elastic

ELASTIC SIEM FUNDAMENTALS

An Elastic Training Course

7.5.1

elastic.co/training

ELASTIC SIEM FUNDAMENTALS

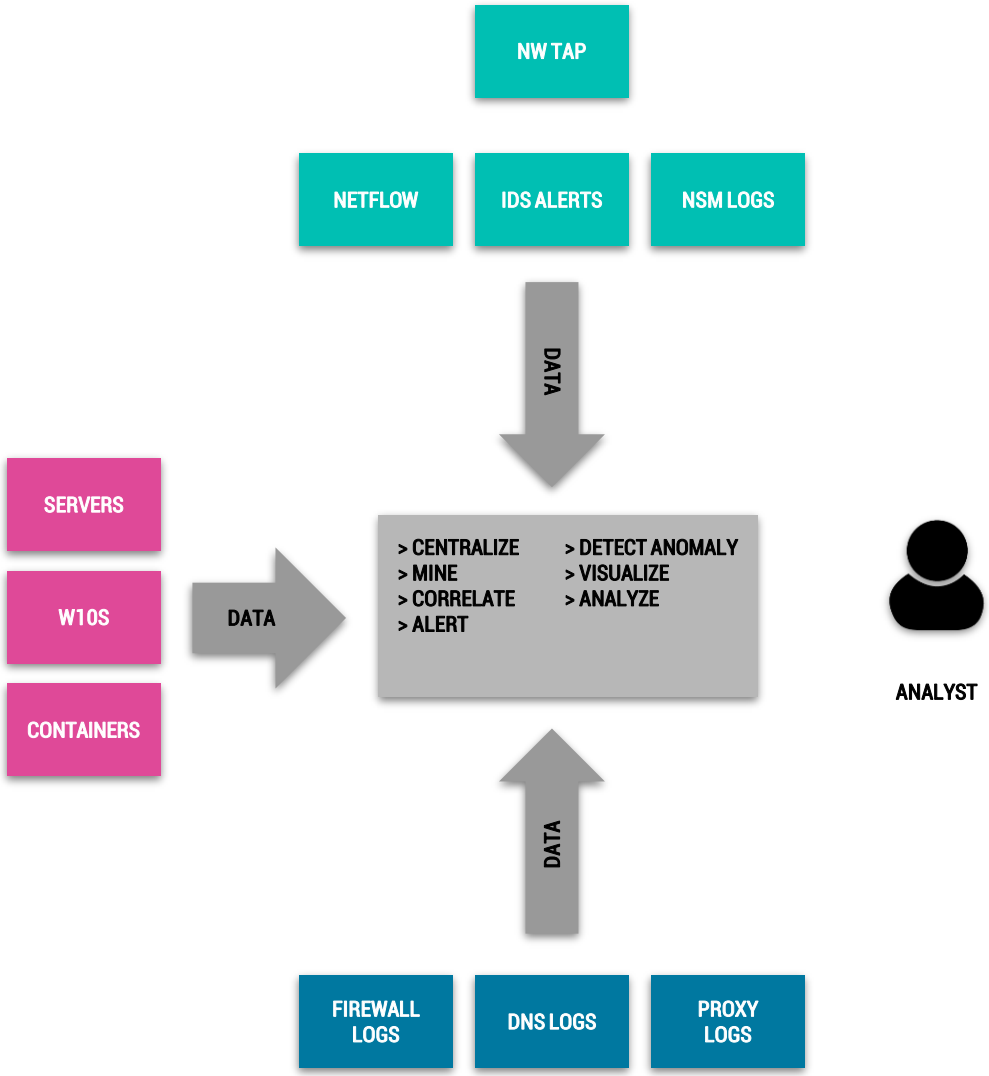
Course: ELASTIC SIEM FUNDAMENTALS

Version 7.5.1

LESSON 1

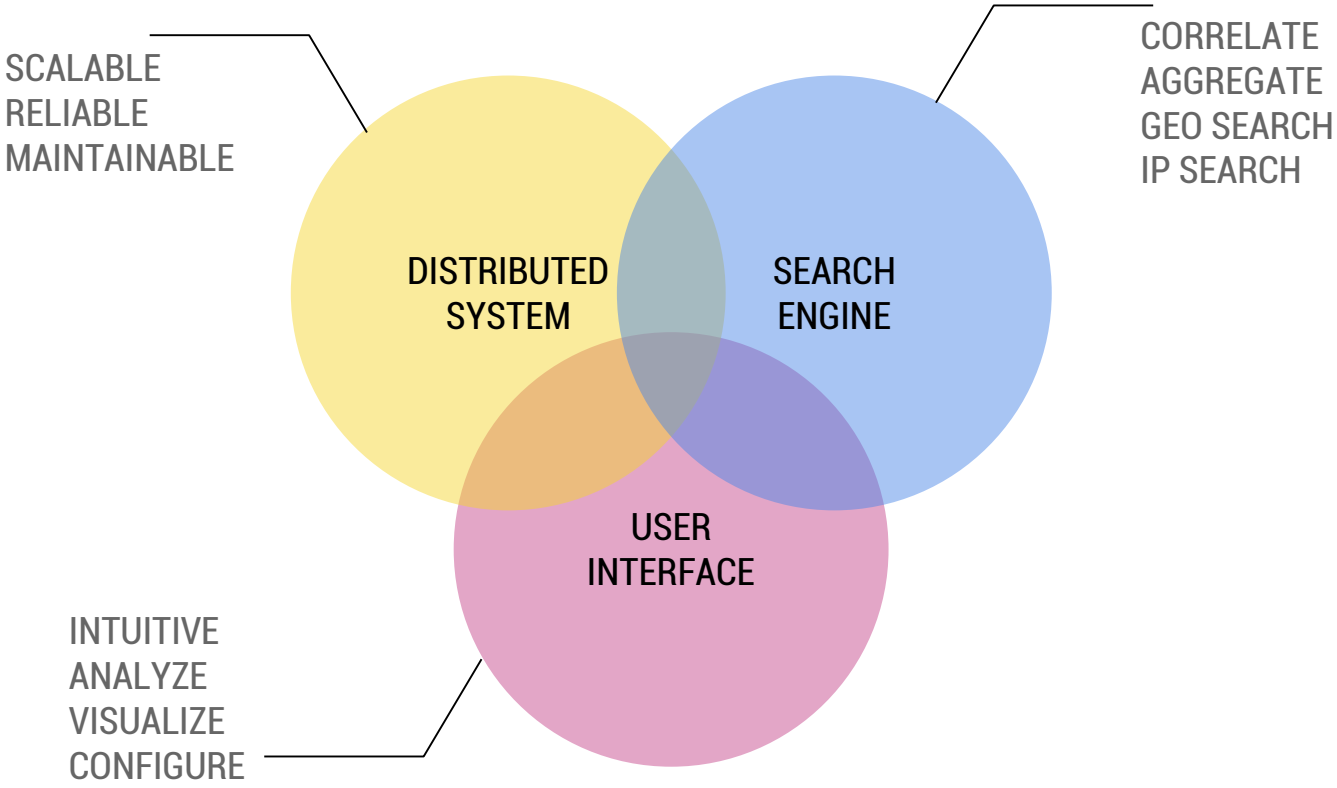
ELASTIC SIEM UI

PROBLEM

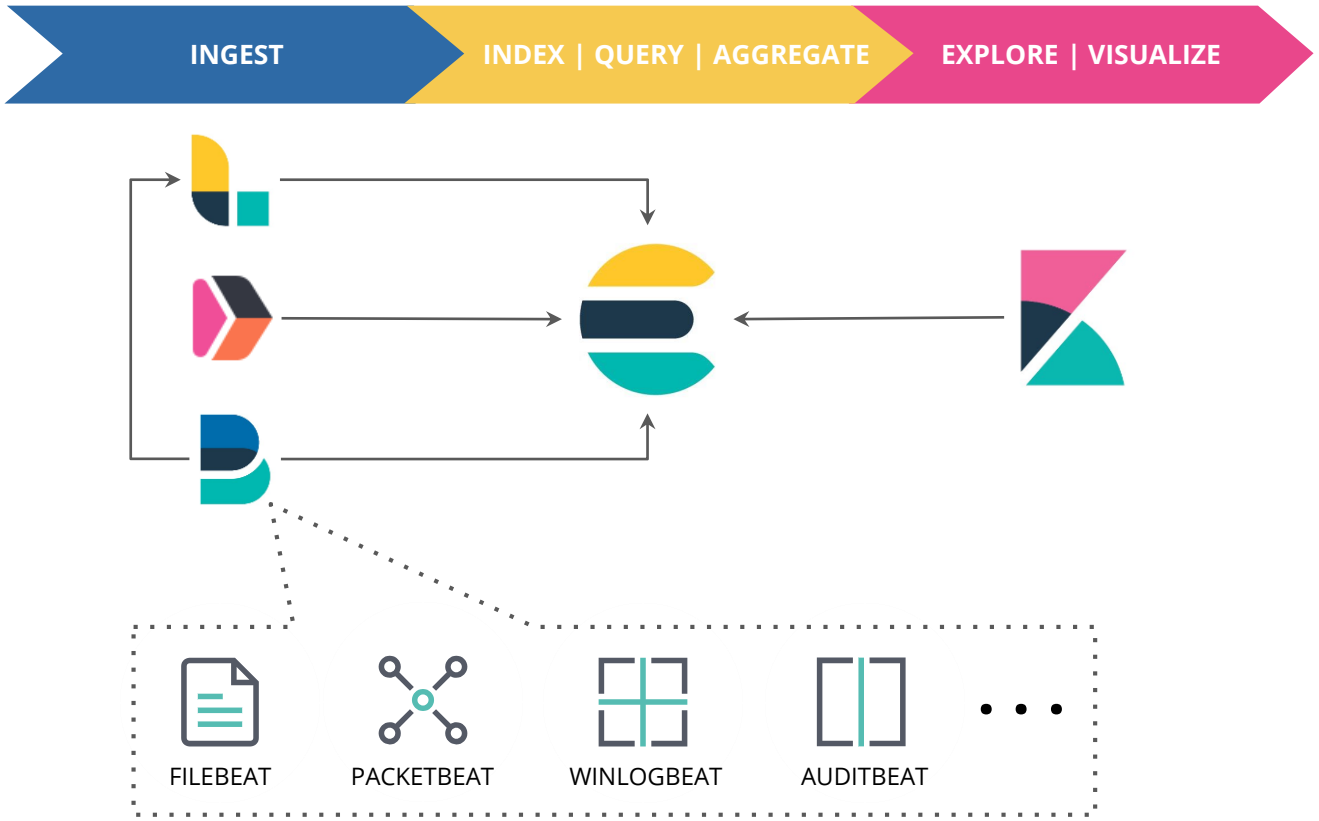


REQUIREMENTS

REQUIREMENTS

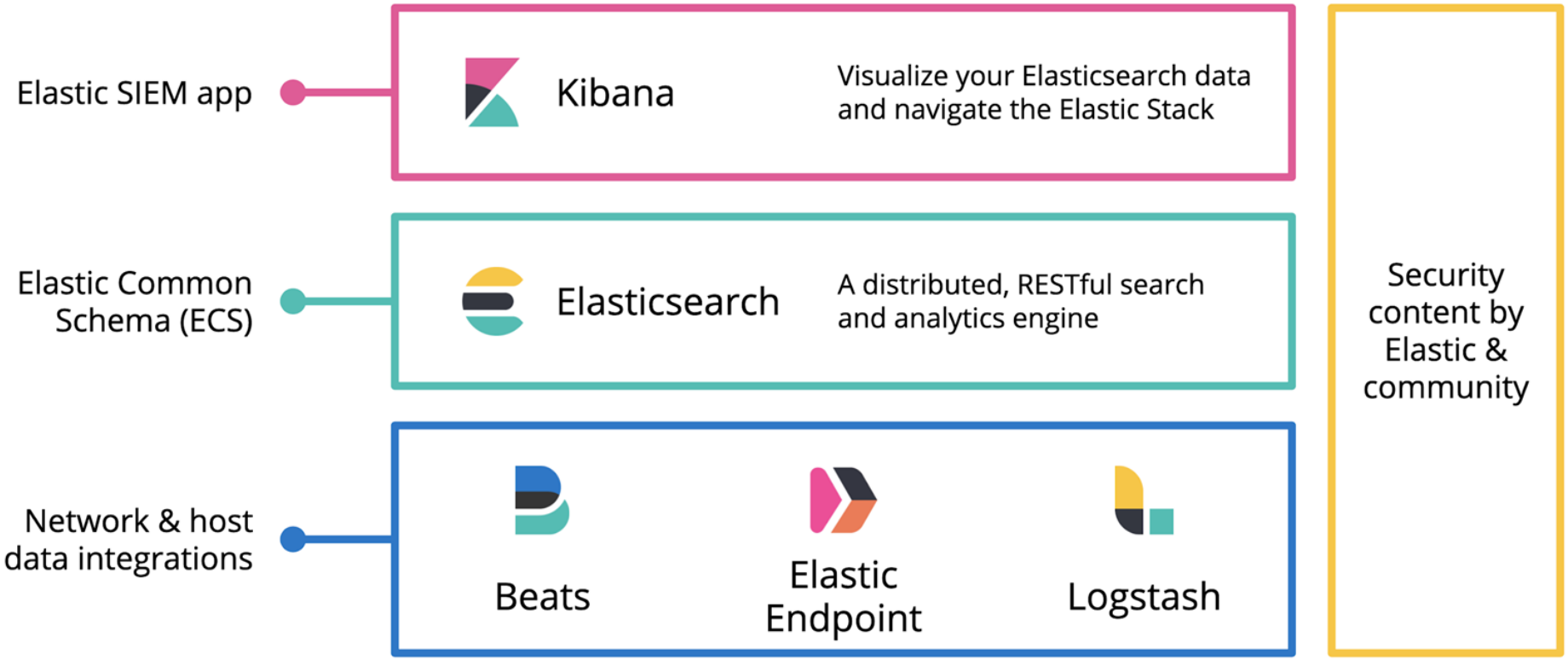


ELASTIC STACK OVERVIEW



elastic

ELASTIC SIEM OVERVIEW



LESSON 1

