Optimizing and Using Snort Data

Joe Abraham
Cybersecurity Consultant

@joeabrah www.defendthenet.com

Snort's Output Modules

Allows Snort users to output data using various methods

Customize the formatting of alerts and logs

After preprocessors and detection engines

Types:

- alert_syslog
- alert_fast
- alert_full
- alert_unixsock
- log_tcpdump
- csv
- unified 2
- log null

Syslog Alert

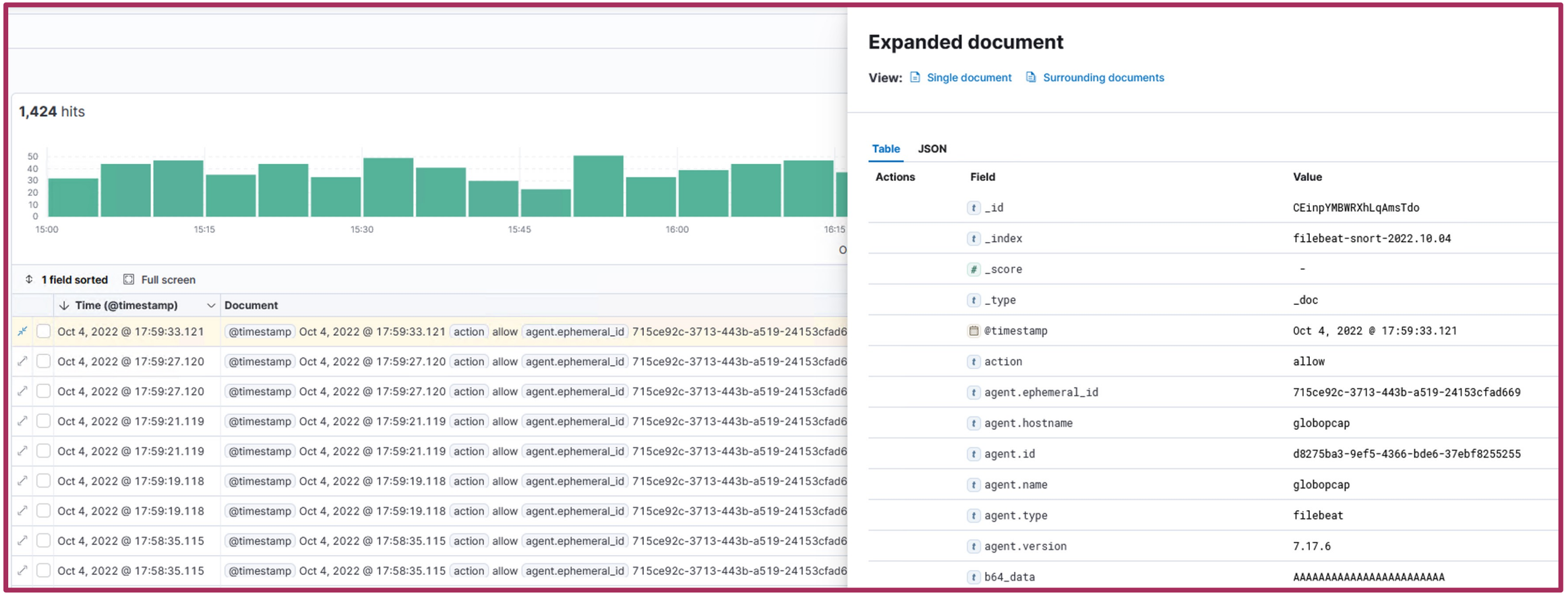
```
output alert_syslog: host=192.168.30.13:3514, log_local3
```

