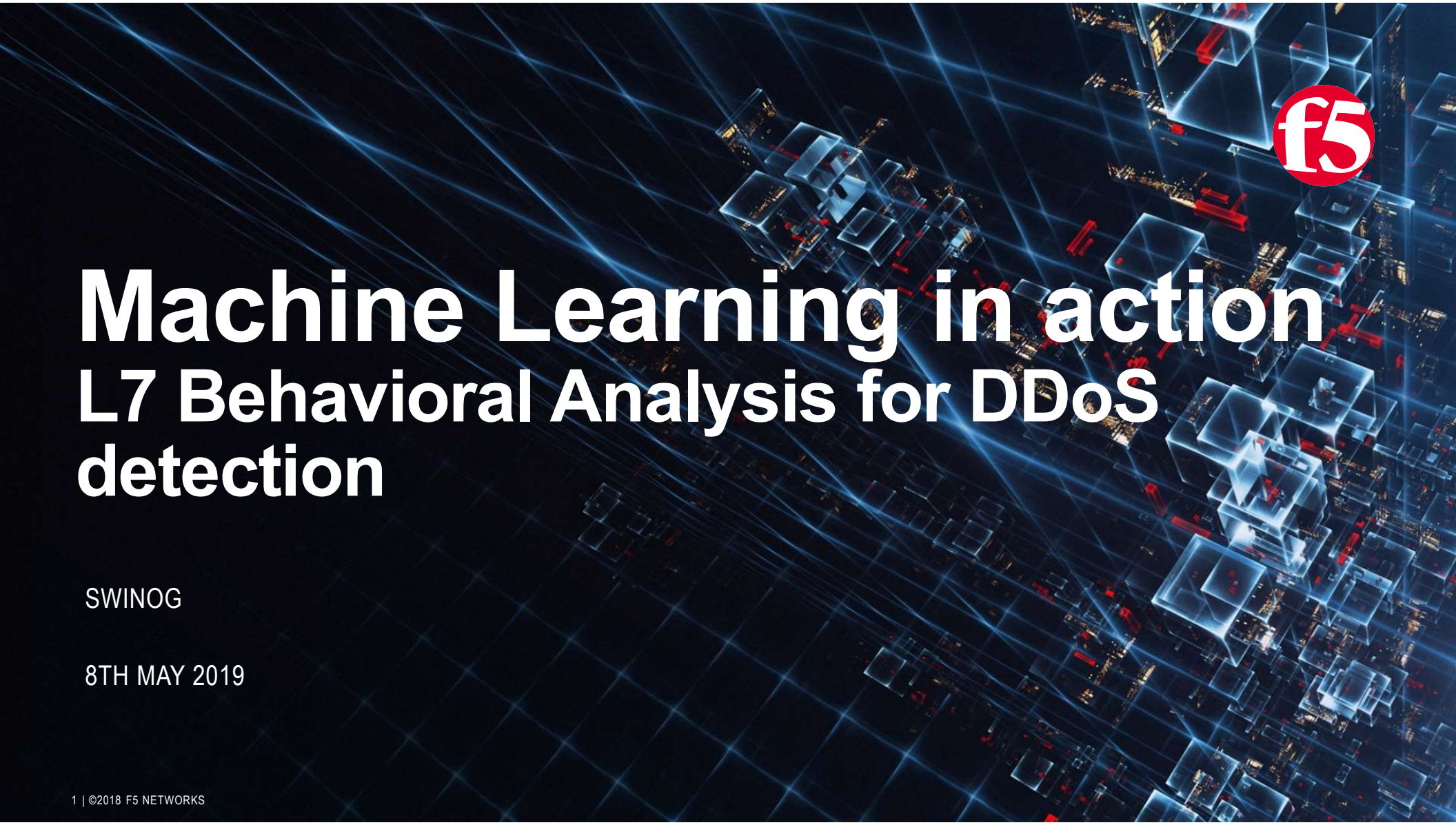
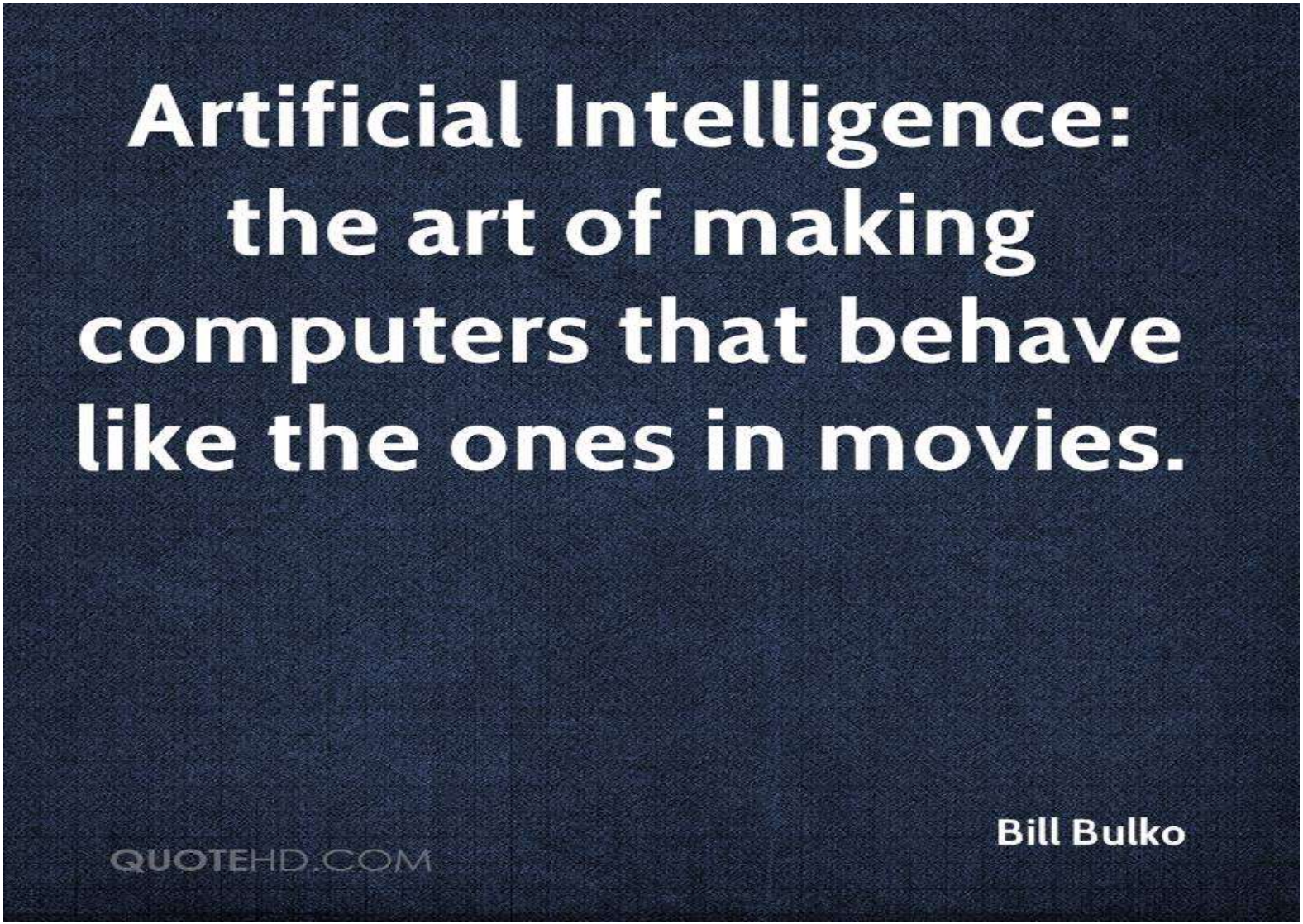
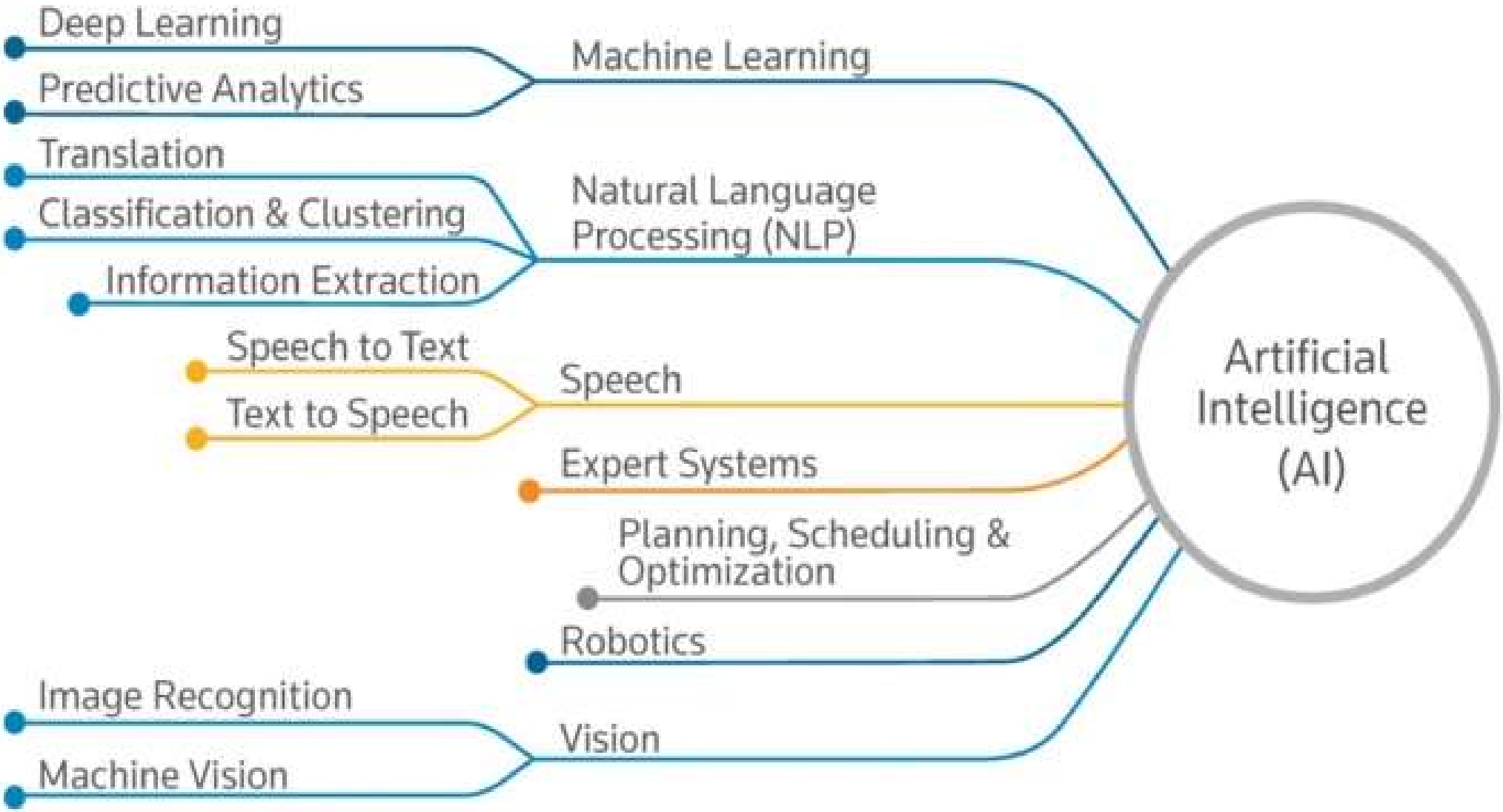


