AUNIDS

AUNIDS actively detects any malicious activity that is occurring inside the network. It continuously monitors the traffic flow across the network and correspondingly reports events and alerts on a real-time basis in the web-based GUI.

Features

Network Security Monitoring

Security Monitoring of network packets to provide information about the potential threats.

Intrusion Detection System

Intrusion Detection System to detect any intrusion inside the network.

Offline Analysis of PCAP files

Provides support for the offline analysis of PCAP files.

Scalable Flow Engine

Provides a scalable flow engine.

IP Reputation

IP reputation provides a way to handle IP addresses with a bad reputation.

Log Rotation

Provides flexibility for the management of log files.

Multi-Threading

Provides a multi-threaded architecture to handle the higher bandwidth.

Web-Based GUI

Provides web-based GUI for the visualization of events and alerts.

Key Benefits

- Real-time detection of the network against malicious activities
- Real-time visualization of events and alerts
- Collection of the logs for the analysis to mitigate the future threats
- Signatures can be written based on collected logs to increase the protection against potential threats
- Give insight into the activities occurring in a network

What is AUNIDS?

- AUNIDS actively detects any malicious activity that is occurring inside the network
- AUNIDS continuously watches the traffic flow across the network
- AUNIDS reports events and alerts in real-time in the web-based GUI

Why AUNIDS?

- AUNIDS can detect any malicious activity occurring inside the network
- AUNIDS provides real-time visualization of the events and alerts of the network and provides security professionals an insight into the network activities

AUNIDS Dashboard

- AUNIDS dashboard provides the visualization of real-time events and alerts
- It also provides log and time-series analytics
- Logs can be exported by security professionals for further analysis from the dashboard

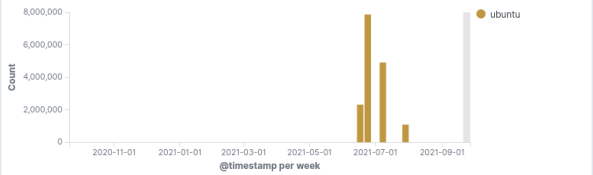
Search | KQL | Last 1 year | Show dates | Refresh

+ Add filter

Navigation [Filebeat Suricata]

SURICATA Events | Alerts

Top Alerting Hosts [Filebeat Suricata]



Top Alert Signatures [Filebeat Suricata]

Alert Signature	Alert Category	Count
ET INFO Observed DNS Query to .cloud TLD	Potentially Bad Traffic	99
ET USER_AGENTS Microsoft Device Metadata Retrieval Client User-Agent	Unknown Traffic	84
ET POLICY Windows Update P2P Activity	Not Suspicious Traffic	73
ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management	Not Suspicious Traffic	56
PROTOCOL-ICMP Unusual PING detected	Information Leak	50
ET POLICY Possible Kali Linux hostname in DHCP Request Packet	Potential Corporate Privacy Violation	27
PROTOCOL-DNS IPv6 host name enumeration	Attempted Information Leak	21
SURICATA STREAM CLOSEWAIT FIN out of window	Generic Protocol Command Decode	19
PROTOCOL-SNMP Broadcast request	Attempted Information Leak	16
SURICATA STREAM bad window update	Generic Protocol Command Decode	16

Export: Raw Formatted

1 2 »

Alerts - Top Source Countries [Filebeat Suricata]

Source Country	Count
US	912
GB	204
PK	98
NL	84
SG	14

Export: Raw Formatted

1 2 »

Alerts - Top Destination Countries [Filebeat Suricata]

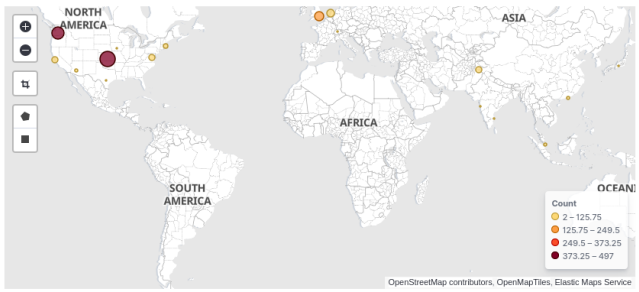
Source Country	Count
US	1,160
GB	214
NL	125
PK	96
HK	19

Export: Raw Formatted

1 2 »

Alert - Source Location [Filebeat Suricata]

