Anomaly Detection for Cybersecurity

An Elastic Training Course

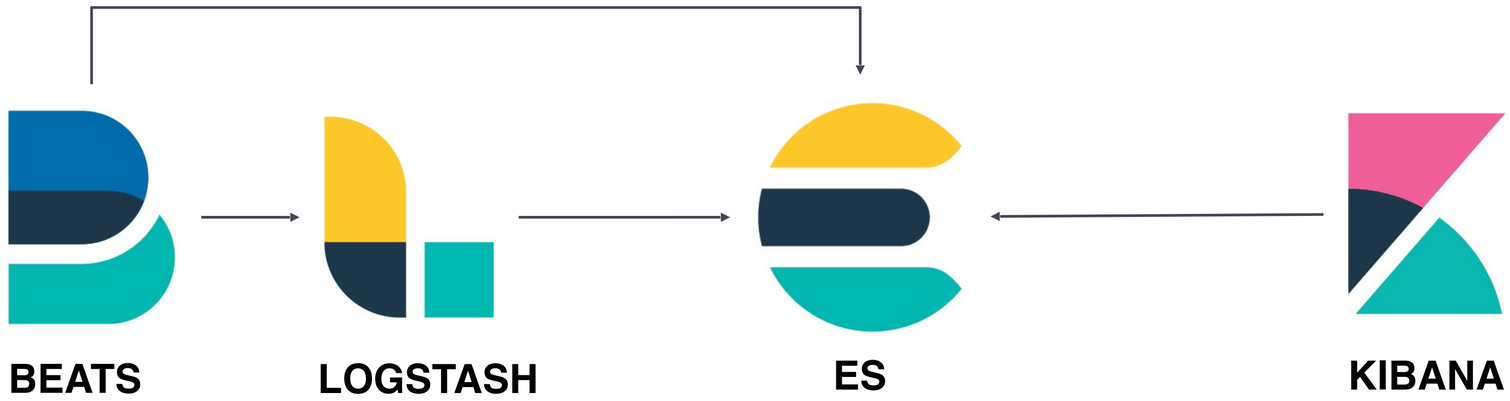
7.6.2

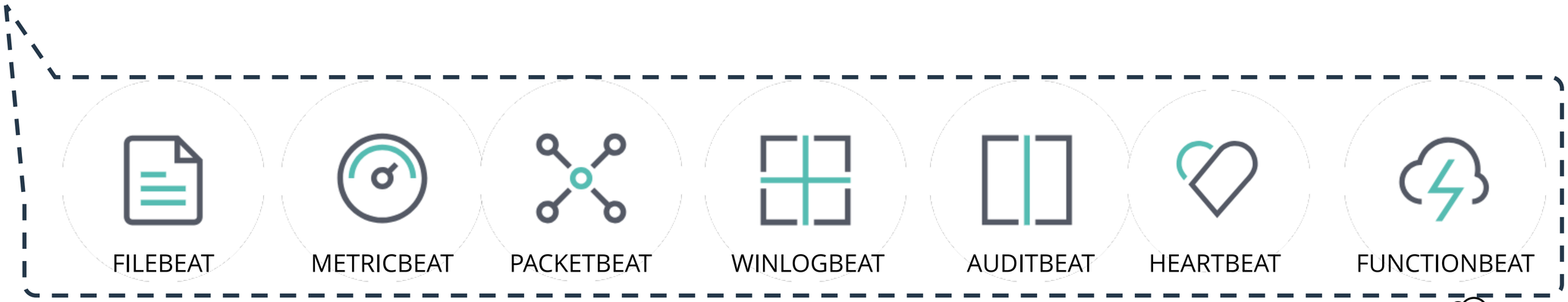
elastic.co/training

COURSE AGENDA

1. Introduction to Elastic Anomaly Detection
2. Configuring Anomaly Detection