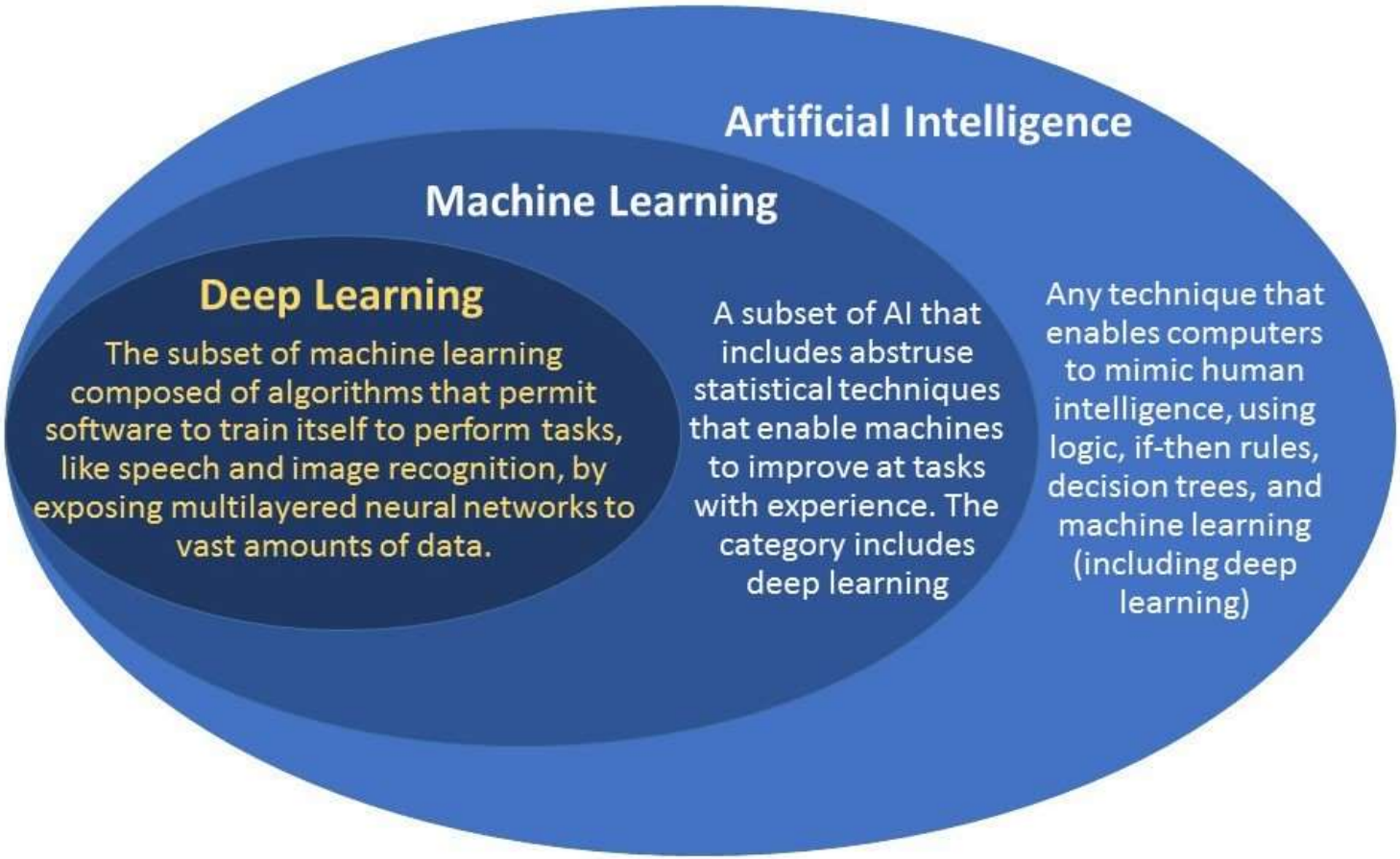
Machine Learning in action
L7 Behavioral Analysis for DDoS detection

SWINOG

8TH MAY 2019

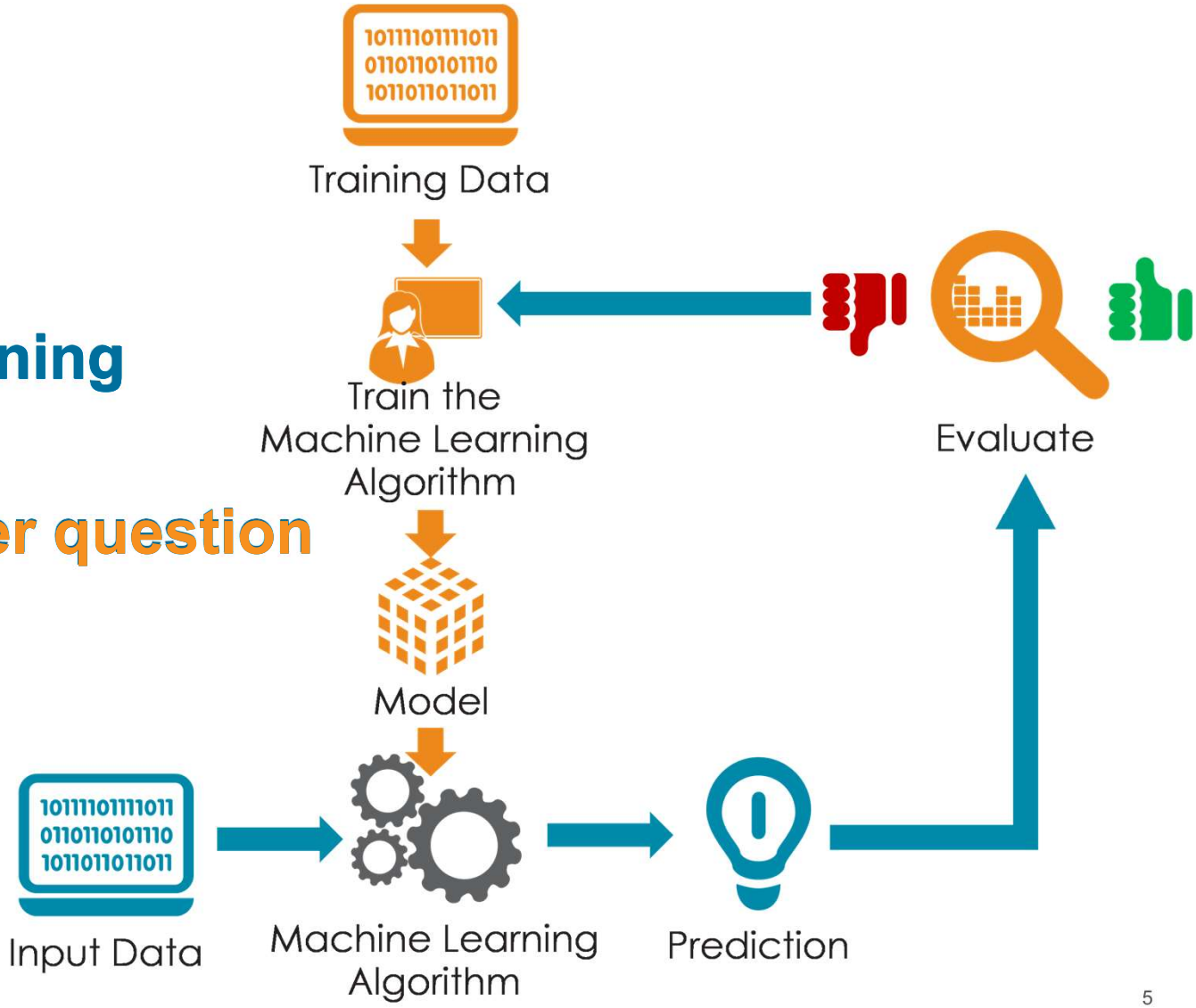

Artificial Intelligence:
the art of making
computers that behave
like the ones in movies.
Bill Bulko
QUOTEHD.COM

