Moogsoft®

Monitoring Modern Architectures with Data Science

QCon 2017

Dave Casper, CTO

QCon SAN FRANCISCO

Abstract

Much has changed since simple distributed client/server architectures and so-too have the technologies and industry practices around monitoring.

Cloud-Native, DevOps, blue/green deployments, server-less, edge/fog, IoT all fit into a world much better handled by the emerging Artificial Intelligence for IT Operations domain more-so than traditional ITIL/SDLC approaches.

NOT FOR GENERAL DISTRIBUTION ONLY INTENDED FOR REGISTERED ATTENDEES OF QCON SF 2017

Abstract

Software continues to eat the world. Software automates, defines.

The world is "going digital" and it's quite exciting -- but this always-connected from-everything-to-everywhere world adds complexity to software systems and this talk will dive in to some of that complexity and how modern data science and algorithms are being applied to "fight machines with machines," so to speak.

NOT FOR GENERAL DISTRIBUTION ONLY INTENDED FOR REGISTERED ATTENDEES OF QCON SF 2017

-25822282

623992118

1343963318

NOT FOR GENERAL DISTRIBUTION ONLY INTENDED FOR REGISTERED ATTENDEES OF QCON SF 2017

moogsoft

NOT FOR GENERAL DISTRIBUTION ONLY INTENDED FOR REGISTERED ATTENDEES OF QCON SF 2017

NOT FOR GENERAL DISTRIBUTION ONLY INTENDED FOR REGISTERED ATTENDEES OF QCON SF 2017

discovery

monitoring

(observing)

analytics

NOT FOR GENERAL DISTRIBUTION ONLY INTENDED FOR REGISTERED ATTENDEES OF QCON SF 2017

fluid infrastructure

containers dc/os | server-less | software defined/dynamic

NOT FOR GENERAL DISTRIBUTION ONLY INTENDED FOR REGISTERED ATTENDEES OF QCON SF 2017

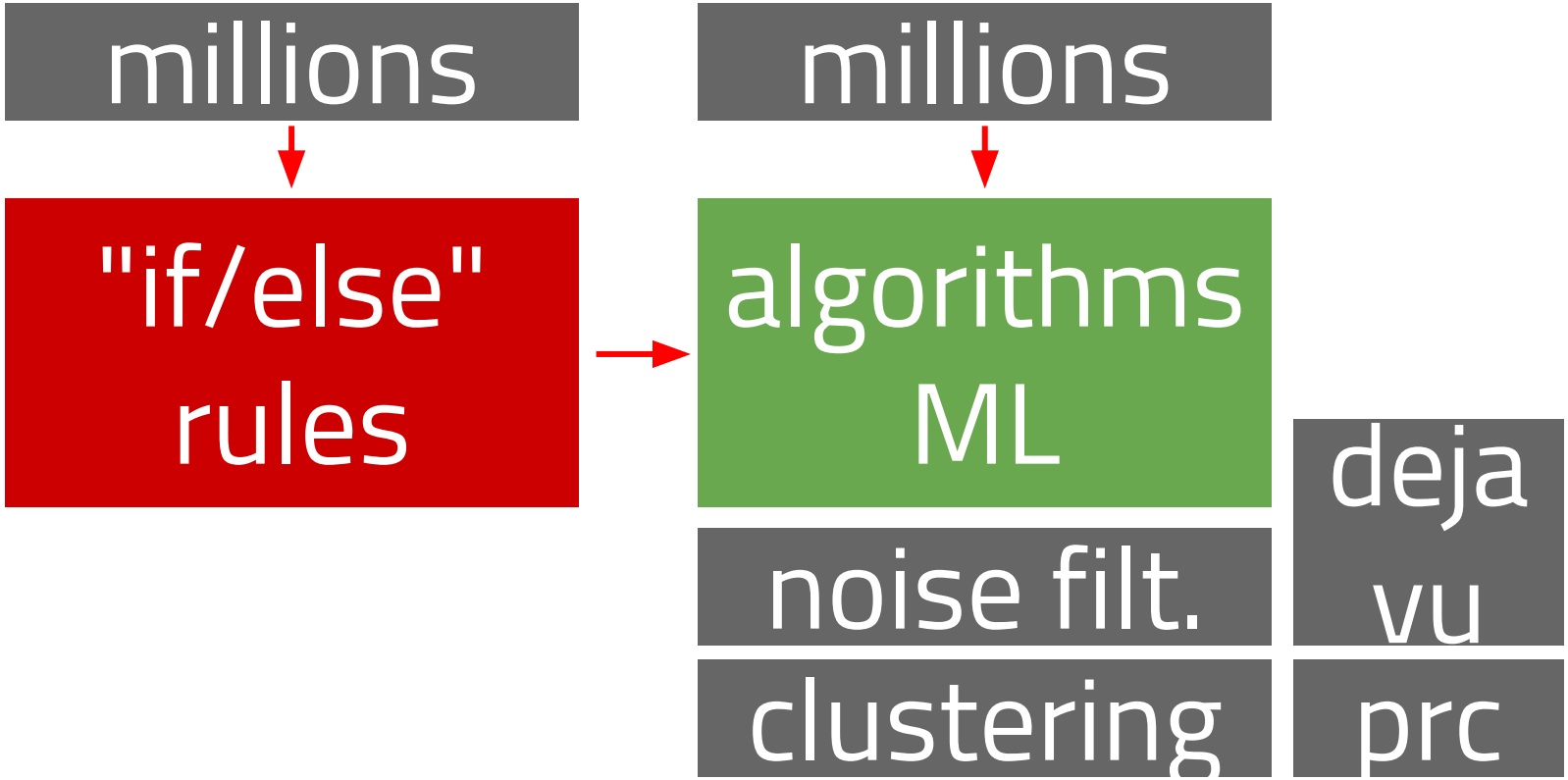
data/tx from

anything anywhere anytime

mobile | IoT | bots/RUM

NOT FOR GENERAL DISTRIBUTION ONLY INTENDED FOR REGISTERED ATTENDEES OF QCON SF 2017

NOT FOR GENERAL DISTRIBUTION ONLY INTENDED FOR REGISTERED ATTENDEES OF QCON SF 2017



NOT FOR GENERAL DISTRIBUTION ONLY INTENDED FOR REGISTERED ATTENDEES OF QCON SF 2017

AIOps
AI for IT Ops

Gartner®

NOT FOR GENERAL DISTRIBUTION ONLY INTENDED FOR REGISTERED ATTENDEES OF QCON SF 2017

customer/ business perspective

NOT FOR GENERAL DISTRIBUTION ONLY INTENDED FOR REGISTERED ATTENDEES OF QCON SF 2017

This slide courtesy Andy Brown, Sandhill East
https://www.linkedin.com/in/andybrown63/

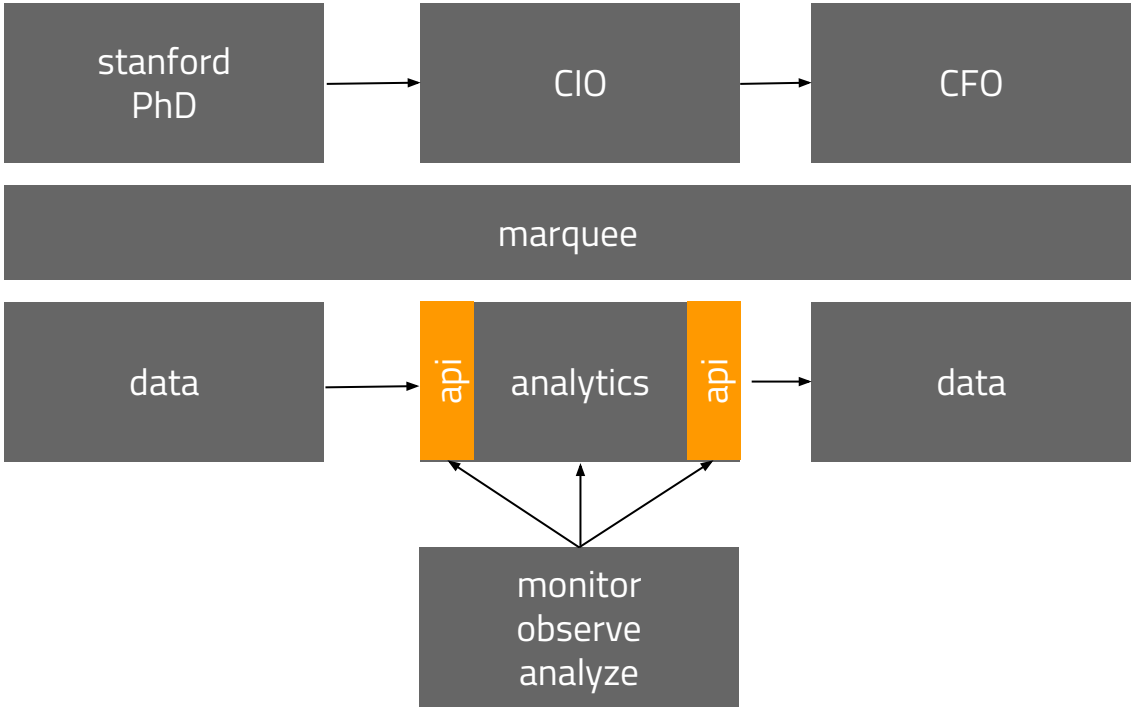
“**Silicon Valley is coming.**
There are hundreds of startups with a lot of brains and money working on various alternatives to traditional banking. **They are very good at reducing the ‘pain points’ …**”
JAMIE DIMON
JPMorgan Chase & Co.
Chairman & Chief Executive Officer
April 2015
This slide courtesy Andy Brown, Sandhill East
https://www.linkedin.com/in/andybrown63/

