

Security Project1

Φώτης Παπαδήμας, Δημήτρης Σοφός, Γιώργος Φασάκης
2022202204022, 2022202204013, 2022202204011

Τμήμα Πληροφορικής και Τηλεπικοινωνιών
Πανεπιστήμιο Πελοποννήσου

Email: dit2222@go.uop.gr, dit2213@go.uop.gr, dit2211@go.uop.gr

ΑΣΦΑΛΕΙΑ ΚΑΙ ΟΠΤΙΚΟΠΟΙΗΣΗ ΜΕΓΑΛΩΝ ΔΕΔΟΜΕΝΩΝ

Νικόλαος Κολοκοτρώνης, Αναπληρωτής Καθηγητής

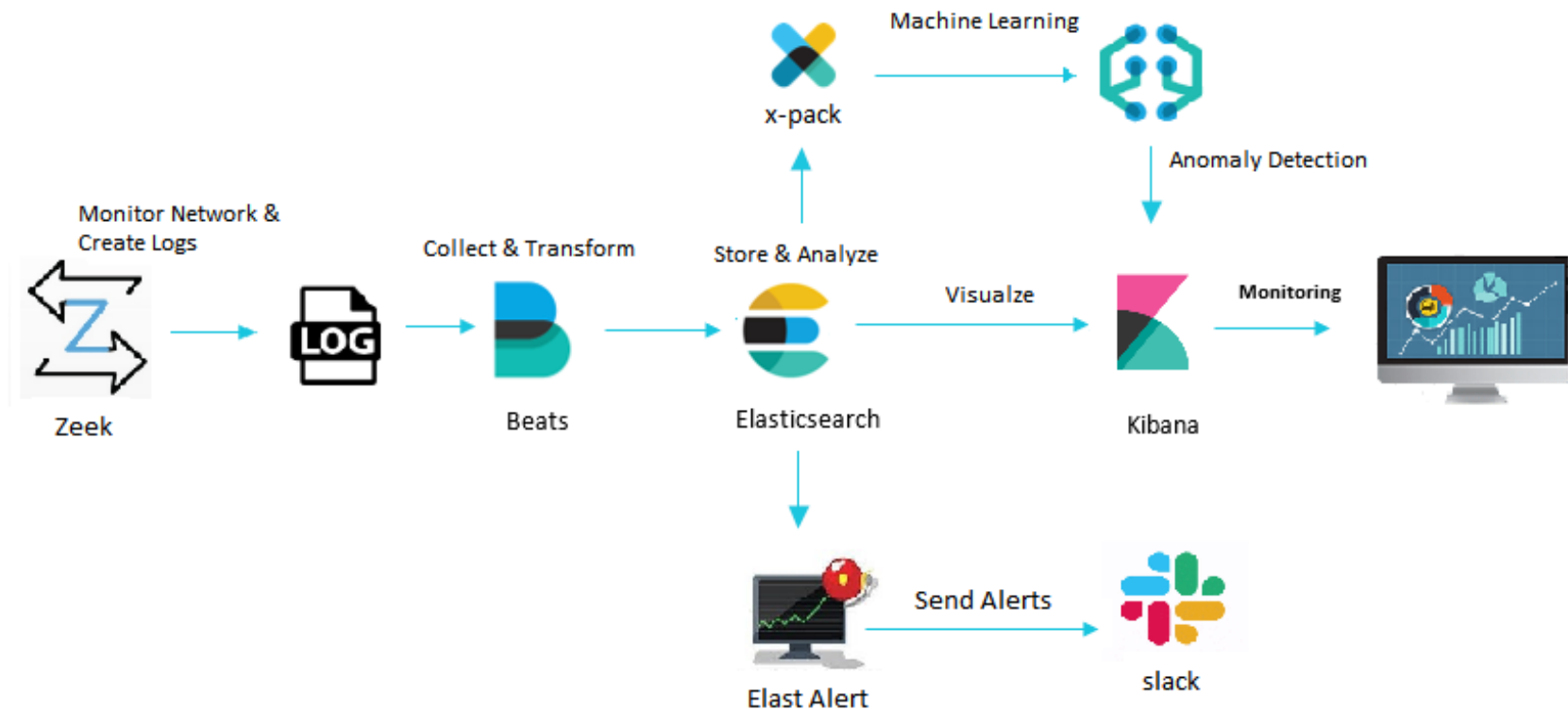
Νικόλαος Πλατής, Επίκουρος Καθηγητής

System

- **Ubuntu 20.04.06 VM (2 CPU, 8GB RAM, 30GB Storage)**
- **Zeek + ELK Stack** running on a docker container