3. Detecting DNS Data Exfiltration

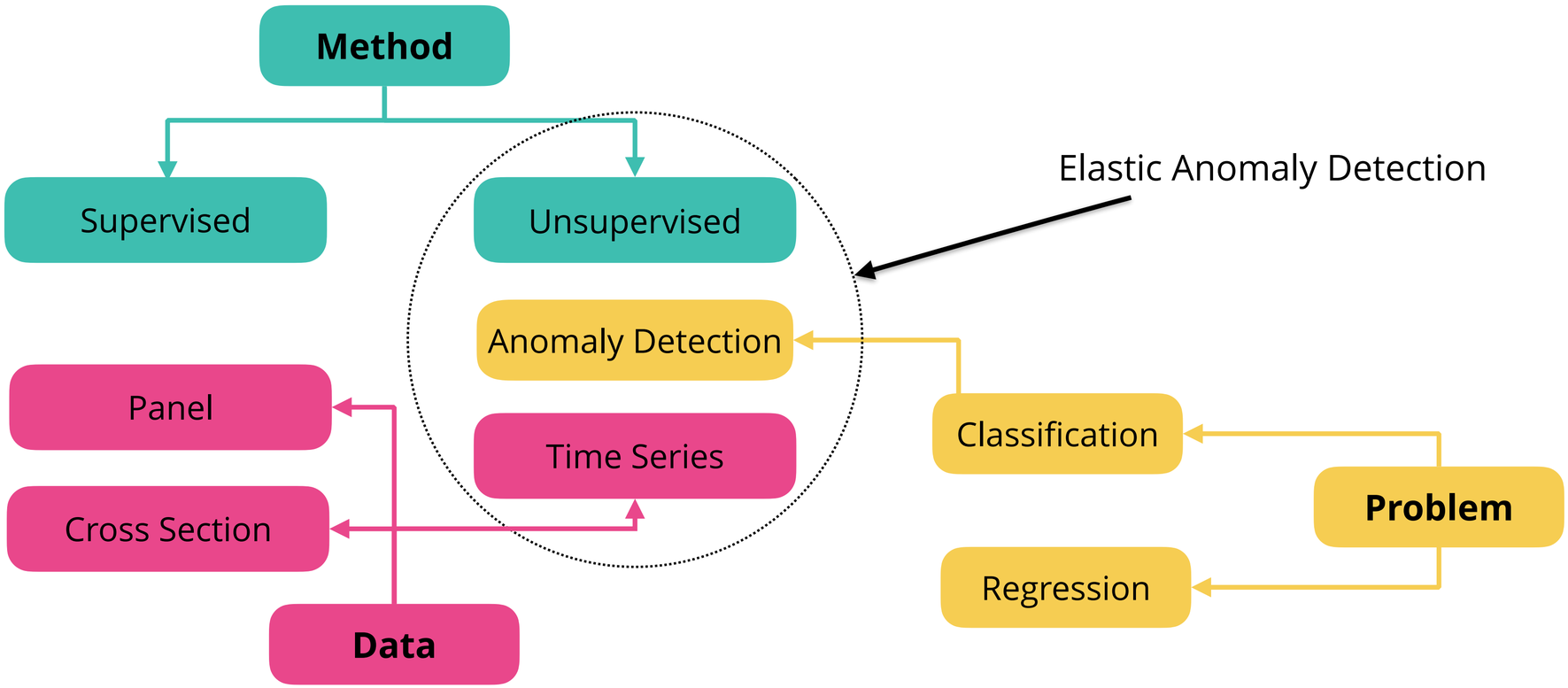
ELASTIC STACK OVERVIEW



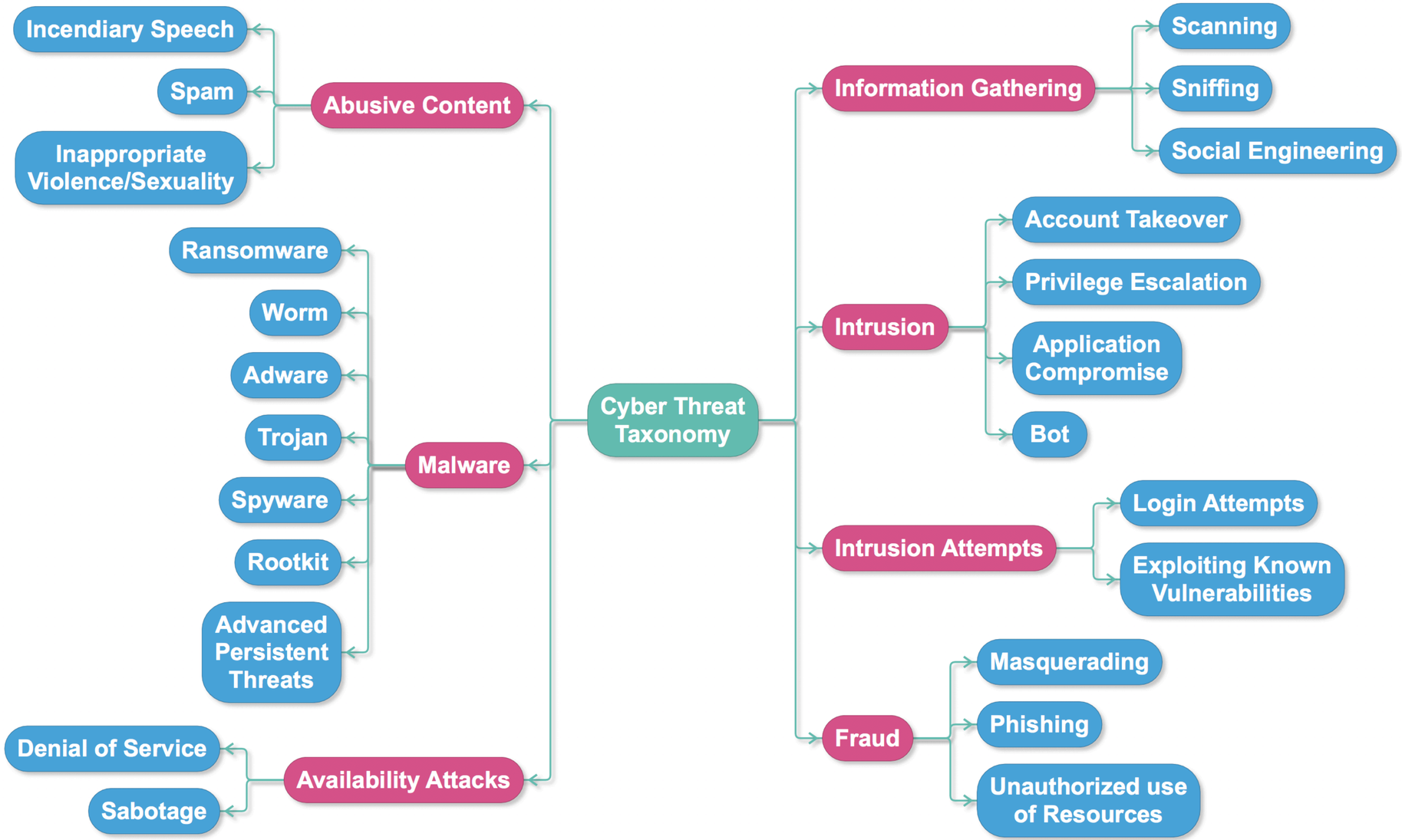


elastic

MACHINE LEARNING

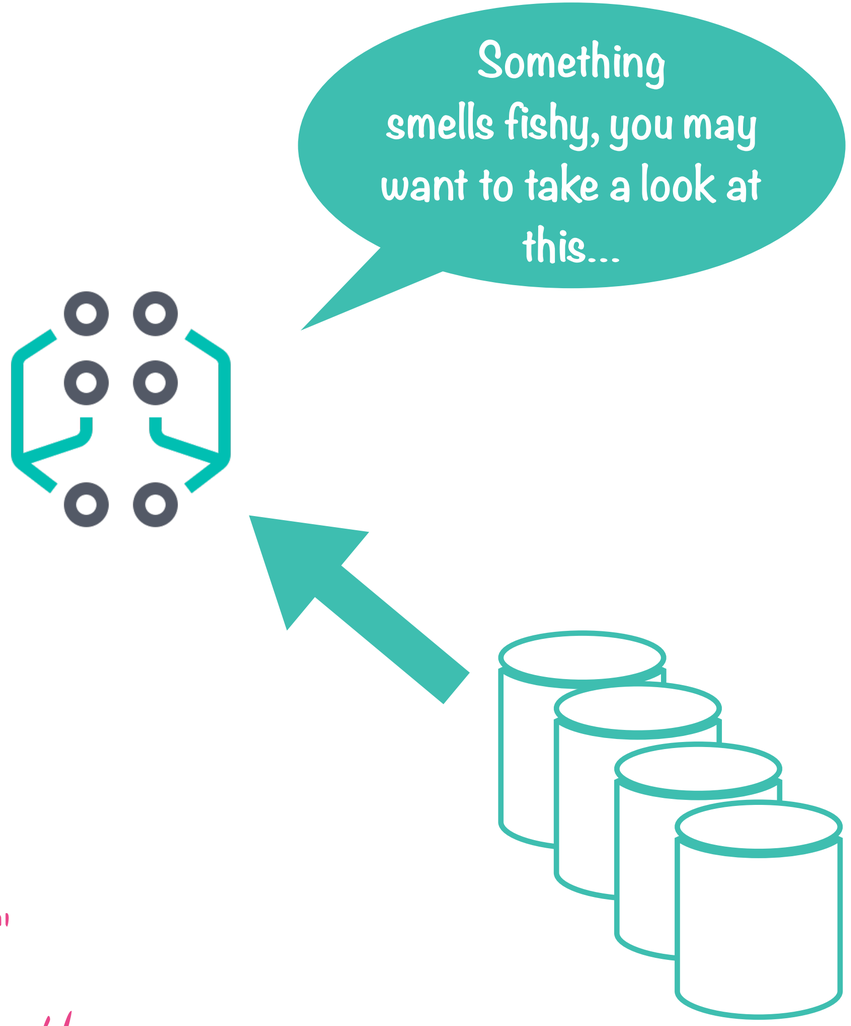


CYBER THREAT TAXONOMY



WHY ANOMALY DETECTION FOR CYBERSECURITY ?

- Automated Detection of Attack Behavior
  - System / Network Complexity
  - Attack Sophistication
  - Volume of Data
  - Resources



"Is my network under attack?"

"Is my system compromised?"

"Which of my user is an insider threat?"