go digital
or die trying

NOT FOR GENERAL DISTRIBUTION ONLY INTENDED FOR REGISTERED ATTENDEES OF QCON SF 2017

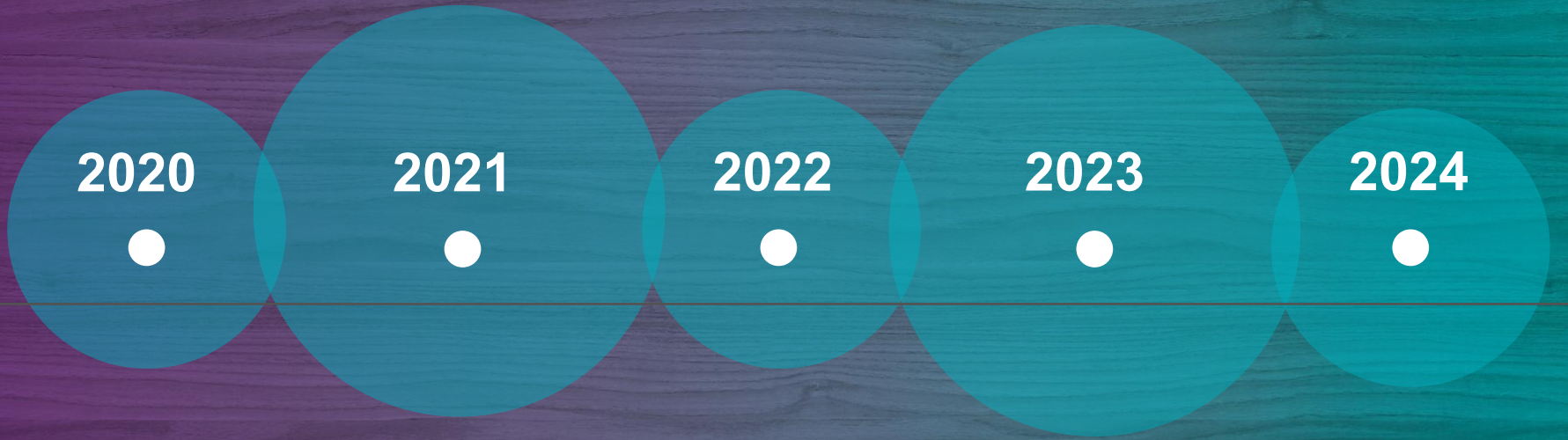
gs wants to become "google of wall st."

NOT FOR GENERAL DISTRIBUTION ONLY INTENDED FOR REGISTERED ATTENDEES OF QCON SF 2017



NOT FOR GENERAL DISTRIBUTION ONLY INTENDED FOR REGISTERED ATTENDEES OF QCON SF 2017

THE REALLY BIG PICTURE



In 5 – 10 years, every company will be a **Digital Software Business**

Security, service assurance and consumer centricity become **THE BOARD LEVEL PRIORITY**

Enterprises going **DIGITAL ADOPT HYBRID IT**

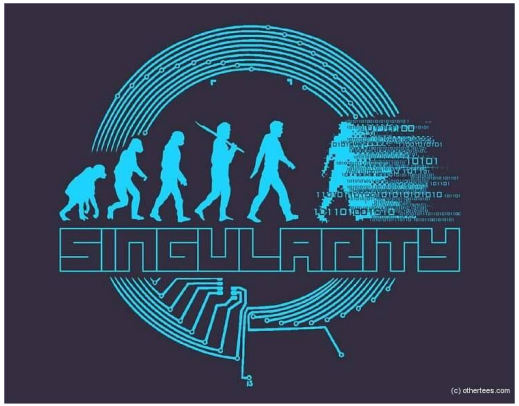
This slide courtesy Andy Brown, Sandhill East
https://www.linkedin.com/in/andybrown63/

traditional	hybrid	digital
40% Change 60% Run **Infrastructure Led** **Owns Facilities, Data Centers, Hardware, Networks et al** **Has Refresh Cycles caused by Capital Depreciation** **Still using Waterfall for App Dev** **Thinking led by Inf Technologists (hardware, DB, OS et al)** **Traditional Procurement** **Less Agile, Change resistant**	**60% Change 40% Run** **AppDev starting to lead** **Owns less Facilities, Data Centers, Hardware, Networks, et al** **Still Has Refresh Cycles caused by CapitalDepreciation** **Combination Waterfall & Agilefor App Dev** **Thinking led by CIO "Move to Cloud" Traditional Procurement weakening** **More Agile, Less Change resistant**	**80% Change 20% Run** **AppDev leads decisioning** **Doesn't own hardware** **Refresh doesn't exist** **All Agile for App Dev** **Thinking led by CIO "Move to Cloud"** **Cloud Centric "Marketplace" Procurement** **Embraces Change, Very Agile**

This slide courtesy Andy Brown, Sandhill East
https://www.linkedin.com/in/andybrown63/

2045

?



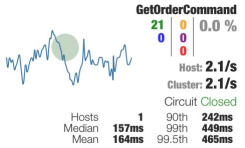
NOT FOR GENERAL DISTRIBUTION ONLY INTENDED FOR REGISTERED ATTENDEES OF QCON SF 2017

