

Bkav[®] Pro SIEM Collector for DC

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

Thu thập dữ liệu, tiền xử lý và vận chuyển log trong thời gian thực để phát hiện sớm các bất thường, các cuộc tấn công có chủ đích và vi phạm chính sách an toàn thông tin của cơ quan, tổ chức, doanh nghiệp, đồng thời có chức năng lưu trữ dữ liệu thô phục vụ công tác hỗ trợ điều tra, xử lý sự cố

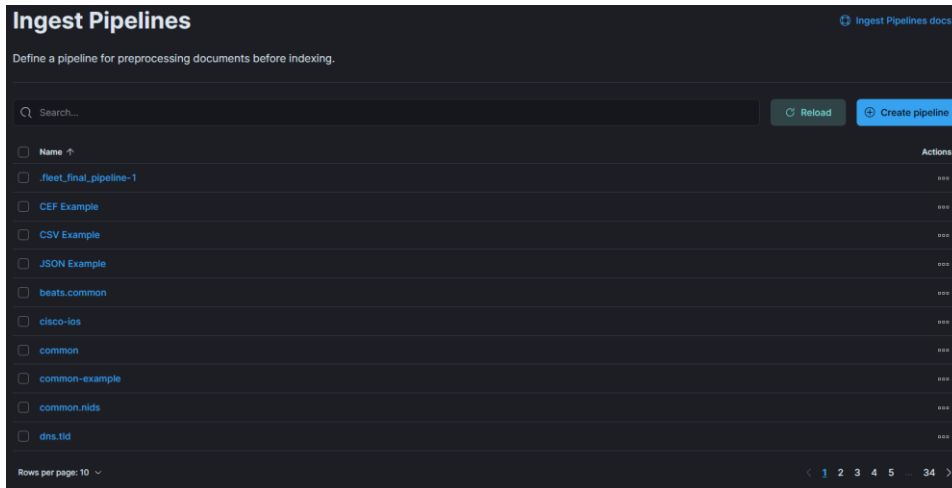


Tính năng

- Có khả năng tiếp nhận log của 04 nguồn log thiết yếu: thiết bị mạng (Router, Switch), thiết bị bảo mật (Firewall, IDS, Endpoint server), hệ điều hành (Linux, Windows), ứng dụng (Web, Mail, DNS, DHCP). Ngoài ra có khả năng thu thập log, alert từ các Agent. Kết nối đến các thiết bị an ninh: Network Inspector, GatewayScan & AntiSpam.

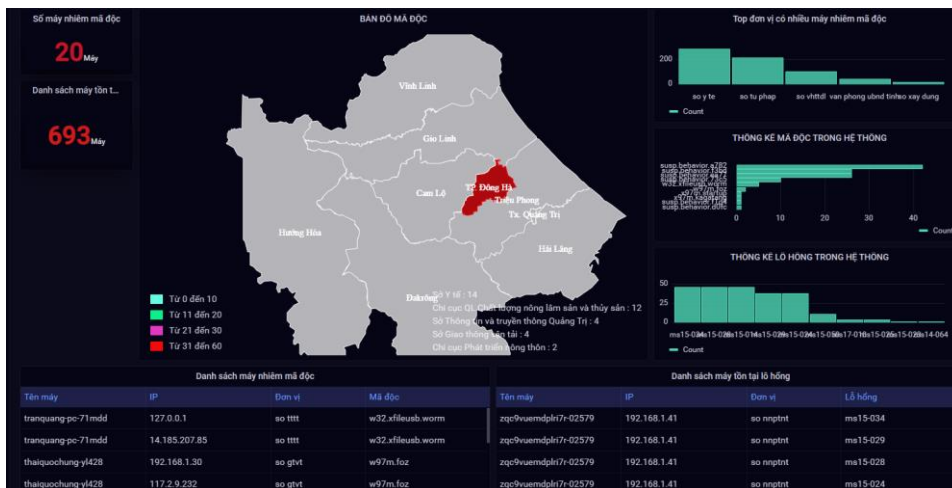
Index	Tình trạng	Trạng thái	Primary shards	Replicas	Docs count
so-zeek-2023.04.07	green	open	2	0	84962
so-firewall-2023.04.07	green	open	1	0	2617
so-linux.system-2023.0...	green	open	1	0	10
so-mail-2023.04.07	green	open	1	0	0
so-kibana-2023.04.07	green	open	1	0	5
so-endpoint-2023.04.07	green	open	1	0	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

- Thu thập dữ liệu từ các nguồn trong hệ thống mạng, thiết bị theo định dạng có sẵn và hỗ trợ tùy biến cấu hình định dạng dữ liệu mới



(Phần mềm cung cấp sẵn các bộ xử 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)