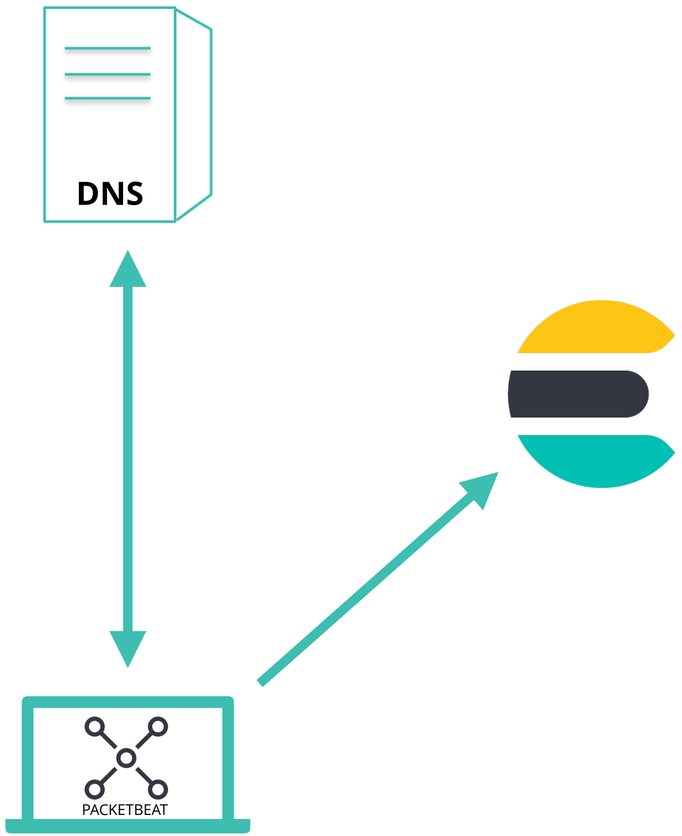
Well, let's setup an ML Job and find out!

SSH LOGS

filebeat-*

- Timestamp
- SSH Server Host Name
- SSH Client IP
- User
- Authentication Method
- IP Geo Location Info
- ...

