	14.185.207.85	so tttt	w32.xfileusb.worm	zqc9vuemdplri7r-02579	192.168.1.41	so nnptnt	ms15-029
thaiquochung-yl428	192.168.1.30	so gtvt	w97m.foz	zqc9vuemdplri7r-02579	192.168.1.41	so nnptnt	ms15-028

(Phân giải chuỗi ký tự định danh thành tên tài khoản người dùng)

destination.geo.conti	destination.geo.coun	destination.geo.coun	destination.geo.ip
Europe	GB	United Kingdom	149.154.167.220
Europe	GB	United Kingdom	149.154.167.220
Asia	VN	Vietnam	103.245.249.90
Asia	VN	Vietnam	103.245.249.90

(Tọa độ, vị trí địa lý cho địa chỉ IP public)

```
"syslog": {
  "severity": 6,
  "priority": 134,
  "facility": 16,
  "severity_label": "INFO",
  "timestamp": "May 22 06:44:24",
  "facility_label": "LOCAL0"
},
```

(Thời gian sinh log)

3.10. Giám sát hiệu năng quá trình tiếp nhận log

Cho phép giám sát thông qua giao diện đồ họa các thông số hiệu năng sau của quá trình tiếp nhận log:

- Số lần thử kết nối lại đến Collector

(Trường Reconnect)

- Thông báo về kết nối không thành công đến Collector

(Trường Status)

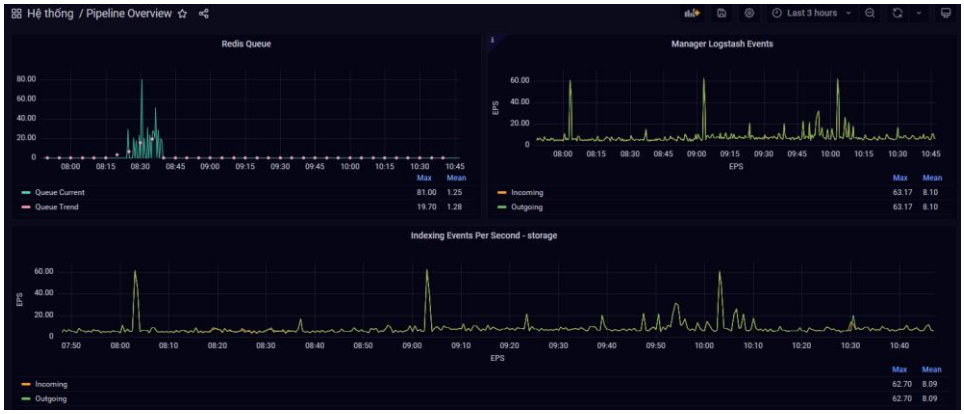
- Số lượng tác vụ tiếp nhận log mà không được thực hiện thành công

(Trường Missing)

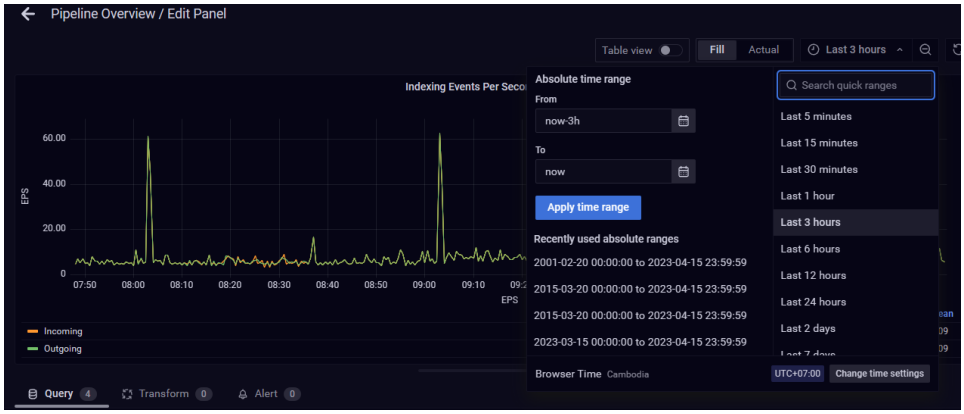
3.11. Giám sát log tiếp nhận được theo thời gian thực

Cho phép giám sát thông qua giao diện đồ họa log gửi từ Collector:

- Tạo thống kê dữ liệu theo thời gian thực

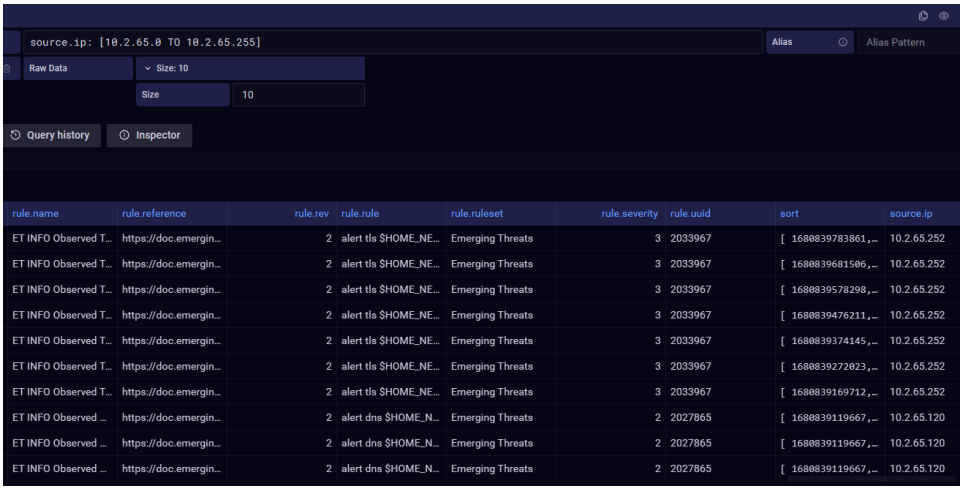


- Cho phép tìm kiếm và tạo thống kê dữ liệu theo khoảng thời gian xác định



3.12. Xử lý thông tin trong log có kiểu dữ liệu địa chỉ IP

- Cho phép xử lý thông tin trong log có kiểu dữ liệu địa chỉ IP theo định dạng IPv4. Phần mềm có khả năng xử lý truy vấn tìm kiếm dữ liệu bằng dải địa chỉ IP



rule.name	rule.reference	rule.rev	rule.rule	rule.ruleset	rule.severity	rule.uuid	sort	source.ip
ET INFO Observed T...	https://doc.emergin...	2	alert tls $HOME_NE...	Emerging Threats	3	2033967	[1680839783861,...	10.2.65.252
ET INFO Observed T...	https://doc.emergin...	2	alert tls $HOME_NE...	Emerging Threats	3	2033967	[1680839681506,...	10.2.65.252
ET INFO Observed T...	https://doc.emergin...	2	alert tls $HOME_NE...	Emerging Threats	3	2033967	[1680839578298,...	10.2.65.252
ET INFO Observed T...	https://doc.emergin...	2	alert tls $HOME_NE...	Emerging Threats	3	2033967	[1680839476211,...	10.2.65.252
ET INFO Observed T...	https://doc.emergin...	2	alert tls $HOME_NE...	Emerging Threats	3	2033967	[1680839374145,...	10.2.65.252
ET INFO Observed T...	https://doc.emergin...	2	alert tls $HOME_NE...	Emerging Threats	3	2033967	[1680839272023,...	10.2.65.252
ET INFO Observed T...	https://doc.emergin...	2	alert tls $HOME_NE...	Emerging Threats	3	2033967	[1680839169712,...	10.2.65.252
ET INFO Observed ...	https://doc.emergin...	2	alert dns $HOME_N...	Emerging Threats	2	2027865	[1680839119667,...	10.2.65.120
ET INFO Observed ...	https://doc.emergin...	2	alert dns $HOME_N...	Emerging Threats	2	2027865	[1680839119667,...	10.2.65.120
ET INFO Observed ...	https://doc.emergin...	2	alert dns $HOME_N...	Emerging Threats	2	2027865	[1680839119667,...	10.2.65.120

3.13. Truyền dữ liệu an toàn

- Cho phép mã hóa dữ liệu để trao đổi dữ liệu giữa Collector và Receiver

```
1333 output:
1334   enabled: true
1335   hosts:
1336     - "Master:5644" #10.2.65.215
1337   loadbalance: false
1338   worker: 1
1339   bulk_max_size: 2048
1340   ssl.verification_mode: full
1341   ssl.supported_protocols: [TLSv1.0, TLSv1.1, TLSv1.2]
1342   ssl.certificate_authorities: ["/usr/share/receiver/intraca.crt"]
1343   ssl.certificate: "/usr/share/receiver/receiver.crt"
1344   ssl.key: "/usr/share/receiver/receiver.key"
1345
```

4. Hiệu năng xử lý

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

- Đảm bảo rằng độ trễ thời gian tìm kiếm log với độ phức tạp bất kỳ, có phản hồi trong khoảng thời gian tối đa là 02 phút

4.2. Xử lý đồng thời nhiều tác vụ

Cho phép xử lý đồng thời tối thiểu 03 tác vụ khác nhau:

- Tiếp nhận log theo thời gian thực đồng thời từ tối thiểu 03 nguồn log khác nhau.

Index	Tình trạng	Trạng thái	Primary shards	Replicas	Docs count	Docs deleted	Store size	Primary store size
so-zeek-2023.04.07	green	open	2	0	68923	0	82.5mb	82.5mb
so-firewall-2023.04.07	green	open	1	0	1674	0	2mb	2mb
so-ossec-2023.04.07	green	open	1	0	18478	0	32.1mb	32.1mb
so-elasticsearch-2023....	green	open	1	0	271	0	506.9kb	506.9kb
so-kibana-2023.04.07	green	open	1	0	4	0	69kb	69kb
so-zeek_dns-2023.04.07	green	open	2	0	20070	0	21.1mb	21.1mb
so-beats-2023.04.07	green	open	1	0	7115	0	7.2mb	7.2mb
so-ids-2023.04.07	green	open	1	0	546	0	2.4mb	2.4mb
so-syslog-2023.04.07	green	open	1	0	336	0	352.1kb	352.1kb

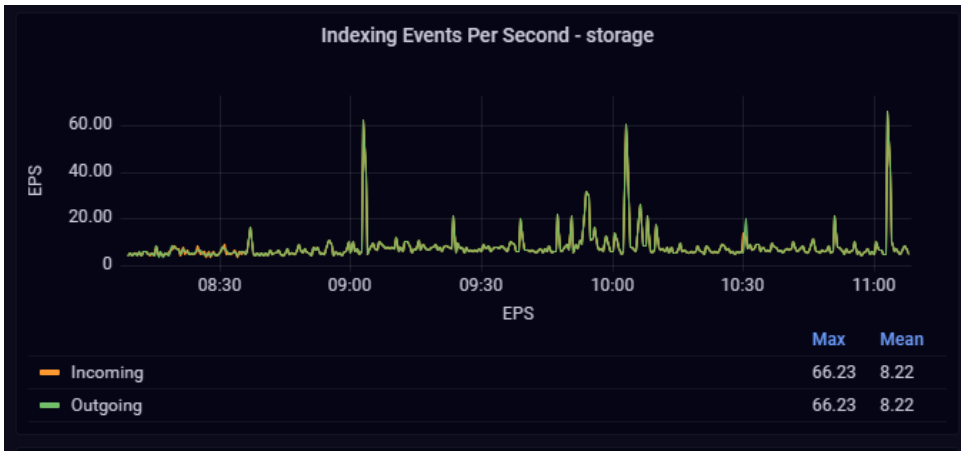
(Hệ thống đang tiếp nhận nhiều nguồn log khác nhau cùng lúc)

4.2. Xử lý đồng thời nhiều tác vụ (tiếp)

- Có khả năng xử lý đồng thời theo thời gian thực tối thiểu 02 tác vụ cho việc tìm kiếm log và phân tích tương quan sự kiện

4.3. Xử lý đồng thời nhiều sự kiện

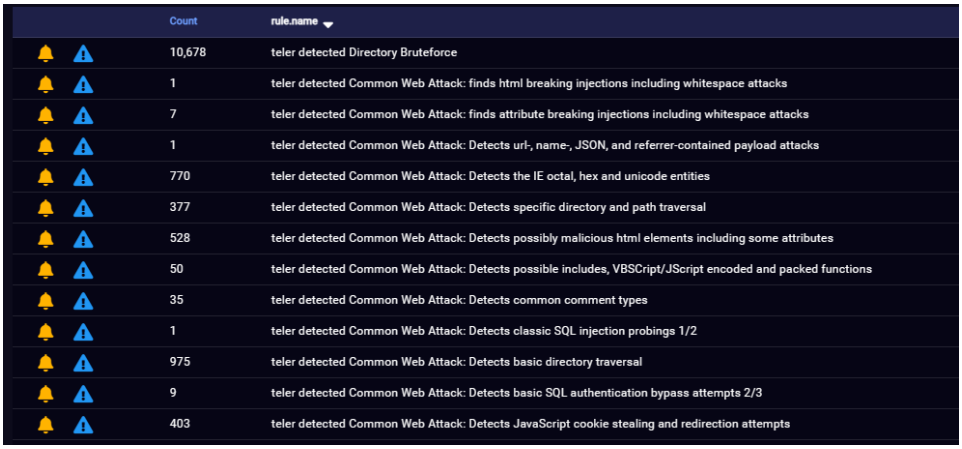
- Tối thiểu cho phép xử lý và lưu trữ dữ liệu đồng thời 5.000 sự kiện trong khoảng thời gian là 01 giây.