SNMP / traps

or

Daylight Savings

NOT FOR GENERAL DISTRIBUTION ONLY INTENDED FOR REGISTERED ATTENDEES OF QCON SF 2017



AIOps

EdgeOps

AMRS

EPS

every ip interface globally

APAC

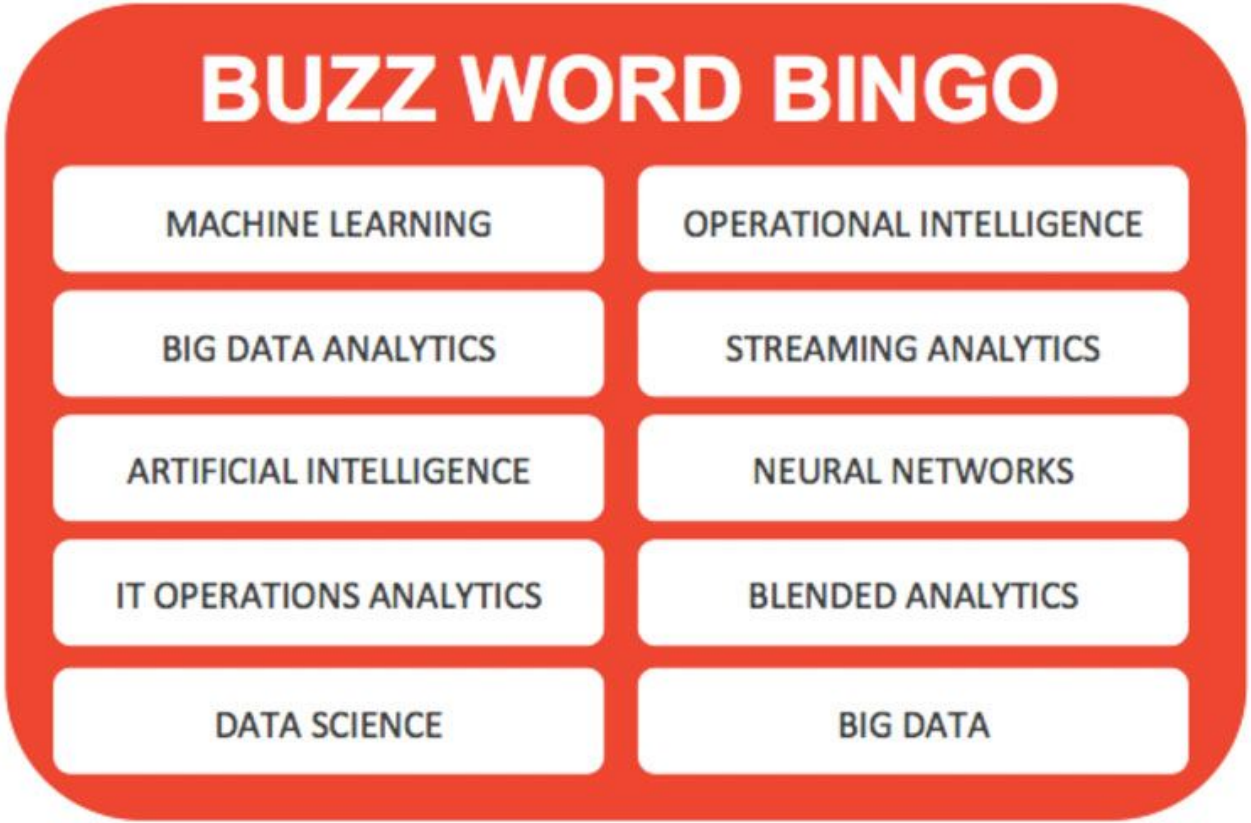
EdgeOps

EMEA

EdgeOps

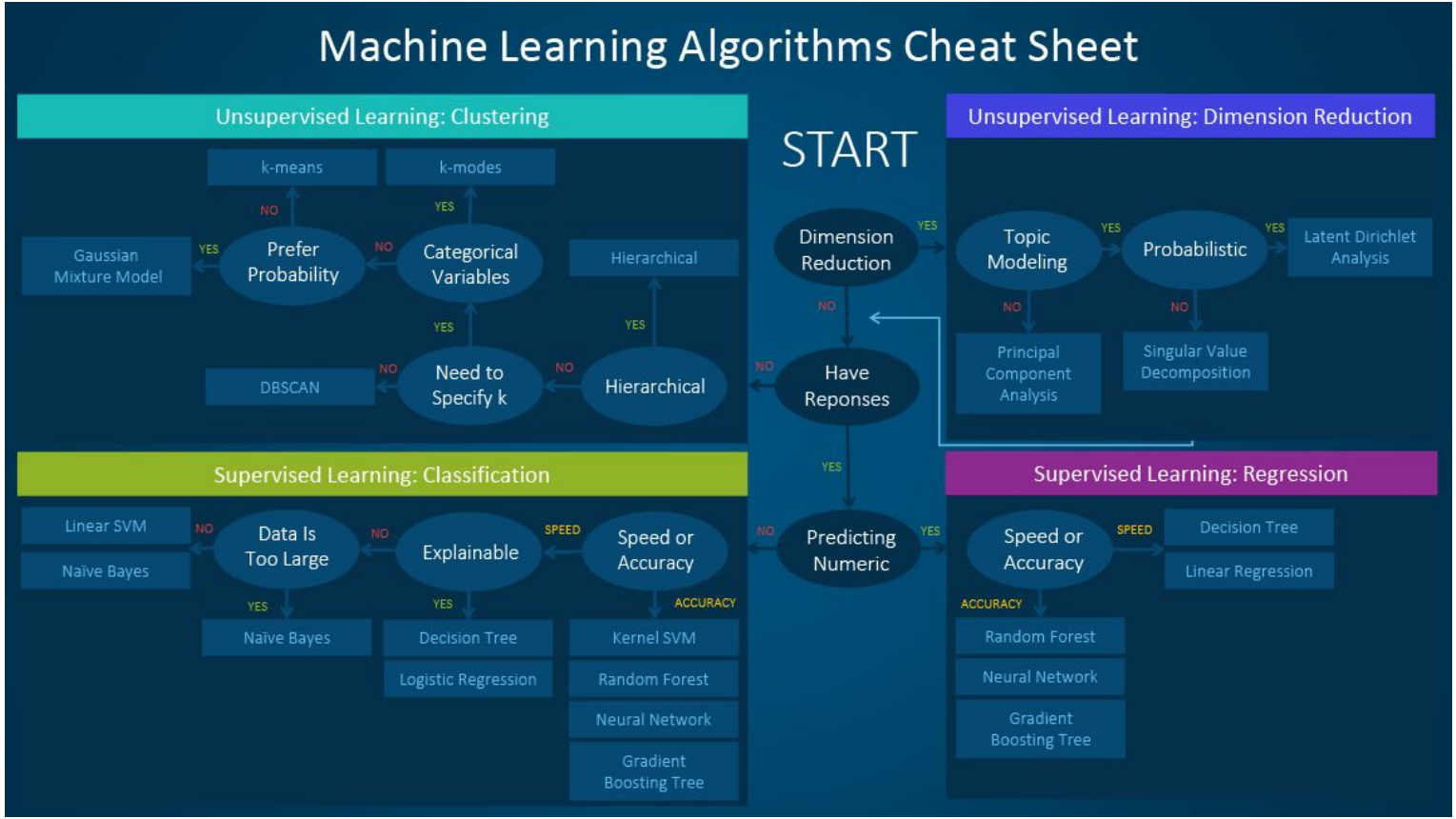
algorithms we use

NOT FOR GENERAL DISTRIBUTION ONLY INTENDED FOR REGISTERED ATTENDEES OF QCON SF 2017



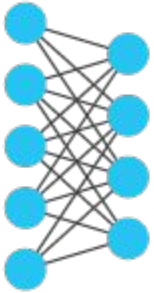
This slide courtesy our Chief Scientist Dr. Rob Harper -- Do check out his great 3-part blog on Machine Learning in Moogsoft AIOps: https://www.moogsoft.com/author/robharper/

NOT FOR GENERAL DISTRIBUTION ONLY INTENDED FOR REGISTERED ATTENDEES OF QCON SF 2017

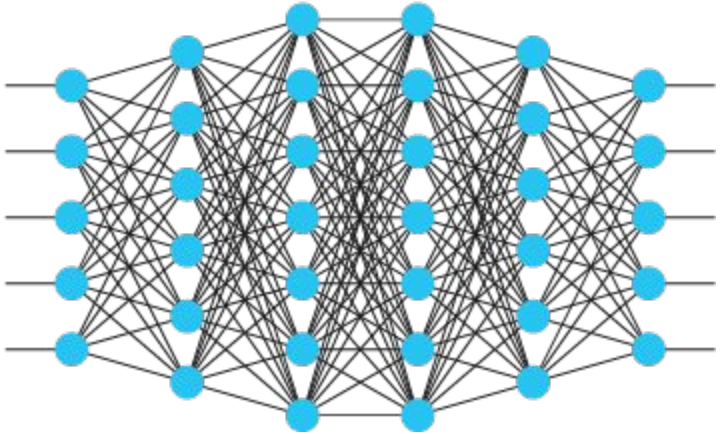


By Hui Li on Subconscious Musings April 12, 2017

Simple Neural Network

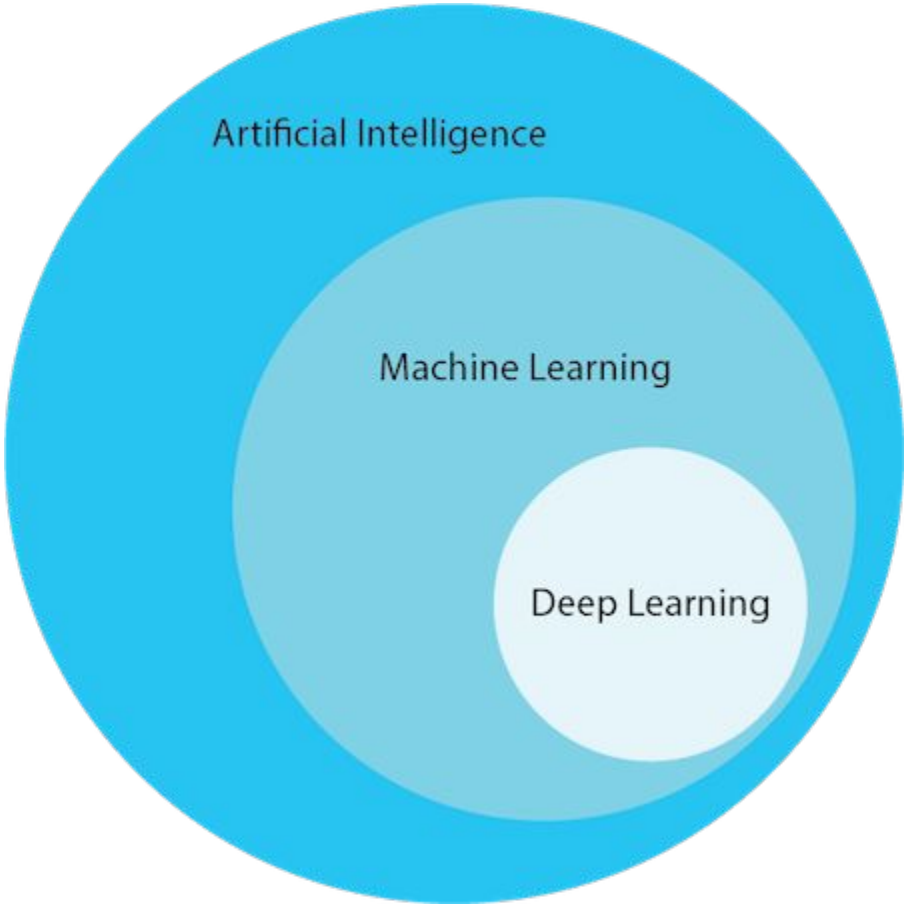


Deep Learning Neural Network



This slide courtesy our Chief Scientist Dr. Rob Harper -- Do check out his great 3-part blog on Machine Learning in Moogsoft AIOps: https://www.moogsoft.com/author/robharper/