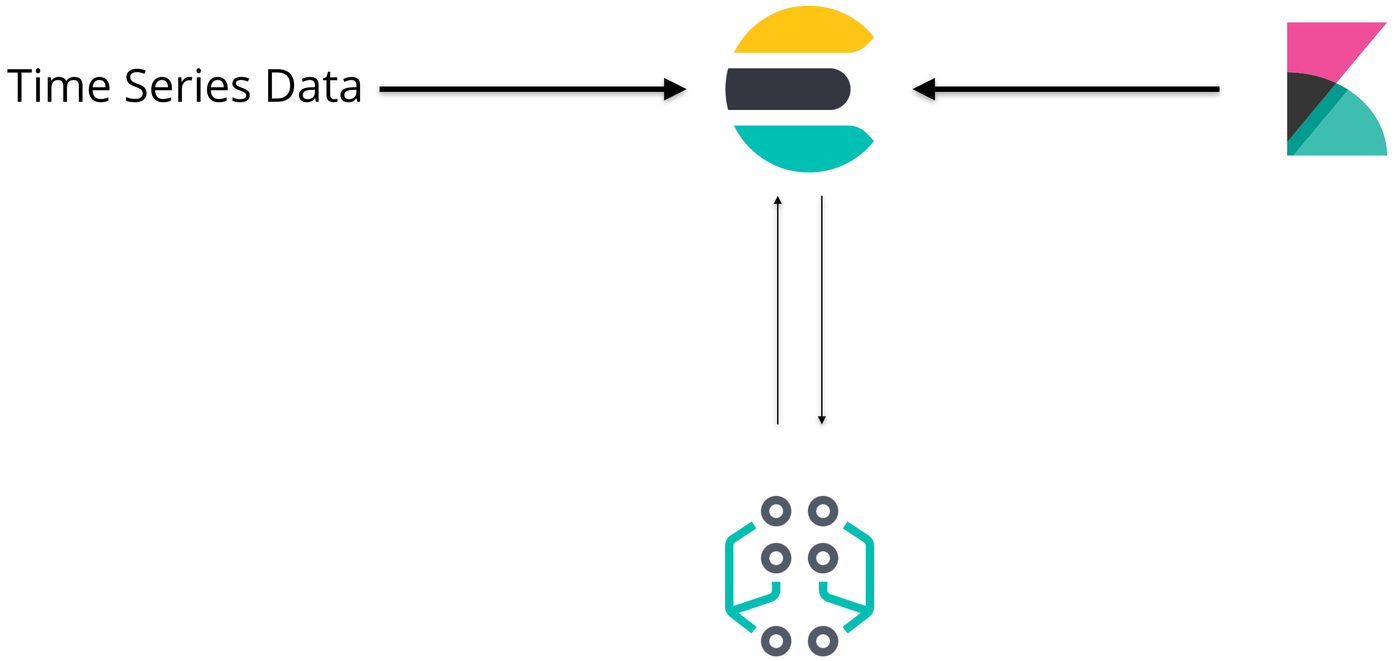
DNS TRAFFIC



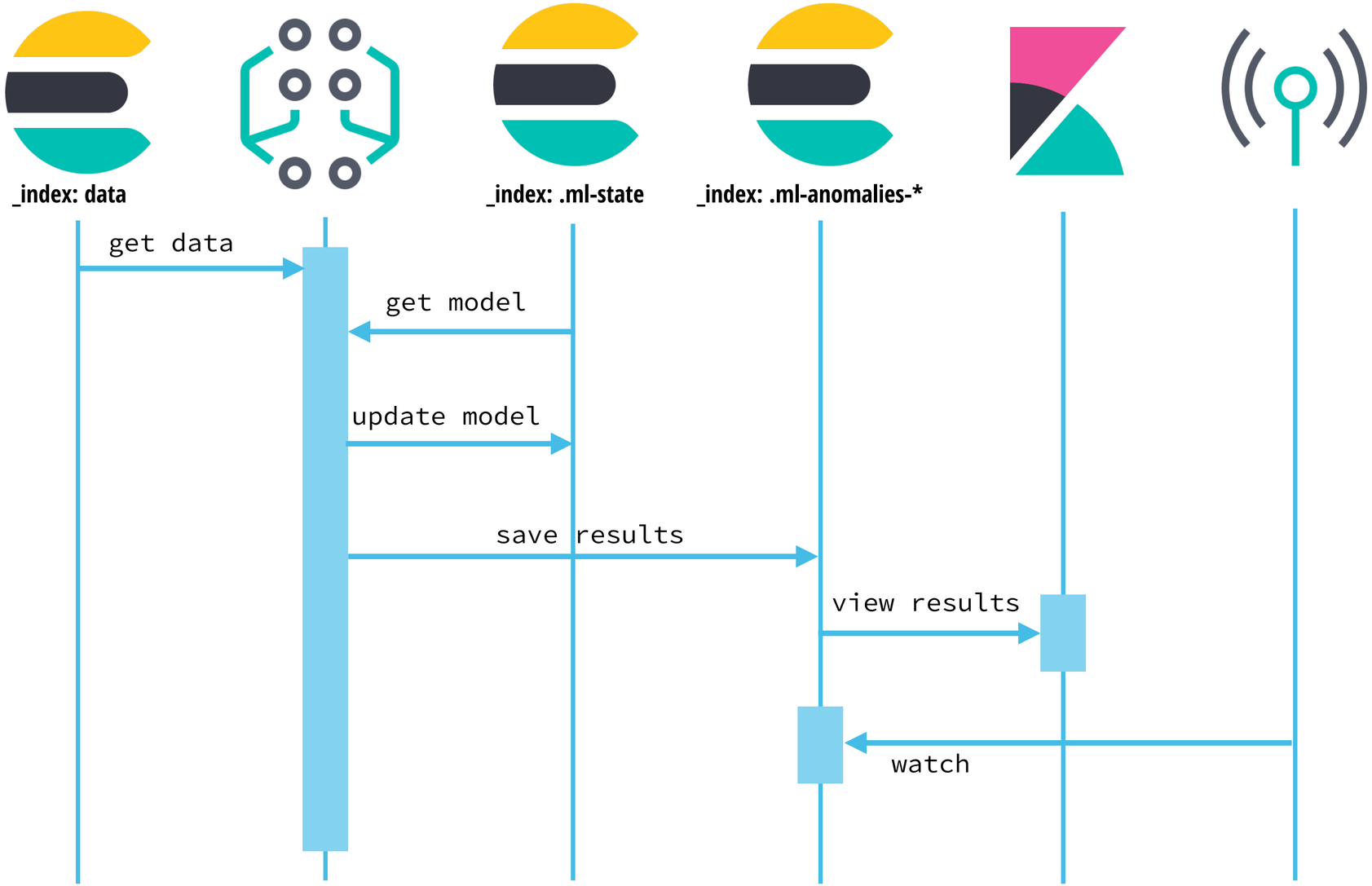
security-analytics-packetbeat-*

- Timestamp
- Client IP
- Source Host
- Destination IP
- Highest Registered Domain
- Subdomain
- ...