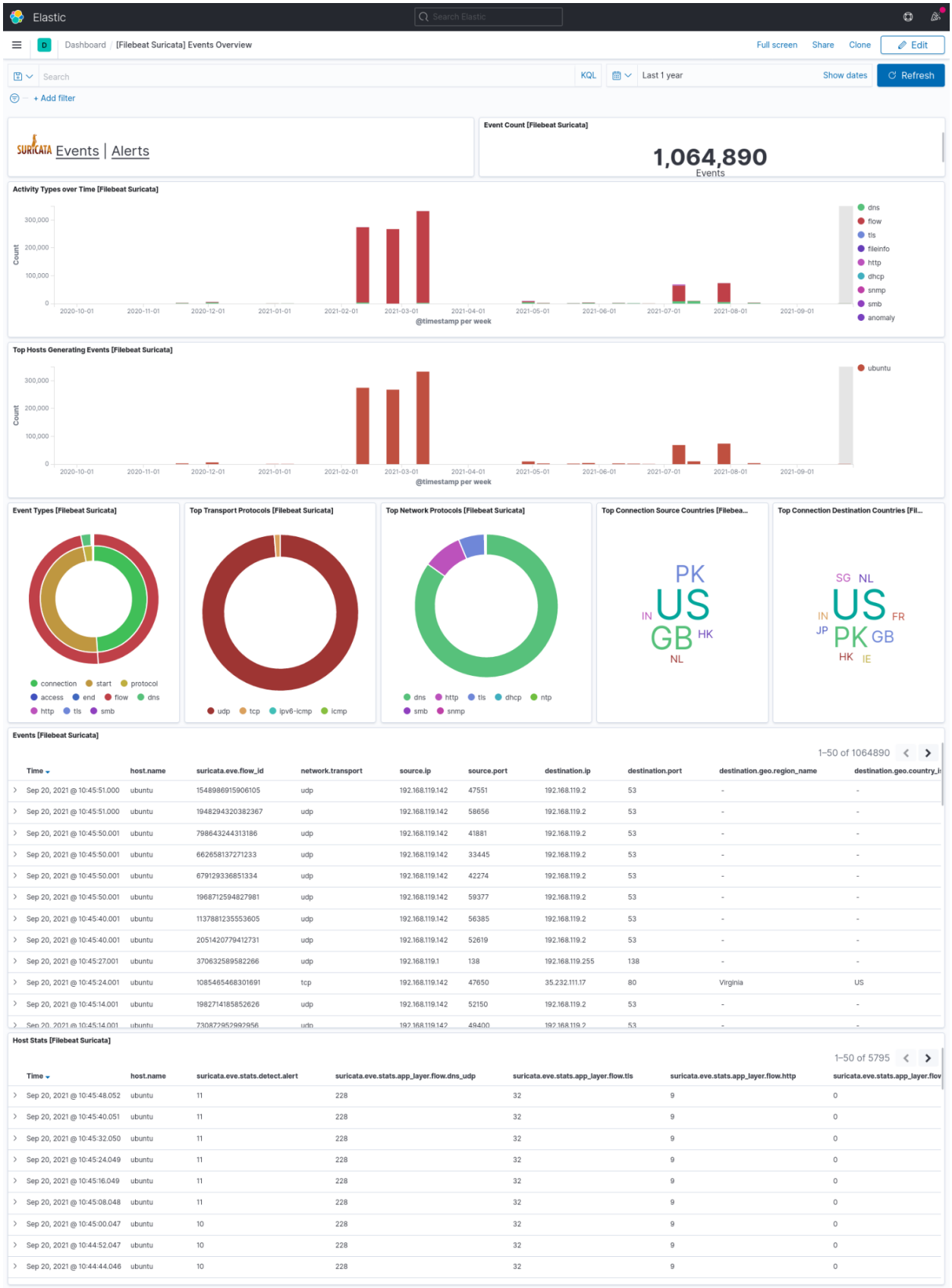
Alert - Destination Location [Filebeat Suricata]



Alerts [Filebeat Suricata]

1–50 of 16181527

Time	host.name	suricata.eve.flow_id	source.ip	source.port	destination.ip	destination.port	source.geo.country_iso_code	destination.geo.country_iso_code
Sep 20, 2021 @ 10:47:09.409	ubuntu	1668344081818264	192.168.119.142	34128	91.189.91.39	80	-	US
Sep 20, 2021 @ 10:47:09.146	ubuntu	1668344081818264	192.168.119.142	34128	91.189.91.39	80	-	US
Sep 20, 2021 @ 10:47:08.598	ubuntu	1668344081818264	192.168.119.142	34128	91.189.91.39	80	-	US
Sep 20, 2021 @ 10:45:01.773	ubuntu	2155268803235507	13.35.181.51	443	192.168.119.142	54290	US	-
Sep 20, 2021 @ 10:44:22.294	ubuntu	1751224051643041	192.168.119.142	33984	91.189.91.39	80	-	US
Sep 20, 2021 @ 10:43:41.289	ubuntu	1751224051643041	192.168.119.142	33984	91.189.91.39	80	-	US
Sep 20, 2021 @ 10:42:28.684	ubuntu	566848160822653	192.168.119.142	33950	91.189.91.39	80	-	US
Sep 20, 2021 @ 10:41:30.626	ubuntu	753273348718079	34.120.127.120	443	192.168.119.142	48544	US	-
Sep 20, 2021 @ 10:40:49.364	ubuntu	842007380989880	192.168.119.142	33944	91.189.91.39	80	-	US