5. Chức năng tự bảo vệ

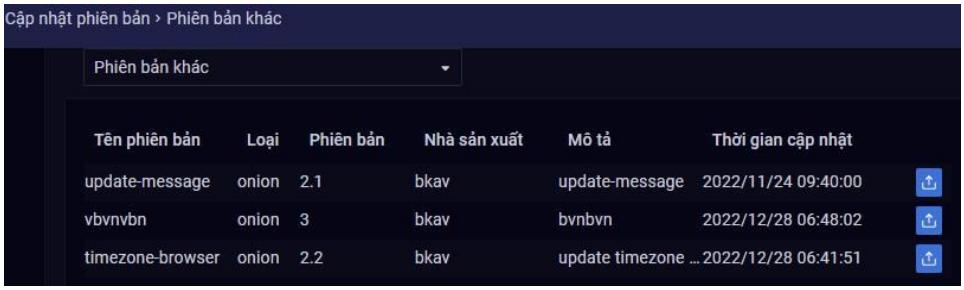
5.1. Phát hiện và ngăn chặn tấn công hệ thống

- Có khả năng tự bảo vệ, ngăn chặn các dạng tấn công phổ biến sau vào giao diện ra bên ngoài của hệ thống, bao gồm các dạng sau:
  - ✓ SQL Injection; OS Command Injection; XPath Injection; Remote File Inclusion (RFI)
  - ✓ Local File Inclusion (LFI)
  - ✓ Cross-Site Scripting (XSS)
  - ✓ Cross-Site Request Forgery (CSRF)



5.2. Cập nhật bản vá hệ thống

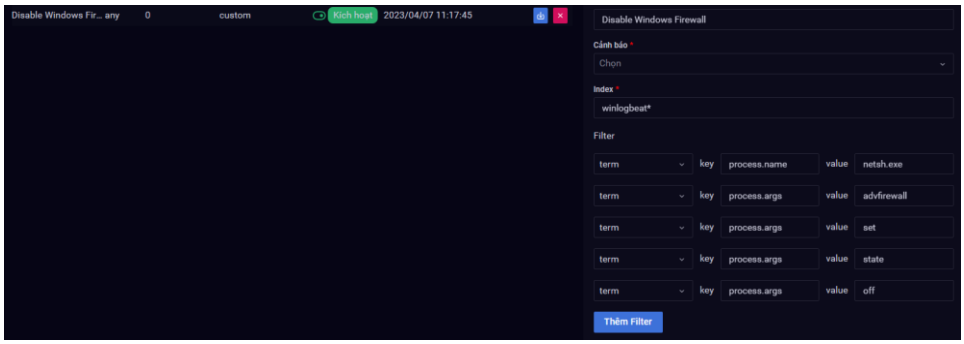
- Có chức năng cho phép cập nhật bản vá để xử lý các điểm yếu, lỗ hổng bảo mật



6. Chức năng phân tích tương quan sự kiện và cảnh báo

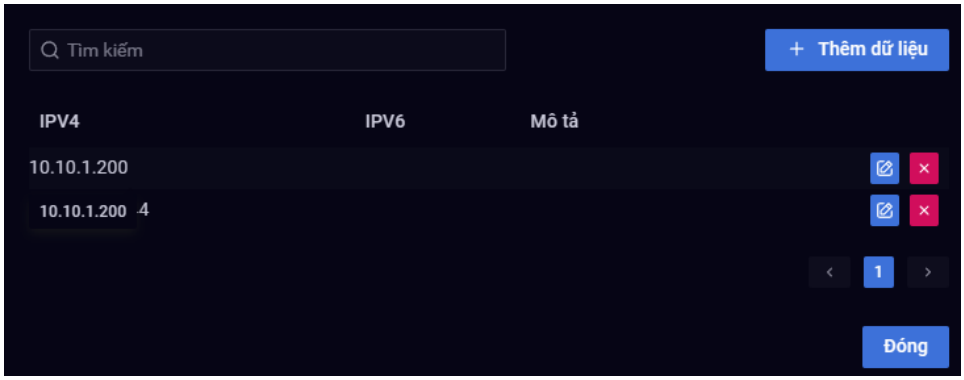
6.1. Phân tích tương quan sự kiện theo thời gian thực

- Cho phép phân tích tương quan sự kiện theo thời gian thực đối với dữ liệu log thu thập được



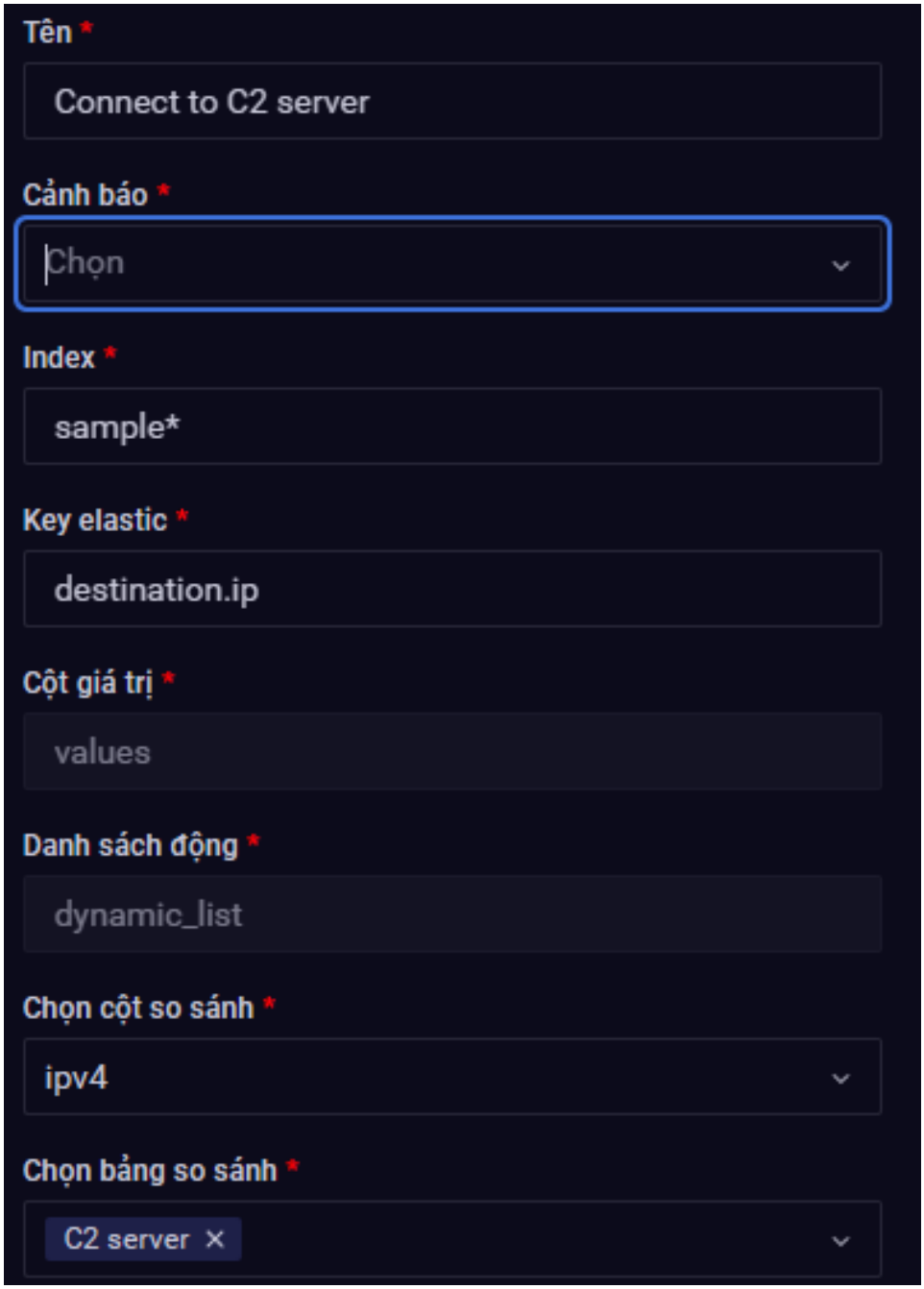
6.2. Phân tích tương quan sự kiện sử dụng danh sách động

- Cho phép phân tích tương quan sự kiện sử dụng thông tin trong danh sách động



6.2. Phân tích tương quan sự kiện sử dụng danh sách động (tiếp)

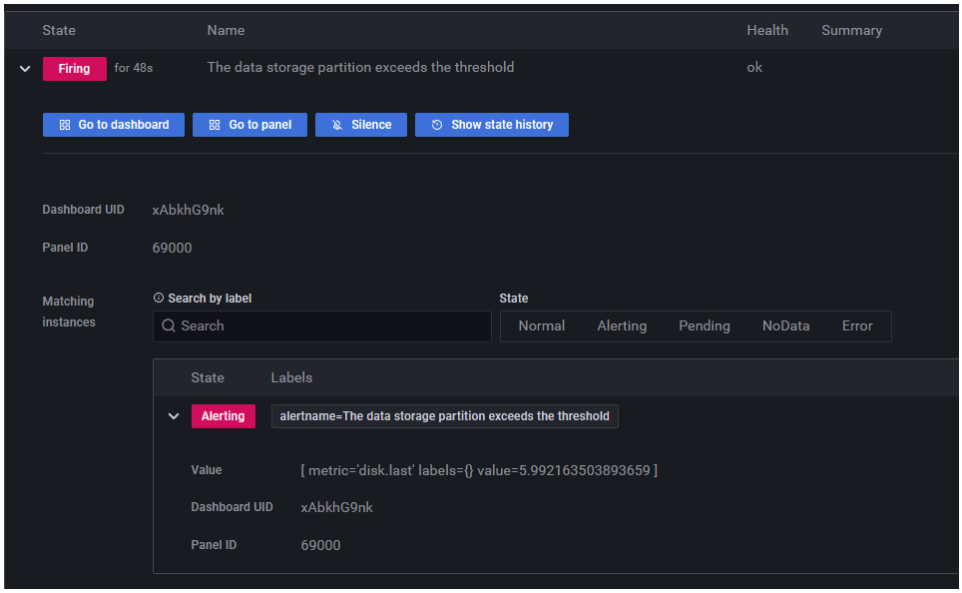
- Cho phép phân tích tương quan sự kiện sử dụng thông tin trong danh sách động (tiếp)



6.3. Cảnh báo theo thời gian thực

Cho phép tự động cảnh báo tới người dùng theo thời gian thực đối với các loại sự kiện sau:

- Cảnh báo về việc hệ thống ngừng lưu trữ thêm dữ liệu mới khi Storage đã đạt ngưỡng giới hạn lưu trữ mà không thể lưu được dữ liệu mới

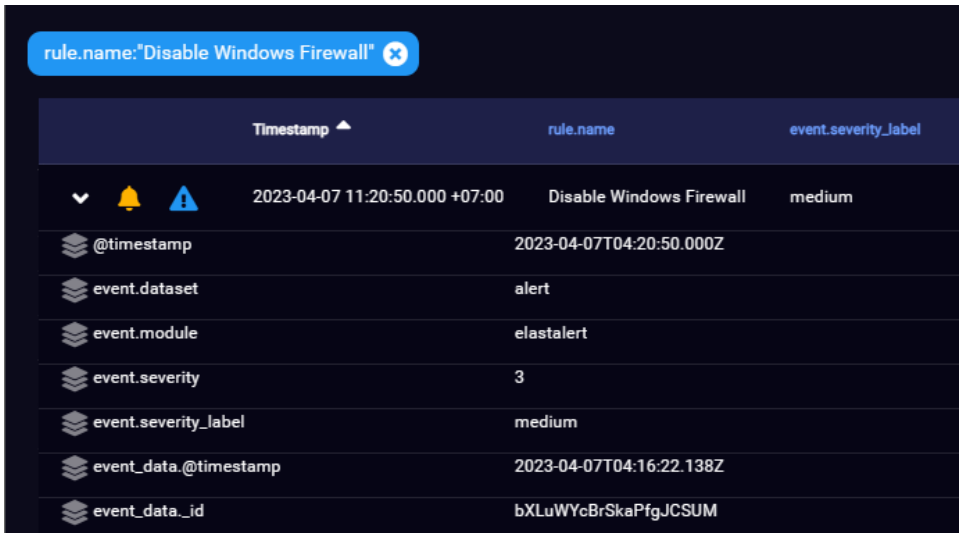


(Cảnh báo dung lượng lưu trữ đạt tới ngưỡng giới hạn được cấu hình)

```
21    log_size_limit: 46 # GB
22    node_route_type: 'hot'
```