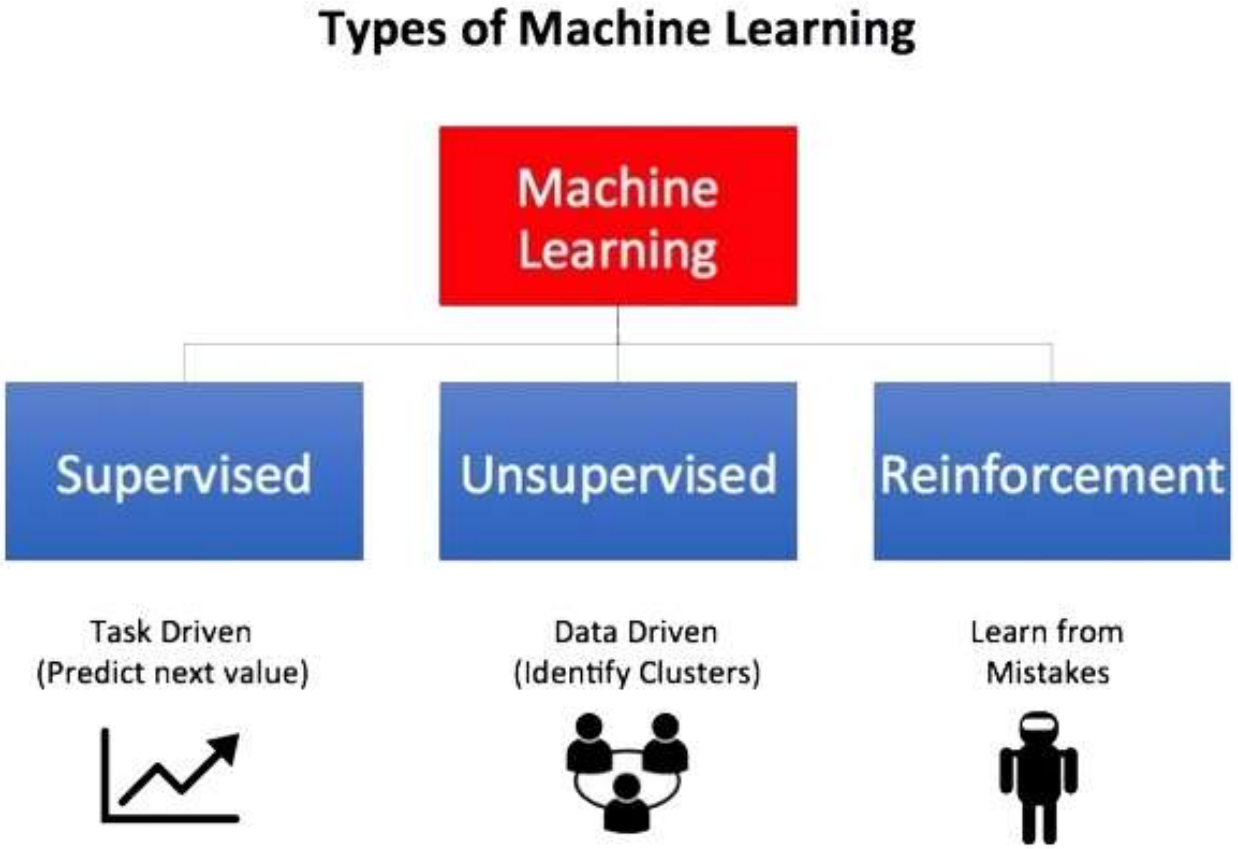

Deep Learning
Predictive Analytics
Machine Learning
Translation
Classification & Clustering
Information Extraction
Natural Language Processing (NLP)
Speech to Text
Text to Speech
Speech
Expert Systems
Planning, Scheduling & Optimization
Robotics
Image Recognition
Machine Vision
Vision
Artificial Intelligence (AI)


Artificial Intelligence
Any technique that enables computers to mimic human intelligence, using logic, if-then rules, decision trees, and machine learning (including deep learning)
Machine Learning
A subset of AI that includes abstruse statistical techniques that enable machines to improve at tasks with experience. The category includes deep learning
Deep Learning
The subset of machine learning composed of algorithms that permit software to train itself to perform tasks, like speech and image recognition, by exposing multilayered neural networks to vast amounts of data.

Machine Learning

Using data to answer question

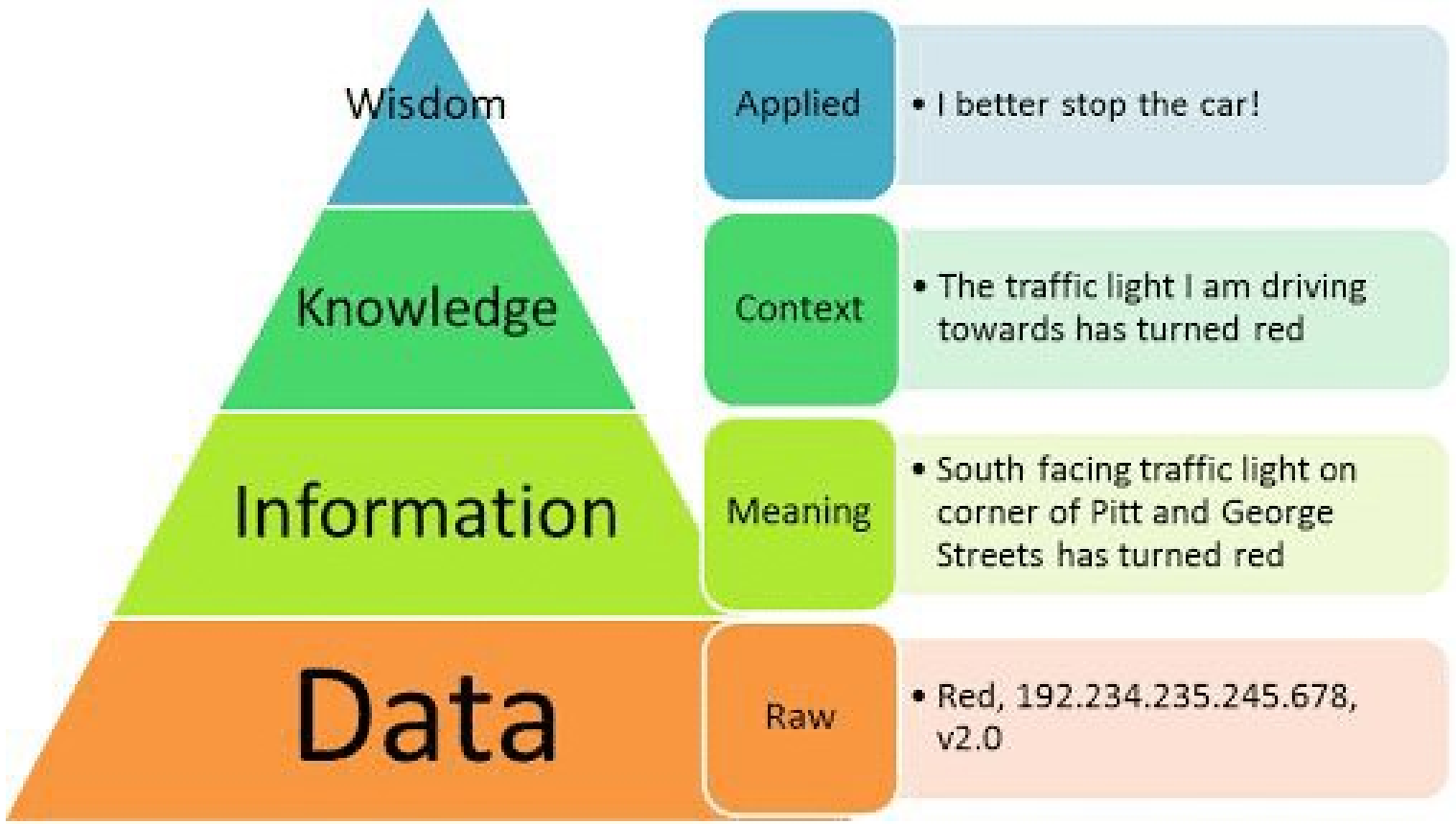




Source: https://techgrabyte.com/10-machine-learning-algorithms-application/

Why AI/ML in Cybersecurity?

- MORE AND MORE THREATS AND MORE COMPLEX ONES
- THE ATTACK SURFACE FOR MANY COMPANIES IS INCREASING
  - **public clouds**
- THE HUMAN BRAIN CANNOT PROCESS SO MUCH DATA
  - **Data vs Information vs Knowledge**



Source: https://www.researchgate.net/publication/323446419_Cervical_Cancer_Prediction_using_Data_Mining

Why AI/ML in cybersecurity?

- MORE AND MORE THREATS AND MORE COMPLEX ONES
- THE ATTACK SURFACE FOR MANY COMPANIES IS INCREASING
  - **public clouds**
- THE HUMAN BRAIN CANNOT PROCESS SO MUCH DATA
  - **Data vs Information vs Knowledge**
- LACK OF QUALIFIED CYBERSECURITY PROFESSIONALS
  - **1.5 Millions missing in 2020. estimate from Global Information Security Workforce Study**


Hey, COACH! WAS it "KEEP YOUR HEAD UP, FEET APART AND eyes STRAIGHT AHEAD", OR "FEET UP, eYes APART AND HEAD ON STRAIGHT," OR...
OY! IF THE KID GETS OUT OF THIS ALIVE, iT'LL Be A MiRACLE!
CARTOONSTOCK .com
Search ID: bwhn1433

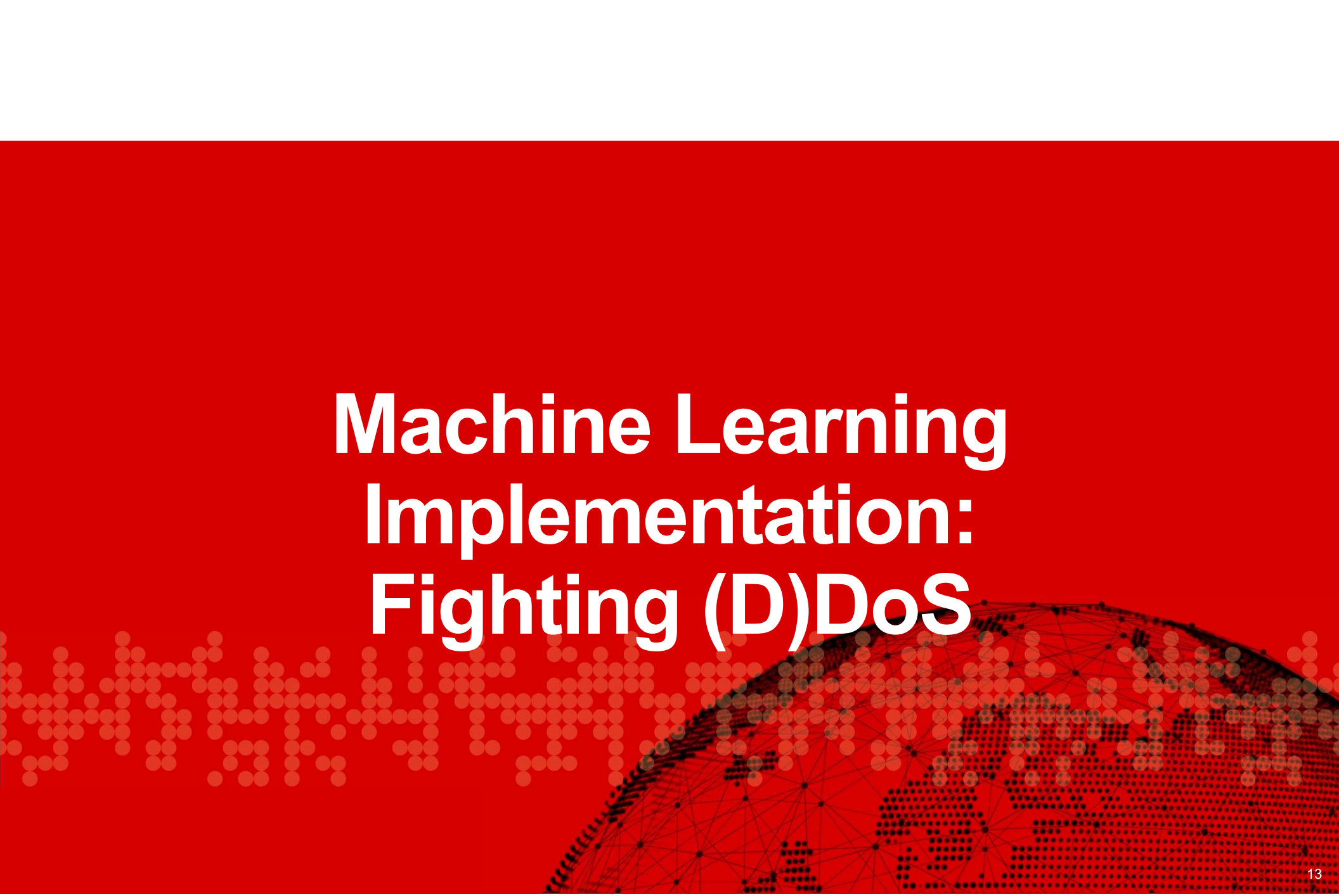
So, what can we do?