HOW ANOMALY DETECTION WORKS



ANOMALY DETECTION SEQUENCE



LAB 1

ELASTIC ML KEY CONCEPTS

JOB

DATAFEED

BUCKET

METRIC

FUNCTION

DETECTOR

INFLUENCER

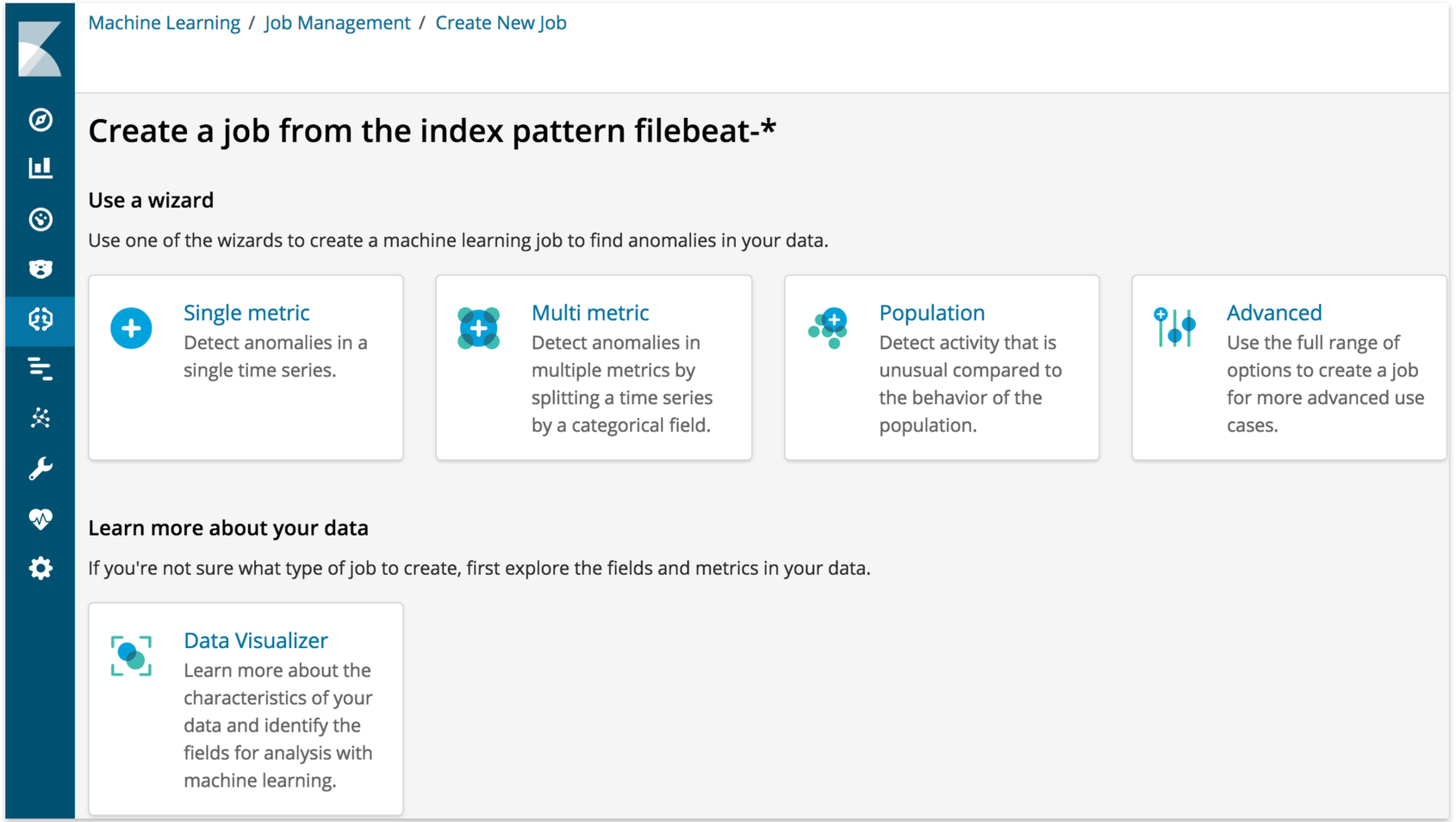
MODEL

WATCH

JOBS API

```
PUT _xpack/ml/anomaly_detectors/suspicious_login_activity
{
  "description": "suspicious login activity",
  "established_model_memory": 69458,
  "analysis_config": {
    "bucket_span": "5m",
    "detectors": [
      {
        "detector_description": "high_count",
        "function": "high_count",
        "partition_field_name": "system.auth.hostname",
        "detector_index": 0
      }
    ],
```

JOBS WIZARD


Machine Learning / Job Management / Create New Job
Create a job from the index pattern filebeat-*
Use a wizard
Use one of the wizards to create a machine learning job to find anomalies in your data.
Single metric
Detect anomalies in a single time series.
Multi metric
Detect anomalies in multiple metrics by splitting a time series by a categorical field.
Population
Detect activity that is unusual compared to the behavior of the population.
Advanced
Use the full range of options to create a job for more advanced use cases.
Learn more about your data
If you're not sure what type of job to create, first explore the fields and metrics in your data.
Data Visualizer
Learn more about the characteristics of your data and identify the fields for analysis with machine learning.

USER EXPERIENCE IN KIBANA

- User configures a *Job* using the Job wizard
  - Job Type
    - Single metric
    - Multi metric
    - Advanced
    - Population

USER EXPERIENCE IN KIBANA

- User configures a *Data Feed* for the job to consume
  - Index Pattern
  - Query
  - Time Range
- User starts the *Data Feed*

USER EXPERIENCE IN KIBANA

- Explore *Job Results*
  - Single metric viewer
  - Anomaly explorer
- Optionally, Configure a *Watch* for realtime data
  - Schedule
  - Query
  - Condition
  - Action