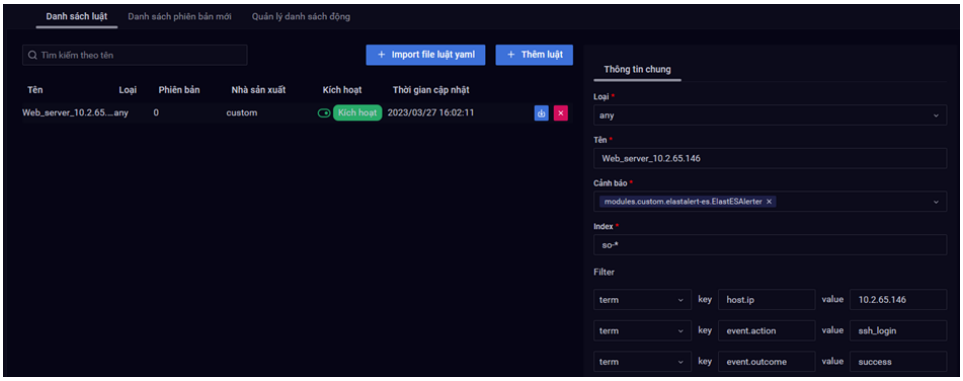
(Phần mềm tự động xóa log khi dung lương lưu trữ đạt tới giá trị "log_size_limit". Vì vậy, hệ thống luôn đảm bảo có thể lưu trữ dữ liệu mới vào CSDL ➔ không có cảnh báo)

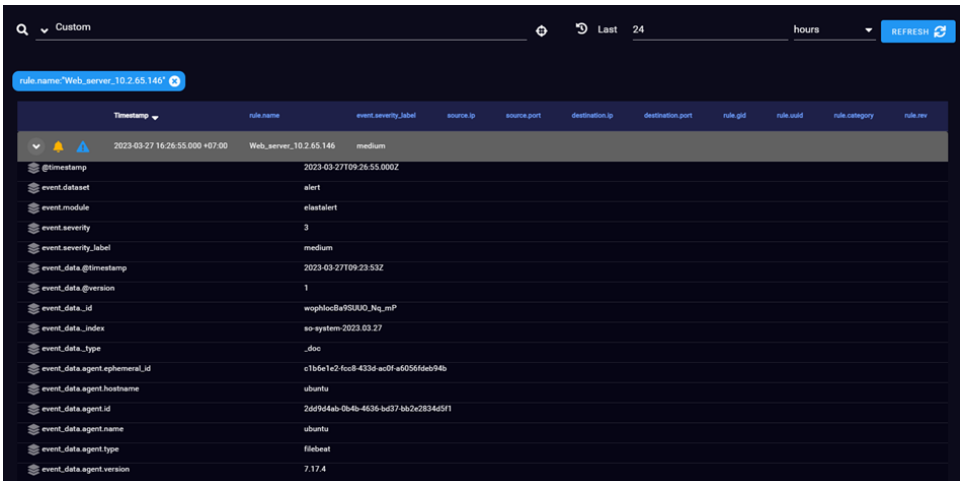
- Cảnh báo về dấu hiệu, nguy cơ, sự cố, cuộc tấn công và các hành vi gây mất an toàn thông tin khác dựa trên kết quả thực thi luật phân tích tương quan sự kiện



6.4. Cảnh báo về nhóm đối tượng được giám sát

- Cho phép sinh cảnh báo chứa các thông tin thuộc nhóm đối tượng được giám sát: cảnh báo có truy cập từ xa vào dải địa chỉ IP dành cho các máy chủ.





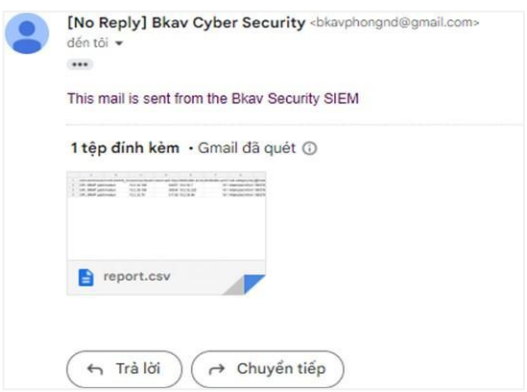
(Cảnh báo khi máy chủ được truy cập từ xa qua giao thức SSH)

6.5. Cảnh báo theo nhiều phương thức

Cho phép tự động cảnh báo theo các phương thức sau:

- Hiển thị nội dung cảnh báo trên giao diện đồ họa về quản lý cảnh báo

- Cảnh báo qua phương thức gửi thư điện tử hoặc tin nhắn SMS



7. Tài liệu

- Hướng dẫn triển khai và thiết lập cấu hình
- Hướng dẫn sử dụng và quản trị

8. Hiệu quả của hệ thống

8.1. Thu thập, xử lý, phân tích Log

- Có khả năng tiếp nhận log của 04 nguồn log thiết yếu: thiết bị mạng (Router, Switch), thiết bị bảo mật (Firewall, NIDS, Endpoint AV server), hệ điều hành (Linux, Windows), ứng dụng (Web, Mail, DNS, DHCP)

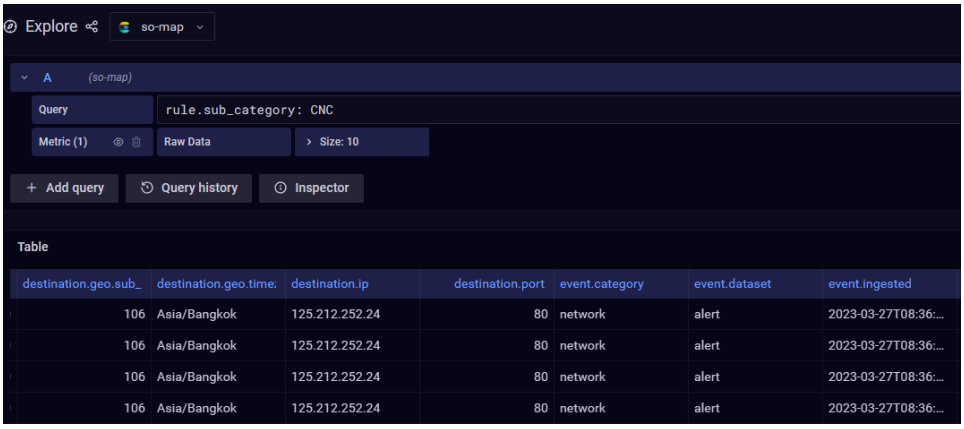
Index	Tình trạng	Trạng thái	Primary shards	Replicas	Docs count
so-zeek-2023.04.07	green	open	2	0	84962
so-firewall-2023.04.07	green	open	1	0	2617
so-linux.system-2023.0...	green	open	1	0	10
so-mail-2023.04.07	green	open	1	0	0
so-kibana-2023.04.07	green	open	1	0	5
so-endpoint-2023.04.07	green	open	1	0	20
so-apache.access-202...	green	open	1	0	17
so-zeek_dns-2023.04.07	green	open	2	0	25091
so-dhcp-2023.04.07	green	open	1	0	0
so-beats-2023.04.07	green	open	1	0	9742
so-ossec-2023.04.07	green	open	1	0	19592
so-windows.system-20...	green	open	1	0	22
so-ids-2023.04.07	green	open	1	0	664
so-elasticsearch-2023....	green	open	1	0	354
so-syslog-2023.04.07	green	open	1	0	404

8.2. Phân tích phát hiện tấn công dựa vào phân tích lưu lượng mạng

- Có khả năng phát hiện tấn công cơ bản lớp mạng

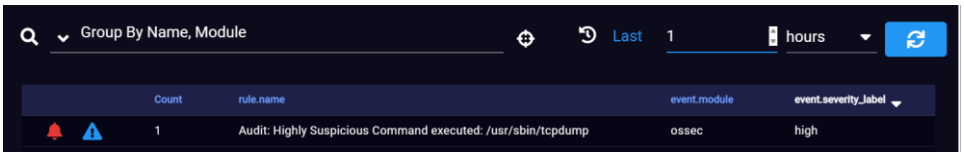
Count	rule.name	event.module	event.severity_label
4	ET POLICY GNU/Linux YUM User-Agent Outbound likely related to package management	suricata	high
2	ET INFO Session Traversal Utilities for NAT (STUN Binding Request On Non-Standard High Port)	suricata	high
2	ET POLICY SSL/TLS Certificate Observed (AnyDesk Remote Desktop Software)	suricata	high
1	ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted	suricata	high
1	ET POLICY Outgoing Basic Auth Base64 HTTP Password detected unencrypted	suricata	high
1	ET USER_AGENTS AnyDesk Remote Desktop Software User-Agent	suricata	high
340	ET INFO Observed DNS Query to .cloud TLD	suricata	medium
33	ET INFO Observed DNS Query to .biz TLD	suricata	medium

- Khả năng phát hiện kết nối đến máy chủ điều khiển của mã độc

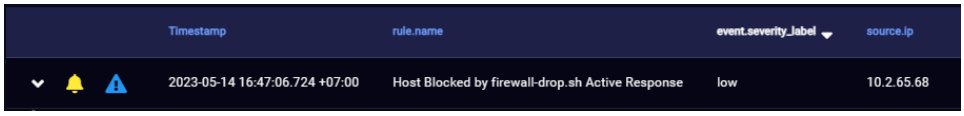


8.3. Phân tích phát hiện tấn công Endpoints, Server

- Có khả năng phát hiện các hành vi bất thường như:
  - ✓ Chạy các lệnh nguy hiểm

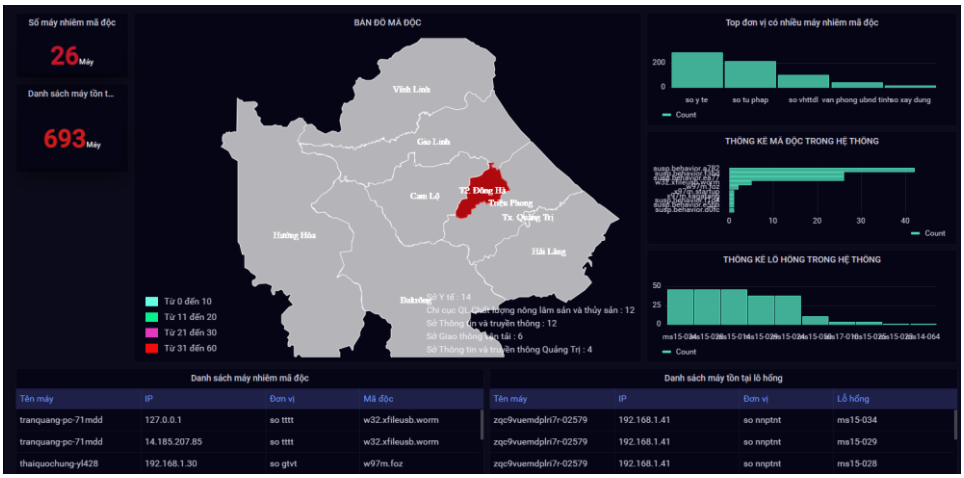


  - ✓ Ngăn chặn từ trung tâm khi cần thiết



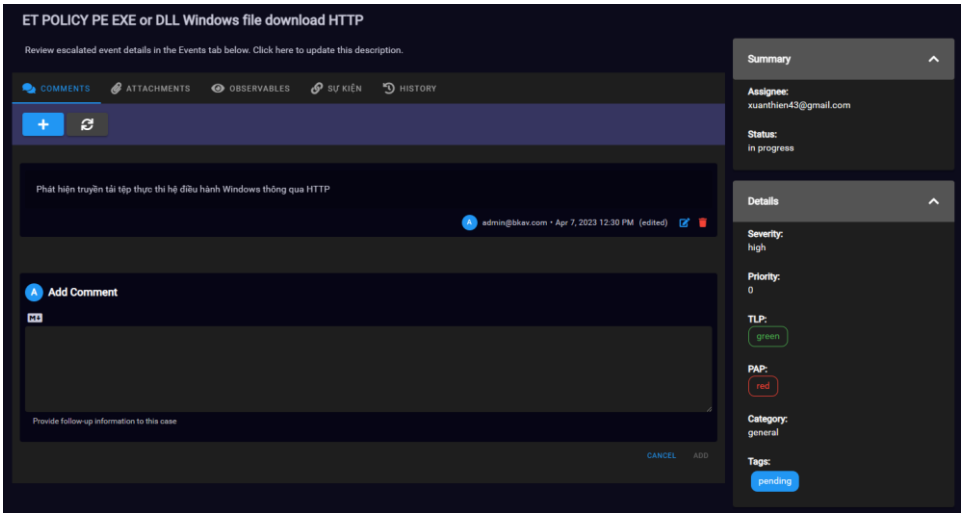
8.4. Phát hiện, ngăn chặn tấn công lớp ứng dụng

- Tích hợp được với giải pháp có sẵn đang có (giải pháp quản lý mã độc tập trung sẵn có)