- IMPROVE OUR CAPABILITIES….

- THE HUMAN FACTOR
  - **Recruit more and include more diversity!**
  - **Use « Artificial Intelligence » for non human-related tasks**

- ON THE TECHNOLOGY SIDE
  - **Use Machine Learning to solve the most common tasks:**
    - **Regression, prediction and classification**
  - **Complement the traditionnal security solutions with ML**
    - **It works now and soon will be mandatory**

Machine Learning Implementation: Fighting (D)DoS



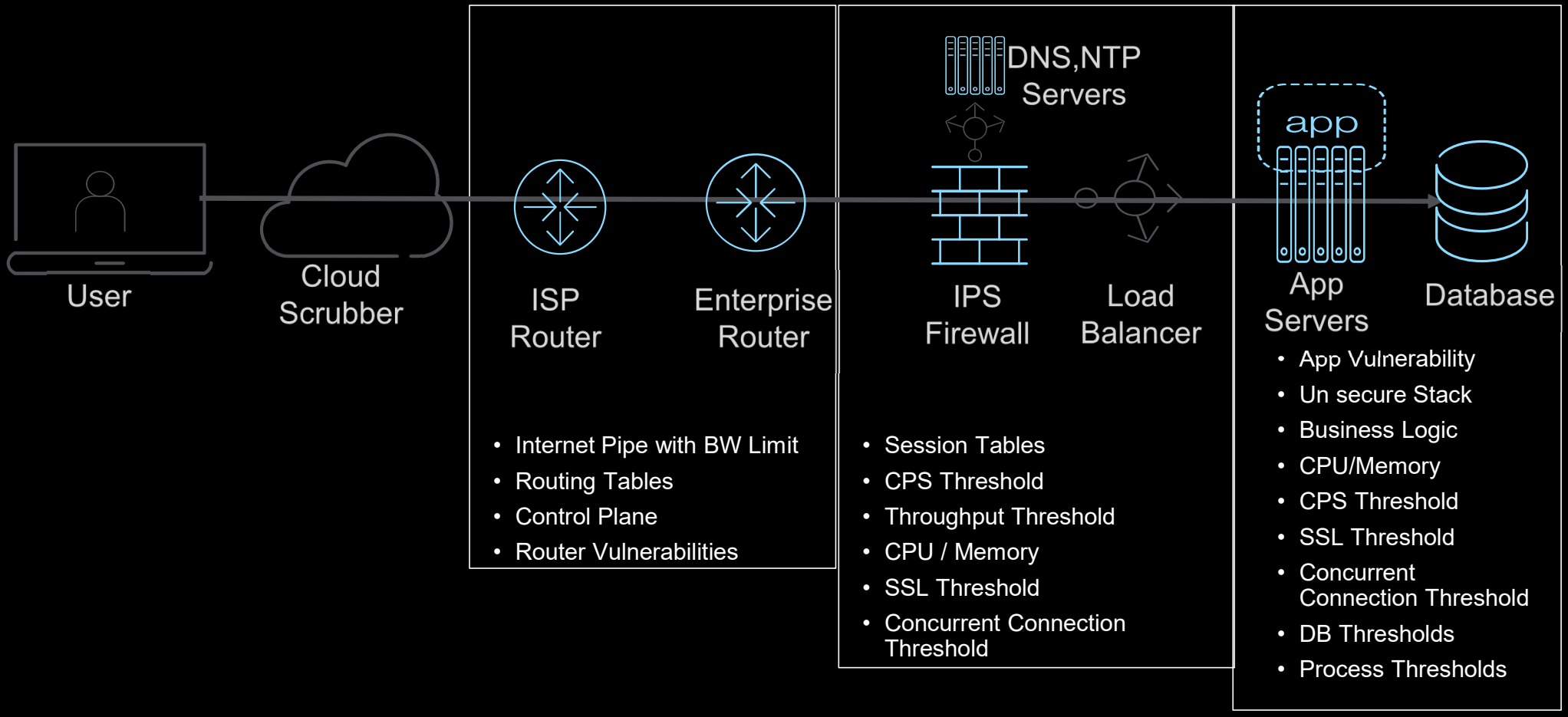
What is a (D)DoS?