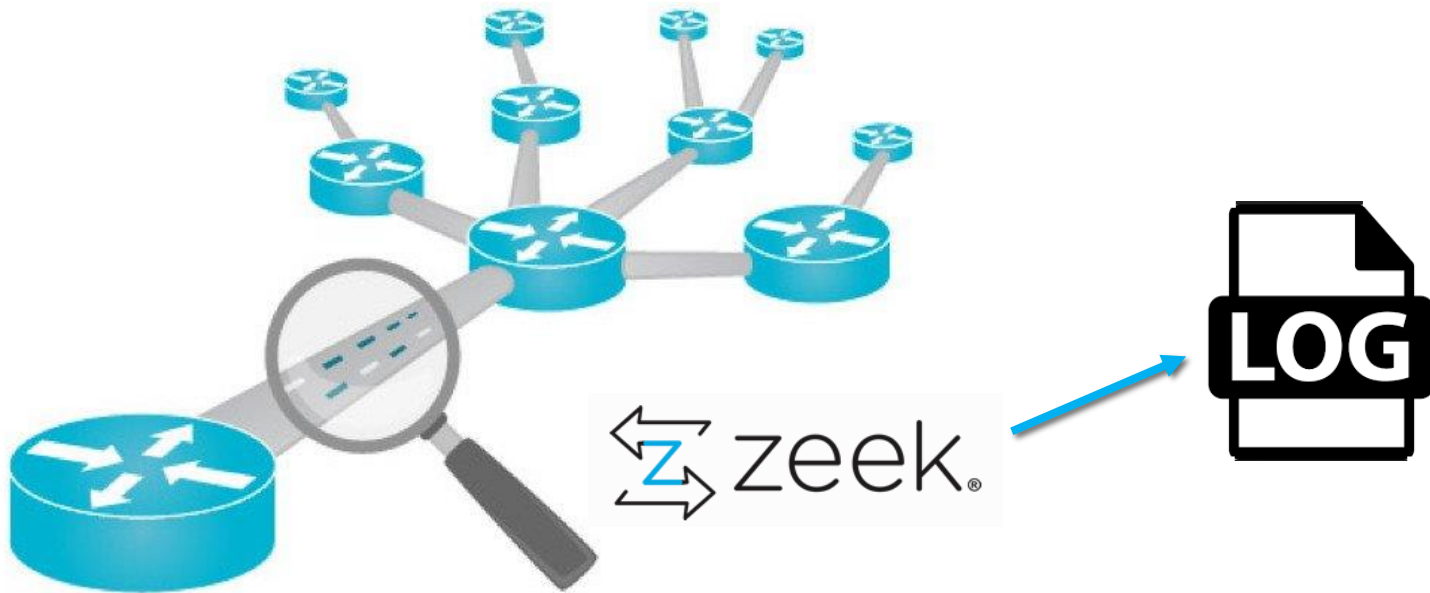
Intrusion Detection System



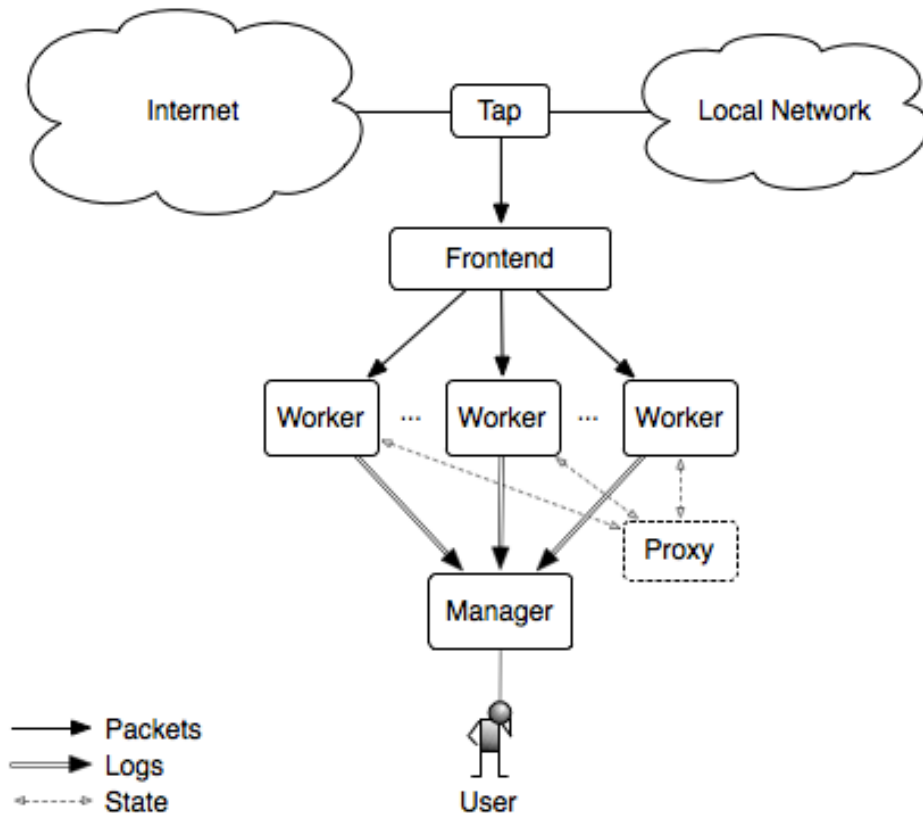
Zeek

Zeek

- A Network Monitoring tool to create Logs



Zeek Cluster



■ Workers

- Monitor network and capture logs

■ Manager

- Gather and Manage logs

■ Logger

- Help Manager

■ Proxy

- Help for load balancing

Zeek Config

```
GNU nano 4.8 /opt/zeek/etc/node.cfg

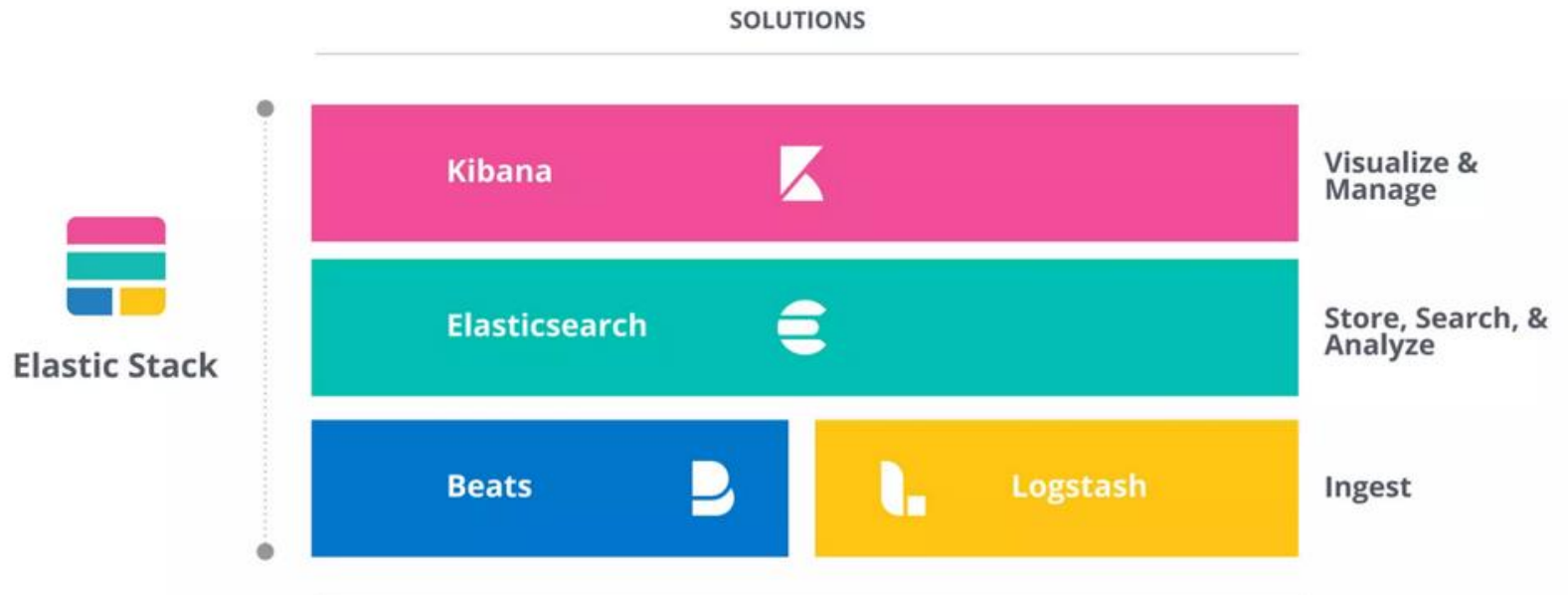
[logger-1]
type=logger
host=localhost
#
[manager]
type=manager
host=localhost
#
[proxy-1]
type=proxy
host=localhost
#
[worker-1]
type=worker
host=localhost
interface=enp0s3
lb_method=pf_ring
lb_procs=1
#
[worker-2]
type=worker
host=localhost
interface=enp0s3
lb_method=pf_ring
lb_procs=1
#
[worker-3]
type=worker
host=localhost
interface=enp0s3
lb_method=pf_ring
lb_procs=1

env_vars=PCAP_PF_RING_CLUSTER_ID=99
```

ELK Stack

ELK Stack

- A set of working-together tools to store, analyze and visualize network logs and events.
- Provide a variety of addons and interfaces.



FileBeat

FileBeat

- FileBeat gather logs from Zeek
- Transform them to json format
- Send the logs to ElasticSearch

FileBeat Config

```
GNU nano 4.8 /etc/filebeat/modules.d/zeek.yml
# Module: zeek
# Docs: https://www.elastic.co/guide/en/beats/filebeat/7.17/filebeat-module-zeek.html

module: zeek
capture_loss:
  enabled: true
  var.paths: ["/opt/zeek/logs/current/capture_loss.log", "/opt/zeek/logs/*.capture_loss.json"]
connection:
  enabled: true
  var.paths: ["/opt/zeek/logs/current/conn.log", "/opt/zeek/logs/*.conn.json"]
dce_rpc:
  enabled: false
dhcp:
  enabled: true
  var.paths: ["/opt/zeek/logs/current/dhcp.log", "/opt/zeek/logs/*.dhcp.json"]
dnp3:
  enabled: false
dns:
  enabled: true
  var.paths: ["/opt/zeek/logs/current/dns.log", "/opt/zeek/logs/*.dns.json"]
dpd:
  enabled: false
files:
  enabled: true
  var.paths: ["/opt/zeek/logs/current/files.log", "/opt/zeek/logs/*.files.json"]
ftp:
  enabled: false
http:
  enabled: true
  var.paths: ["/opt/zeek/logs/current/http.log", "/opt/zeek/logs/*.http.json"]
intel:
  enabled: false
```

```
GNU nano 4.8 /etc/filebeat/filebeat.yml
# ===== Outputs =====
# Configure what output to use when sending the data collected by the beat.
# ----- Elasticsearch Output -----
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["localhost:9200"]

  # Protocol - either 'http' (default) or 'https'.
  #protocol: "https"

  # Authentication credentials - either API key or username/password.
  #api_key: "id:api_key"
  username: "elastic"
  password: "lKmwDjHkItH5k41KNA9F"
```