- Kết nối, thu thập và đồng bộ dữ liệu về tình trạng lây nhiễm mã độc từ hệ thống phòng chống mã độc tập trung



- Tiền xử lý dữ liệu raw log (chuẩn hóa log tiền phân tích)

```

1 input {
2   syslog {
3     port => "5047"
4     tags => ["syslog", "external"]
5   }
6 }
    
```

- Tiền xử lý dữ liệu raw log (chuẩn hóa log tiền phân tích) (tiếp)

```

1 filter {
2   if [@metadata][input][tcp][source] and ![host] {
3     mutate {
4       copy => {
5         "[@metadata][input][tcp][source][name]" => "[host][name]"
6         "[@metadata][input][tcp][source][ip]" => "[host][ip]"
7       }
8     }
9   }
10 }
11

```

- Lưu trữ raw log full packet tại Collector

```

[root@Sensor_pcap]# ls
1680369172622639 1680454632141135 1680590431113266 1680675877109141 1680761346115158
1680369234177675 1680454694140418 1680590493095143 1680675938126613 1680761407123351
1680369296116535 1680454755169071 1680590554100361 1680675999298132 1680761469114278
1680369357170634 1680454816205202 1680590616098152 1680676061166230 1680761530129588
1680369418171646 1680454878140382 1680590677534183 1680676123140052 1680761592109327
1680369480099621 1680454939996017 1680590739102770 1680676184444019 1680761653142354
1680369541126679 1680455001175996 1680590800130453 1680676245446524 1680761714377750
1680369603116816 1680455063170615 1680590862106423 1680676307124487 1680761776145438
1680369664133400 1680455125163213 1680590923133186 1680676368128366 1680761838115173
1680369725135801 1680455186341088 1680590984173700 1680676429129147 1680761899148152

```

- Phát hiện các dấu hiệu bất thường, nghi vấn, truy cập độc hại theo thời gian thực

IP CỎ HÀNH VI RÀ QUÉT MẠNG		IP CỎ HÀNH VI RÀ QUÉT MẠNG			
IP Nguồn	IP đích	Cảnh báo	rule.sub_category.keyword	Count	
181	79.137.73.44	125.212.252.24	ET INFO Observed Telegram API Domain (api.telegram.org in TLS SNI)	SCAN	13
	79.137.73.44	125.212.252.24	ET INFO Observed Telegram API Domain (api.telegram.org in TLS SNI)	DDOS	8
	79.137.73.44	125.212.252.24	ET INFO Observed Telegram API Domain (api.telegram.org in TLS SNI)	CNC	9
	52.148.114.188	193.0.9.10	ET INFO Observed Telegram API Domain (api.telegram.org in TLS SNI)	SCAN	2
	52.148.114.188	193.0.9.10	ET INFO Observed Telegram API Domain (api.telegram.org in TLS SNI)	DNS	2
	52.148.114.188	193.0.9.10	ET INFO Observed Telegram API Domain (api.telegram.org in TLS SNI)	DDOS	2
SỐ HÀNH VI KẾT NỐI CÁC SERVER		IP CỎ HÀNH KẾT NỐI CÁC SERVER			
IP Nguồn	IP đích	Cảnh báo			
731	92.223.85.54	10.2.65.120	ET POLICY SSL/TLS Certificate Observed (AnyDesk Remote Desktop Soft...		
	92.223.85.147	10.2.65.120	ET POLICY SSL/TLS Certificate Observed (AnyDesk Remote Desktop Soft...		
	92.223.85.120	10.2.65.120	ET POLICY SSL/TLS Certificate Observed (AnyDesk Remote Desktop Soft...		
	91.215.216.11	10.8.5.101	ET POLICY PE EXE or DLL Windows file download HTTP		
	34.104.35.123	10.2.65.219	ET POLICY PE EXE or DLL Windows file download HTTP		

- Cân bằng tải: nâng cao năng lực xử lý thông qua việc phân phối luồng dữ liệu tới các thành phần xử lý song song

