Bkav Pro SIEM Storage

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

Giải pháp lưu trữ log tập trung để cải thiện hiệu quả cho phần mềm giám sát an ninh trong việc phân tích và xử lý các sự cố. Các chuyên gia bảo mật sẽ tốn ít thời gian cho việc thu thập các dữ liệu trên nhiều giải pháp, thiết bị khác nhau trong phần mềm

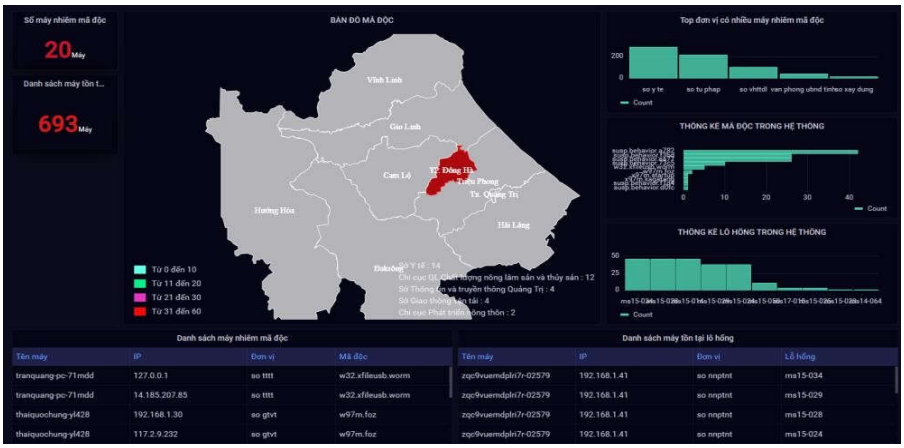
Tính năng

- Lưu trữ Metadata theo dạng mã hóa

```
[root@soc index]# ls
_5l.fdm  _5l.kdm              _5l_Lucene84_0.tip  _5v.fdt  _5v_Lucene80_0.dvd  _5v_Lucene84_0.tmd
_5l.fdt  _5l_Lucene80_0.dvd   _5l_Lucene84_0.tmd  _5v.fdx  _5v_Lucene80_0.dvm  _5v.nvd
_5l.fdx  _5l_Lucene80_0.dvm   _5l.nvd             _5v.fnm  _5v_Lucene84_0.doc  _5v.nvm
_5l.fnm  _5l_Lucene84_0.doc   _5l.nvm             _5v.kdd  _5v_Lucene84_0.pos  _5v.si
_5l.kdd  _5l_Lucene84_0.pos   _5l.si              _5v.kdi  _5v_Lucene84_0.tim  _67.cfe
_5l.kdi  _5l_Lucene84_0.tim   _5v.fdm             _5v.kdm  _5v_Lucene84_0.tip  _67.cfs
[root@soc index]# cat _5l.fdm
?lLucene85FieldsIndexMeta>-"BU w/Bi=
S0[8]E RR[root@soc index]#
```

Mô tả: Với khả năng lưu trữ dữ liệu metadata, BkavPro SIEM Storage giúp các chuyên gia bảo mật mạng phân tích và đánh giá tình trạng bảo mật hệ thống một cách chính xác và hiệu quả.Tính năng nén dữ liệu của SIEM Storage cũng rất hữu ích để tối ưu hóa hệ thống lưu trữ. Với việc nén dữ liệu, không chỉ giúp giảm thiểu tải cho hệ thống lưu trữ, giảm chi phí lưu trữ, mà còn giúp cho việc truy xuất và xử lý dữ liệu trở nên nhanh chóng hơn. Ngoài ra, SIEM Storage còn tích hợp các công nghệ và giao thức bảo mật mạnh mẽ để đảm bảo tính bảo mật của dữ liệu khi lưu trữ và truy xuất. Các tính năng bảo mật này bao gồm mã hóa dữ liệu, chứng thực người dùng và kiểm soát truy cập để đảm bảo rằng chỉ những người được ủy quyền mới có thể truy cập vào dữ liệu

- Đồng bộ và lưu trữ dữ liệu lịch sử về tình trạng lây nhiễm mã độc từ hệ thống phòng chống mã độc tập trung