Fast and Full Alerting

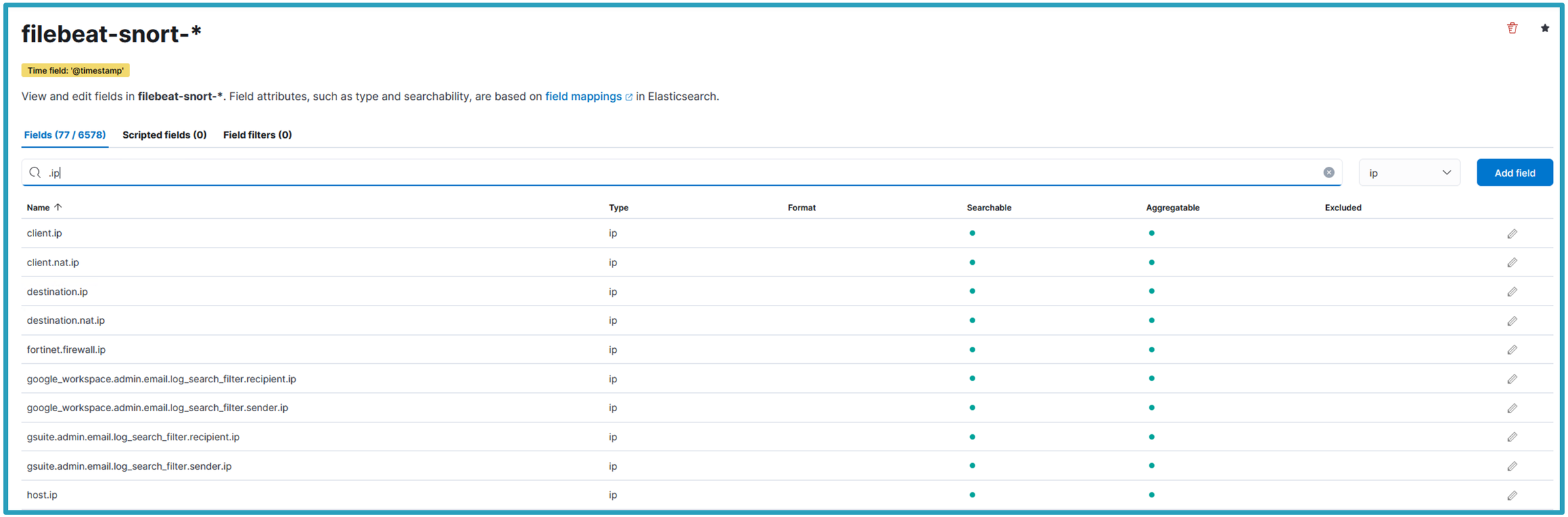
alert_fast logs data without the packet header

alert_full logs data with the packet header

Searching in Kibana



Controlling the Snort Fields

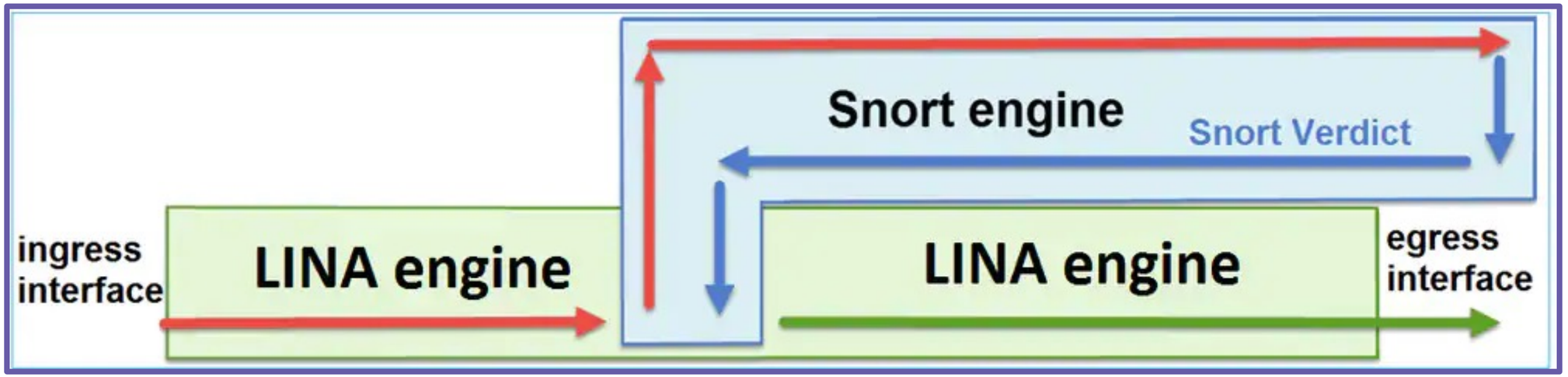


Demo

Explore Snort data in Kibana

Cisco Secure Firewall and Snort

Secure Firewall Traffic Flow



Source: https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212321-clarify-the-firepower-threat-defense-acc.html

Snort Policies

Can create multiple inspection policies

Can control behavior on per-rule basis

Granular rule management

Secure Firewall intrusion policy recommendations

Making Use of Snort Data

Context information helps with workflows

Visibility is necessary for investigations and threat hunting

Integrations with other Cisco Security products provides:

- **Streamlined investigations**
- **Response orchestration**
- **Additional context sharing**

Investigating Events

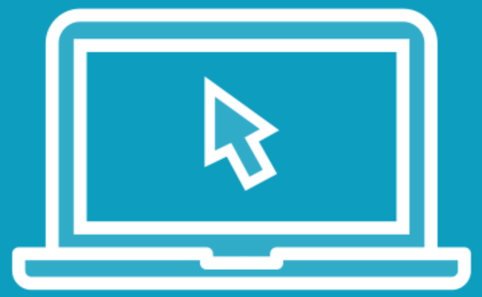
Prioritizes events

Classifies events

Download relevant packets

Easier investigations

Demo



Explore Snort inspection with Cisco Secure Firewall

Up Next:
Snort Pre-processors