DEMO

LAB 2

TOPICS

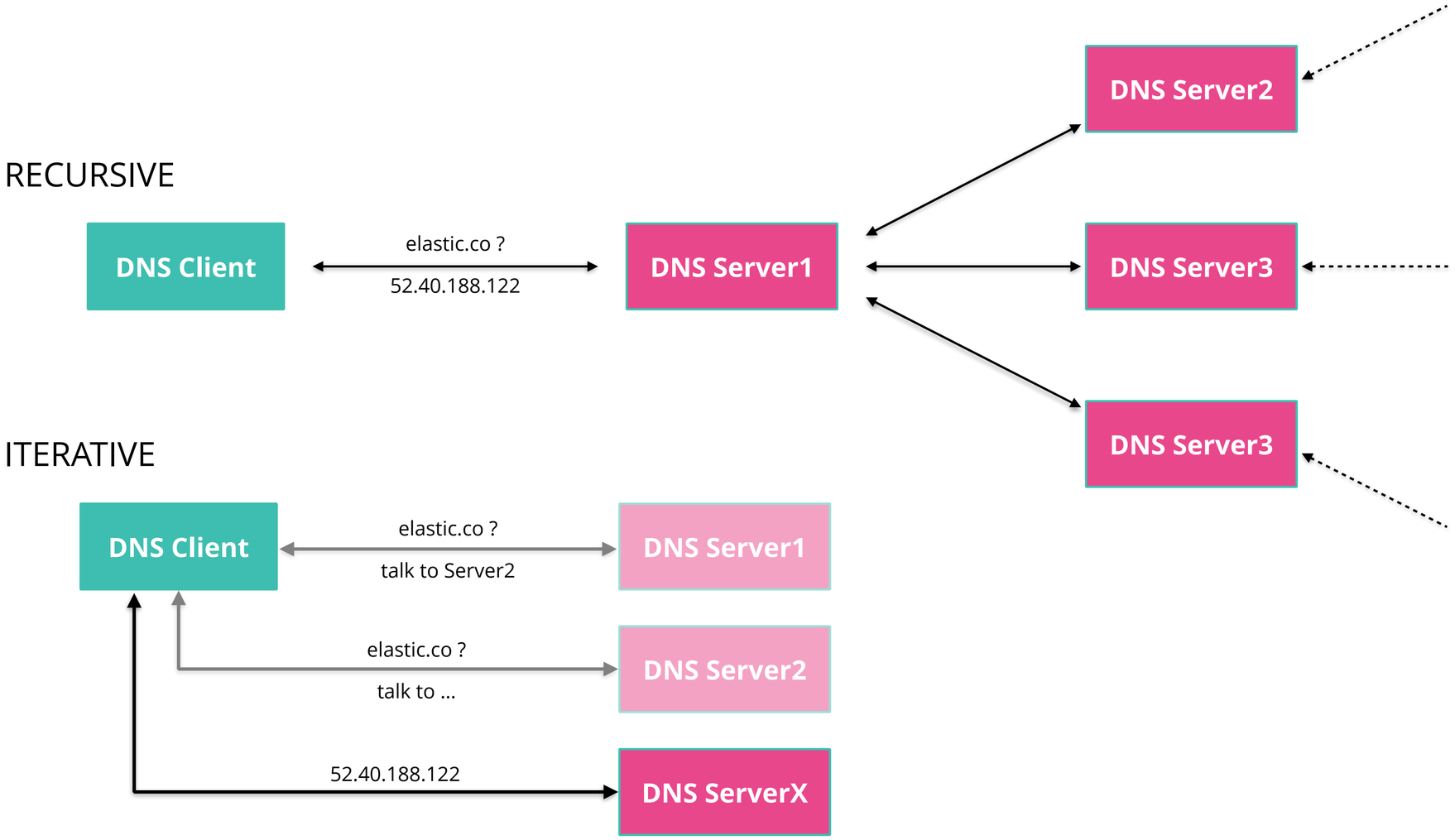
- DNS
- DNS Tunneling
- DNS Data Exfiltration
- Elastic ML Advanced Configurations
- Demo, Unit Review & Lab

DNS

DNS BASICS

- Domain Name System
- Domain Name => IP Address
- Record Types
  - A
  - AAAA
  - MX
  - NS