REVIEW - ELASTIC SIEM UI

SUMMARY

- Being able to centralize, correlate, analyze, and aggregate security events from disparate sources is the essence of SIEM's purpose
- Elastic SIEM is built on top of Elastic stack by providing a formal schema, powerful set of UI elements for analyzing security events and growing number of pre_built machine learning jobs
- Elastic SIEM Kibana UI includes an overview page, host page, network page and timeline tool

QUIZ

1. The three ingest layer components of Elastic Stack that provides network and host data integration for Elastic SIEM are Beats, Logstash and _____
   a. Alerting
   b. Elastic Machine Learning
   c. Elastic Endpoint Security
   d. Kibana

1. Which of the following tabs can be used to investigate uncommon processes?
   a. Overview
   b. Network
   c. Host
   d. Timelines

1. In Timeline, if you place the element "user.name" : "bgates" directly to the right "os.family": "windows" what will the resulting relationship be?
   a. "user.name" : "bgates" AND "os.family": "windows"
   b. No Relation
   c. "user.name" : "bgates" OR "os.family": "windows"
   d. "user.name" : "bgates" XOR "os.family": "windows"

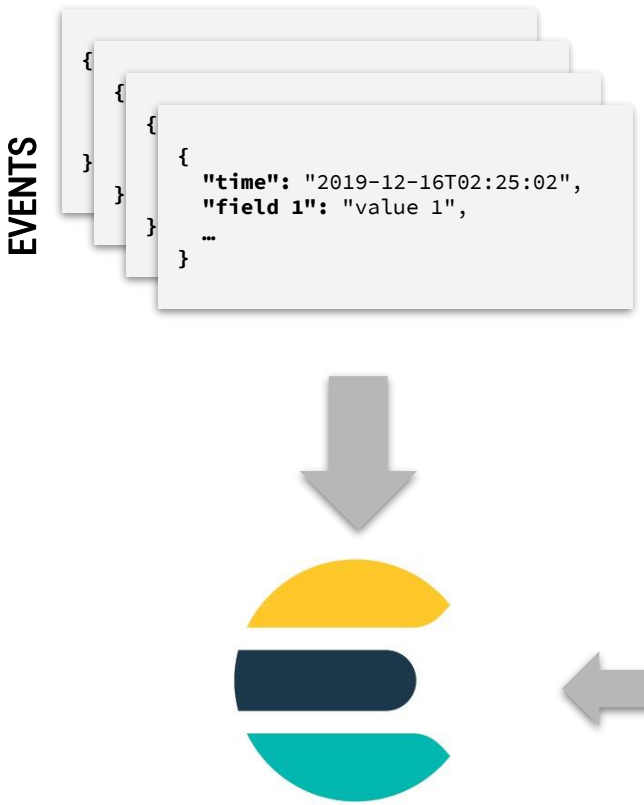
LESSON 1

LAB - ELASTIC SIEM UI

LESSON 2

GETTING SIEM DATA IN

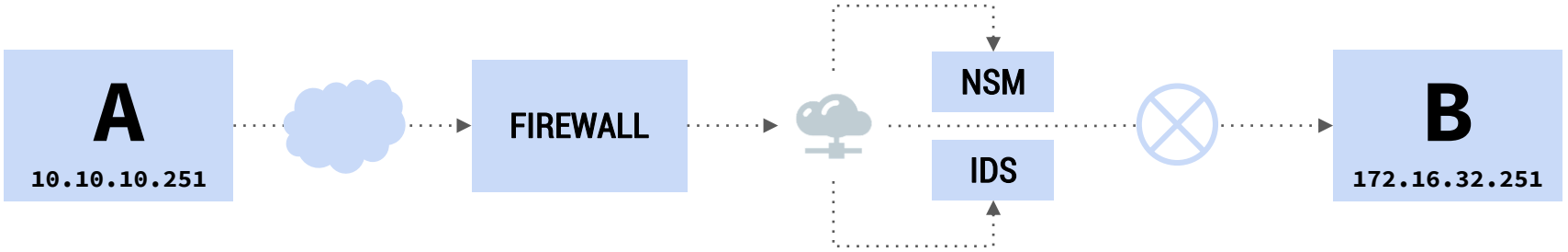
SCHEMA




```
"ip": "10.10.250.52"

"source" :
{
    "ip" : "10.10.250.52"
}
```