ElasticSearch

ElasticSearch

- Store logs from FileBeat into a NoSQL db
- Assist on search and Analysis of the logs
- Send Data to Kibana

ElasticSearch Config

```
GNU nano 4.8 /etc/elasticsearch/elasticsearch.yml
# ----- Network -----
#
# By default Elasticsearch is only accessible on localhost. Set a different
# address here to expose this node on the network:
#
network.host: 0.0.0.0
#
# By default Elasticsearch listens for HTTP traffic on the first free port it
# finds starting at 9200. Set a specific HTTP port here:
#
http.port: 9200
#
# For more information, consult the network module documentation.
#
# ----- Discovery -----
#
# Pass an initial list of hosts to perform discovery when this node is started:
# The default list of hosts is ["127.0.0.1", "[::1]"]
#
discovery.type: single-node
#discovery.seed_hosts: ["host1", "host2"]
#
```

Kibana

Kibana

- Read the logs from ElasticSearch
- Provide a variety of Visualization and Analysis tools
- Provide a variety of addons and interfaces
- Service running at <http://localhost:5601/>

Kibana Config

```
GNU nano 4.8 /etc/kibana/kibana.yml Modified
# The URLs of the Elasticsearch instances to use for all your queries.
#elasticsearch.hosts: ["http://localhost:9200"]

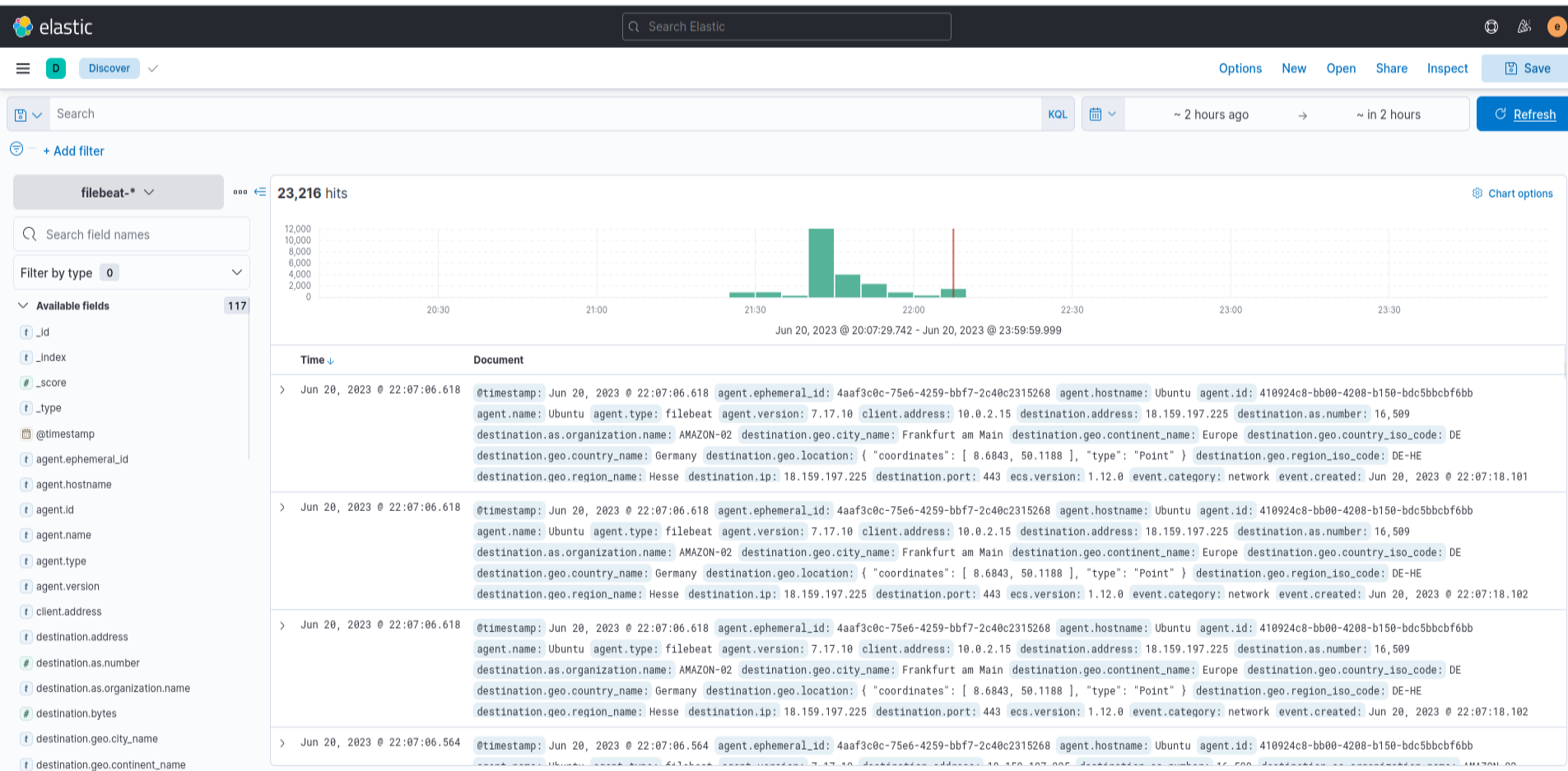
# Kibana uses an index in Elasticsearch to store saved searches, visualizations and
# dashboards. Kibana creates a new index if the index doesn't already exist.
#kibana.index: ".kibana"

# The default application to load.
#kibana.defaultAppId: "home"

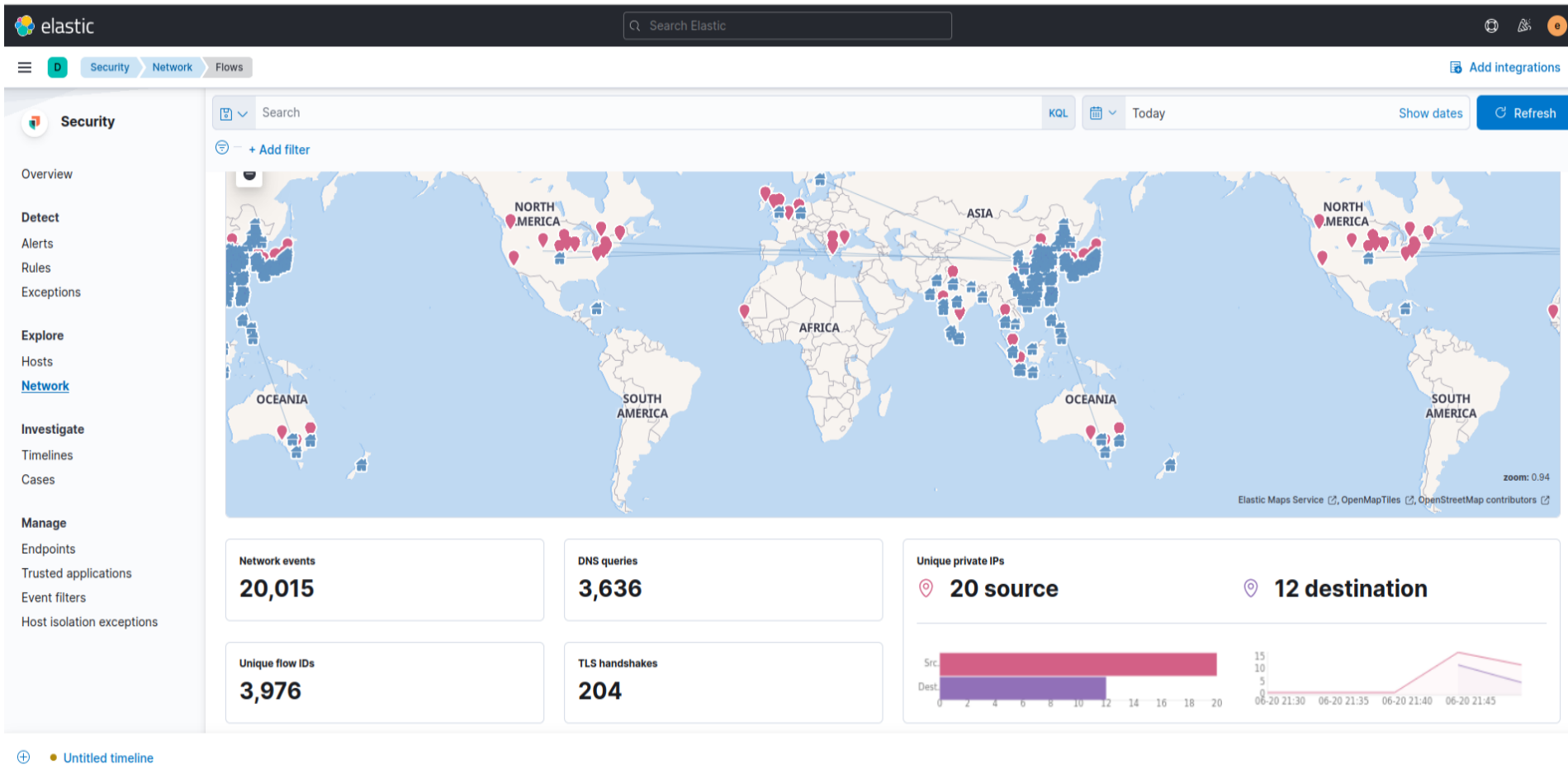
# If your Elasticsearch is protected with basic authentication, these settings provide
# the username and password that the Kibana server uses to perform maintenance on the
# index at startup. Your Kibana users still need to authenticate with Elasticsearch if
# is proxied through the Kibana server.
elasticsearch.username: "kibana_system"
elasticsearch.password: "QB3FUPpHEMK74rVsmTa4"

xpack.encryptedSavedObjects.encryptionKey: 0091010eb3082bb013046f3fb903739a
xpack.reporting.encryptionKey: cad5119eae2932e1c8e5ecd2549dd027
xpack.security.encryptionKey: a6781652340f1afb79c4ad454ce2c8dd
```