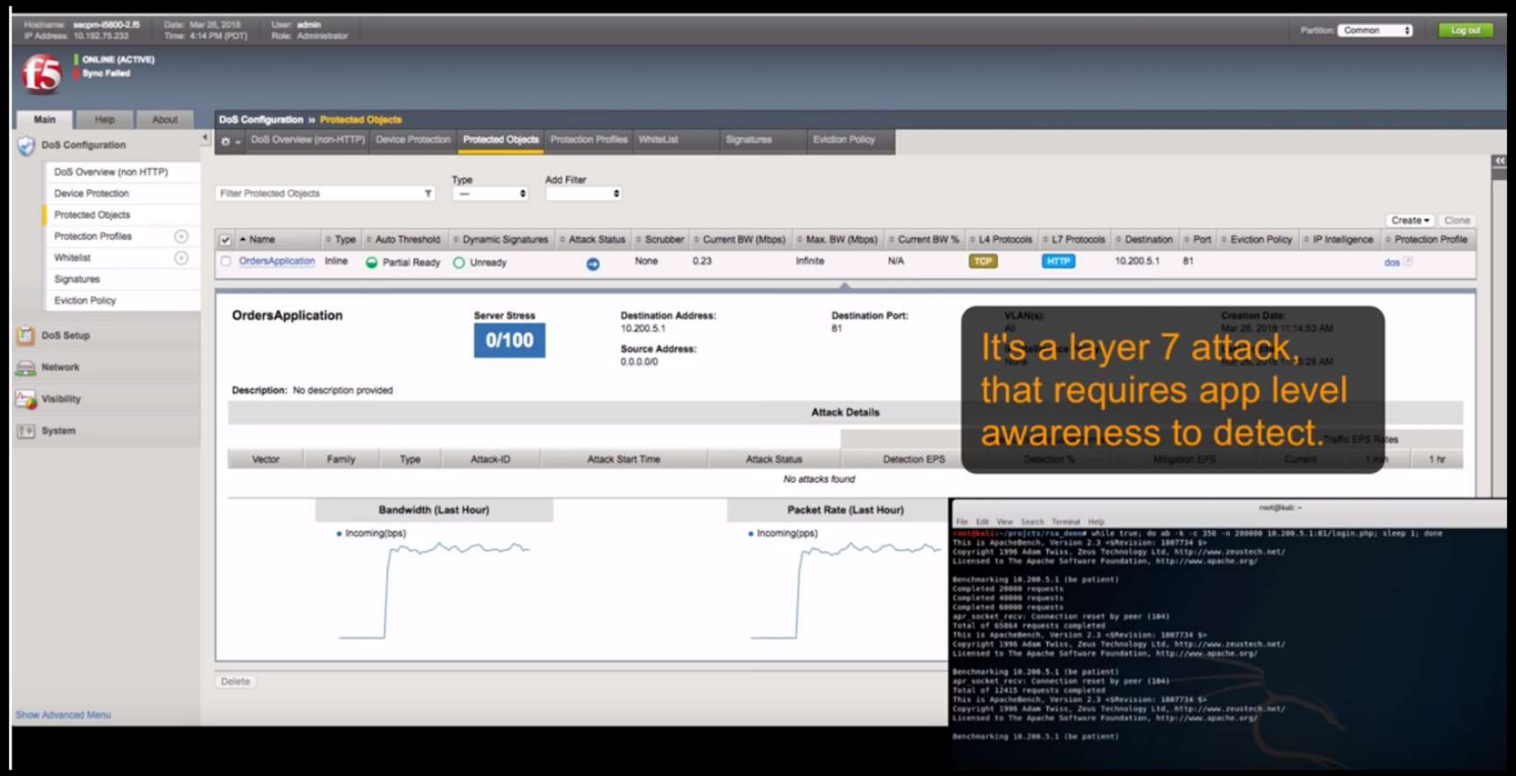

Volumetric Attacks


Known Attacks

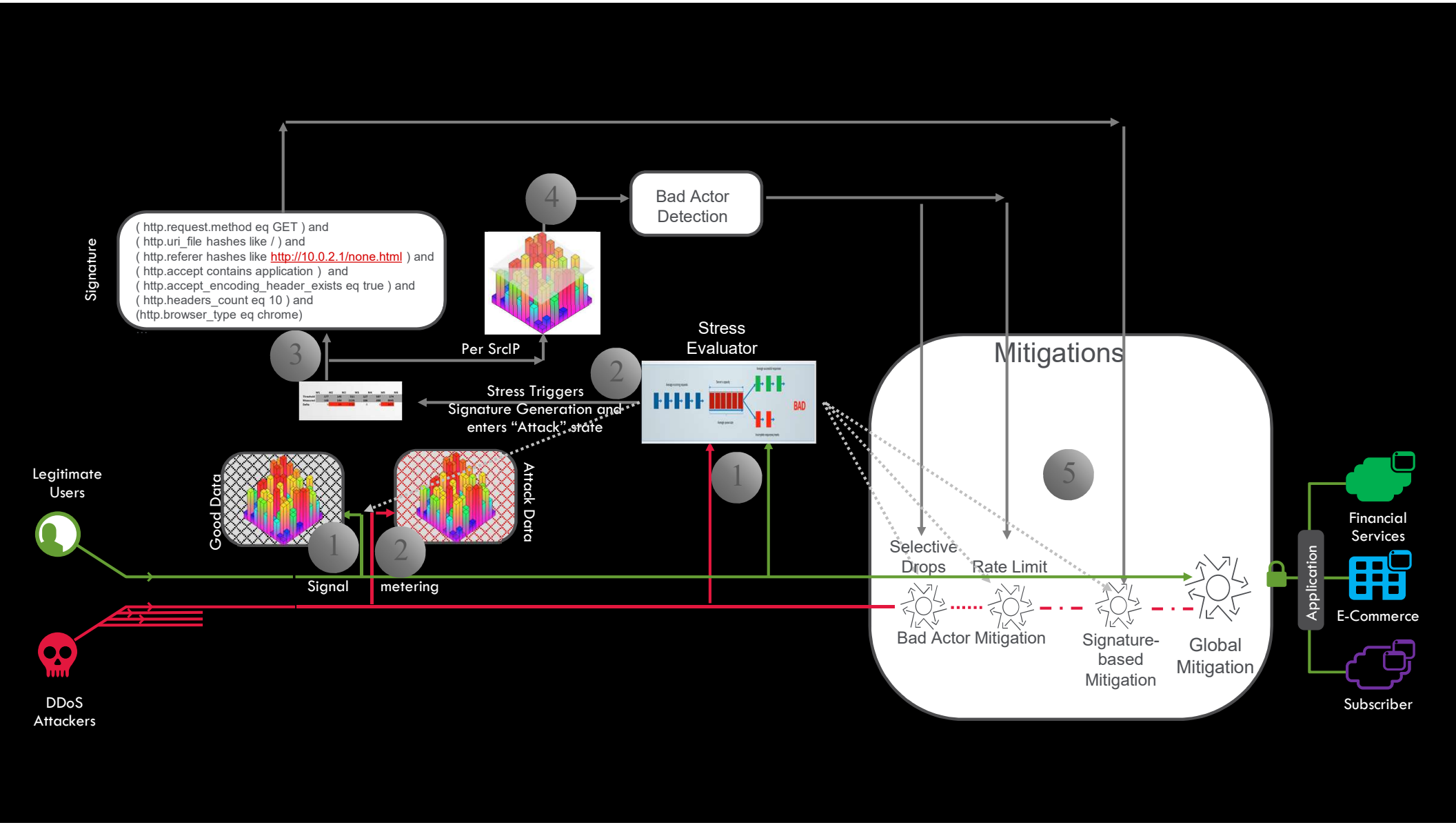

Invisible Attacks

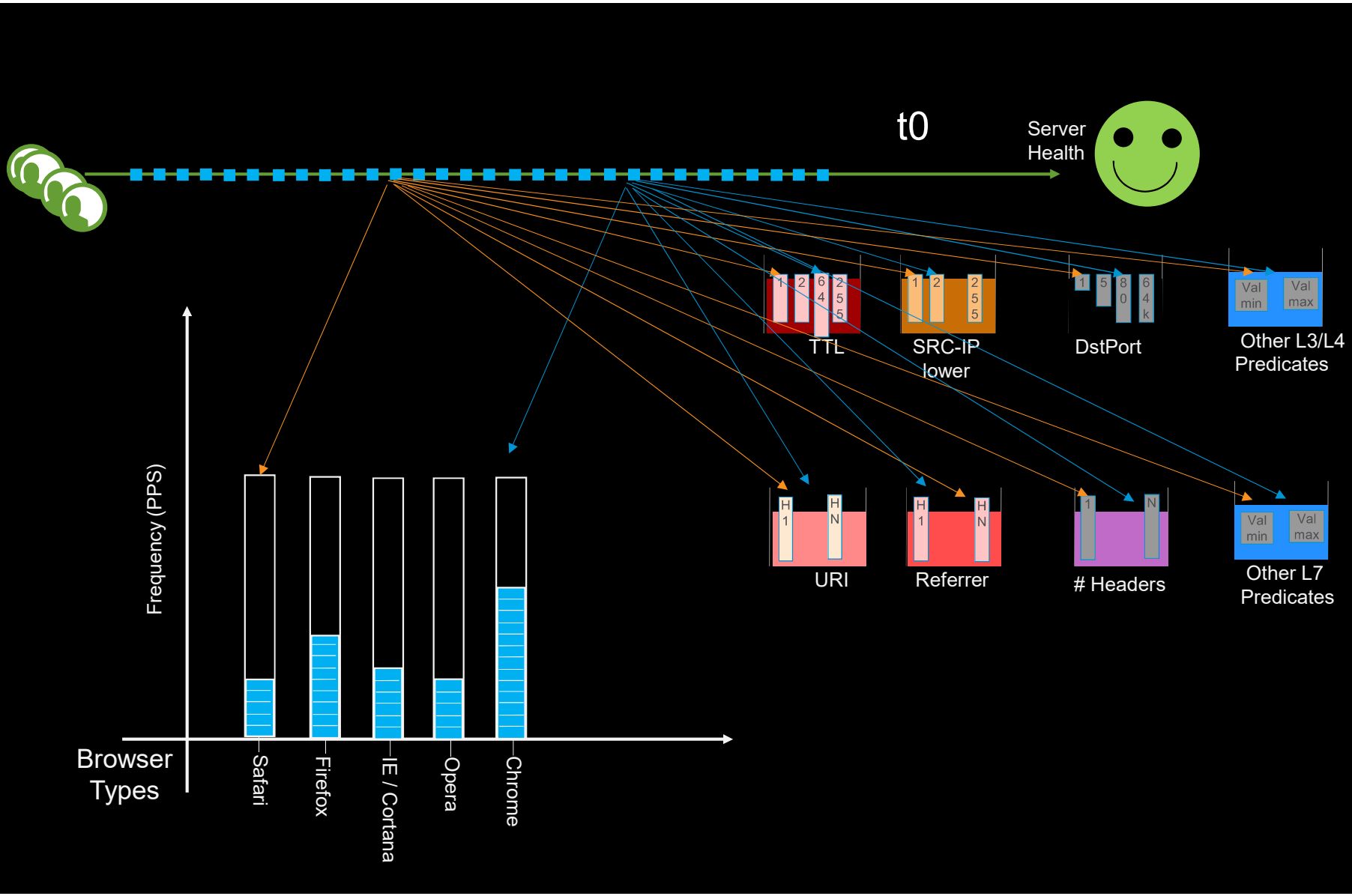
Each component has its limitation

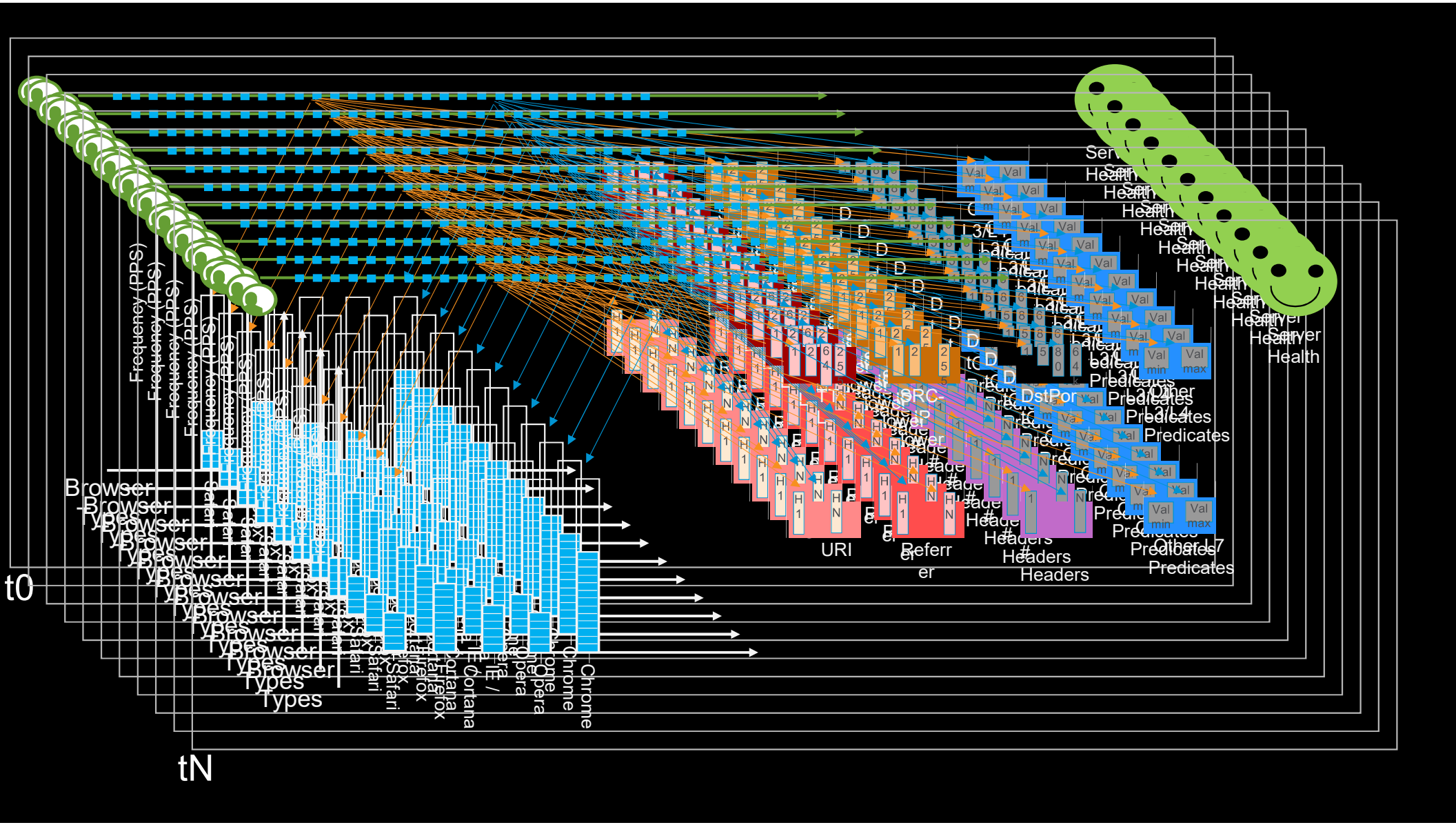


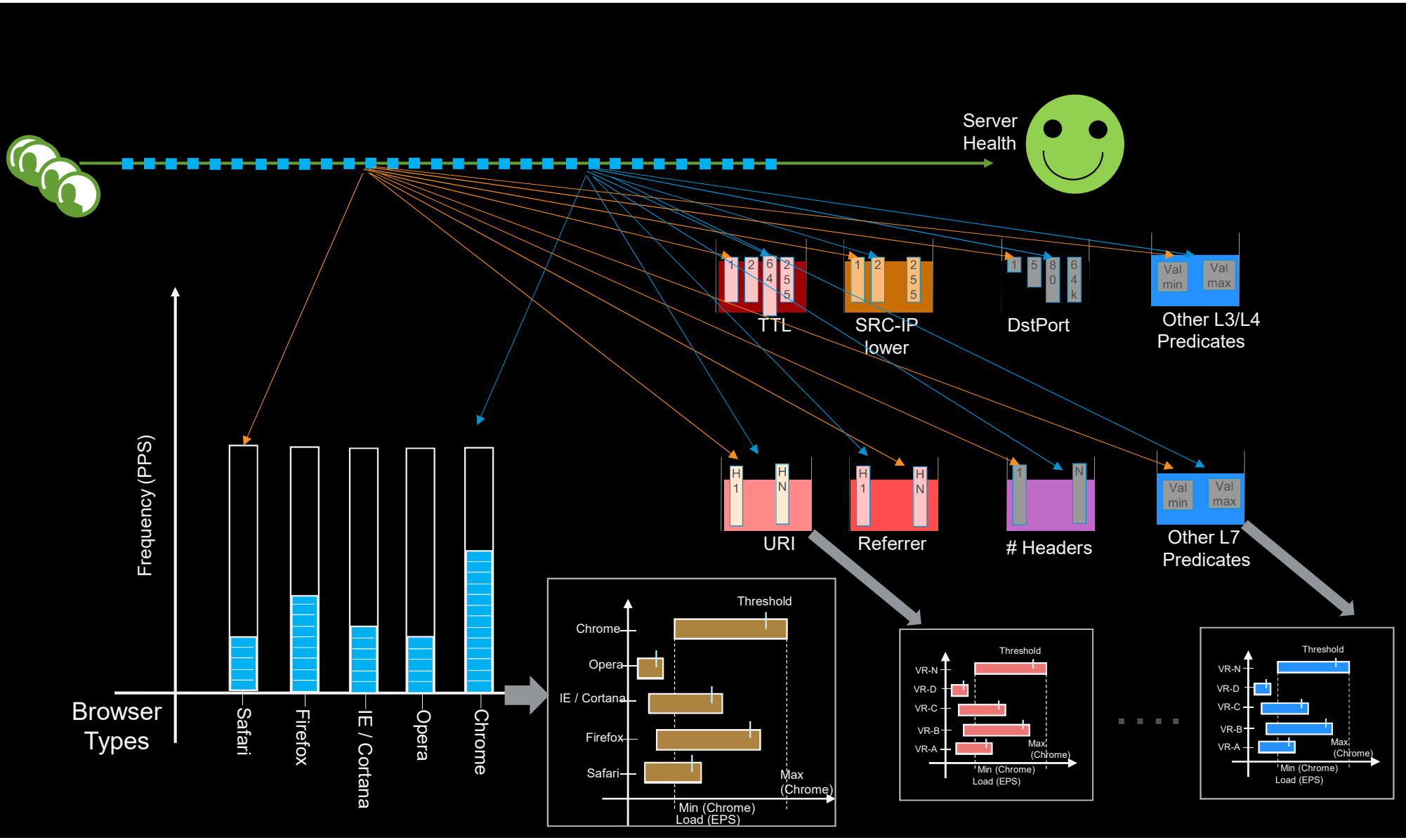


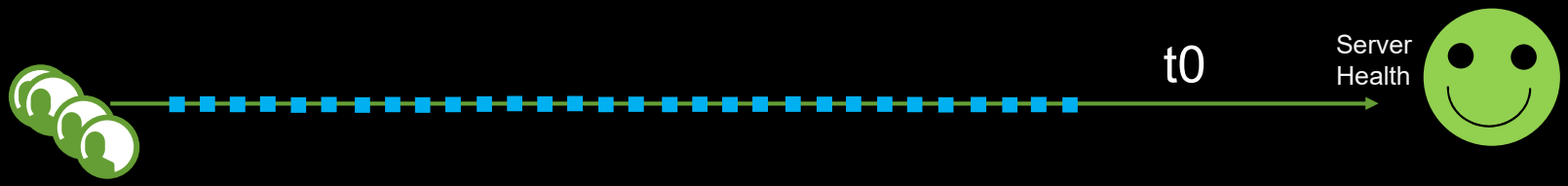
Demo video: https://www.youtube.com/watch?v=vw8NXSdS7L8

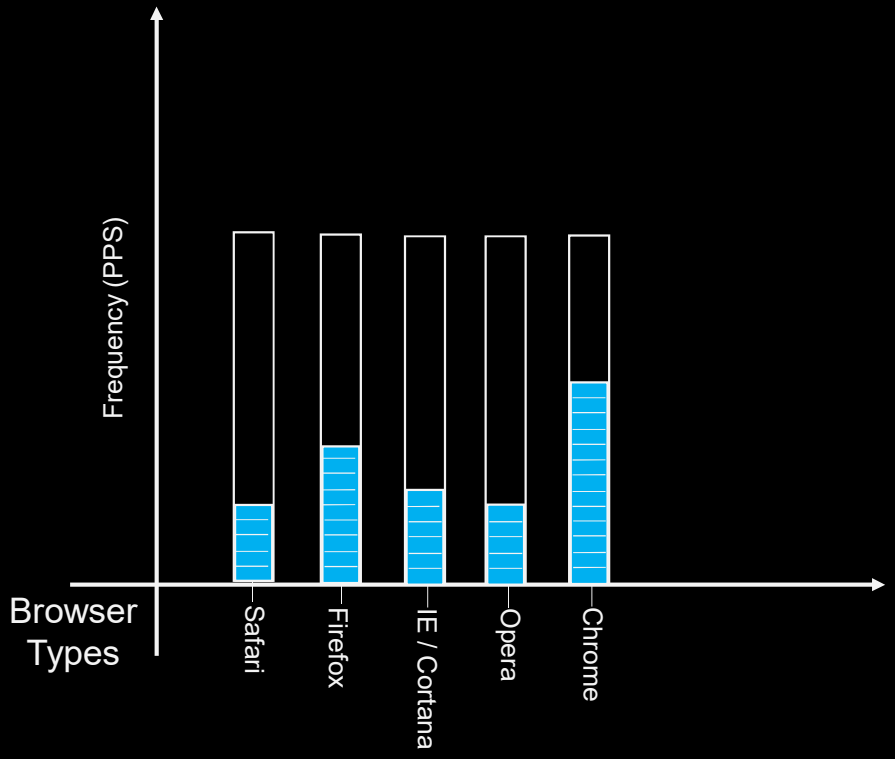

Signature
(http.request.method eq GET) and
(http.uri_file hashes like /) and
(http.referer hashes like http://10.0.2.1/none.html) and
(http.accept contains application) and
(http.accept_encoding_header_exists eq true) and
(http.headers_count eq 10) and
(http.browser_type eq chrome)
4
Bad Actor Detection
Per SrcIP
3
Stress Evaluator