ELASTIC COMMON SCHEMA



FIREWALL	IDS	NSM
Source IP (src)	source.ip	id.orig_h

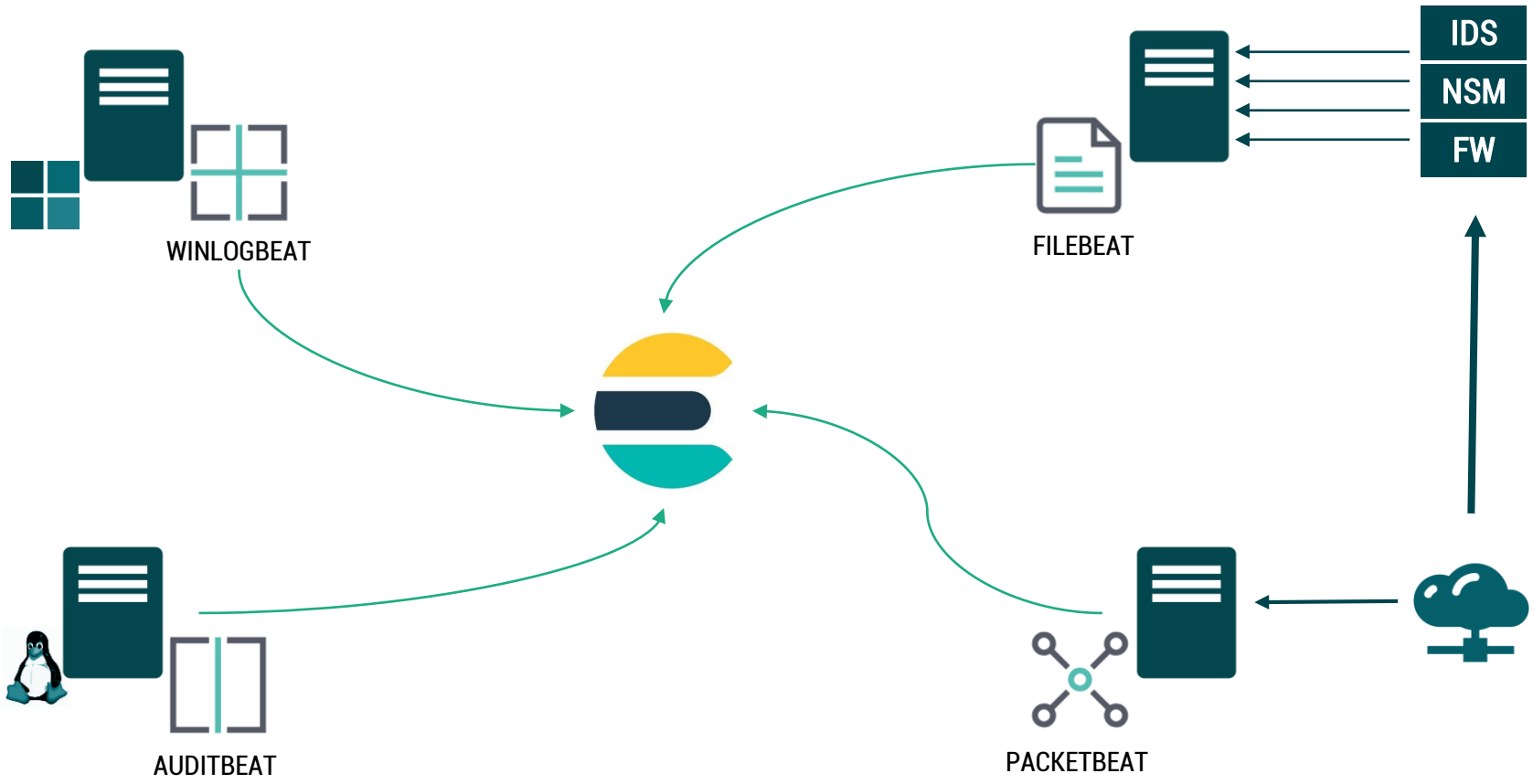
@timestamp	_index
Jun 26, 2019 @ 10:18:08.754	fw_logs
Jun 26, 2019 @ 10:18:08.765	zeek
Jun 26, 2019 @ 10:18:08.839	suricata
Jun 26, 2019 @ 10:18:08.982	winlogbeat

"Show me all the events with source ip 10.10.10.251"