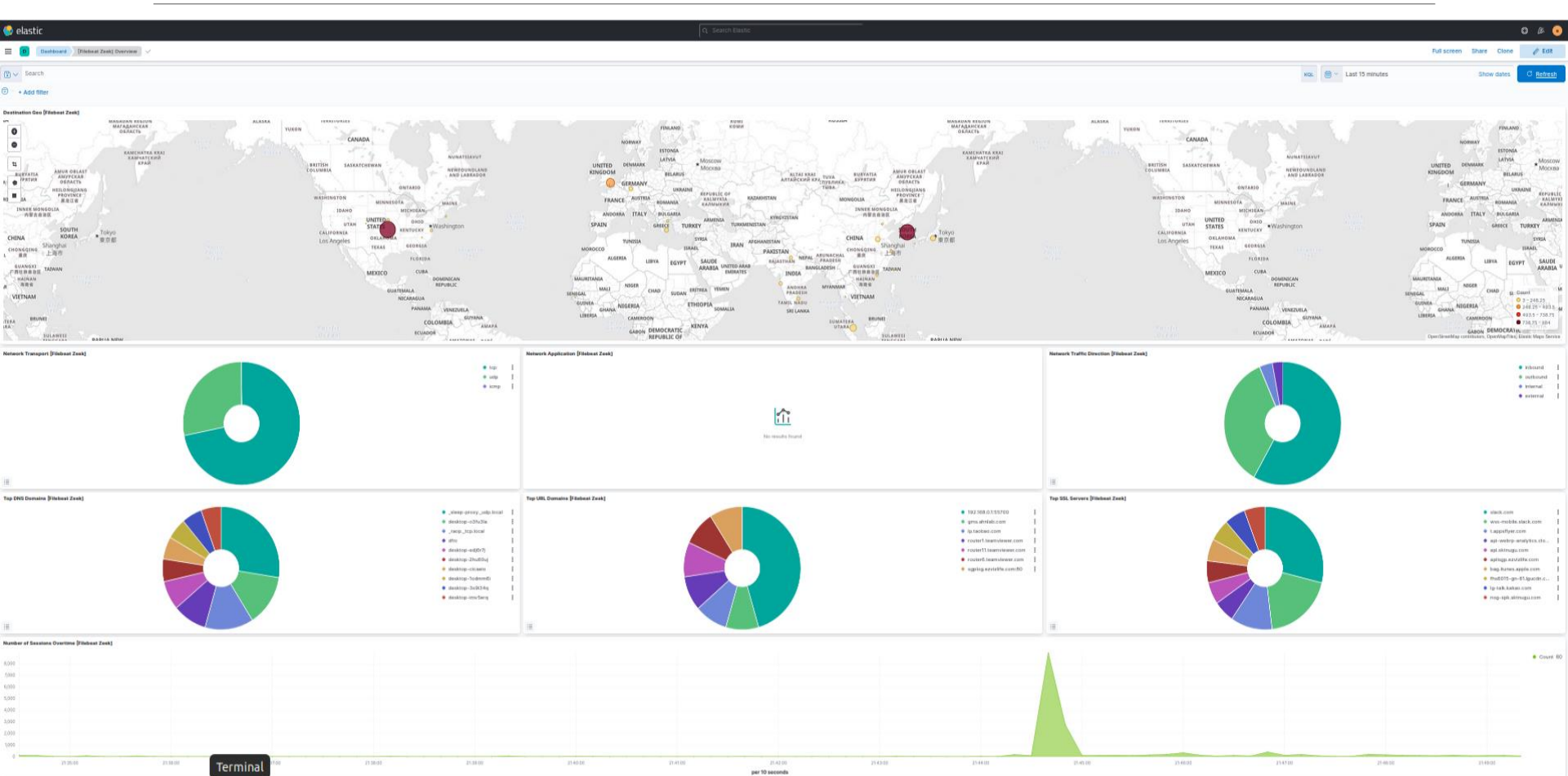
Kibana - Discovery



Kibana – Security / Network



Kibana – Dashboard



ElastAlert

ElastAlert

- Read logs from ElasticSearch
- A rule based tool
- Create alerts



ElastAlert – Rules (1)

```
# Rule name, must be unique
name: Big Data Security and Visualization

# (Required)
# Type of alert.
# the frequency rule type alerts when num_events events occur with timeframe time
type: frequency

# (Required)
# Index to search, wildcard supported
index: filebeat-*

# (Required, frequency specific)
# Alert when this many documents matching the query occur within a timeframe
num_events: 20

# (Required, frequency specific)
# num_events must occur within this amount of time to trigger an alert
timeframe:
  hours: 1

# (Required)
# A list of Elasticsearch filters used for find events
# These filters are joined with AND and nested in a filtered query
# For more info: http://www.elasticsearch.org/guide/en/elasticsearch/reference/current/query-dsl.html
filter:
- term:
    source.as.organization.name: "China Mobile Communications Group Co., Ltd."

# (Required)
# The alert is use when a match is found
alert:
- "slack"

# (required, email specific)
# a list of email addresses to send alerts to
slack:
slack_webhook_url: "https://hooks.slack.com/services/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"
slack_title: "China Mobile Communications Group Co., Ltd. EVENT!!!"
```