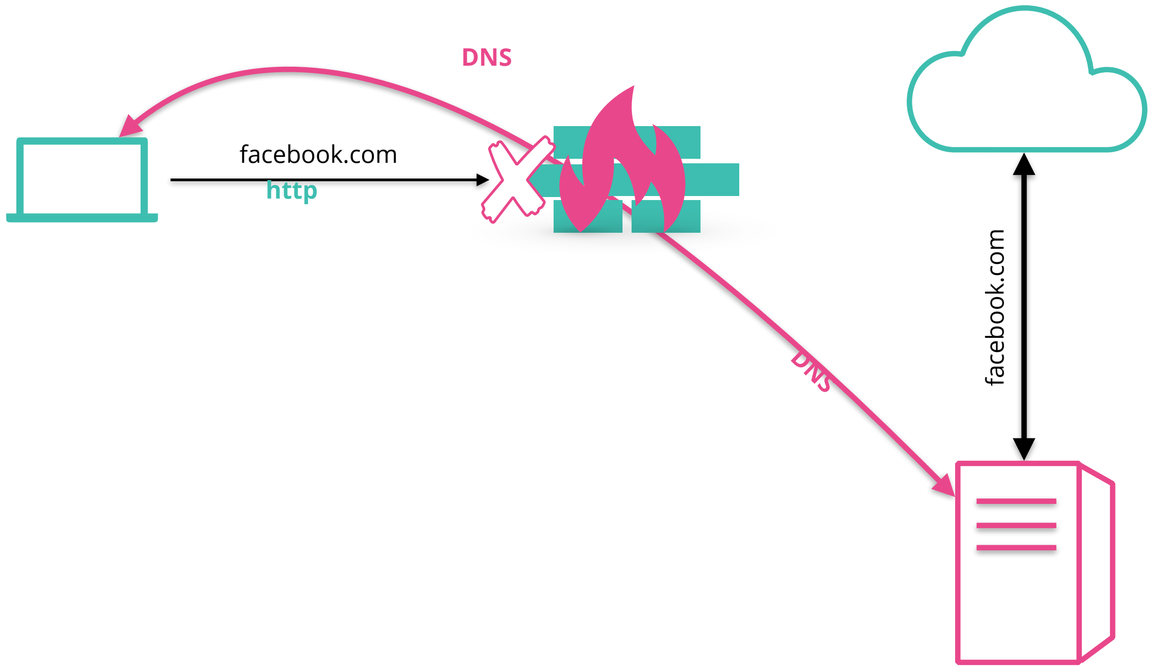
DNS IMPLEMENTATIONS



DNS DATA EXFILTRATION

DNS TUNNELING

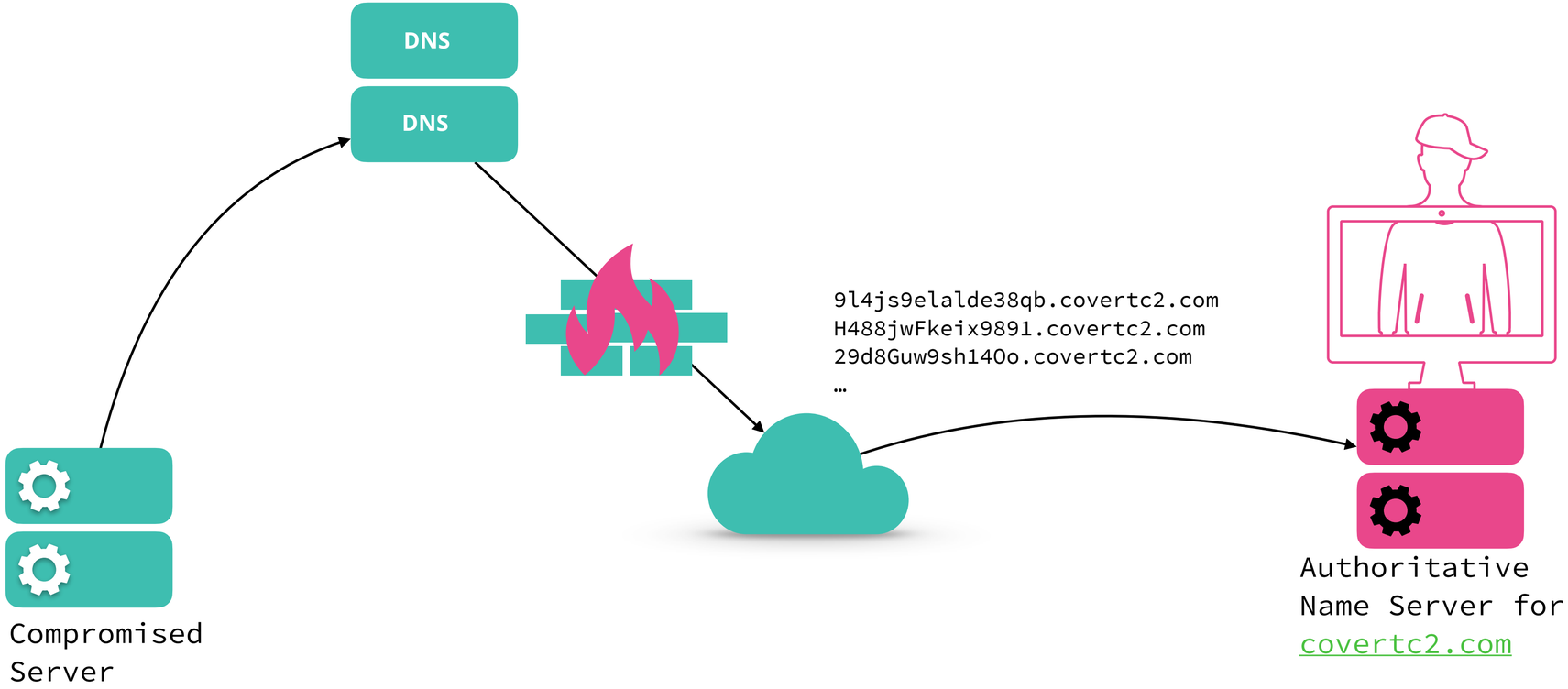
- Tools that support DNS Tunneling
  - Iodine
  - DNS2TCP
  - DNSCat



DNS DATA EXFILTRATION

- Overview
  - DNS is an Excellent Covert Channel
    - » Malware ⟷ C&C Server
    - » Never / Rarely Restricted (Crucial Role)
    - » Seldom Monitored
  - However, Attacker must
    - » Compromise Internal Host
    - » Control an External Domain
    - » Control the Authoritative Name Server for the Domain

DNS DATA EXFILTRATION



ELASTIC ML ADVANCED CONFIGURATIONS

ML ADVANCED CONFIGURATIONS

- Using the APIs
- Configure Custom URL
- Memory Model Limit
- Query Delay
- Scroll Size
- JSON Editor

DEMO

UNIT REVIEW

LAB 3