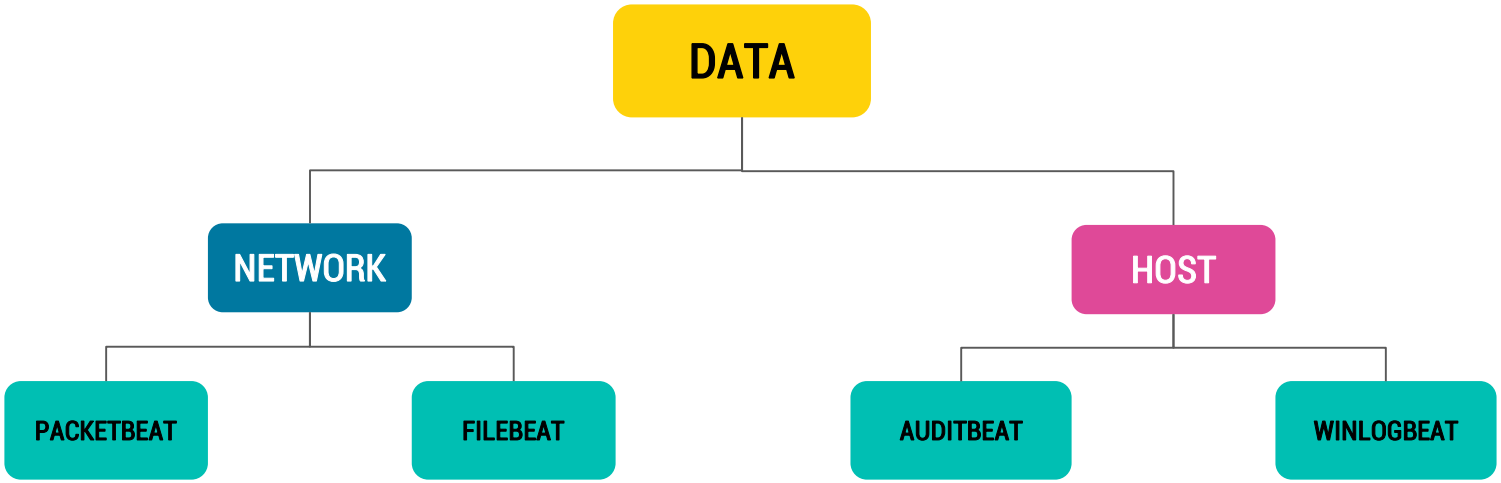
https://github.com/elastic/ecs

elastic

BEATS



RIGHT TOOL FOR THE DATA



LESSON 2

REVIEW - GETTING SIEM DATA IN

SUMMARY

- ECS defines a common set of fields to be used when storing event data in Elasticsearch, such as logs and metrics
- All beats can ship data to elasticsearch in ecs format
- Packetbeat and Filebeat are helpful in ingesting logs and network data into Elastic SIEM
- Auditbeat and Winlogbeat are used to ship host data into Elastic SIEM