ElastAlert – Rules (2)

```
# Alert when this many documents matching the query occur within a timeframe
num_events: 3

# num_events must occur within this amount of time to trigger an alert
timeframe:
  minutes: 1

# A list of elasticsearch filters used for find events
# These filters are joined with AND and nested in a filtered query
# For more info: http://www.elasticsearch.org/guide/en/elasticsearch/reference/current/query-dsl.html
filter:
- query:
    query_string:
      query: "event.type:authentication_failure"

index: filebeat-*

# When the attacker continues, send a new alert after x minutes
realert:
  minutes: 1

query_key:
- source.ip

include:
- host.hostname
- user.name
- source.ip

include_match_in_root: true

alert_subject: "SSH abuse on <{}> "
alert_subject_args:
- host.hostname

alert_text: |-
  An attack on {} is detected.
  The attacker looks like:
  User: {}
  IP: {}
alert_text_args:
- host.hostname
- user.name
- source.ip

# The alert is use when a match is found
alert:
- "slack"

slack:
  slack_webhook_url: "https://hooks.slack.com/services/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"
  slack_title: "SSH Attack Event!!"

alert_text_type: alert_text_only
```


Elastic ML

Elastic ML

- Read logs from ElasticSearch
- Accessible from Kibana -> Analytics -> Machine Learning
- Ready to use Jobs from -> Network -> System Security
- Option to create custom Jobs
- Create oversights and detect Anomalies on Data
- Possible to Create alerts



Elastic ML – Population Job



Q Search Elastic

Machine Learning

Anomaly Detection

Create job

Population

Create job: Population

Using index pattern filebeat-*

1

2

3

4

5

Time range

Pick fields

Job details

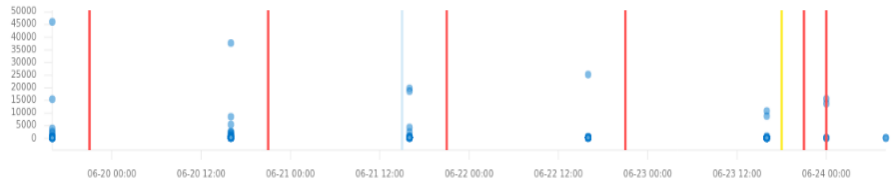
Validation

Summary

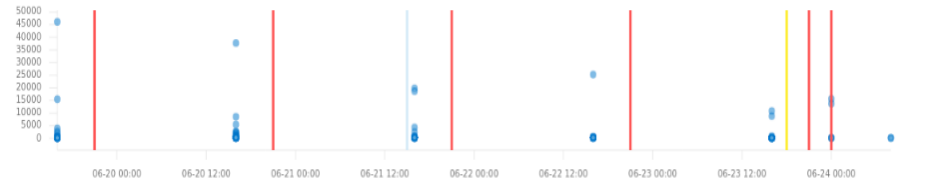
New job from index pattern filebeat-*

Population split by destination.ip

High count(Event rate)



Count(Event rate)



Job ID population	Bucket span 3h	Enable model plot False	Start Jun 19, 2023 @ 19:02:39.117
Job description No description provided	Population field destination.ip	Use dedicated index False	End Jun 24, 2023 @ 13:58:05.579
Groups security	Influencers destination.ip	Model memory limit 13MB	

☒ Start immediately

If unselected, job can be started later from the jobs list.

View results

Reset job

Start job running in real time

Create alert rule

Elastic ML – Multi metric Job

elastic

Search Elastic

Machine Learning

Anomaly Detection

Create job

Multi-metric

Create job: Multi-metric

Using index pattern filebeat-*

1

2

3

4

5

Time range

Pick fields


Job details

Validation

Summary

New job from index pattern filebeat-*

Count(Event rate)



Job ID

ddos

Job description

No description provided

Groups

security

☒ Start immediately

If unselected, job can be started later from the jobs list.

View results

Reset job

Start job running in real time

Create alert rule

Bucket span

15m

Split field

No split field selected

Influencers

destination.ip

Enable model plot

False

Use dedicated index

False

Model memory limit

11MB

Start

Jun 19, 2023 @ 19:02:39.117

End

Jun 24, 2023 @ 13:58:05.579

Elastic ML – Job Manager

Machine Learning

Anomaly Detection

Job Management

ID ↑	Description	Processed records	Memory status	Job state	Datafeed state	Latest timestamp	
<div><div></div><div>></div></div> ddos	<div>security</div> <p>Security: Network - looks for an unusually large spike in network activity to one destination country in the network logs. This could be due to unusually large amounts of reconnaissance or enumeration traffic. Data exfiltration activity may also produce such a surge in traffic to a destination country which does not normally appear in network traffic or business work-flows. Malware instances and persistence mechanisms may communicate with command-and-control (C2) infrastructure in their country of origin, which may be an unusual destination country for the source network.</p> <div>network</div> <div>security</div>	366,319	ok	opened	started	2023-06-24 14:06:37	<div><div></div><div></div><div></div></div> <div>...</div>
<div><div></div><div>></div></div> high_count_network_events high_count_by_destination_co untry	<p>Security: Network - looks for an unusually large spike in network traffic that was denied by network ACLs or firewall rules. Such a burst of denied traffic is usually either 1) a misconfigured application or firewall or 2) suspicious or malicious activity. Unsuccessful attempts at network transit, in order to connect to command-and-control (C2), or engage in data exfiltration, may produce a burst of failed connections. This could also be due to unusually large amounts of reconnaissance or enumeration traffic. Denial-of-service attacks or traffic floods may also produce such a surge in traffic.</p> <div>network</div> <div>security</div>	102,883	ok	closed	stopped	2023-06-20 22:14:06	<div><div></div><div></div><div></div></div> <div>...</div>
<div><div></div><div>></div></div> high_count_network_events high_count_network_denies	<p>Security: Network - looks for an unusually large spike in network traffic. Such a burst of traffic, if not caused by a surge in business activity, can be due to suspicious or malicious activity. Large-scale data exfiltration may produce a burst of network traffic; this could also be due to unusually large amounts of reconnaissance or enumeration traffic. Denial-of-service attacks or traffic floods may also produce such a surge in traffic.</p> <div>network</div> <div>security</div>	385	ok	closed	stopped	2023-06-20 21:44:50	<div><div></div><div></div><div></div></div> <div>...</div>
<div><div></div><div>></div></div> high_count_network_events high_count_network_events	<p>Security: Network - looks for an unusual destination country name in the network logs. This can be due to initial access, persistence, command-and-control, or exfiltration activity. For example, when a user clicks on a link in a phishing email or opens a malicious document, a request may be sent to download and run a payload from a server in a country which does not normally appear in network traffic or business work-flows. Malware instances and persistence mechanisms may communicate with command-and-control (C2) infrastructure in their country of origin, which may be an unusual destination country for the source network.</p> <div>network</div> <div>security</div>	142,218	ok	closed	stopped	2023-06-20 22:14:06	<div><div></div><div></div><div></div></div> <div>...</div>
<div><div></div><div>></div></div> high_count_network_events rare_destination_country	<p>Security: Network - looks for an unusually large spike in network traffic. Such a burst of traffic, if not caused by a surge in business activity, can be due to suspicious or malicious activity. Large-scale data exfiltration may produce a burst of network traffic; this could also be due to unusually large amounts of reconnaissance or enumeration traffic. Denial-of-service attacks or traffic floods may also produce such a surge in traffic.</p> <div>network</div> <div>security</div>	102,883	ok	closed	stopped	2023-06-20 22:14:06	<div><div></div><div></div><div></div></div> <div>...</div>
<div><div></div><div>></div></div> population	<div>security</div>	366,313	ok	closed	stopped	2023-06-24 13:58:05	<div><div></div><div></div><div></div></div> <div>...</div>