2
Stress Triggers
Signature Generation and enters "Attack" state
BAD
Mitigations
5
1
Legitimate Users
Good Data
Attack Data
1
2
Signal
metering
Selective Drops
Rate Limit
Bad Actor Mitigation
Signature-based Mitigation
Global Mitigation
Application
Financial Services
E-Commerce
Subscriber
DDoS Attackers

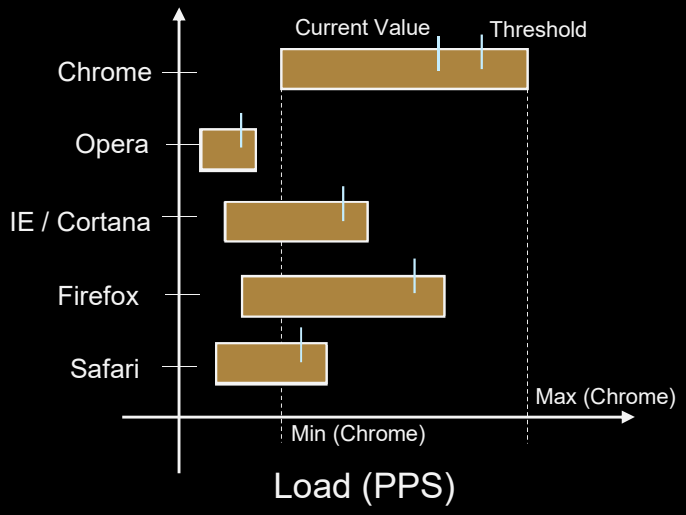

t0
Server Health
1
2
64
255
TTL
1
2
255
SRC-IP lower
1
5
80
64k
DstPort
Val min
Val max
Other L3/L4 Predicates
H 1
H N
URI
H 1
H N
Referrer
1
N
Headers
Val min
Val max
Other L7 Predicates
Frequency (PPS)
Browser Types
Safari
Firefox
IE / Cortana
Opera
Chrome

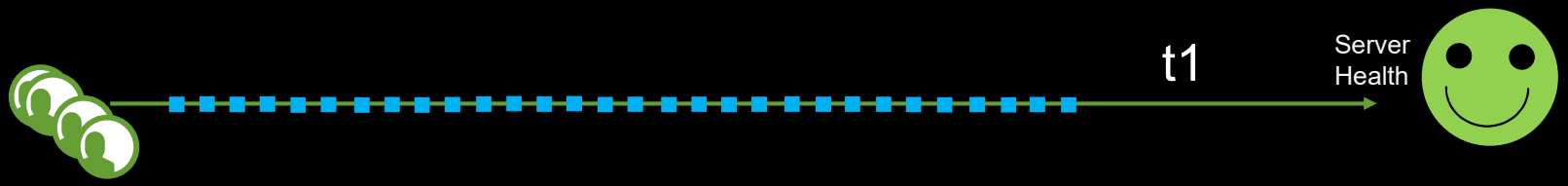

t0
tN
Frequency (PPS)
Browser
Types
Chrome
Cortana
Opera
Safari
Firefox
URI
Referrer
Headers
Predicates
DstPor
SRC-