QUIZ

1. Every event should contain a timestamp.
   a. True
   b. False

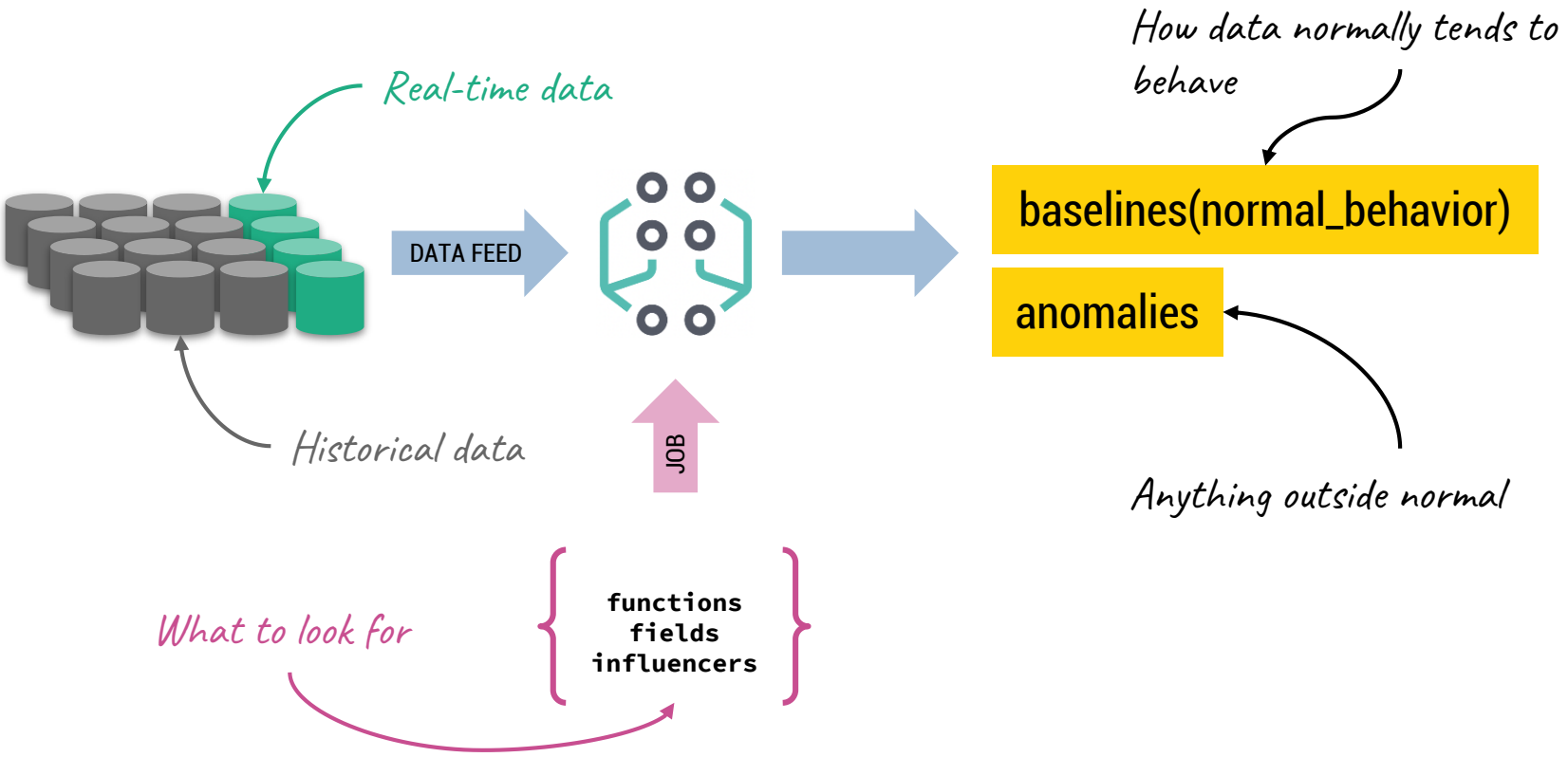
1. Beats installed using .deb or .rpm distribution can be configured using the <beat_name>.yml file located in which of the following?
   a. /usr/share/<beat_name>/<beat_name>.cfg
   b. /etc/<beat_name>/<beat_name>.cfg
   c. /etc/<beat_name>/<beat_name>.yml
   d. /home/<user>/<beat_name>/config/<beat_name>.yml

1. Which command would you use to turn on a filebeat module?
   a. filebeat <module_name> on
   b. filebeat enable <module_name>
   c. filebeat <module_name> enable
   d. filebeat -e <module_name>