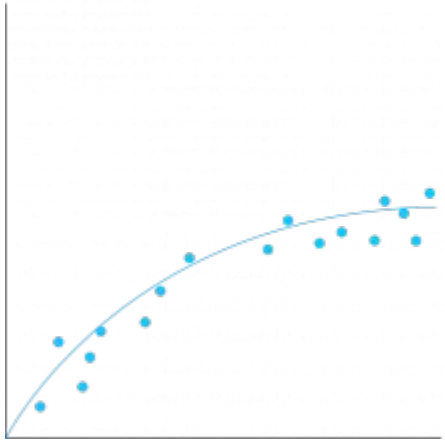
NOT FOR GENERAL DISTRIBUTION ONLY INTENDED FOR REGISTERED ATTENDEES OF QCON SF 2017



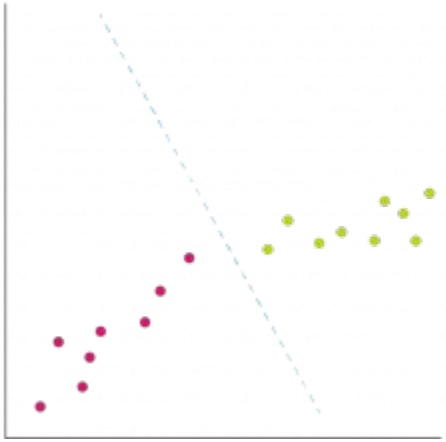
This slide courtesy our Chief Scientist Dr. Rob Harper -- Do check out his great 3-part blog on Machine Learning in Moogsoft AIOps: https://www.moogsoft.com/author/robharper/

NOT FOR GENERAL DISTRIBUTION ONLY INTENDED FOR REGISTERED ATTENDEES OF QCON SF 2017

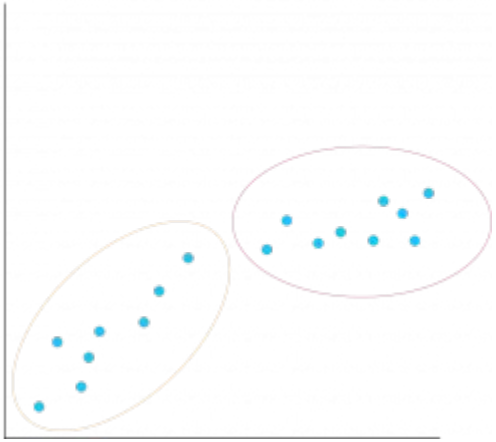
regression



classification

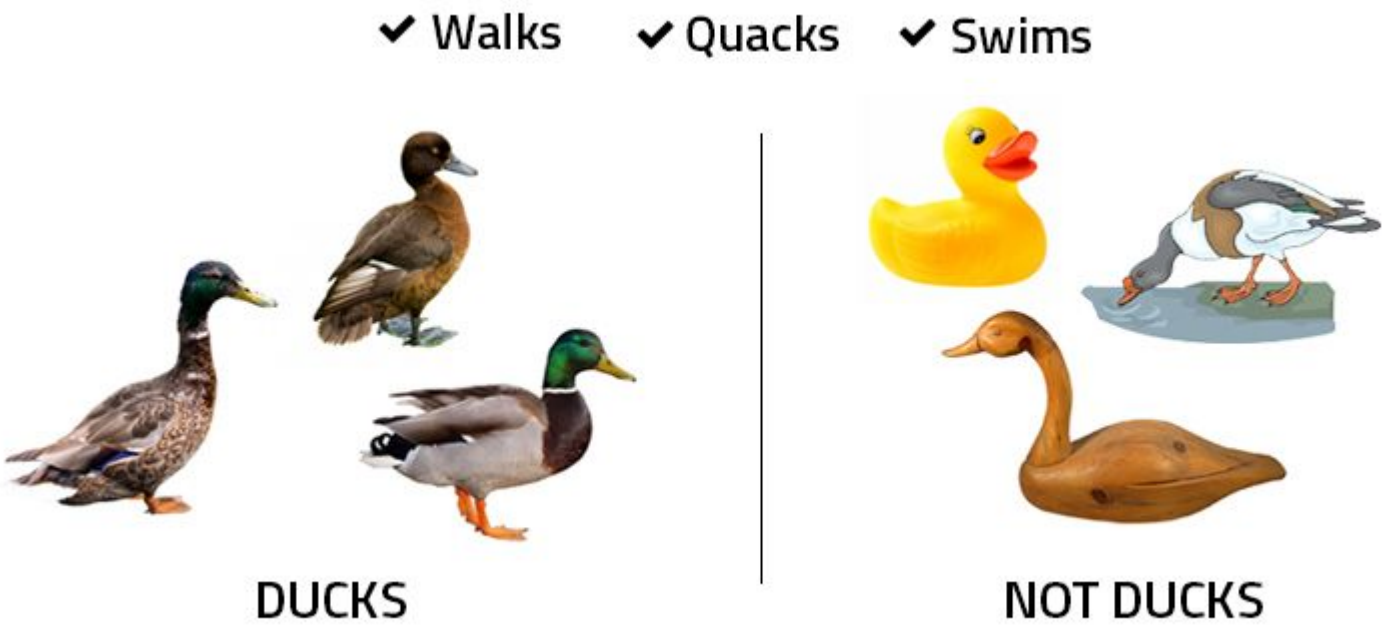


clustering



This slide courtesy our Chief Scientist Dr. Rob Harper -- Do check out his great 3-part blog on Machine Learning in Moogsoft AIOps: https://www.moogsoft.com/author/robharper/

classification supervised



"learn by example" approach. Supervised learning systems need to be given examples of what is "good" and what is "bad"

This slide courtesy our Chief Scientist Dr. Rob Harper -- Do check out his great 3-part blog on Machine Learning in Moogsoft AIOps: https://www.moogsoft.com/author/robharper/

NOT FOR GENERAL DISTRIBUTION ONLY INTENDED FOR REGISTERED ATTENDEES OF QCON SF 2017

classification

NOT FOR GENERAL DISTRIBUTION ONLY INTENDED FOR REGISTERED ATTENDEES OF QCON SF 2017

clustering unsupervised

Patterns that you didn't know existed prior. Recommender systems rely heavily on these techniques.

NOT FOR GENERAL DISTRIBUTION ONLY INTENDED FOR REGISTERED ATTENDEES OF QCON SF 2017

supervised machine learning "hot dog?" "not hot dog?"