- Cung cấp khả năng truy vấn theo cấu trúc và keywords

- Sắp xếp dữ liệu theo dạng index với quy tắc, định dạng được cấu hình sẵn, có thể chỉnh sửa theo yêu cầu

Index	Tình trạng	Trạng thái	Primary shards	Replicas	Docs count
so-zeek-2023.04.07	green	open	2	0	103654
so-zeek-2023.04.07	green	open	2	0	361024
so-linux.system-2023.0...	green	open	1	0	10
so-firewall-2023.04.07	green	open	1	0	2890
so-mail-2023.04.07	green	open	1	0	9
so-firewall-2023.04.05	green	open	1	0	3624
so-kibana-2023.04.07	green	open	1	0	5
so-firewall-2023.04.06	green	open	1	0	8994

(Định dạng: name-yyyy.MM.dd - Có thể thay đổi theo yêu cầu)

- Module xác thực và tiếp nhận dữ liệu gửi về từ Master

```
input {
        redis {
                host => 'Master'
                port => 9696
                ssl => true
                data_type => 'list'
                key => 'logstash:unparsed'
                type => 'redis-input'
                threads => 1
                batch_count => 125
        }
}
```

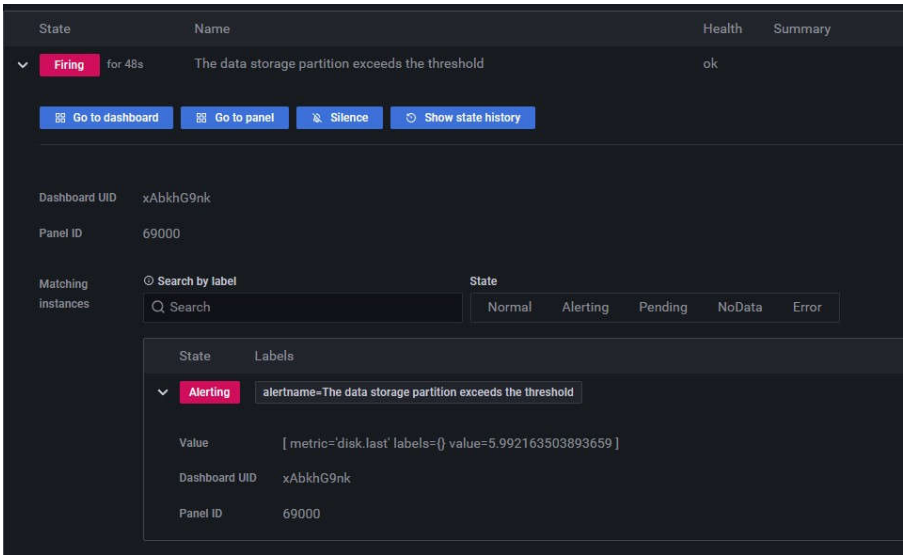
- Module lưu trữ sự kiện đã qua xử lý

  Mô tả: Các module lưu trữ sự kiện đã qua xử lý trong BkavPro SIEM Storage là các module được thiết kế để lưu trữ các sự kiện bảo mật đã được xử lý và phân tích. Các sự kiện này có thể là các cảnh báo, cảnh báo giả, các lỗi, các tấn công bảo mật đã bị chặn hoặc các hành động bảo mật khác. Việc lưu trữ các sự kiện đã qua xử lý là cần thiết để tạo ra các báo cáo và phân tích bảo mật sau này, giúp người dùng có thể hiểu rõ hơn về mối đe dọa bảo mật và các hành động được thực hiện để đối phó với chúng.

- Module truy vấn dữ liệu lớn theo thời gian dài

  Mô tả: Trong BkvPro SIEM Storage, các module truy vấn dữ liệu lớn theo thời gian dài là các module được thiết kế để giúp người dùng truy vấn và phân tích các sự kiện bảo mật trong một khoảng thời gian dài, thường là trong thời gian từ vài tháng đến vài năm. Điều này giúp người dùng có thể phát hiện và giải quyết các mối đe dọa bảo mật một cách hiệu quả, giúp bảo vệ hệ thống mạng và dữ liệu của tổ chức.