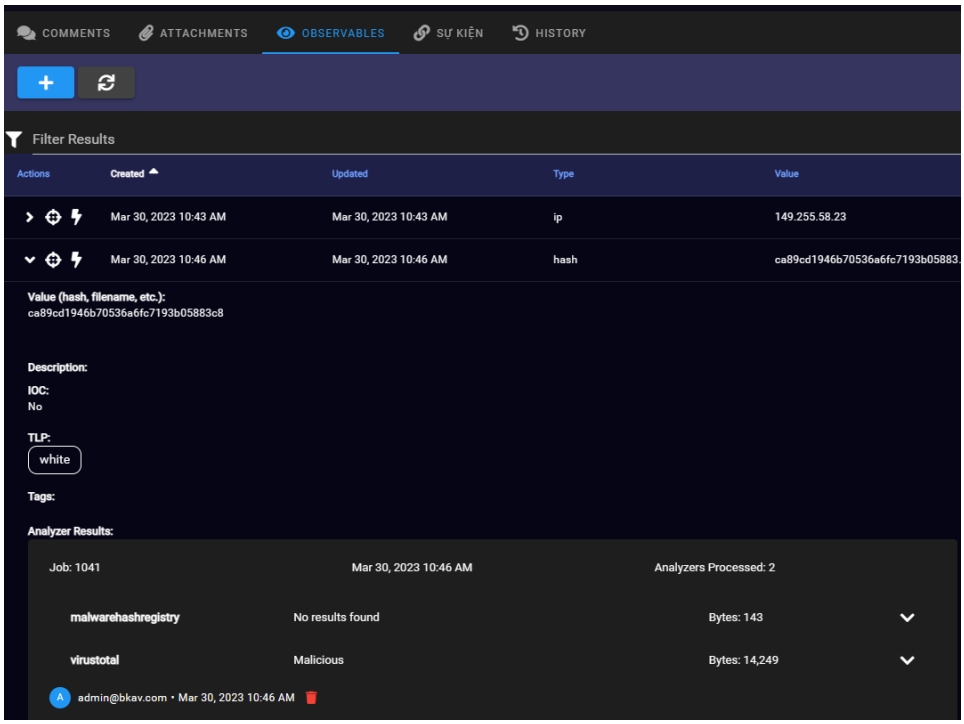
8.5. Quản lý, phân tích, cảnh báo

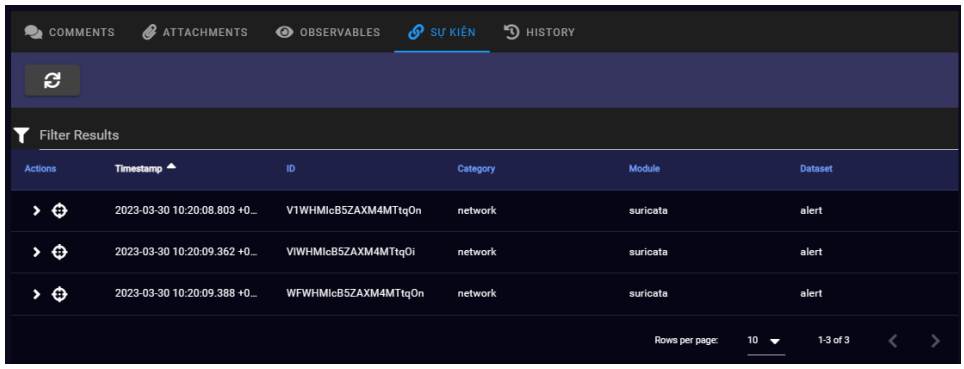
- Có hệ thống phần mềm hỗ trợ khách hàng đảm bảo có các thông tin: Chi tiết về sự cố, tương quan giữa các sự kiện, mức độ, tình trạng xử lý

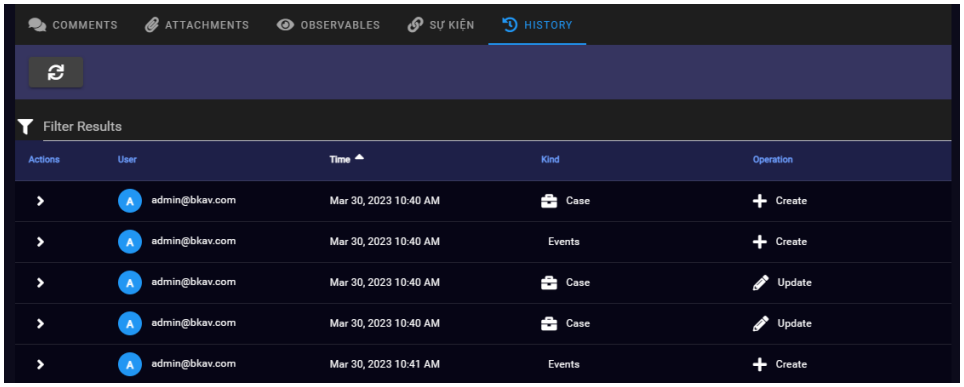


8.5. Quản lý, phân tích, cảnh báo (tiếp)

- Có hệ thống phần mềm hỗ trợ khách hàng đảm bảo có các thông tin: Chi tiết về sự cố, tương quan giữa các sự kiện, mức độ, tình trạng xử lý (tiếp)





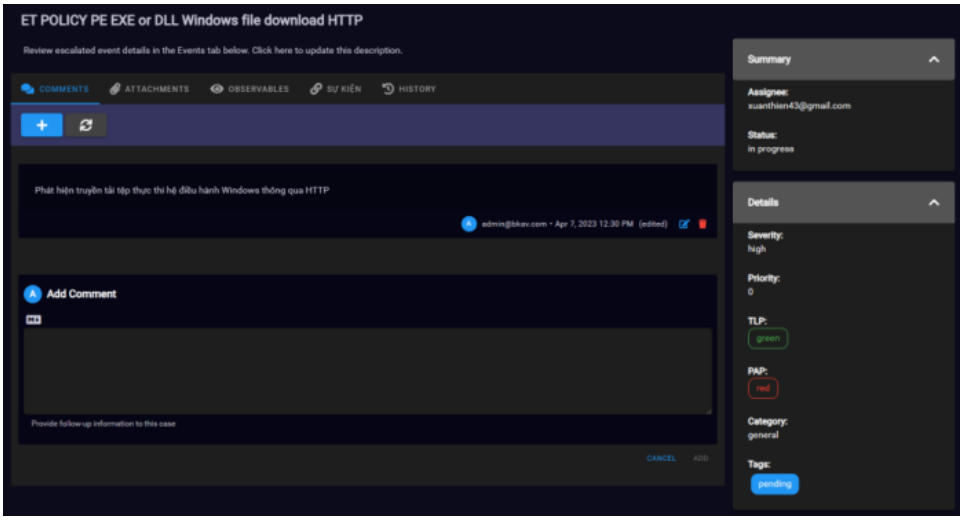


9. Chức năng khác

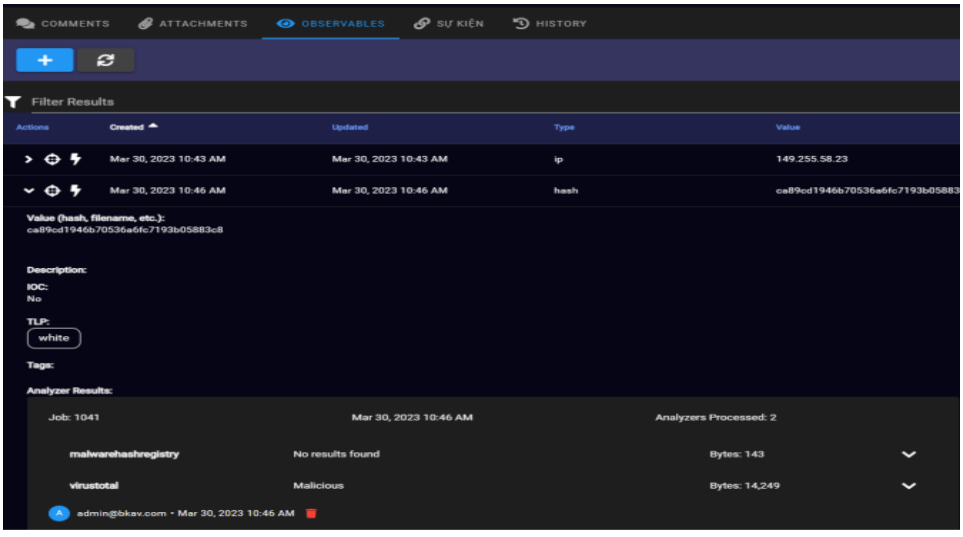
- Tạo kênh kết nối an toàn giữa SOC Master đến các thành phần trong hệ thống.

```
39    transport:
40      ssl:
41        enabled: true
42        verification_mode: none
43        key: /usr/share/master/config/master.key
44        certificate: /usr/share/master/config/master.crt
45        certificate_authorities:
46        - /usr/share/master/config/ca.crt
47    http:
48      ssl:
49        enabled: true
50        client_authentication: none
51        key: /usr/share/master/config/master.key
52        certificate: /usr/share/master/config/master.crt
53        certificate_authorities:
54        - /usr/share/master/config/ca.crt
```

- Tiếp nhận các dữ liệu metadata từ hệ thống thu thập dữ liệu SOC Sensor theo thời gian thực.
- Tích hợp module SOP, giúp phản ứng nhanh khi gặp sự cố, tạo quy trình xử lý và gán việc xử lý theo tình huống, sự cố cụ thể.

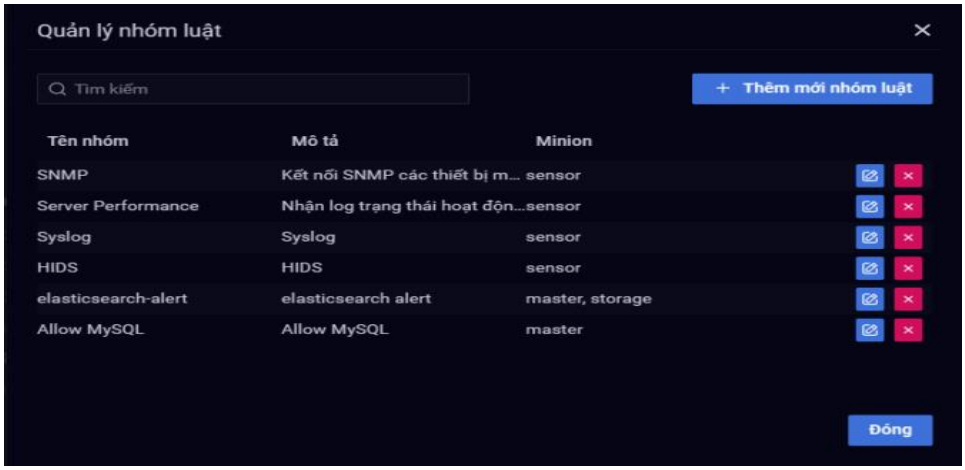


- Tích hợp module Investigation, giúp quản trị viên và các chuyên gia điều tra, xử lý sự cố; cho phép phân tích dữ liệu raw log, mã hóa, giải mã, tính toán hàm băm để phục vụ phân tích.

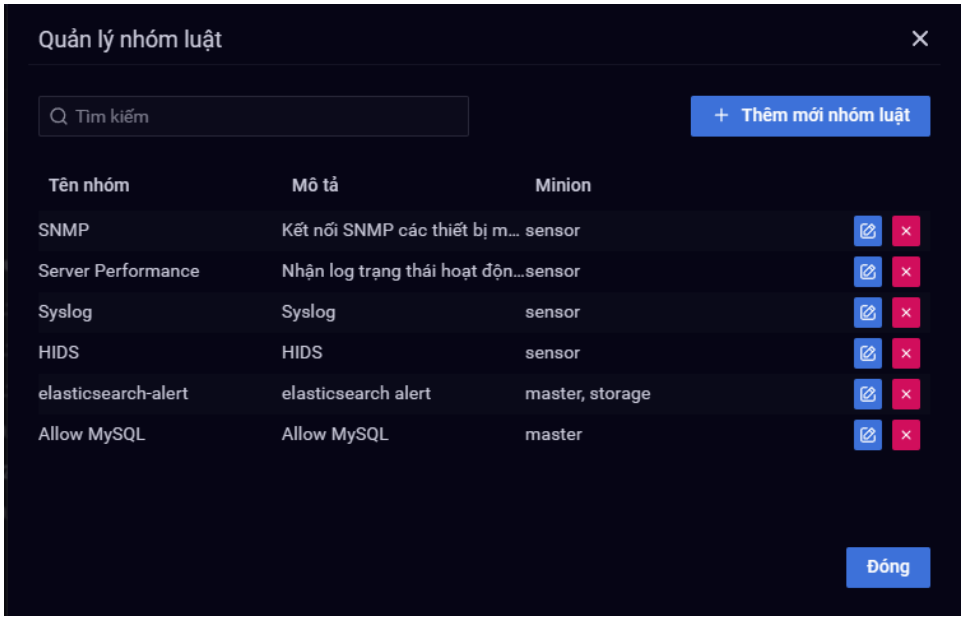


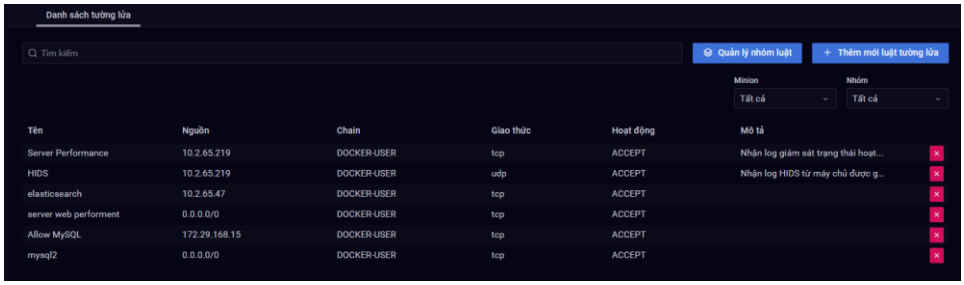
9. Chức năng khác (tiếp)

- Kết nối đến các hệ thống chia sẻ an toàn thông tin để cập nhật các nguy cơ mới nhất.
- Thu thập các thông tin Threat Intelligence để đưa ra các luật chặn bắt nguy cơ mới.
- Cấu hình bộ luật, tự động đồng bộ luật từ SOC Master xuống các thành phần trong hệ thống.