Rows per page:

Settings

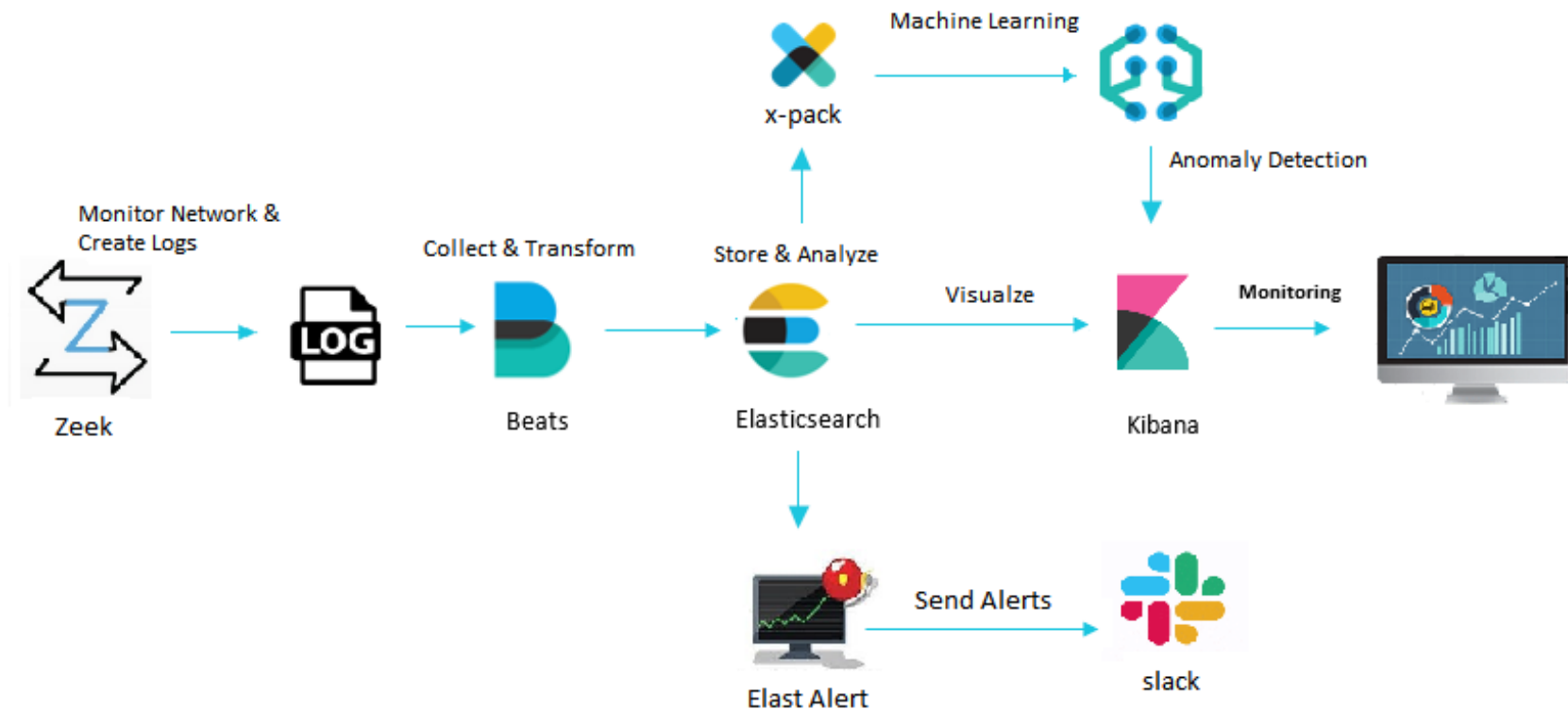
<

1

>

IDS

Intrusion Detection System



Attack Simulation

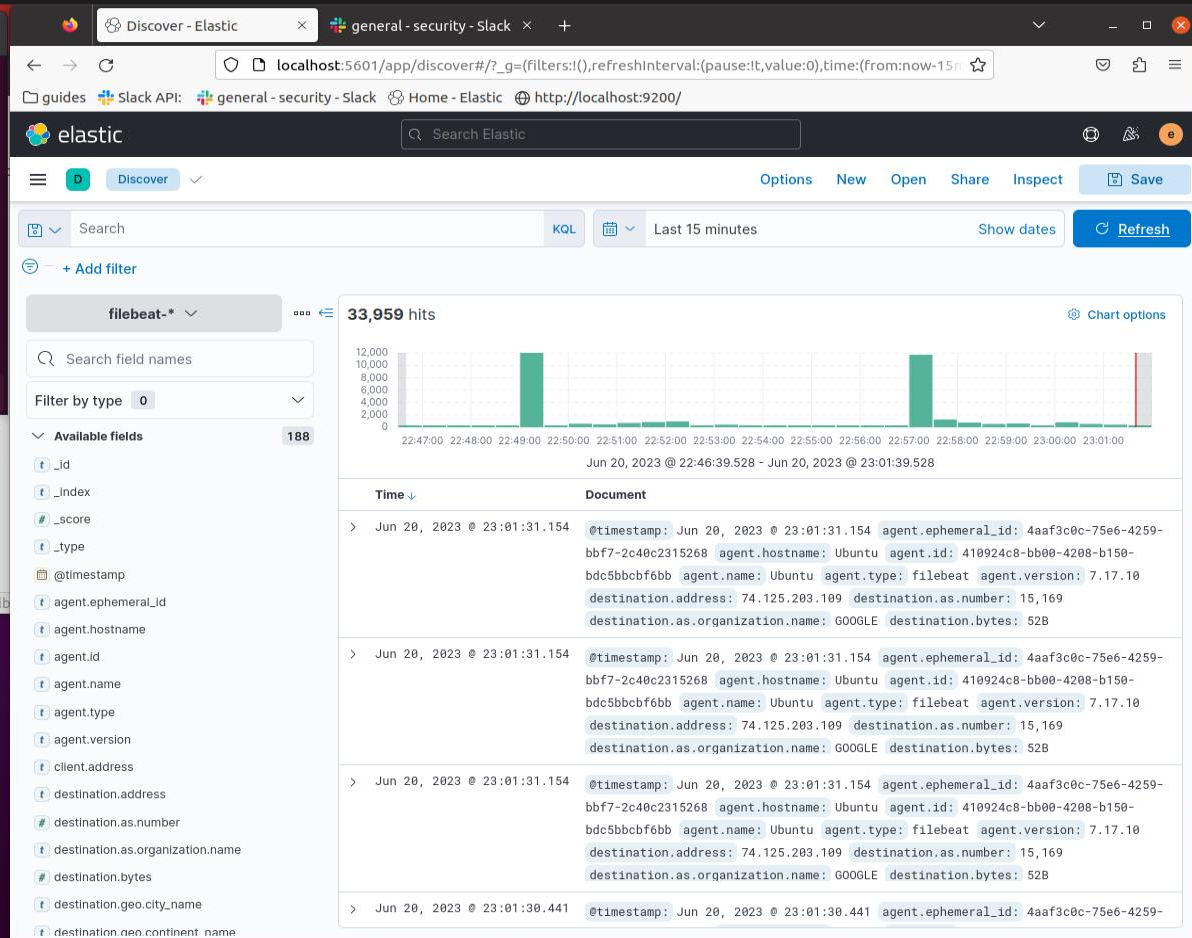
Attack Simulation

- Start ElastAlert service
- Relay pcap files
- Monitor Alerts on Slack
- Investigate Elastic ML findings