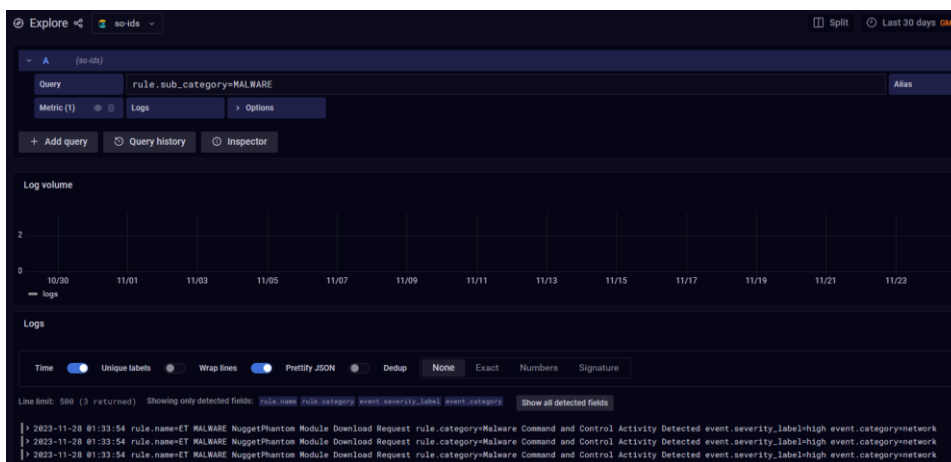
```

1332
1333 output:
1334   enabled: true
1335   hosts:
1336     - "Receiver1:5644"
1337     - "Receiver2:5644"
1338   loadbalance: true
1339   worker: 2
1340   bulk_max_size: 2048
1341

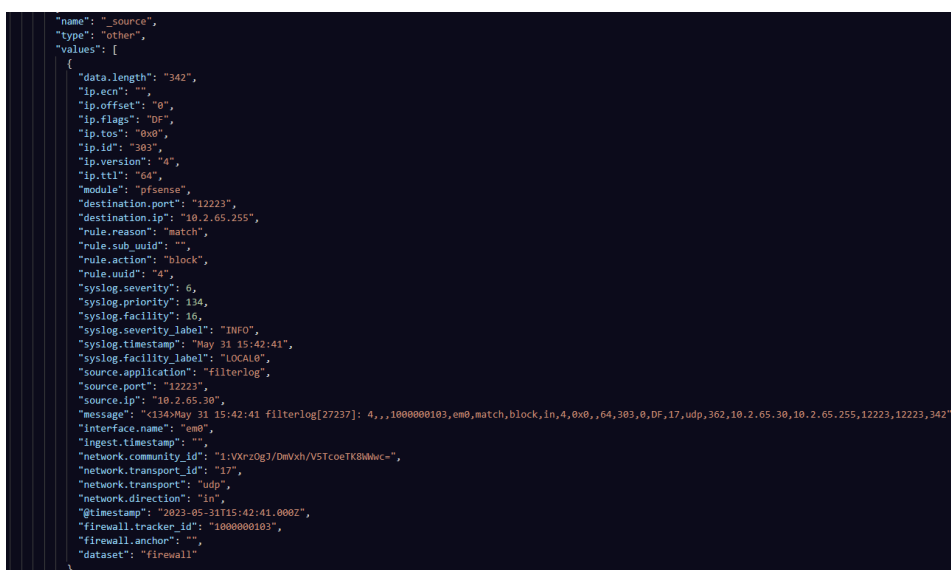
```

- Hỗ trợ xử lý dữ liệu: 10 Gbps

- Hỗ trợ khả năng phát hiện tấn công xâm nhập và malware.



- Cho phép nhận dạng tất cả ứng dụng mạng của Data Center (DC), Sở/ban/ngành, Quận/huyện/thành phố và dự phòng được trong tương lai. SIEM Collector cho phép nhận dạng các ứng dụng mà đơn vị sử dụng. Người dùng có thể tùy chỉnh danh sách ứng dụng được sử dụng trong đơn vị của mình.
- Dữ liệu được giảm thiểu từ PCAP sang metadata với tỉ lệ: 100:1 (SIEM Collector có khả năng chuyển đổi PCAP sang metadata với tỷ lệ nén đạt 100:1).
- Các dữ liệu được bắt như Network, Server, Ứng dụng, người dùng, syslog sẽ được chuyển đổi thành dạng JSON metadata, gửi về Bộ nhận dữ liệu (Receiver) tại trung tâm.



- Cảm biến có thể được sử dụng như một công cụ để phân tích cú pháp và chuyển tiếp log. SIEM Collector có thể được sử dụng như một cảm biến giám sát lưu lượng mạng hay một điểm tiếp nhận dữ liệu log từ các thiết bị điểm cuối để chuyển chúng tới thành phần xử lý trung tâm.