- Hỗ trợ quản lý tập trung tới các thiết bị sensor (collector) trong hệ thống: Đồng bộ thông tin hệ thống trên các thiết bị Collector (thời gian hệ thống, tập luật thực thi, cấu hình Firewall…)





(Trang quản lý firewall cho tất cả các thành phần trong phần mềm SIEM)

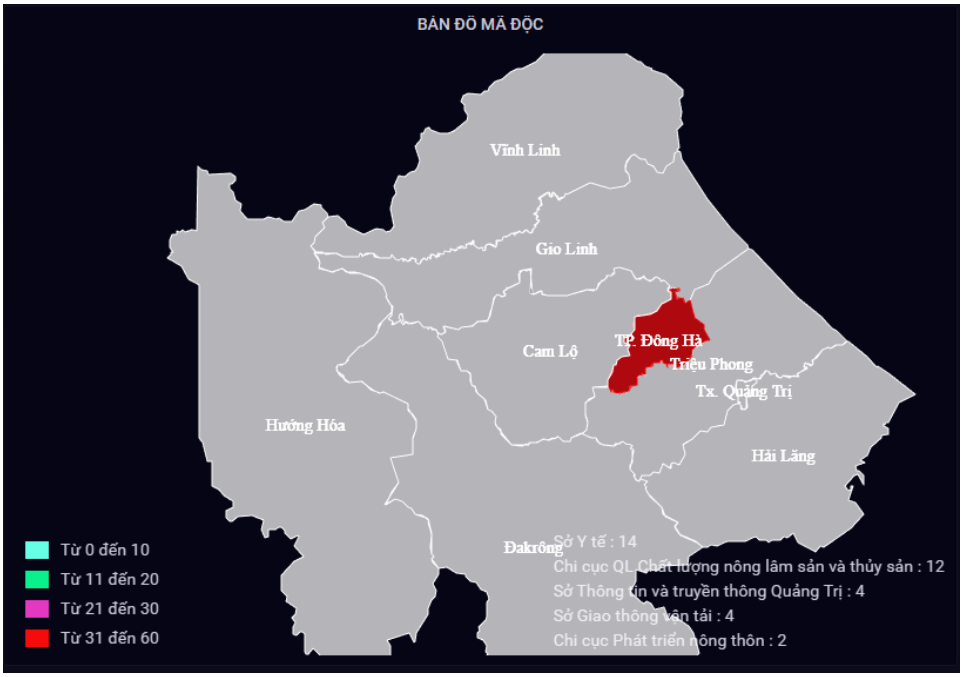
- Làm giàu dữ liệu khi phân tích

destination.geo.city_	destination.geo.conti	destination.geo.coun	destination.geo.coun	destination.geo.ip	destination.geo.locat	destination.geo.locat
London	Europe	GB	United Kingdom	149.154.167.220	51.5	-0.093

(Vị trí địa lý của ip được bổ sung, làm giàu cho log)

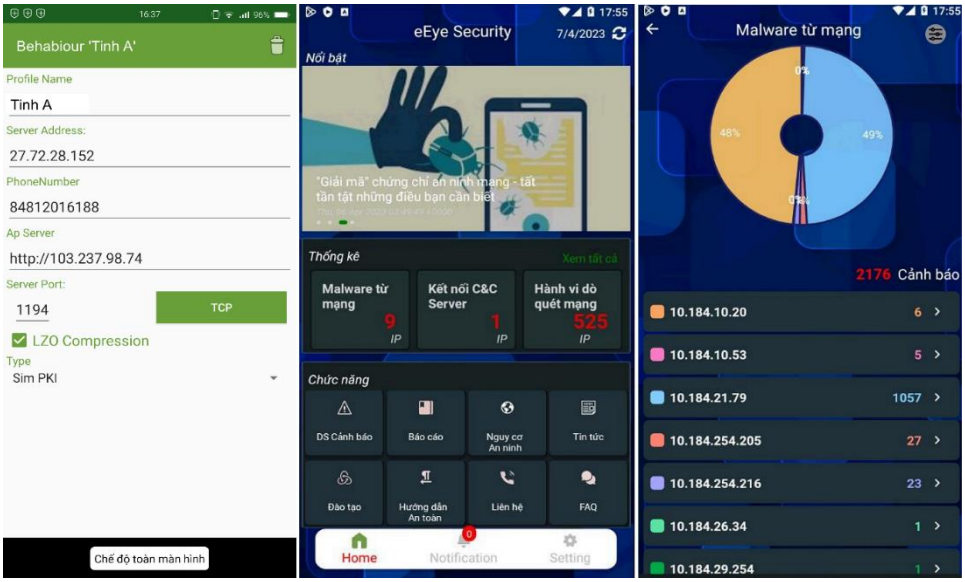
9. Chức năng khác (tiếp)

- Hiển thị bản đồ mã độc của tổ chức (Tỉnh/Huyện) và các đơn vị trực thuộc.



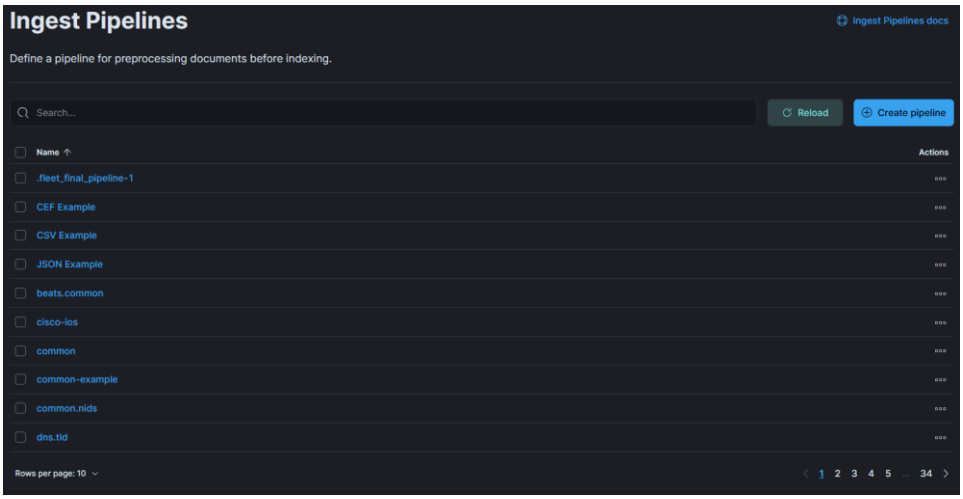
- Có ứng dụng (App Mobile) phục vụ quản trị viên trên thiết bị di động (hệ điều hành iOS và Android). Yêu cầu kết nối từ App Mobile đến hệ thống giám sát sử dụng VPN xác thực thông qua khóa bí mật được lưu trữ trên SIM để tăng cường bảo mật

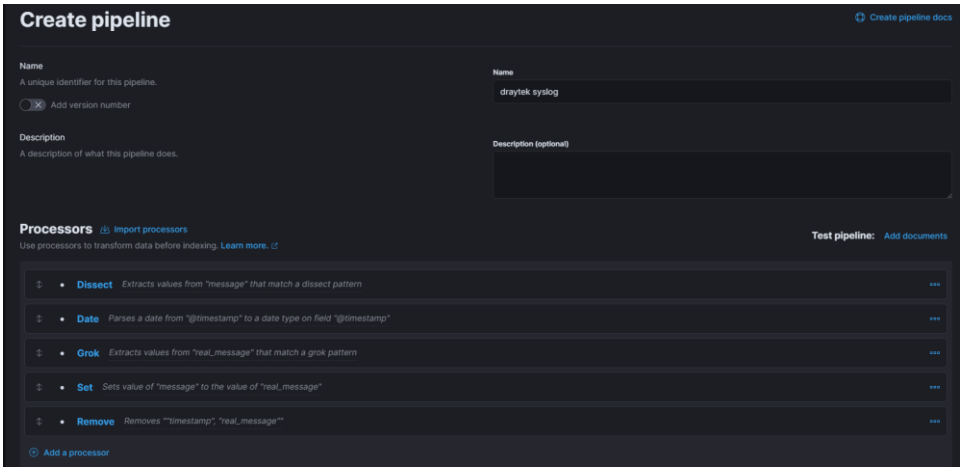
  Mô tả: Ứng dụng di động là một giải pháp mới, cho phép quản trị viên truy cập hệ thống giám sát mạng một cách thuận tiện và linh hoạt trên thiết bị di động. Ứng dụng này cung cấp cho người dùng khả năng truy cập dữ liệu và thông tin về tình hình an ninh mạng của đơn vị bất cứ khi nào và ở bất kỳ đâu, giúp họ quản lý hệ thống mạng của mình một cách hiệu quả hơn. Để đảm bảo tính bảo mật của ứng dụng di động, SIEM sử dụng kết nối VPN và xác thực thông qua khóa bí mật được lưu trữ trên SIM. Khi quản trị viên kết nối ứng dụng di động đến hệ thống giám sát, họ phải sử dụng một khóa bí mật để xác thực truy cập. Khóa bí mật này được lưu trữ trên SIM và được sử dụng để thiết lập kết nối VPN giữa thiết bị di động và hệ thống giám sát mạng. Điều này giúp tăng cường tính bảo mật của hệ thống giám sát mạng, bởi vì VPN kết nối có tính bảo mật cao, ngăn chặn bất kỳ ai khác truy cập vào dữ liệu khi thông tin được truyền đi giữa hai thiết bị. Ngoài ra, khóa bí mật được lưu trữ trên SIM cũng giúp bảo mật các thông tin xác thực truy cập, ngăn chặn bất kỳ ai khác truy cập vào ứng dụng di động



9. Chức năng khác (tiếp)

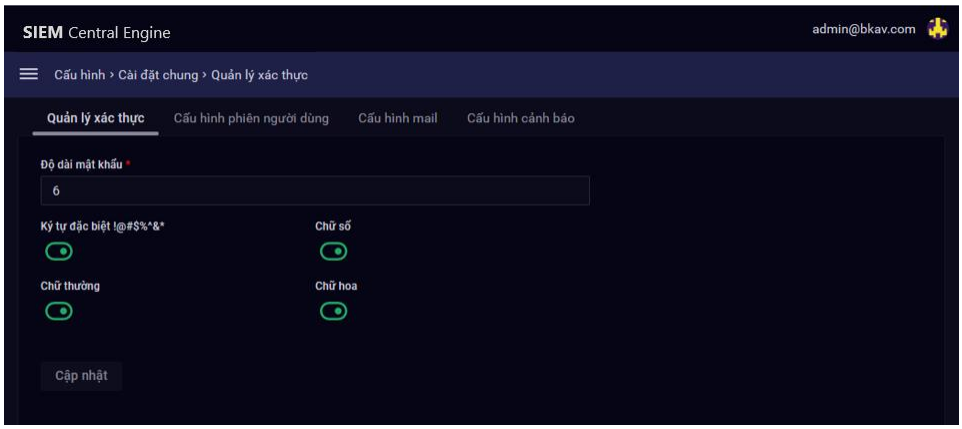
- Hỗ trợ phân tích log theo các cú pháp đã có sẵn hoặc cú pháp tùy biến





(Hệ thống cung cấp sẵn các bộ sử lý đối với dữ liệu từ các thiết bị/hệ thống mạng phổ biến. Nếu chưa có bộ xử lý tương ứng, người dùng có thể tự thiết lập bộ xử lý dữ liệu)

