ELK

operational security at scale

Elastic

- best used with a template / map configuration
- indexes as big as 25 gig
- index runs in memory
- ecs is elastic’s own standard

-What data are we storing
-what index are we in

- Discover

- last 15 minutes, last etc.
- can drag on the histogram to zoom

- if you dont both:
 3 hour timeframe and host filter when looking throuhg PID's you will be wrong

\\\\ field   \\\\ value

Logstash

 - covert data, middleware for elasticsearch

 host ips sometimes show more than 1 set of ips \\\\\

 \\\\\\\\ user.name

 \\\\\\\\ host.ip

 \\\\\\\\ destination.port

finding hostnames:

visualize host.name data into a table

finding usernames :

user.name.keyword visualized into a table

event.category:"network" in query

process.parent.name:"program.exe"