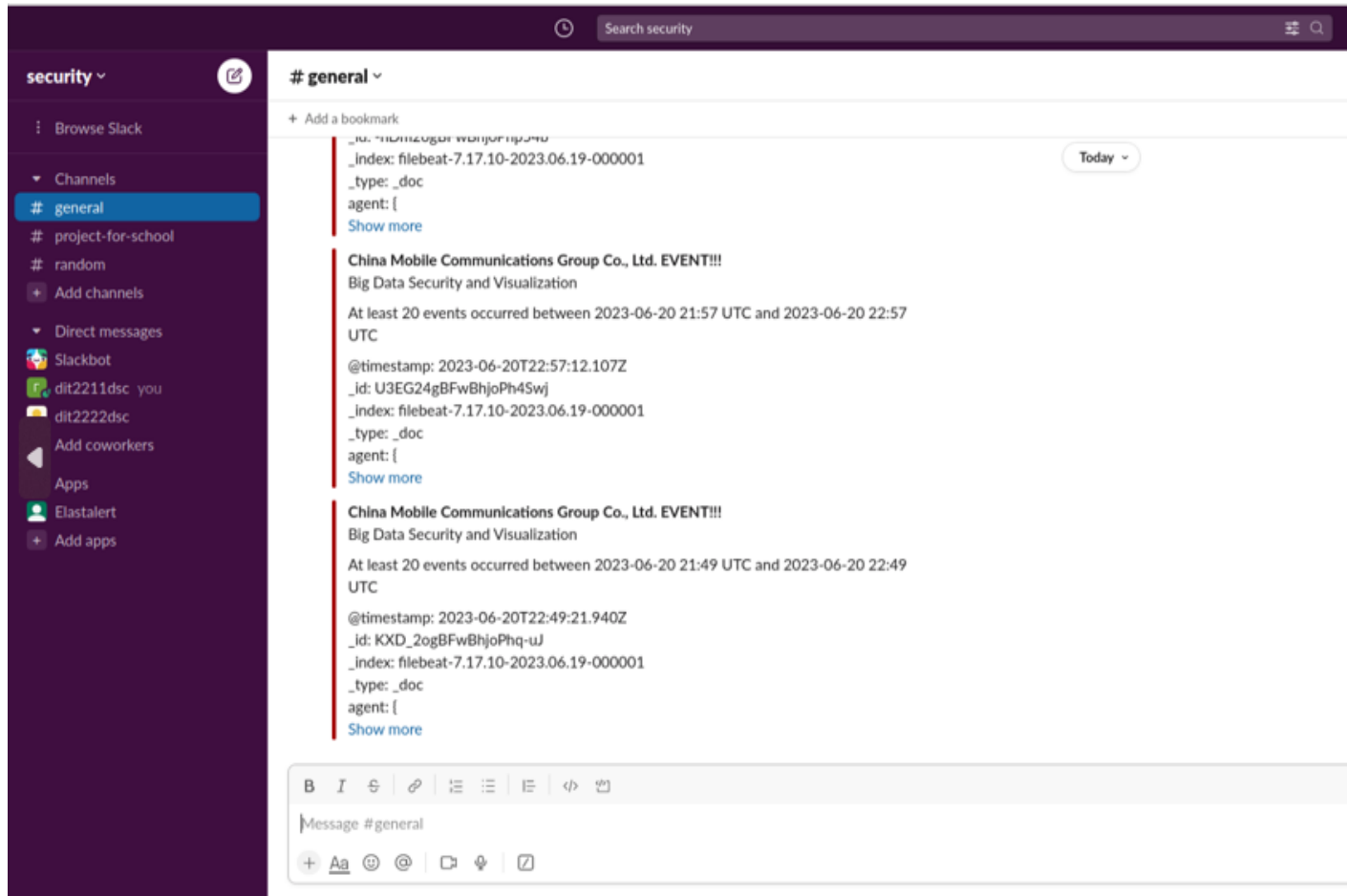
Attack Simulation

```
root@Ubuntu: /elastalert
INFO:elastalert:Background alerts thread 0 pending alerts sent at 2023-06-20 23:01 UTC
INFO:elastalert:Disabled rules are: []
INFO:elastalert:Sleeping for 59.999729 seconds
INFO:elastalert:Queried rule Big Data Security and Visualization from 2023-06-20 22:53 UTC to 2023-06-20 23:01 UTC: 1443 / 1443 hits
INFO:elastalert:Ran Big Data Security and Visualization from 2023-06-20 22:53 UTC to 2023-06-20 23:01 UTC: 1443 query hits (1443 already seen), 0 matches, 0 alerts sent
INFO:elastalert:Background configuration change check run at 2023-06-20 23:02 UTC
INFO:elastalert:Background alerts thread 0 pending alerts sent at 2023-06-20 23:02 UTC
INFO:elastalert:Disabled rules are: []
INFO:elastalert:Sleeping for 59.999729 seconds
INFO:elastalert:Queried rule Big Data Security and Visualization from 2023-06-20 22:53 UTC to 2023-06-20 23:02 UTC: 1443 / 1443 hits
INFO:elastalert:Ran Big Data Security and Visualization from 2023-06-20 22:53 UTC to 2023-06-20 23:02 UTC: 1443 query hits (1443 already seen), 0 matches, 0 alerts sent
```