- Quản lý hệ thống thông qua cả giao diện đồ họa và giao diện dòng lệnh



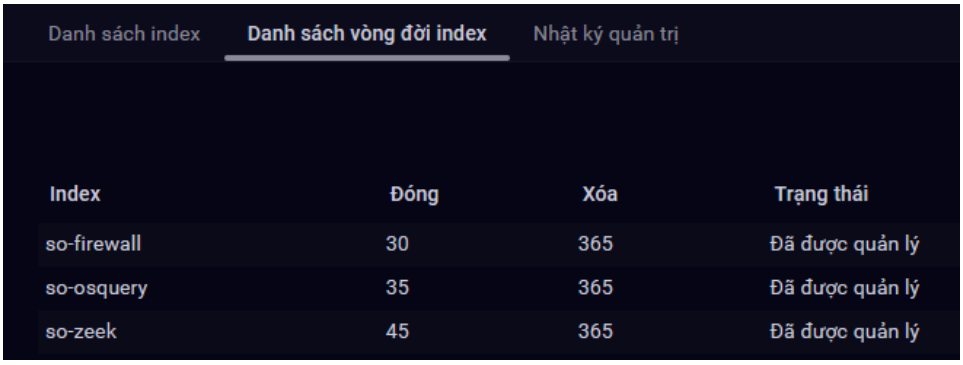
9. Chức năng khác (tiếp)

- Quản lý hệ thống thông qua cả giao diện đồ họa và giao diện dòng lệnh (tiếp)

```
157     so-linux.system:
158       warm: 7
159       close: 1
160       delete: 1
161     so-eventcorrelate:
162       warm: 1
163       close: 4
164       delete: 1
165     so-endpoint:
166       warm: 7
167       close: 1
168       delete: 1
169   cluster_routing_allocation_disk_watermark_low: 95%
170   cluster_routing_allocation_disk_watermark_high: 98%
171   cluster_routing_allocation_disk.threshold_enabled: true
172   cluster_routing_allocation_disk_watermark_flood_stage: 98%
173 redis_settings:
174   redis_maxmemory: 812
```

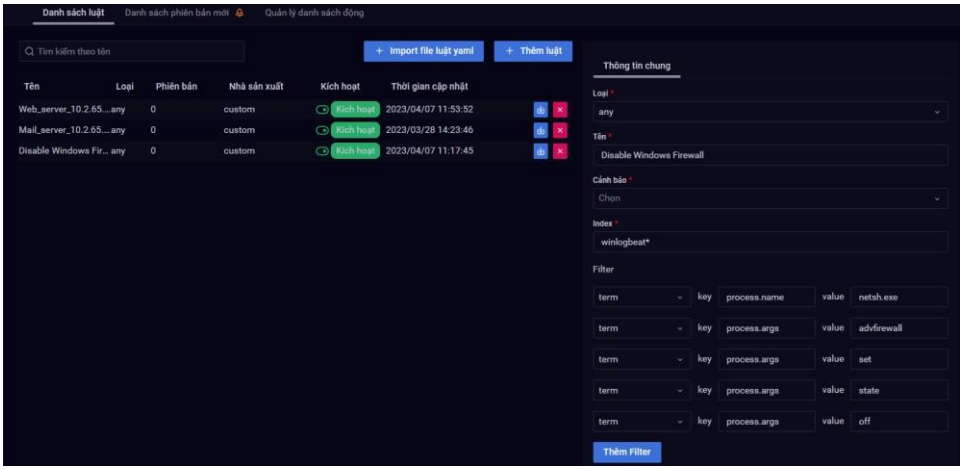
- Quản lý cấu hình Collector, Storage

(Cấu hình Collector)



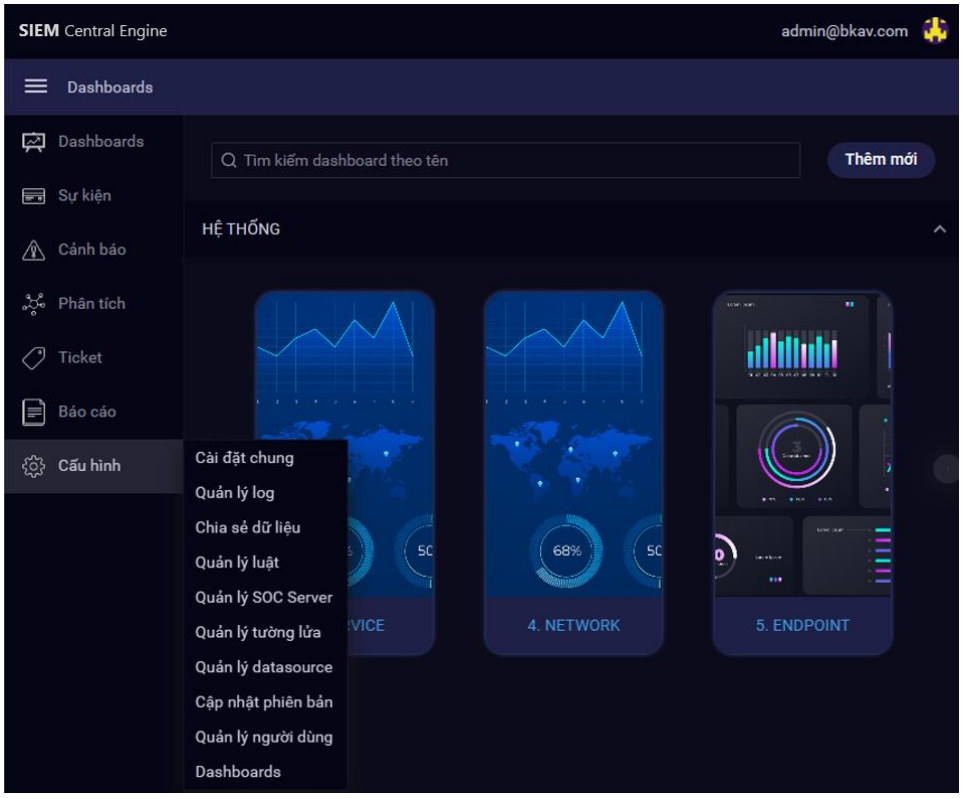
(Cấu hình Storage)

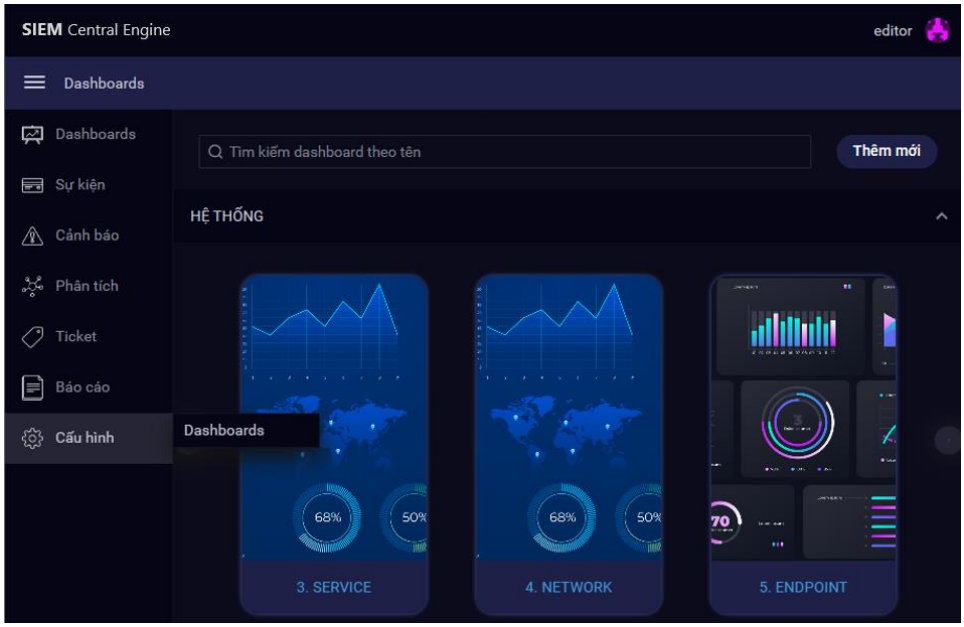
- Hỗ trợ thêm, sửa, xóa bộ luật thực thi qua giao diện đồ họa



9. Chức năng khác (tiếp)

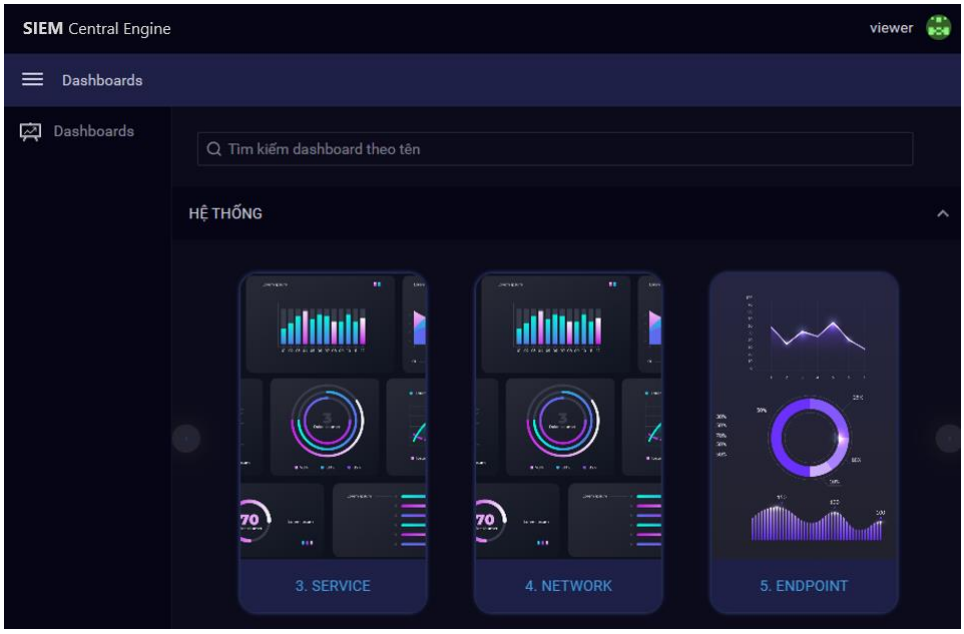
- Quản lý phân quyền đối tượng và thông tin giám sát



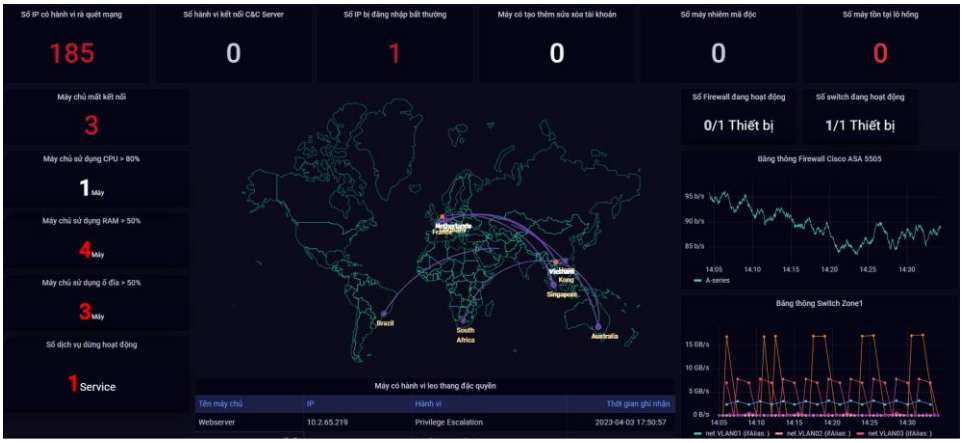


9. Chức năng khác (tiếp)

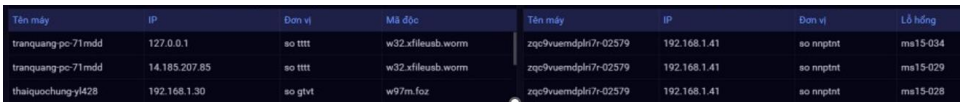
- Quản lý phân quyền đối tượng và thông tin giám sát (tiếp)



- Hiển thị thông tin tổng hợp dữ liệu theo thời gian thực dưới dạng đồ họa và số liệu trực quan



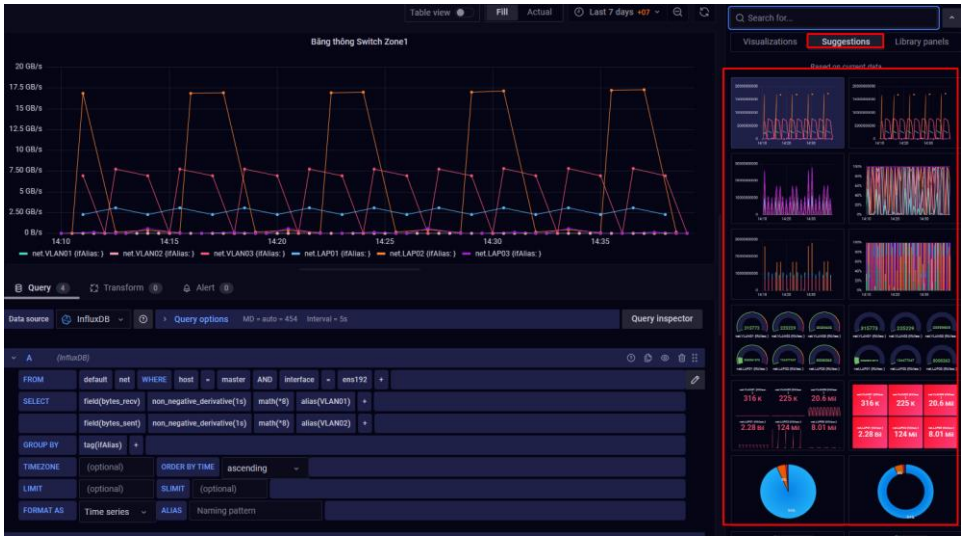
- Hiển thị dữ liệu về tình trạng lây nhiễm mã độc từ hệ thống phòng chống mã độc tập trung đang triển khai tại tổ chức. Hiển thị được thông tin máy nhiễm mã độc theo từng đơn vị trực thuộc, thông tin theo từng IP máy, thông tin chi tiết người dùng bị nhiễm mã độc mà có thể điều tra được