Elastic
Search Elastic
Dashboard / [Filebeat Suricata] Events Overview
Full screen
Share
Clone
Edit
Search
KQL
Last 1 year
Show dates
Refresh
+ Add filter
SURICATA Events | Alerts
Event Count [Filebeat Suricata]
1,064,890
Events
Activity Types over Time [Filebeat Suricata]
Count
@timestamp per week
dns
flow
tls
fileinfo
http
dhcp
snmp
smb
anomaly
Top Hosts Generating Events [Filebeat Suricata]
ubuntu
Event Types [Filebeat Suricata]
connection
start
protocol
access
end
flow
dns
http
tls
smb
Top Transport Protocols [Filebeat Suricata]
udp
tcp
ipv6-icmp
icmp
Top Network Protocols [Filebeat Suricata]
dns
http
tls
dhcp
ntp
smb
snmp
Top Connection Source Countries [Filebea...
PK
US
IN
GB
HK
NL
Top Connection Destination Countries [Fil...
SG
NL
US
IN
FR
JP
PK
GB
HK
IE
Events [Filebeat Suricata]
1–50 of 1064890
Time
host.name
suricata.eve.flow_id
network.transport
source.ip
source.port
destination.ip
destination.port
destination.geo.region_name
destination.geo.country_i
Sep 20, 2021 @ 10:45:51.000 ubuntu 1548986915906105 udp 192.168.119.142 47551 192.168.119.2 53 - -
Sep 20, 2021 @ 10:45:51.000 ubuntu 1948294320382367 udp 192.168.119.142 58656 192.168.119.2 53 - -
Sep 20, 2021 @ 10:45:50.001 ubuntu 798643244313186 udp 192.168.119.142 41881 192.168.119.2 53 - -
Sep 20, 2021 @ 10:45:50.001 ubuntu 662658137271233 udp 192.168.119.142 33445 192.168.119.2 53 - -
Sep 20, 2021 @ 10:45:50.001 ubuntu 679129336851334 udp 192.168.119.142 42274 192.168.119.2 53 - -
Sep 20, 2021 @ 10:45:50.001 ubuntu 1968712594827981 udp 192.168.119.142 59377 192.168.119.2 53 - -
Sep 20, 2021 @ 10:45:40.001 ubuntu 1137881235553605 udp 192.168.119.142 56385 192.168.119.2 53 - -
Sep 20, 2021 @ 10:45:40.001 ubuntu 2051420779412731 udp 192.168.119.142 52619 192.168.119.2 53 - -
Sep 20, 2021 @ 10:45:27.001 ubuntu 370632589582266 udp 192.168.119.1 138 192.168.119.255 138 - -
Sep 20, 2021 @ 10:45:24.001 ubuntu 1085465468301691 tcp 192.168.119.142 47650 35.232.111.17 80 Virginia US
Sep 20, 2021 @ 10:45:14.001 ubuntu 1982714185852626 udp 192.168.119.142 52150 192.168.119.2 53 - -
Sep 20, 2021 @ 10:45:14.001 ubuntu 730872952992956 udp 192.168.119.142 49400 192.168.119.2 53 - -
Host Stats [Filebeat Suricata]
1–50 of 5795
Time
host.name
suricata.eve.stats.detect.alert
suricata.eve.stats.app_layer.flow.dns_udp
suricata.eve.stats.app_layer.flow.tls
suricata.eve.stats.app_layer.flow.http
suricata.eve.stats.app_layer.flow
Sep 20, 2021 @ 10:45:48.052 ubuntu 11 228 32 9 0
Sep 20, 2021 @ 10:45:40.051 ubuntu 11 228 32 9 0
Sep 20, 2021 @ 10:45:32.050 ubuntu 11 228 32 9 0
Sep 20, 2021 @ 10:45:24.049 ubuntu 11 228 32 9 0
Sep 20, 2021 @ 10:45:16.049 ubuntu 11 228 32 9 0
Sep 20, 2021 @ 10:45:08.048 ubuntu 11 228 32 9 0
Sep 20, 2021 @ 10:45:00.047 ubuntu 10 228 32 9 0
Sep 20, 2021 @ 10:44:52.047 ubuntu 10 228 32 9 0
Sep 20, 2021 @ 10:44:44.046 ubuntu 10 228 32 9 0