- Module tự động cảnh báo và xử lý dữ liệu khi kho lưu trữ đầy



(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, phần mềm luôn đảm bảo có thể lưu trữ dữ liệu mới vào CSDL ➔ không có cảnh báo)

- Module cấu hình tích hợp mở rộng các nút lưu trữ

  Mô tả: BkavPro SIEM Storage sử dụng các module mở rộng để phân tán dữ liệu trên các nút lưu trữ khác nhau, tạo ra một hệ thống lưu trữ phân tán, có khả năng mở rộng linh hoạt và đảm bảo tính sẵn sàng cao. Các module mở rộng cho SIEM Storage được thiết kế để tương thích với các nút lưu trữ khác nhau, cho phép các nút này giao tiếp và chia sẻ dữ liệu một cách hiệu quả. Những module này được xây dựng trên cơ chế phân tán, cho phép hệ thống có thể tự động phân bổ và quản lý dữ liệu trên các nút lưu trữ khác nhau, giúp tăng hiệu suất và tính sẵn sàng của hệ thống

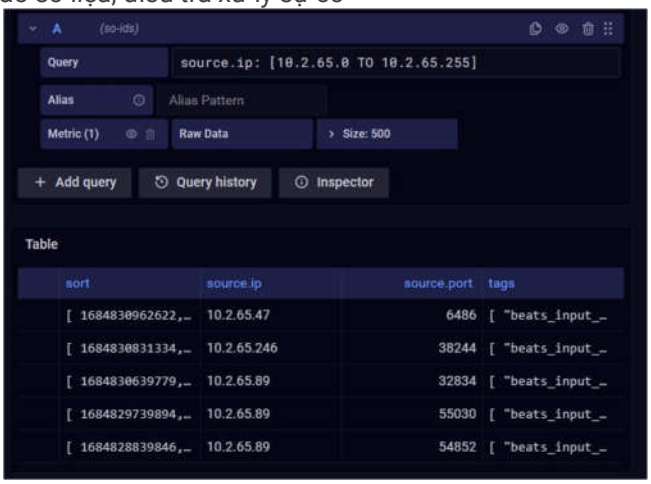
- Sử dụng các đường truyền được thiết lập và xác thực riêng để tiếp nhận các dữ liệu từ Master gửi tới

```
38    transport:
39      ssl:
40        enabled: true
41        verification_mode: none
42        key: /usr/share/elasticsearch/config/elasticsearch.key
43        certificate: /usr/share/elasticsearch/config/elasticsearch.crt
44        certificate_authorities:
45        - /usr/share/elasticsearch/config/ca.crt
```