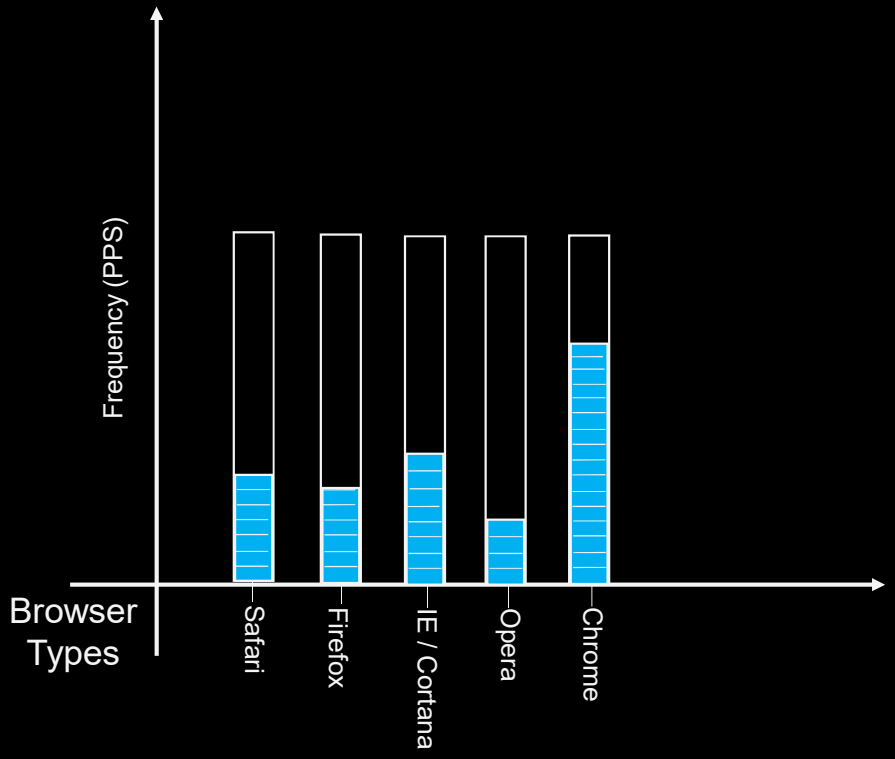

Server Health
TTL
SRC-IP lower
DstPort
Other L3/L4 Predicates
Val min
Val max
URI
Referrer
Headers
Other L7 Predicates
Frequency (PPS)
Browser Types
Safari
Firefox
IE / Cortana
Opera
Chrome
Threshold
Max (Chrome)
Min (Chrome) Load (EPS)
VR-N
VR-D
VR-C
VR-B
VR-A

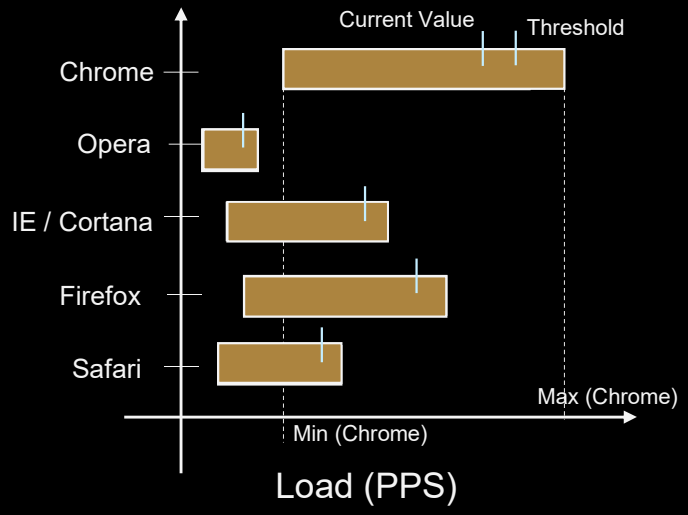

t0
Server
Health

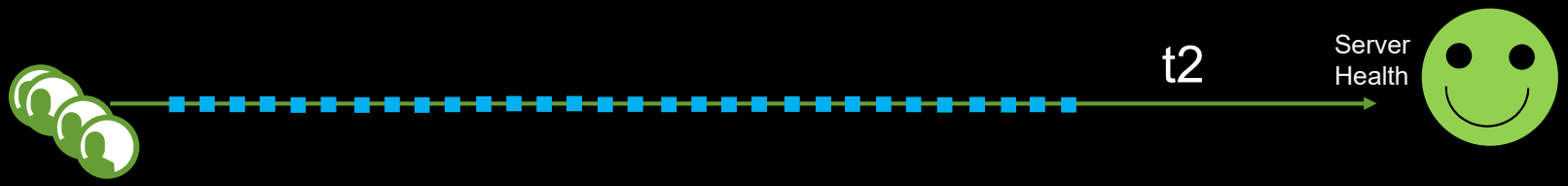

Frequency (PPS)
Browser
Types
Safari
Firefox
IE / Cortana
Opera
Chrome

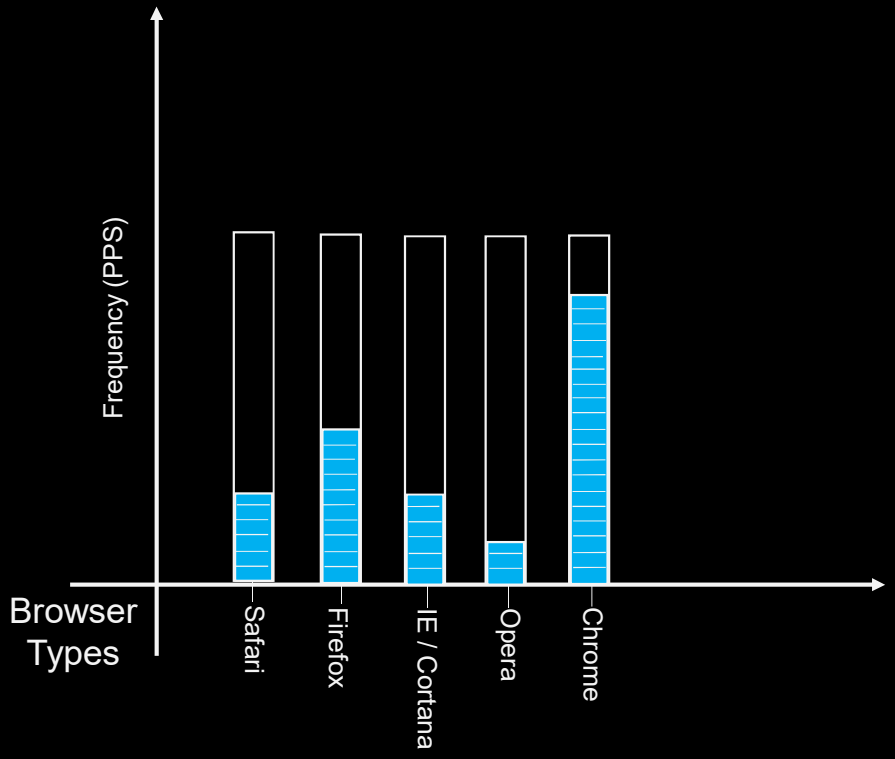

Current Value
Threshold
Chrome
Opera
IE / Cortana
Firefox
Safari
Max (Chrome)
Min (Chrome)
Load (PPS)

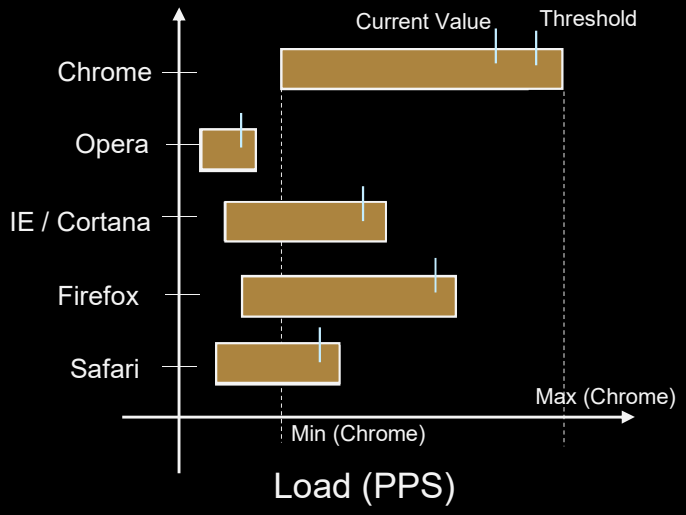

t1
Server
Health

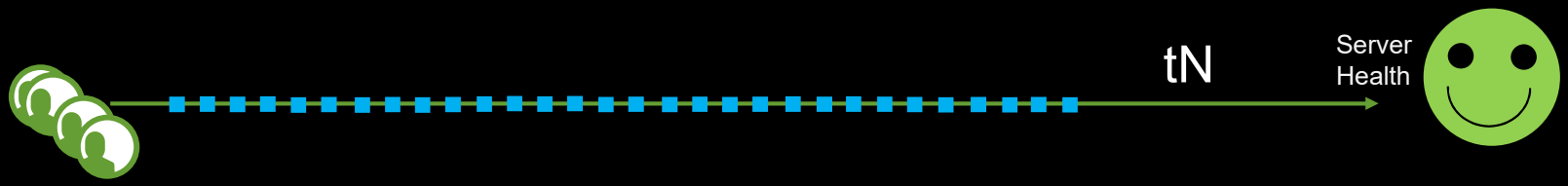

Frequency (PPS)
Browser
Types
Safari
Firefox
IE / Cortana
Opera
Chrome

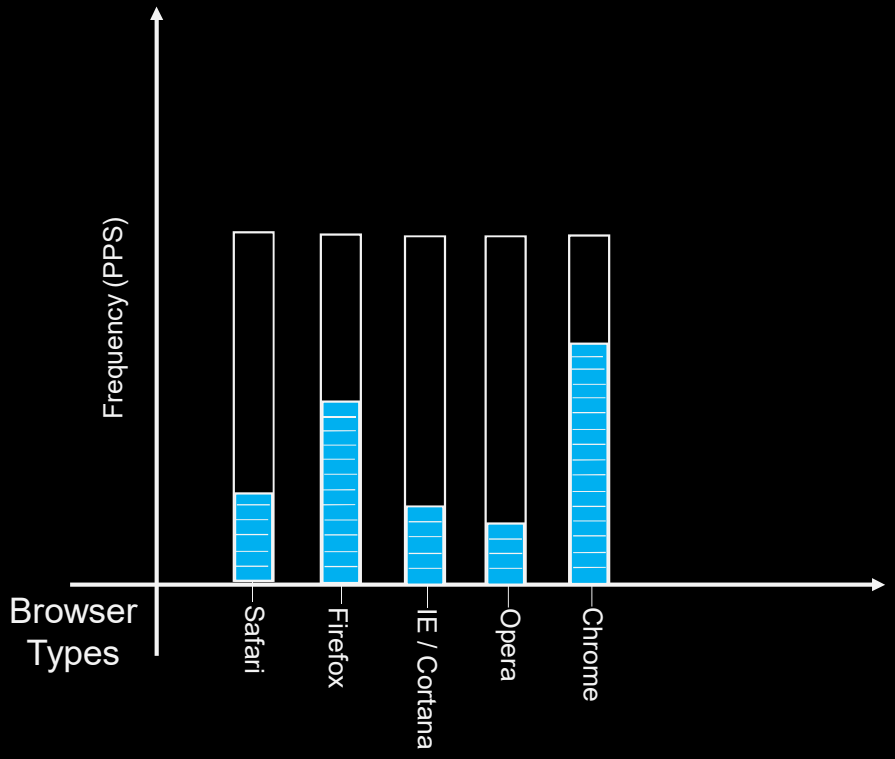

Current Value
Threshold
Chrome
Opera
IE / Cortana
Firefox
Safari
Max (Chrome)
Min (Chrome)
Load (PPS)