NOT FOR GENERAL DISTRIBUTION ONLY INTENDED FOR REGISTERED ATTENDEES OF QCON SF 2017

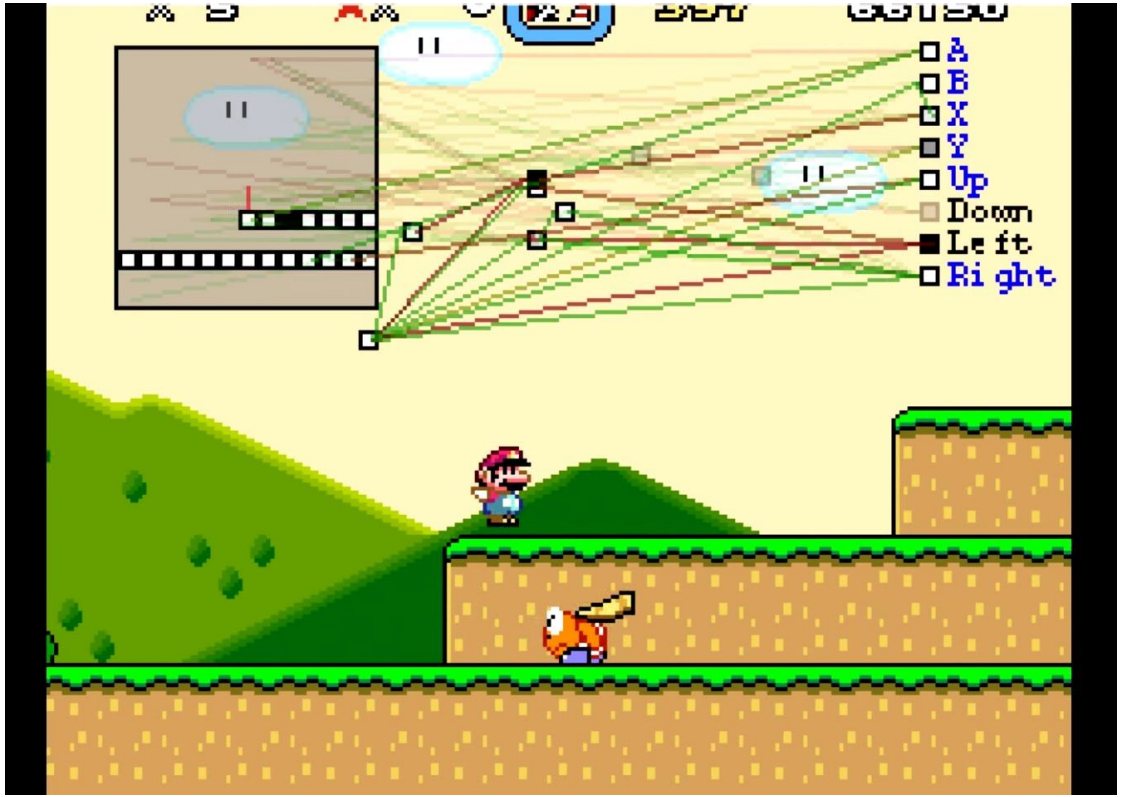
edwin.moogsoft.com:moog:aws:AWSCloudWatch:AWSLambdaDuration:filterByUserProfile
ANOMALIES
227
HIGH
19967.58
Threshold
value
Anomalies
Average
24 k
18 k
12 k
6 k
0
10:45:18 PM
11:00:18 PM
11:15:18 PM
11:30:18 PM
11:45:18 PM
Untitled graph
1h
3h
12h
1d
3d
1w
custom
Line
Actions
Milliseconds
20.0k
10.0k
70.5
22:45
22:50
22:55
23:00
23:05
23:10
23:15
23:20
23:25
23:30
23:35
23:40
23:45
Duration
4:12 / 6:01

algorithms we use

NOT FOR GENERAL DISTRIBUTION ONLY INTENDED FOR REGISTERED ATTENDEES OF QCON SF 2017

neural nets

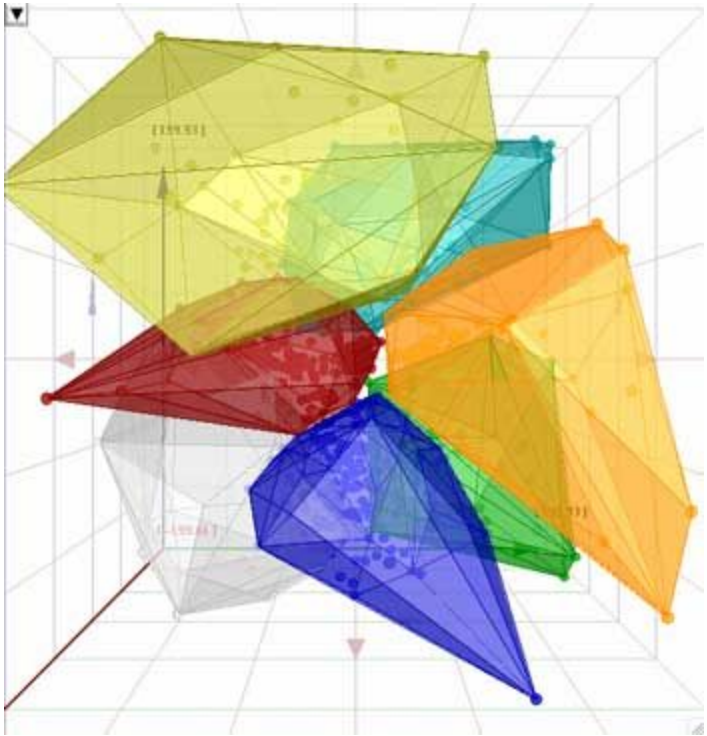
SethBling mar i/o



https://www.youtube.com/watch?v=qv6UVOQ0F44 lua code: https://pastebin.com/ZZmSNaHX

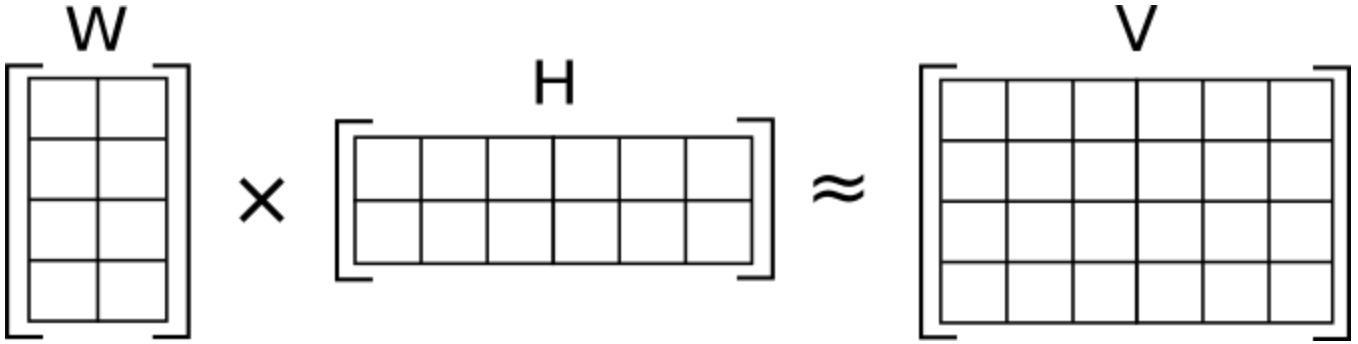
NOT FOR GENERAL DISTRIBUTION ONLY INTENDED FOR REGISTERED ATTENDEES OF QCON SF 2017