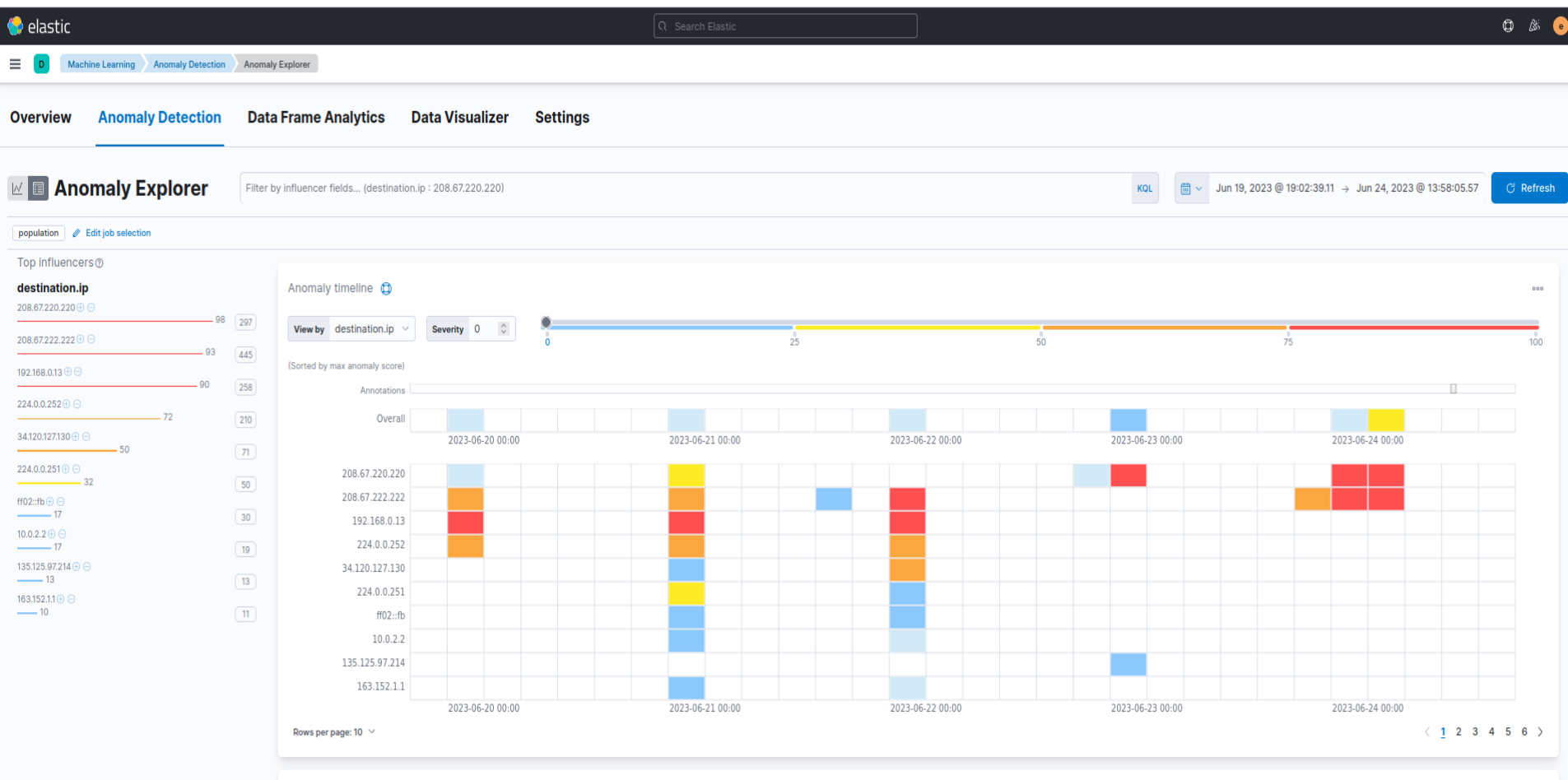
```
ubuntu@Ubuntu: ~/Desktop/Security/pcaps-IoT
Truncated packets: 0
Retried packets (ENOBUFS): 0
Retried packets (EAGAIN): 0
ubuntu@Ubuntu: ~/Desktop/Security/pcaps-IoT$ sudo tcpreplay --intf=enp0s3 mirai-udpflooding-1-dec.pcap
Warning in replay.c:replay_file() line 137:
mirai-udpflooding-1-dec.pcap was captured using a snaplen of 1500 bytes. This may mean you have truncated packets.
Actual: 417863 packets (39980899 bytes) sent in 154.36 seconds
Rated: 258996.0 Bps, 2.07 Mbps, 2706.91 pps
Statistics for network device: enp0s3
Successful packets: 417863
Failed packets: 0
Truncated packets: 0
Retried packets (ENOBUFS): 0
Retried packets (EAGAIN): 0
ubuntu@Ubuntu: ~/Desktop/Security/pcaps-IoT$ sudo tcpreplay --intf=enp0s3 *
Warning in send_packets.c:send_packets() line 644:
Unable to send packet: Error with PF_PACKET send() [637]: Message too long (errno = 90)
Warning in send_packets.c:send_packets() line 644:
Unable to send packet: Error with PF_PACKET send() [8344]: Message too long (errno = 90)
Warning in replay.c:replay_file() line 137:
mirai-udpflooding-1-dec.pcap was captured using a snaplen of 1500 bytes. This may mean you have truncated packets.
```



ElastAlert Notification to Slack



Elastic ML - Anomaly Detection (1)



Elastic ML - Anomaly Detection (2)

Severity ● warning ▾		Interval Auto ▾ ⓘ						
Time	Severity [®] ▾	Detector	Found for	Influenced by	Actual [®]	Typical [®]	Description	Actions
> June 22nd 2023	● 98	count over "destination.ip"	208.67.220.220	destination.ip: 208.67.220.220 ⓘ ⊖	25094	20.3	↑ More than 100x higher	⚙
> June 22nd 2023	● 98	high_count over "destination.ip"	208.67.220.220	destination.ip: 208.67.220.220 ⓘ ⊖	25094	20.3	↑ More than 100x higher	⚙
> June 21st 2023	● 93	count over "destination.ip"	208.67.222.222	destination.ip: 208.67.222.222 ⓘ ⊖	18989	17.9	↑ More than 100x higher	⚙
> June 21st 2023	● 93	high_count over "destination.ip"	208.67.222.222	destination.ip: 208.67.222.222 ⓘ ⊖	18989	17.9	↑ More than 100x higher	⚙
> June 21st 2023	● 90	count over "destination.ip"	192.168.0.13	destination.ip: 192.168.0.13 ⓘ⊕	18661	17.9	↑ More than 100x higher	⚙
> June 21st 2023	● 90	high_count over "destination.ip"	192.168.0.13	destination.ip: 192.168.0.13 ⓘ⊕	18661	17.9	↑ More than 100x higher	⚙
> June 20th 2023	● 87	high_count over "destination.ip"	192.168.0.13	destination.ip: 192.168.0.13 ⓘ⊕	37712	21.5	↑ More than 100x higher	⚙
> June 20th 2023	● 87	count over "destination.ip"	192.168.0.13	destination.ip: 192.168.0.13 ⓘ⊕	37712	21.5	↑ More than 100x higher	⚙
> June 24th 2023	● 85	high_count over "destination.ip"	208.67.220.220	destination.ip: 208.67.220.220 ⓘ ⊖	15622	19.8	↑ More than 100x higher	⚙
> June 24th 2023	● 85	count over "destination.ip"	208.67.220.220	destination.ip: 208.67.220.220 ⓘ ⊖	15622	19.8	↑ More than 100x higher	⚙
> June 24th 2023	● 82	count over "destination.ip"	208.67.222.222	destination.ip: 208.67.222.222 ⓘ ⊖	13730	19.8	↑ More than 100x higher	⚙
> June 24th 2023	● 82	high_count over "destination.ip"	208.67.222.222	destination.ip: 208.67.222.222 ⓘ ⊖	13730	19.8	↑ More than 100x higher	⚙
> June 19th 2023	● 80	count over "destination.ip"	192.168.0.13	destination.ip: 192.168.0.13 ⓘ⊕	15507	73.2	↑ More than 100x higher	⚙
> June 19th 2023	● 80	high_count over "destination.ip"	192.168.0.13	destination.ip: 192.168.0.13 ⓘ⊕	15507	73.2	↑ More than 100x higher	⚙
> June 23rd 2023	● 78	count over "destination.ip"	208.67.220.220	destination.ip: 208.67.220.220 ⓘ ⊖	8824	19.8	↑ More than 100x higher	⚙
> June 23rd 2023	● 78	high_count over "destination.ip"	208.67.220.220	destination.ip: 208.67.220.220 ⓘ ⊖	8824	19.8	↑ More than 100x higher	⚙

Conclusions

- Zeek in combination with ELK stack provide a good standard for Network (and System) Security
- ELK provides many available addons and tools
- Visualization & Analysis options
- Many interfaces

Bibliography

- <https://www.elastic.co/blog/collecting-and-analyzing-zeek-data-with-elastic-security>
- <https://github.com/Yelp/elastalert>
- <https://ieee-dataport.org/open-access/iot-network-intrusion-dataset>
- <https://www.elastic.co/guide/en/machine-learning/current/ml-getting-started.html>
- <https://logz.io/learn/docker-monitoring-elk-stack/>
- <https://devopscube.com/build-docker-image/>
- <https://docs.docker.com/engine/install/ubuntu/>

Thank you!