9. Chức năng khác (tiếp)

- Hỗ trợ tùy biến giao diện và nội dung giám sát:
  - ✓ Cho phép lựa chọn các loại biểu đồ để trực quan hóa dữ liệu (time series, bar chart, Gauge, Bar gauge, Table, Pie chart, smart number, heat map, graph, text, geo map)

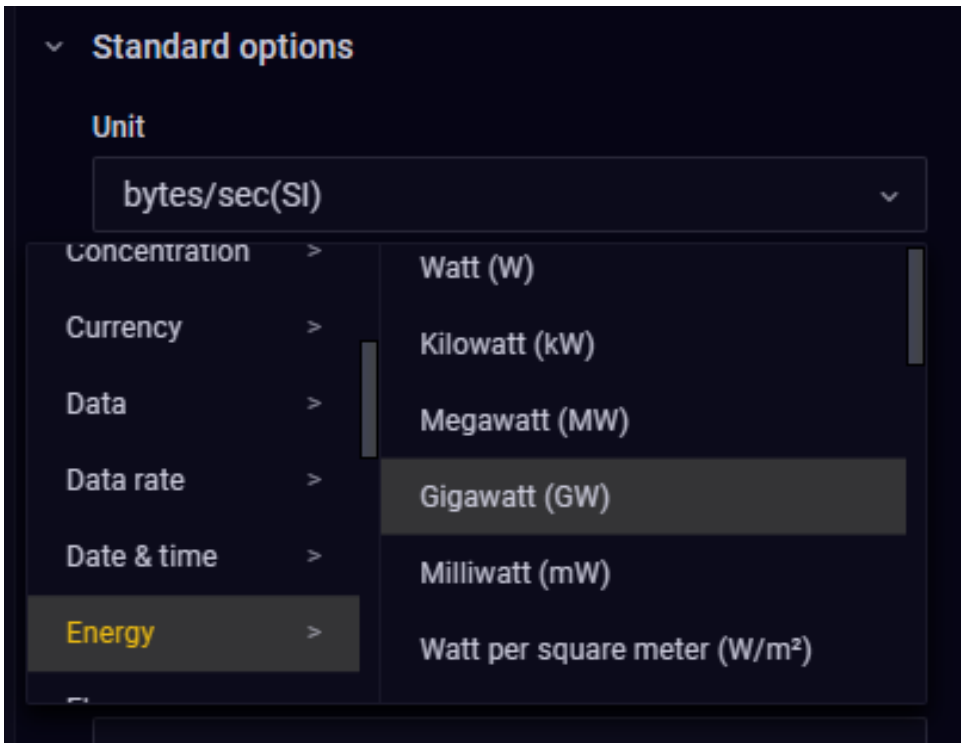
  - ✓ Gợi ý các loại biểu đồ phù hợp với dữ liệu đang lựa chọn



  - ✓ Thay đổi màu dữ liệu trong biểu đồ dựa theo ngưỡng

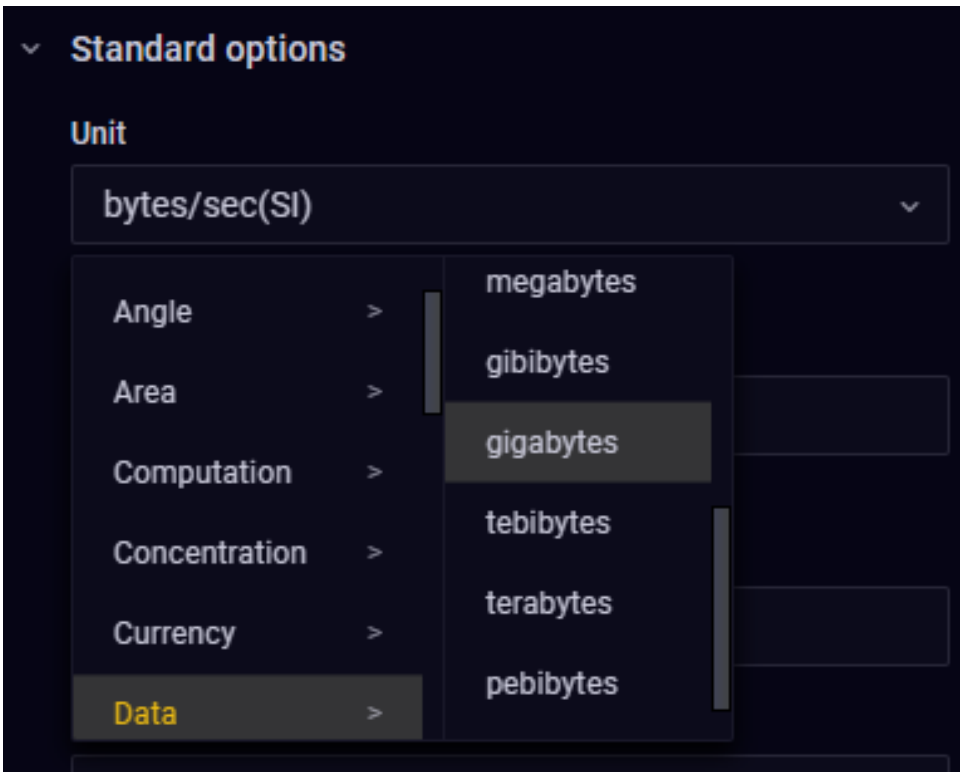
9. Chức năng khác (tiếp)

- Hỗ trợ tùy biến giao diện và nội dung giám sát (tiếp)
  - ✓ Cho phép lựa chọn các loại đơn vị đo phổ biến phù hợp với dữ liệu hiển thị

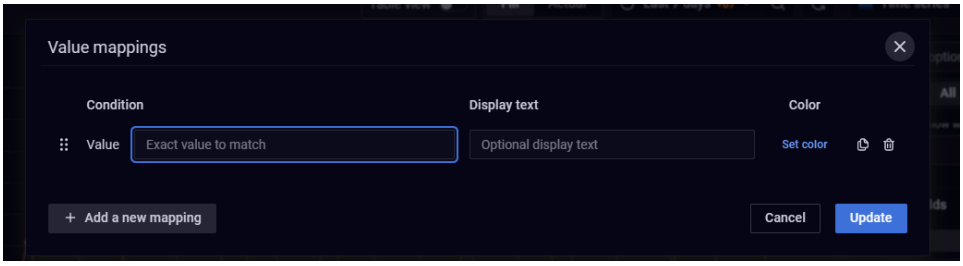


9. Chức năng khác (tiếp)

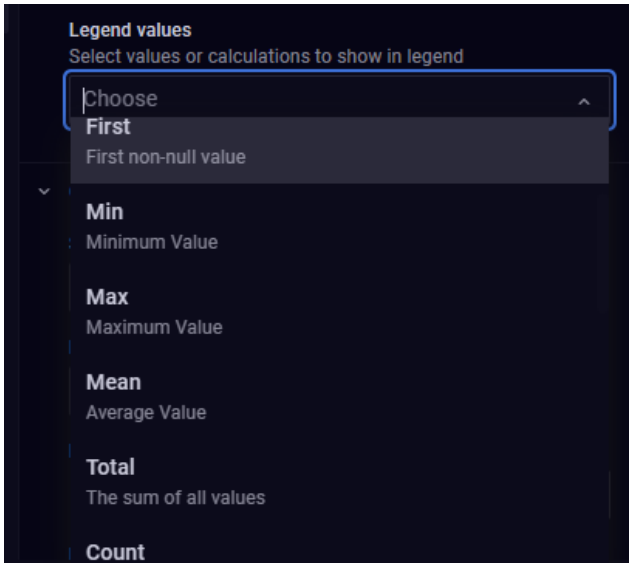
- Hỗ trợ tùy biến giao diện và nội dung giám sát (tiếp)
  - ✓ Cho phép lựa chọn các loại đơn vị đo phổ biến phù hợp với dữ liệu hiển thị (tiếp)



  - ✓ Tùy chỉnh tên hiển thị cho các trường thông tin trong log trên dashboard

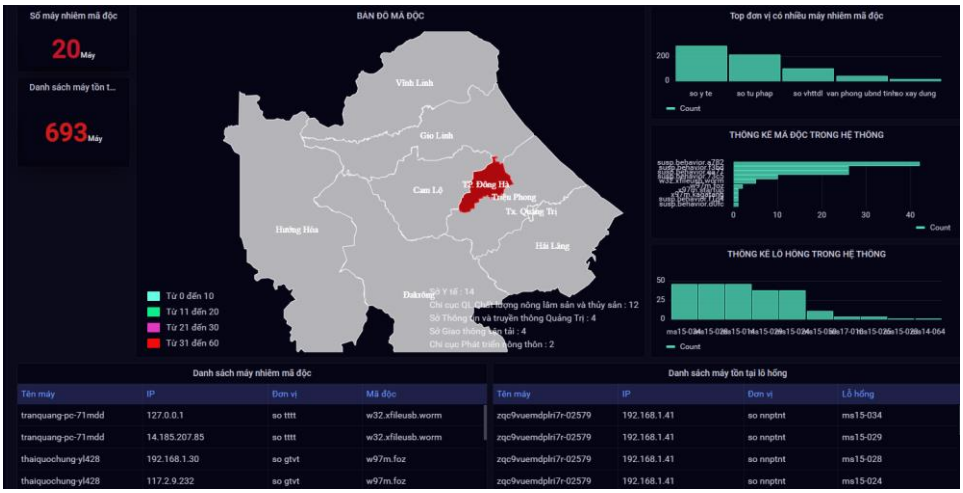


  - ✓ Chỉnh style giá trị dữ liệu và tùy chọn phương pháp xử lý chuỗi dữ liệu được hiển thị trong biểu đồ (mi
max, tổng, lọc trùng, đếm, các giá trị trống)

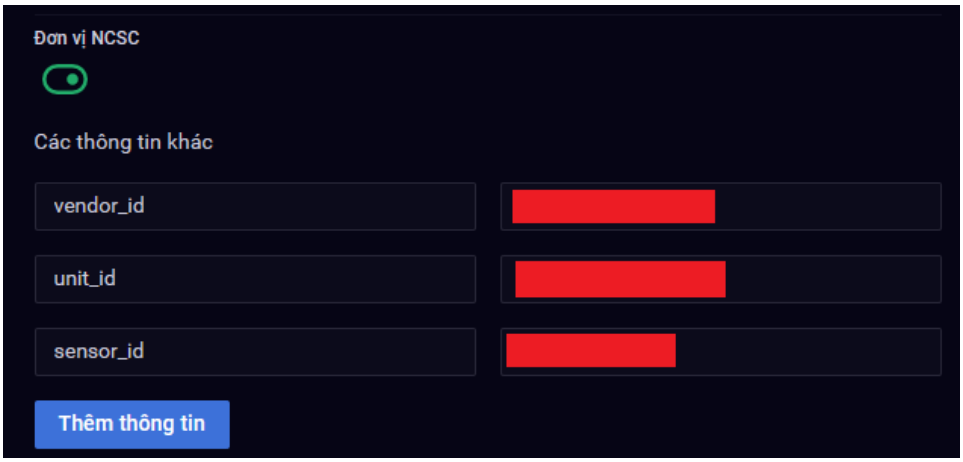


9. Chức năng khác (tiếp)

- Hỗ trợ tùy biến giao diện và nội dung giám sát (tiếp)
  - ✓ Chỉnh style giá trị dữ liệu và tùy chọn phương pháp xử lý chuỗi dữ liệu được hiển thị trong biểu đồ (min, max, tổng, lọc trùng, đếm, các giá trị trống) (tiếp)