k-means clustering

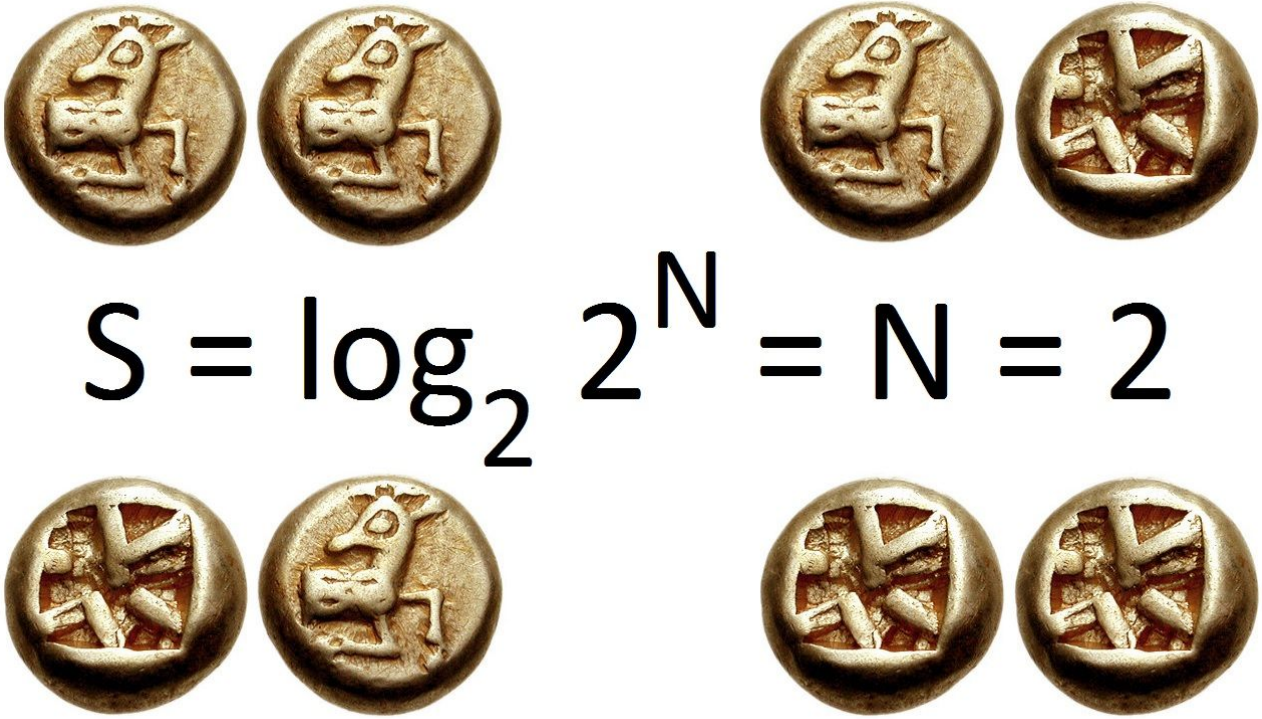


NOT FOR GENERAL DISTRIBUTION ONLY INTENDED FOR REGISTERED ATTENDEES OF QCON SF 2017

matrix factorization

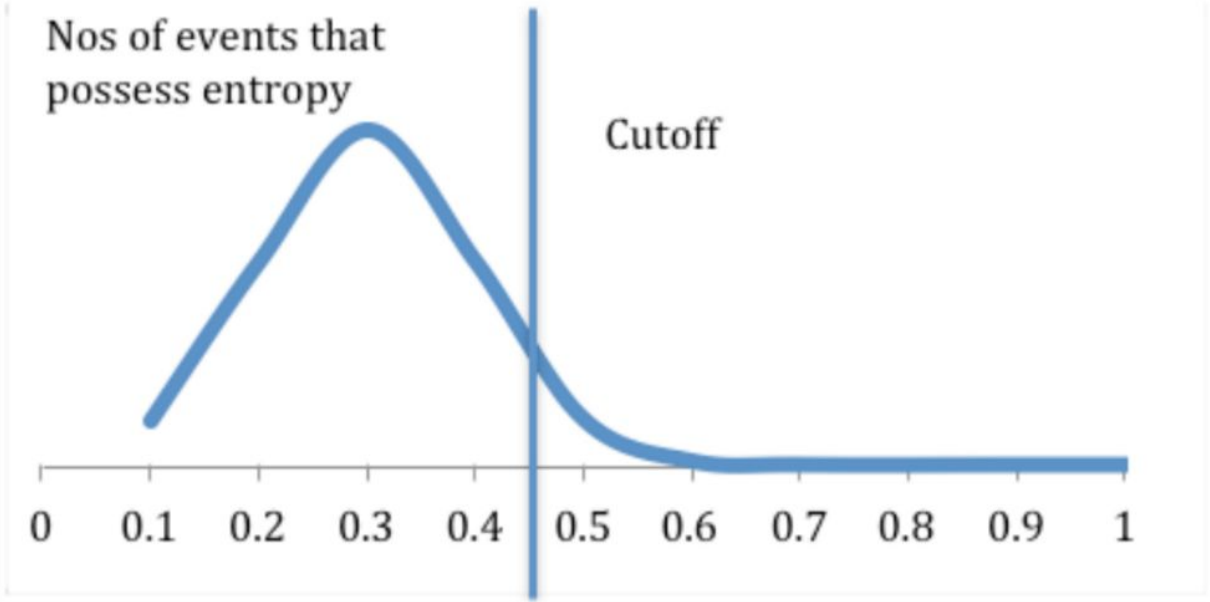


shannon entropy



$$S = \log_2 2^N = N = 2$$

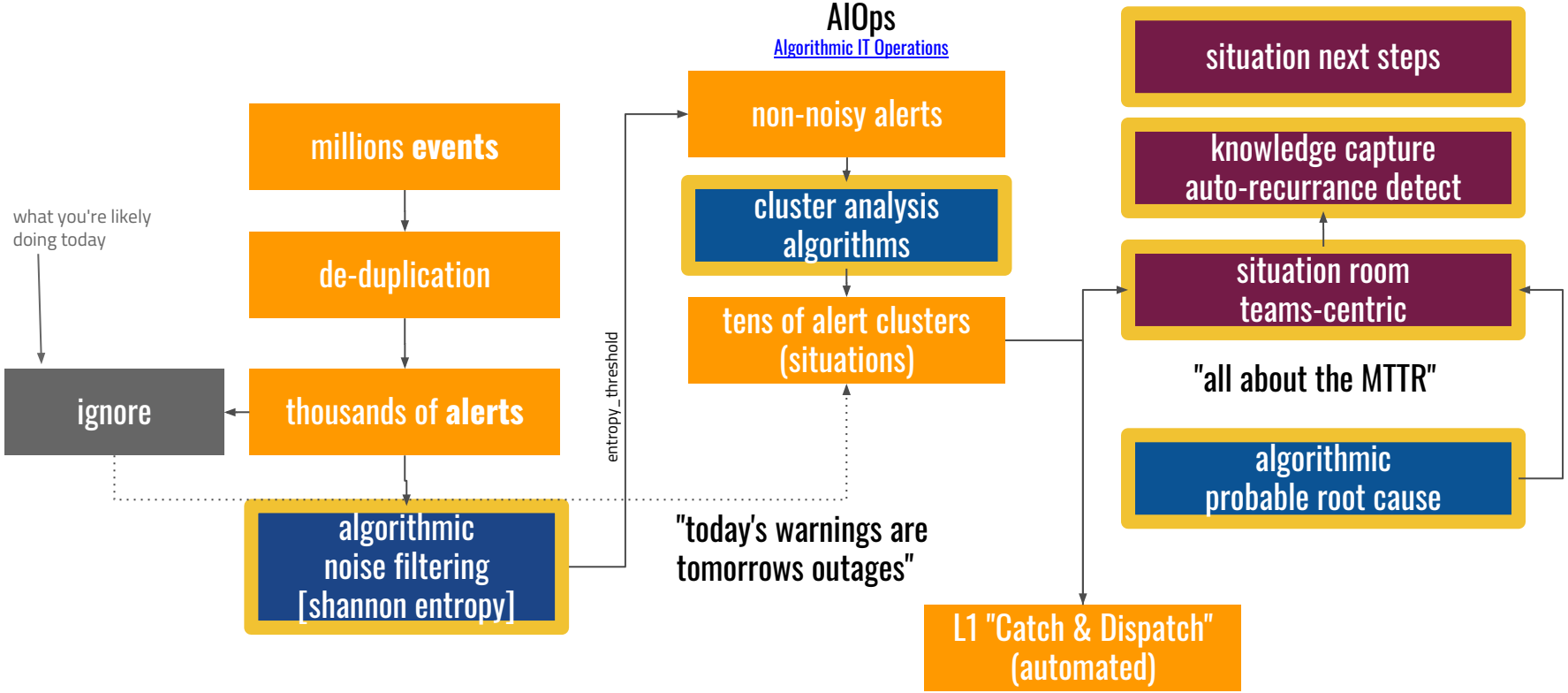
typical entropy distribution



NOT FOR GENERAL DISTRIBUTION ONLY INTENDED FOR REGISTERED ATTENDEES OF QCON SF 2017

algorithmic workflow

NOT FOR GENERAL DISTRIBUTION ONLY INTENDED FOR REGISTERED ATTENDEES OF QCON SF 2017



NOT FOR GENERAL DISTRIBUTION ONLY INTENDED FOR REGISTERED ATTENDEES OF QCON SF 2017

...speaking of classification

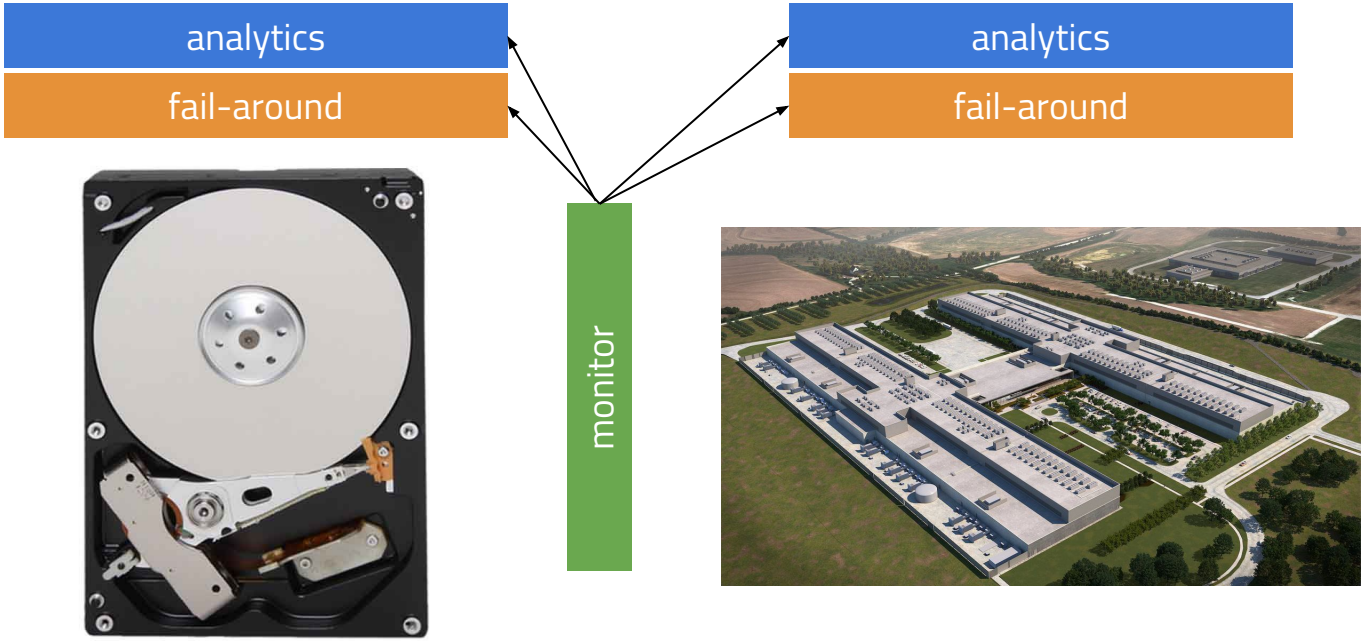
NOT FOR GENERAL DISTRIBUTION ONLY INTENDED FOR REGISTERED ATTENDEES OF QCON SF 2017