- Có khả năng bắt các thông tin sau: Thông tin từ Lớp 2 đến Lớp 7 bao gồm các loại dữ liệu: Dữ liệu Network, Server, ứng dụng, người dùng, syslog.

```

||| @ client.bytes 114047
||| @ client.ip 192.168.100.201
||| @ client.ip_bytes 118683
||| @ client.packets 89
||| @ client.port 49998
||| @ connection.bytes.missed 33304
||| @ connection.history ShADadGFf
||| @ connection.local.originator true
||| @ connection.local.responder true
||| @ connection.state SF
||| @ connection.state_description Normal SYN/FIN completion
||| @ destination.ip 192.168.100.200
||| @ destination.port 4506
||| @ ecs.version 1.12.0
||| @ event.category network
||| @ event.dataset conn
||| @ event.duration 0.017503976821899414
||| @ event.ingested 2023-11-28T04:07:20.209Z

```

```

||| @ client.ip 192.168.100.166
||| @ client.port 59206
||| @ destination.ip 192.168.100.1
||| @ destination.port 53
||| @ dns.answers.name 192.168.100.166
||| @ dns.authoritative true
||| @ dns.highest_registered_domain [REDACTED]
||| @ dns.id 7314
||| @ dns.parent_domain [REDACTED]
||| @ dns.parent_domain_length 6
||| @ dns.query.class 1
||| @ dns.query.class_name C_INTERNET
||| @ dns.query.length 14
||| @ dns.query.name [REDACTED]
||| @ dns.query.rejected false
||| @ dns.query.type 1
||| @ dns.query.type_name A
||| @ dns.recursion.available true
||| @ dns.recursion.desired true
||| @ dns.reserved 0
||| @ dns.response.code 0
||| @ dns.response.code_name NOERROR
||| @ dns.subdomain bti
||| @ dns.subdomain_length 3
||| @ dns.top_level_domain com
||| @ dns.truncated false
||| @ dns.ttls 1
||| @ ecs.version 1.12.0
||| @ event.category network
||| @ event.dataset dns

```

- Có khả năng buffer dữ liệu. SIEM Collector sở hữu cơ chế bufer dữ liệu trên RAM hoặc Disk.
- Làm giàu dữ liệu với các thông tin: Hostname, thông tin người dùng, Threat Intelligence và Vị trí.

destination_geo.conti	destination_geo.coun	destination_geo.coun	destination_geo.ip	destination_geo.locat	destination_geo.locat	destination_geo.time	destination_ip	destination.port	destination_geo.asn	destination_geo.ip
North America	US	United States	8.8.8.8	37.8	-98	America/Chicago	8.8.8.8	53	15169	8.8.8.8
North America	US	United States	8.8.8.8	37.8	-98	America/Chicago	8.8.8.8	53	15169	8.8.8.8
							192.168.100.1	53		
North America	US	United States	8.8.8.8	37.8	-98	America/Chicago	8.8.8.8	53	15169	8.8.8.8
North America	US	United States	8.8.8.8	37.8	-98	America/Chicago	8.8.8.8	53	15169	8.8.8.8

- Giảm thiểu, chuyển đổi, tương quan, có khả năng tìm kiếm, khả năng truy xuất báo cáo và khả năng hành động. SIEM Collector có khả năng giảm thiểu, chuyển đổi cũng như tương quan sự kiện để phát hiện các hành vi bất thường xảy ra trên mạng. Nguồn dữ liệu này có thể được truy xuất phục vụ công tác điều tra hay lập báo cáo. SIEM Collector cũng có khả năng đưa ra các hành động phản ứng trên các điểm cuối nơi mà nó được kết nối.
- Có khả năng điều khiển từ trung tâm:
 - ✓ Có khả năng nâng cấp từ xa
 - ✓ Có khả năng khởi động lại từ xa

The screenshot displays two parts of the SIEM Collector interface. The top part is a table for version management with columns: Tên phiên bản, Loại, Tình trạng, Phiên bản, Nhà sản xuất, Mô tả, and Thời gian cập nhật. It lists two versions of 'version_initial_siem' using 'grafana' and 'onion' types. The bottom part shows a sensor status card for 'Forward' on IP '192.168.100.201', including details like 'Online Since', 'Production EPS', 'Consumption EPS', 'Process Status', 'Connection Status', and 'Raid Status'.

- Có khả năng quản trị, cấu hình từ trung tâm

The screenshot shows the 'Danh sách tường lửa' (Firewall List) interface. It features a search bar, buttons for 'Quản lý nhóm luật' and '+ Thêm mới luật tường lửa', and dropdown menus for 'Minion' and 'Nhóm'. Below is a table with columns: Tên, Nguồn, Chain, Giao thức, Hoạt động, and Mô tả. A rule is listed with 'Tên: Tiếp nhận Syslog', 'Nguồn: 192.168.100.222', 'Chain: INPUT', 'Giao thức: tcp', 'Hoạt động: ACCEPT', and 'Mô tả: Tiếp nhận Syslog TCP'.

- Có khả năng thu thập lưu lượng mạng qua mirror port hoặc thiết bị tap. SIEM Collector có thể sử dụng kết hợp với mirror port hay các thiết bị như TAP nhằm mang lại hiệu quả giám sát tốt nhất.