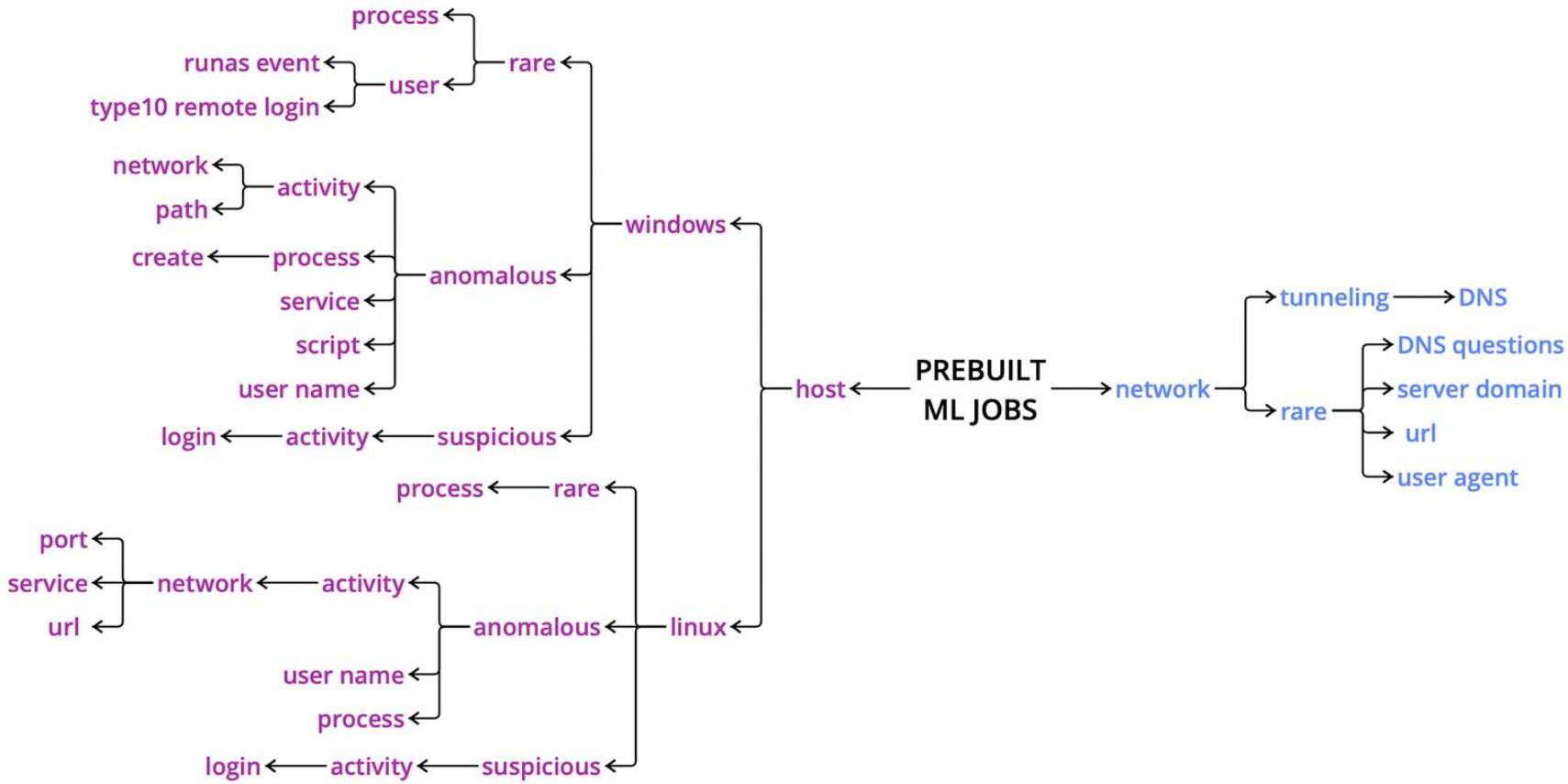
LESSON 3

ANOMALY DETECTION

ANOMALY DETECTION IN A NUTSHELL



OVERVIEW OF PREBUILT JOBS



elastic

LESSON 3

REVIEW - ANOMALY DETECTION

SUMMARY

- Anomaly detection can be used to analyze time series data by creating accurate baselines of normal behavior and identifying anomalous patterns in your dataset
- The SIEM app comes with prebuilt machine learning anomaly detection jobs for automatically detecting host and network anomalies
- To gain clearer insights into real threats, it is possible to tune the anomaly results

QUIZ

1. Machine Learning functionality is available throughout the SIEM app for which of the following deployments
   a. Basic
   b. Free Trial
   c. Platinum Subscription
   d. Elastic Cloud

2. Anomalies tab that shows details of detected anomalies is available in which of the following pages within the SIEM app?
   a. Overview
   b. Hosts
   c. Network
   d. Timelines

1. Results of anomaly detection can never be improved.
   a. True
   b. False

LESSON 3

LAB - ANOMALY DETECTION

QUIZ ANSWERS

QUIZ

1. The three ingest layer components of Elastic Stack that provides network and host data integration for Elastic SIEM are Beats, Logstash and _____
   a. Alerting
   b. Elastic Machine Learning
   c. Elastic Endpoint Security
   d. Kibana

1. Which of the following tabs can be used to investigate uncommon processes?
   a. Overview
   b. Network
   c. Host
   d. Timelines

1. In Timeline, if you place the element "user.name" : "bgates" directly to the right "os.family": "windows" what will the resulting relationship be?
   a. "user.name" : "bgates" AND "os.family": "windows"
   b. No Relation
   c. "user.name" : "bgates" OR "os.family": "windows"
   d. "user.name" : "bgates" XOR "os.family": "windows"

QUIZ

1. Every event should contain a timestamp.
   a. **True**
   b. False

1. Beats installed using .deb or .rpm distribution can be configured using the <beat_name>.yml file located in which of the following?
   a. /usr/share/<beat_name>/<beat_name>.cfg
   b. /etc/<beat_name>/<beat_name>.cfg
   c. /etc/<beat_name>/<beat_name>.yml
   d. /home/<user>/<beat_name>/config/<beat_name>.yml

1. Which command would you use to turn on a filebeat module?
   a. filebeat <module_name> on
   b. filebeat enable <module_name>
   c. filebeat <module_name> enable
   d. filebeat -e <module_name>

QUIZ

1. Machine Learning functionality is available throughout the SIEM app for which of the following deployments
   a. Basic
   b. Free Trial
   c. Platinum Subscription
   d. Elastic Cloud

2. Anomalies tab that shows details of detected anomalies is available in which of the following pages within the SIEM app?
   a. Overview
   b. Hosts
   c. Network
   d. Timelines

1. Results of anomaly detection can never be improved.
   a. True
   b. False

Thank You!

Please complete the online survey.

elastic