fault vs audit

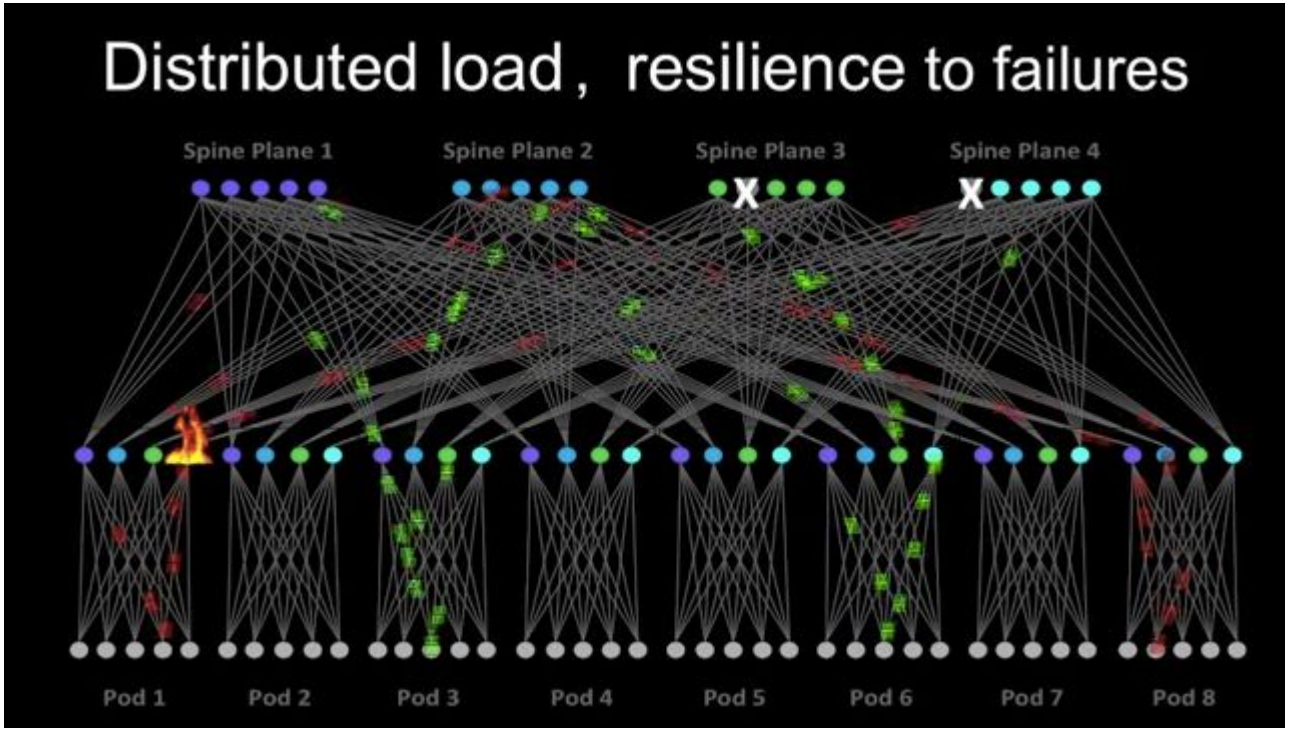
fix ⟶ optimize

NOT FOR GENERAL DISTRIBUTION ONLY INTENDED FOR REGISTERED ATTENDEES OF QCON SF 2017

monitoring fail-around



weld the datacenter doors shut



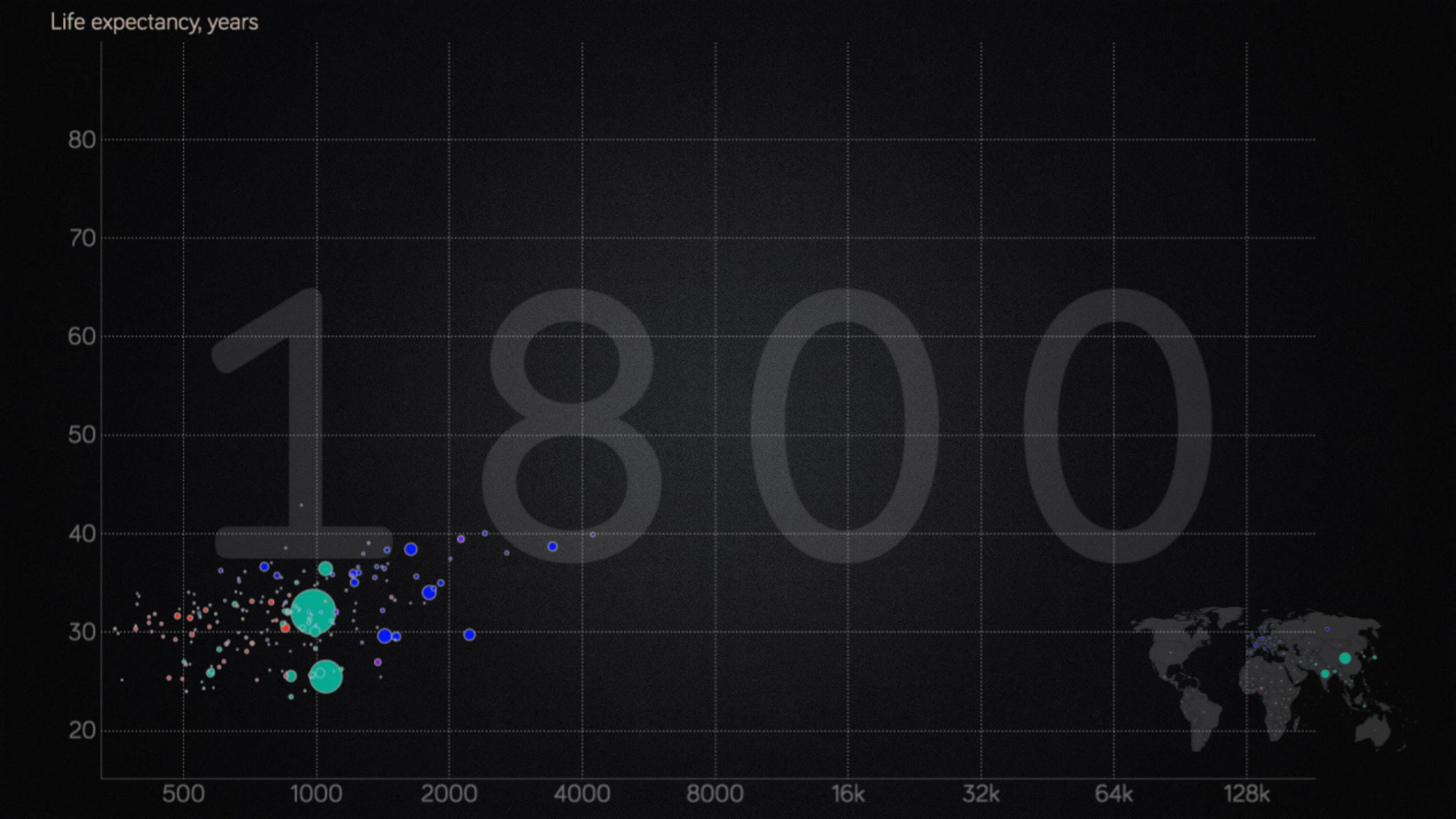
NOT FOR GENERAL DISTRIBUTION ONLY INTENDED FOR REGISTERED ATTENDEES OF QCON SF 2017