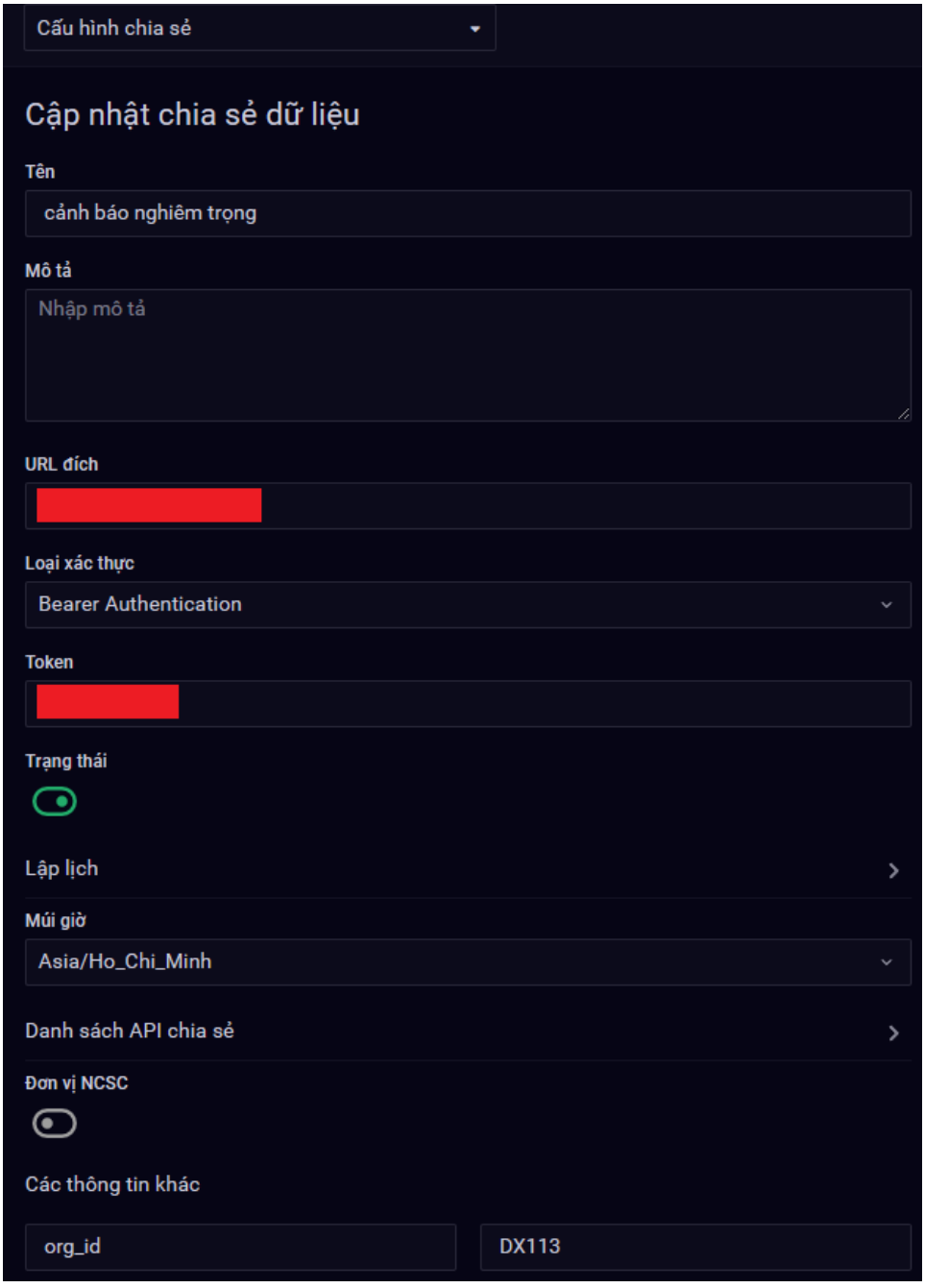


- Hỗ trợ chia sẻ dữ liệu với các kênh được cài đặt sẵn tối thiểu kết nối tới trung tâm giám sát an toàn không gian mạng quốc gia Việt Nam



9. Chức năng khác (tiếp)

- Hỗ trợ chia sẻ dữ liệu tới các kênh tùy chọn khác



- Tính năng Thông tin tình báo mối đe dọa (Threat Intelligence): Thông tin tình báo mối đe dọa (Threat Intelligence). Có thể tích hợp Threat Intelligence bên thứ 3. Mô đun chia sẻ dữ liệu của thống SIEM cung cấp khả năng gửi/nhận dữ liệu với các hệ thống Thông tin tình báo về mối đe dọa.
- Tính năng xử lý dữ liệu: Bộ xử dữ liệu (Data Processor)

9. Chức năng khác (tiếp)

- NTA - Hệ thống phân tích dữ liệu mạng.

- Công nghệ phân tích các dữ liệu thô thành các dữ liệu metadata có chứa các thông tin bao gồm: dữ liệu metadata được lưu theo ngữ cảnh, metadata chứa các thông tin từ layer 2-7 (Network Data, Server Data, Application Data, User Data, Syslog), L4-L7 performance metrics, URIs, và domain names; MD5 hashes of files downloaded.

```
GET /wp-login.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: stuptode.tk
Cookie: antibot_uid=61ec174b651f1b4782e042fd53272632; antibot_country=VN; antibot_ptr=static.vnpt.vn
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Mon, 06 Nov 2023 09:56:10 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Robots-Tag: noindex
Expires: Mon, 26 Jul 1997 05:00:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Link: </antibot/ab.php>; rel=dns-prefetch
Set-Cookie: antibot_country=VN; expires=Thu, 16-Nov-2023 09:56:09 GMT; Max-Age=864000; path=/
Set-Cookie: antibot_lang=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/
Set-Cookie: antibot_ptr=static.vnpt.vn; expires=Thu, 16-Nov-2023 09:56:09 GMT; Max-Age=864000; path=/
CF-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=ZPSyP4DpIpDozuQBK67siTNAHJSg%2BRkx4tGfnnCaG6s73jwYwZZC4vqXzFo42HRXRKwZxXIU5bDxDGGJLvGiFN43tAA%2FK5p
dbozizKJMpXO0wgb59x8xKd%2FevTi7gg%3D%3D"}],"group":"cf-nel","max_age":604800}
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
CF-RAY: 821c77093ba520dd-HKG
alt-svc: h3=":443"; ma=86400

181f
<!DOCTYPE html>
<html dir="ltr" lang="en">
<head>
  <meta charset="utf-8" />
  <meta name="referrer" content="unsafe-url" />
  <meta name="robots" content="noarchive" />
  <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" />
  <link rel="icon" href="/favicon.ico">
  <title>Just a moment...</title>
```

- Dữ liệu Metadata được làm giàu với Threat Intelligence & Geo Location

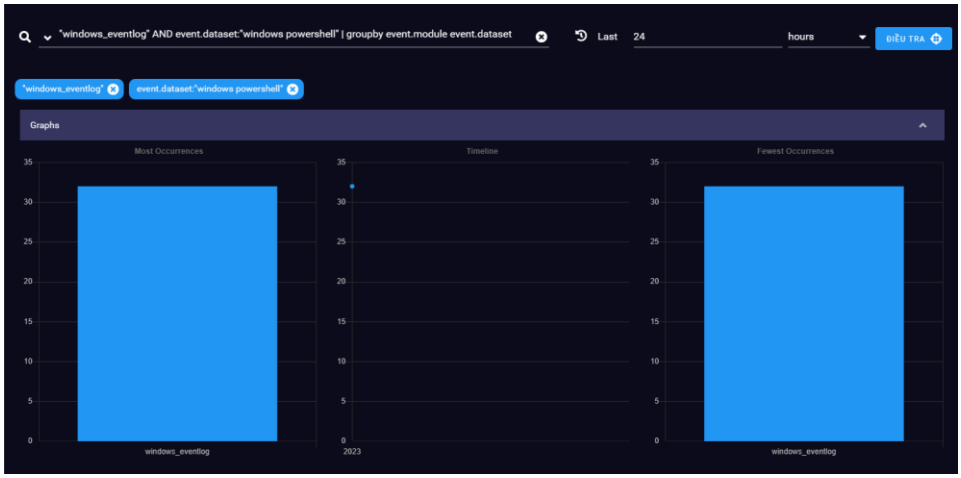
destination.geo.conti	destination.geo.coun	destination.geo.coun	destination.geo.ip	destination.geo.locat	destination.geo.locat
North America	US	United States	3.20.137.44	40.0	-83
North America	US	United States	3.20.137.44	40.0	-83
North America	US	United States	3.20.137.44	40.0	-83
North America	US	United States	3.20.137.44	40.0	-83
North America	US	United States	3.20.137.44	40.0	-83
North America	US	United States	3.20.137.44	40.0	-83
Asia	SG	Singapore	34.87.93.12	1.29	104
Asia	SG	Singapore	34.87.93.12	1.29	104
North America	US	United States	3.20.137.44	40.0	-83

9. Chức năng khác (tiếp)

- Cho phép phân nhóm sự kiện thành cách loại tấn công như Brute Forced User Logins, Exploited C&C Connection, Exploited vulnerability, SYN Flood, SMB Suspicious Copy...

353	Windows Logon Success
310	ET JA3 Hash - Possible Malware - Various Malfams
304	ET POLICY External IP Lookup ip-api.com
284	Windows User Logoff
274	ET INFO Observed ZeroSSL SSL/TLS Certificate
262	ET HUNTING Double User-Agent (User-Agent User-Agent)
193	ET DNS Query for .cc TLD
160	ET WEB_SERVER PHP tags in HTTP POST
151	ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT
148	ET DNS Non-DNS or Non-Compliant DNS traffic on DNS port Opcode 8 through 15 set
145	ET DNS Non-DNS or Non-Compliant DNS traffic on DNS port Opcode 6 or 7 set
131	ET SCAN Behavioral Unusual Port 445 traffic Potential Scan or Infection
128	ET DROP Dshield Block Listed Source group 1
125	ET INFO Executable Download from dotted-quad Host
125	ET MALWARE Terse alphanumeric executable downloader high likelihood of being hostile

- Cho phép phân loại các nhóm sự kiện theo các tiêu chí khác nhau như Command & Control Reputation Anomaly; Domain Generation Algorithm (DGA); Endcoded PowerShell, File Action Anomaly, Malware on Disk...
- Hệ thống cung cấp đa dạng các bộ lọc phân loại dữ liệu với nhiều tiêu chí khác nhau. Người dùng cũng có thể phân loại sự kiện một cách thủ công thông qua cú pháp gom nhóm dữ liệu.



- Cho phép cài đặt các phần mềm trên agent để theo dõi mối nguy cơ trên thiết bị của người dùng.
  - ✓ Thu thập các sự kiện sau trên Windows: Hardware, Security, System, Windows Firewall, Windows Defender, PowerShell
  - ✓ Thu thập các sự kiện sau trên Linux: process info, command execution, files, file events

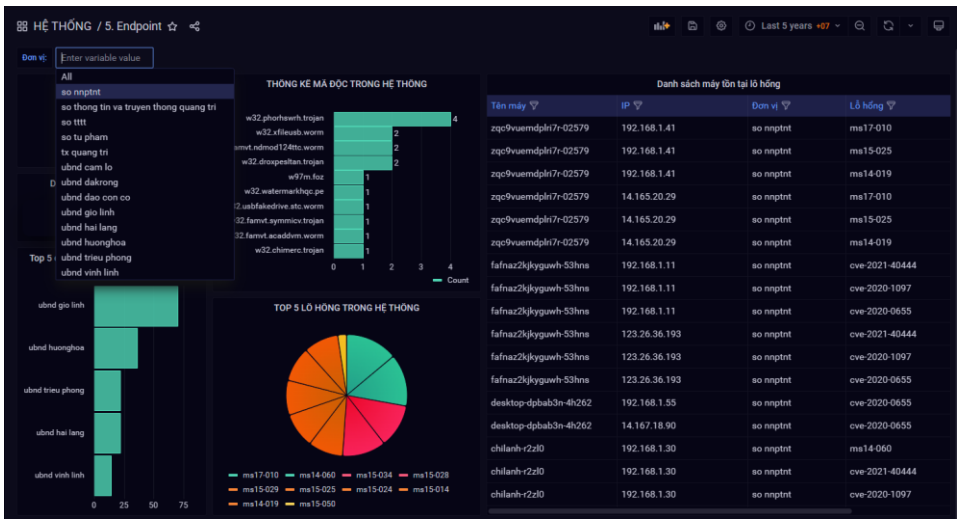
Count	event.module	event.dataset
273,440	windows_eventlog	security
72,324	windows_eventlog	application
24,073	windows_eventlog	alert
12,976	windows_eventlog	system
32	windows_eventlog	windows powershell
30	windows_eventlog	microsoft-windows-powershell/operational

9. Chức năng khác (tiếp)

- Có khả năng phát hiện ra hành vi cài đặt phần mềm, khả năng phát hiện PowerShell Startup, khả năng phát hiện Windows New Processes.

- Có khả năng phát hiện ra các password Plaintext không được mã hóa trên đường truyền.

- Có khả năng cấu hình báo cáo cho từng khách hàng khác nhau trên cùng 1 dashboard hoặc các dashboard cho từng phòng ban, dashboard cho lãnh tạo, dashboard các cuộc tấn công khác nhau... bằng tiếng Việt



- Cho phép khả năng hiển thị mô phỏng cuộc tấn công mạng bằng giao diện web bao gồm IP nguồn và đích đến, cũng như phạm vi lây lan, loại tấn công, số lần của các cuộc tấn công.

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 và 5000 EPS
Bản quyền Virtual Network sensor/ Linux Agents / Container Agents: Tối thiểu 100 xCảm biến mạng ảo / Linux Agents / Container Agents
Bản quyền Windows Agent: Tối thiểu 100 x Bản quyền Windows Agent