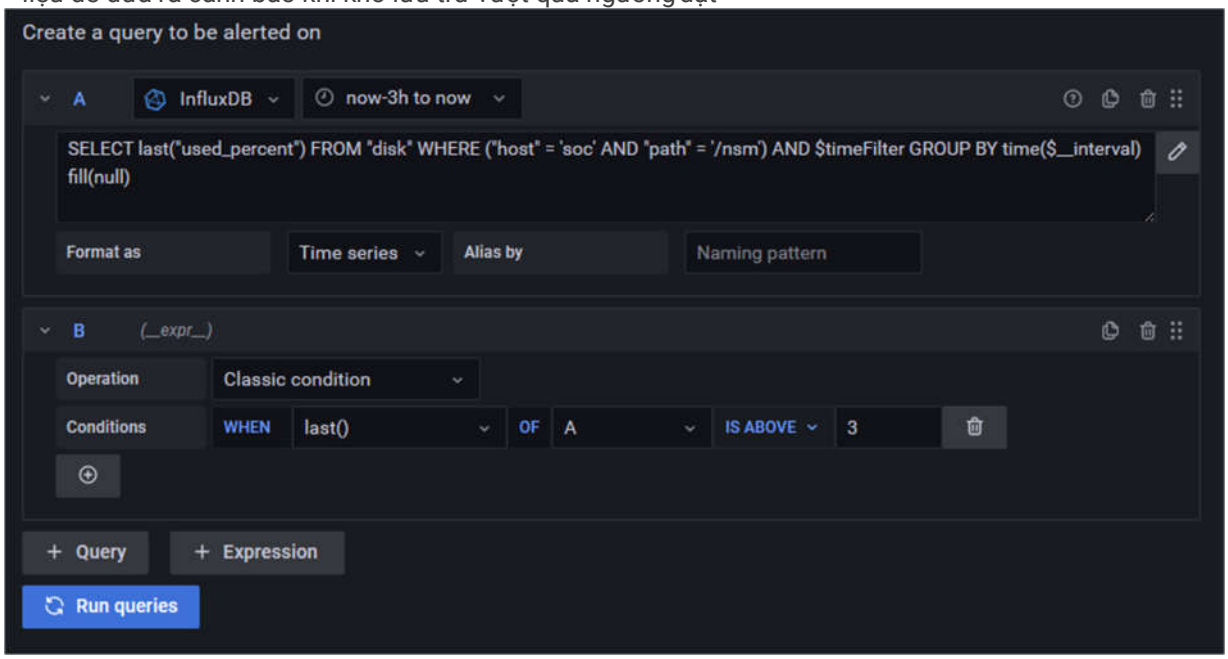
- Các sự kiện đã qua xử lý được đẩy tập trung và lưu trữ một kho thời gian dài để phục vụ cho việc thống kê báo cáo và điều tra xử lý sự cố

  Mô tả: BkavPro SIEM Storage có khả năng lưu trữ log, các sự kiện đã qua xử lý được đẩy tập trung và lưu trữ một kho thời gian dài để phục vụ cho việc thống kê báo cáo và điều tra xử lý sự cố. Khi các sự kiện bảo mật xảy ra, SIEM Storage sẽ thu thập và lưu trữ thông tin chi tiết về các sự kiện này, bao gồm thời gian, nguồn, đích, loại sự kiện, thông tin người dùng và các chi tiết khác. Sau đó, các sự kiện này sẽ được xử lý và đẩy tập trung vào SIEM Storage, nơi chúng sẽ được lưu trữ trong một kho thời gian dài. Quá trình lưu trữ và duy trì dữ liệu là rất quan trọng, bởi vì các sự kiện cũng có thể được sử dụng cho các mục đích pháp lý

- Cho phép truy vấn, tìm kiếm, thống kê nhiều dữ liệu với dung lượng lớn cùng lúc phục vụ cho bảng điều khiển thông minh, báo cáo số liệu, điều tra xử lý sự cố



- Kết hợp các công cụ cho phép cấu hình ngưỡng cảnh báo và liên tục theo dõi trạng thái kho lưu trữ dữ liệu để đưa ra cảnh báo khi kho lưu trữ vượt quá ngưỡng đặt



- Tự động xóa hoặc nén các dữ liệu để duy trì trạng thái ổn định cho kho lưu trữ

```
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, phần mềm luôn đảm bảo có thể lưu trữ dữ liệu mới vào CSDL ➔ không có cảnh báo)

- Cho phép thiết lập để mở rộng thêm phần cứng kho lưu trữ tránh để xảy ra tình trạng mất hoặc tràn dữ liệu tại kho lưu trữ tập trung

  Mô tả: Để đáp ứng việc mở rộng kho lưu trữ, BkavPro SIEM Storage sử dụng cơ chế cluster. Cơ chế này cho phép kết nối nhiều máy chủ với nhau để tạo thành một hệ thống lưu trữ lớn hơn và có khả năng chịu tải cao hơn. Khi một máy chủ trong cluster gặp sự cố hoặc quá tải, các máy chủ khác trong cluster sẽ tiếp tục xử lý và lưu trữ dữ liệu, đảm bảo tính khả dụng của hệ thống. Người quản trị có thể thêm các máy chủ mới vào cluster để tăng khả năng lưu trữ và chịu tải của hệ thống. Các máy chủ mới này có thể được cấu hình và thêm vào cluster một cách đơn giản và nhanh chóng, giúp người quản trị tiết kiệm thời gian và công sức.