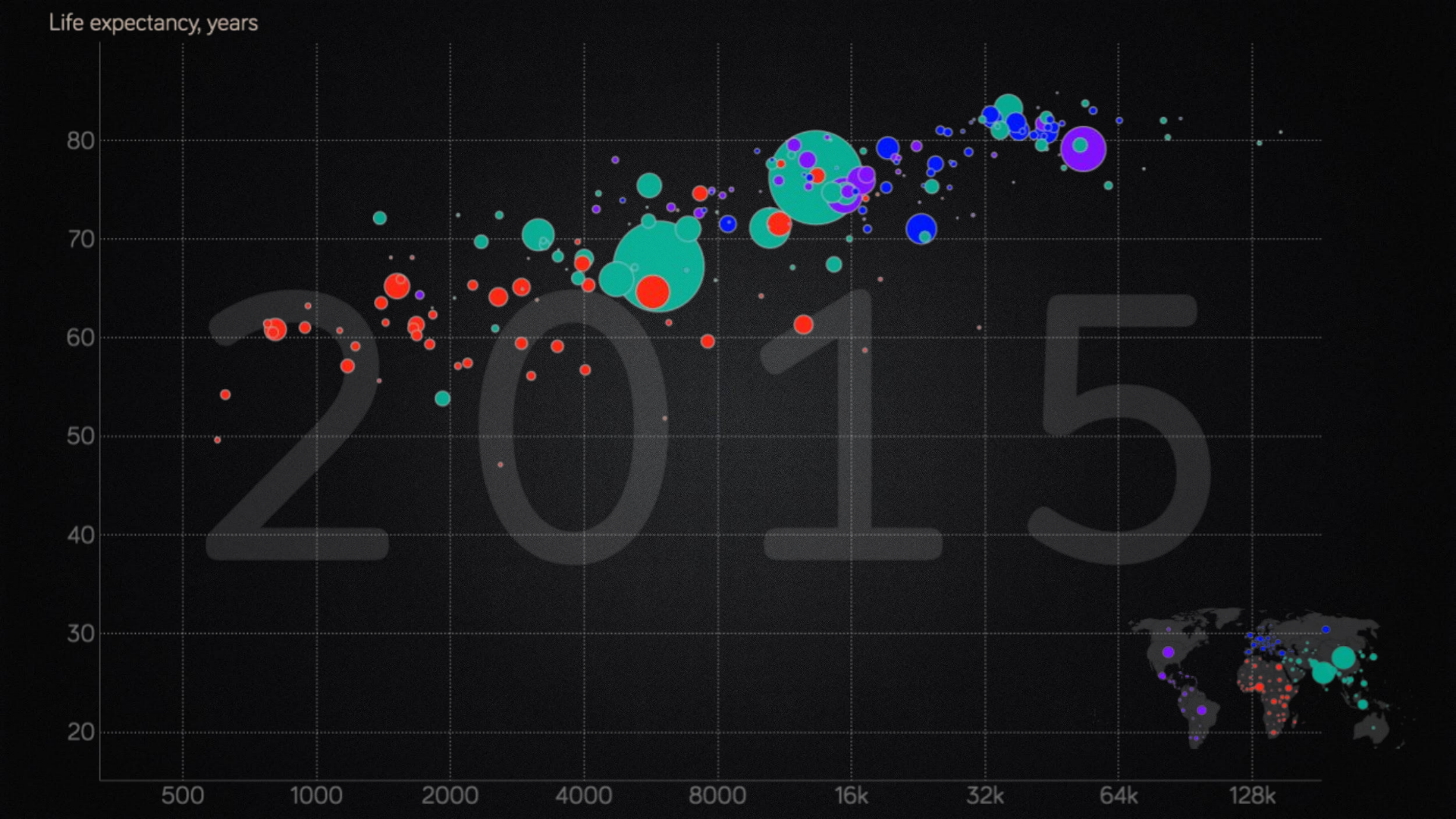
<lofty_ tangent>

non-technical

NOT FOR GENERAL DISTRIBUTION ONLY INTENDED FOR REGISTERED ATTENDEES OF QCON SF 2017

THE
INDUSTRIAL
REVOLUTION
1.0


Life expectancy, years
80
70
60
50
40
30
20
1800
500
1000
2000
4000
8000
16k
32k
64k
128k


Life expectancy, years
80
70
60
50
40
30
20
2015
500
1000
2000
4000
8000
16k
32k
64k
128k

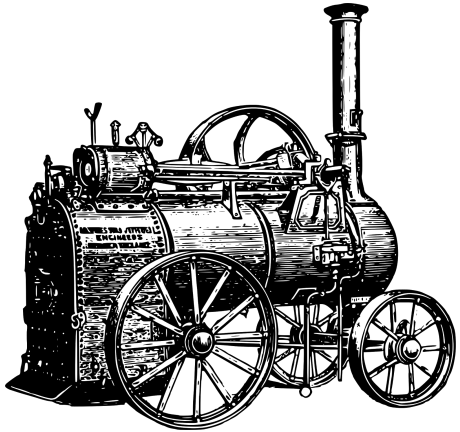
BBC FOUR
lifespan
75 years
50 years
25 years
1927
income
$400
$4 000
$40 000

WE FACE
EXISTENTIAL
THREATS
TO OUR PROGRESS

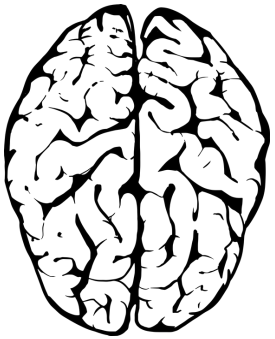
#
Country
340 China
298 United States
97 Netherlands
57 Canada
56 South Korea
50 Russia
48 Hong Kong
45 France
40 Sweden
32 India
#
Country
999 United States
54 Hong Kong
33 Portugal
29 Bulgaria
28 Canada
26 Turkey
26 Germany
23 United Kingdom
22 France
18 Singapore
ATTACKS
Timestamp
Attacker
Organization
Location
IP
Target
Location
Type
Service
Port
2014-06-25 11:47:03.66 Iturricane Electric Stanford, United States 184.105.139.114 Seattle, United States NetController, ntp 123
2014-06-25 11:47:03.97 TOT Public Company Thanyaburi, Thailand 101.108.250.0 Saint Louis, United States unknown 52421
2014-06-25 11:47:04.53 Webhosting.Net Miami, United States 67.215.180.162 Miami, United States discard 9
2014-06-25 11:47:04.53 Webhosting.Net Miami, United States 67.215.180.162 Miami, United States discard 9
ATTACK TYPES
#
Service
Port
115 ssh 22
93 ms-term-services 3389
84 isakmp 500
70 microsoft-ds 445

THE
INDUSTRIAL
REVOLUTION 2.0
CAN HELP SAVE US

v1.0



v2.0

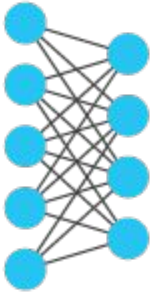


COMPLEXITY IS
THE PRINCIPAL
THREAT
TO THE REVOLUTION

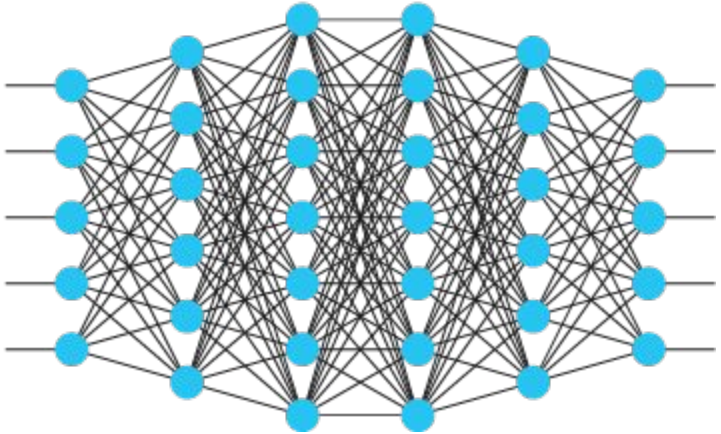
</lofty_non-technical_tangent>

NOT FOR GENERAL DISTRIBUTION ONLY INTENDED FOR REGISTERED ATTENDEES OF QCON SF 2017

Simple Neural Network



Deep Learning Neural Network



NOT FOR GENERAL DISTRIBUTION ONLY INTENDED FOR REGISTERED ATTENDEES OF QCON SF 2017

```
{
      # The following defines the input neurons in the net
      # and which activities will prompt a reinforcement learning
      # step, or a brain to be shot!

      inputs          : [ "source","description","severity","manager" ],
      learn_queues    : [ "manual_create","rated","merge_create","split_create","annotated","diagnosed","refined"],
      unlearn_queues  : [ "rated","split" ],
      rating_threshold: 3,


      # When training a brain, how many negative alerts to
      # train with positive hits

      alert_pool_size : 100,


      # Ok, brain configuration


      # The followings are the default values that do not need to be specified,
      # and in fact not recommended to change by customers
      neurons             : 7,          # number of hidden neurons is dynamically set
      layers              : 2,          # number of hidden layer is default to 1
      learning_rate       : 0.15,
      activation_func     : "Hyperbolic",
      epochs              : 500,


      # Match strategy can be "Best" (closest to 1) or "Min_Error" (closest to trained result)
      # Match strategy can be omitted, in which case it is default to "Min_Error"

      # match_strategy      : "Min_Error",

      precision           : 92.0,         # % precision to train for
      tolerance           : 0.3,          # % tolerance of error in match
      exact_match         : false,

}
```

NOT FOR GENERAL DISTRIBUTION ONLY INTENDED FOR REGISTERED ATTENDEES OF QCON SF 2017

theory

applied

sharing | giving back

NOT FOR GENERAL DISTRIBUTION ONLY INTENDED FOR REGISTERED ATTENDEES OF QCON SF 2017

Moogsoft®