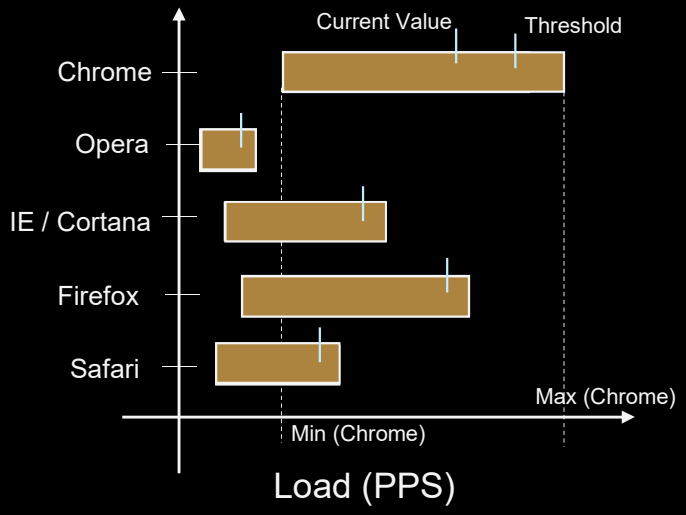

t2
Server
Health


Frequency (PPS)
Browser
Types
Safari
Firefox
IE / Cortana
Opera
Chrome


Current Value
Threshold
Chrome
Opera
IE / Cortana
Firefox
Safari
Max (Chrome)
Min (Chrome)
Load (PPS)


tN
Server
Health


Frequency (PPS)
Browser
Types
Safari
Firefox
IE / Cortana
Opera
Chrome


Current Value
Threshold
Chrome
Opera
IE / Cortana
Firefox
Safari
Max (Chrome)
Min (Chrome)
Load (PPS)

Best predictive indicator for denial of service is …

Stress on the service

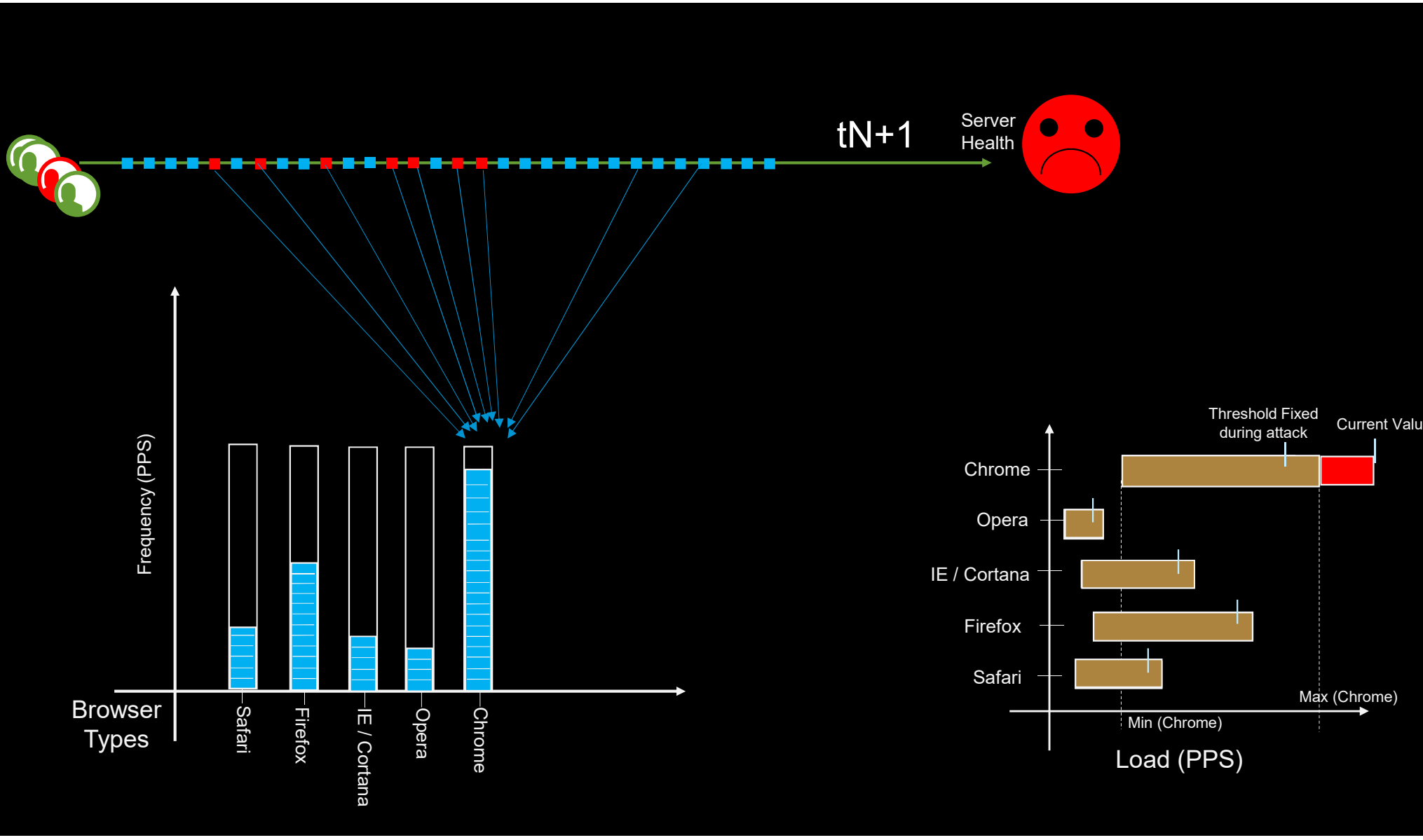
Stress != Attack

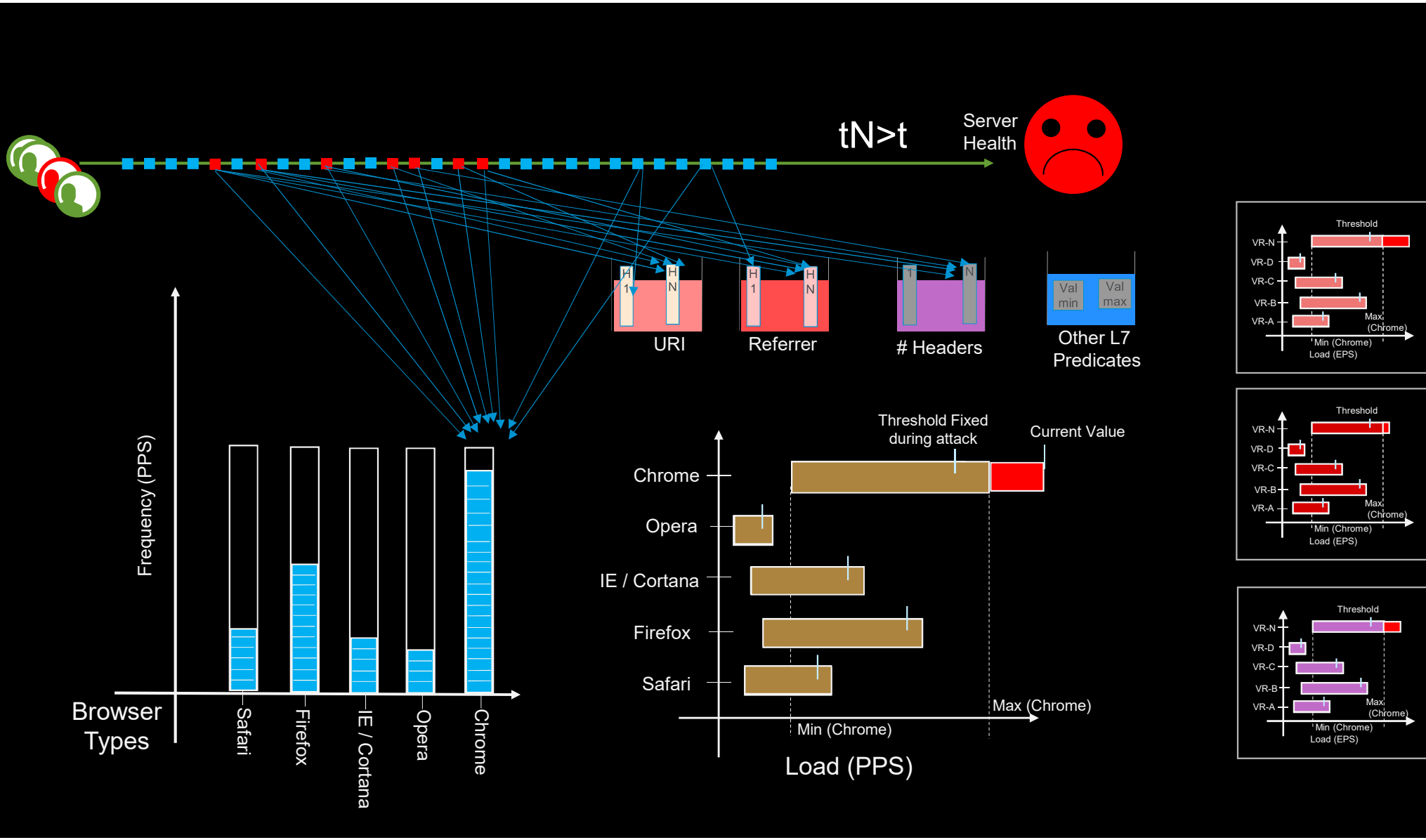
Stress = Bad User Experience

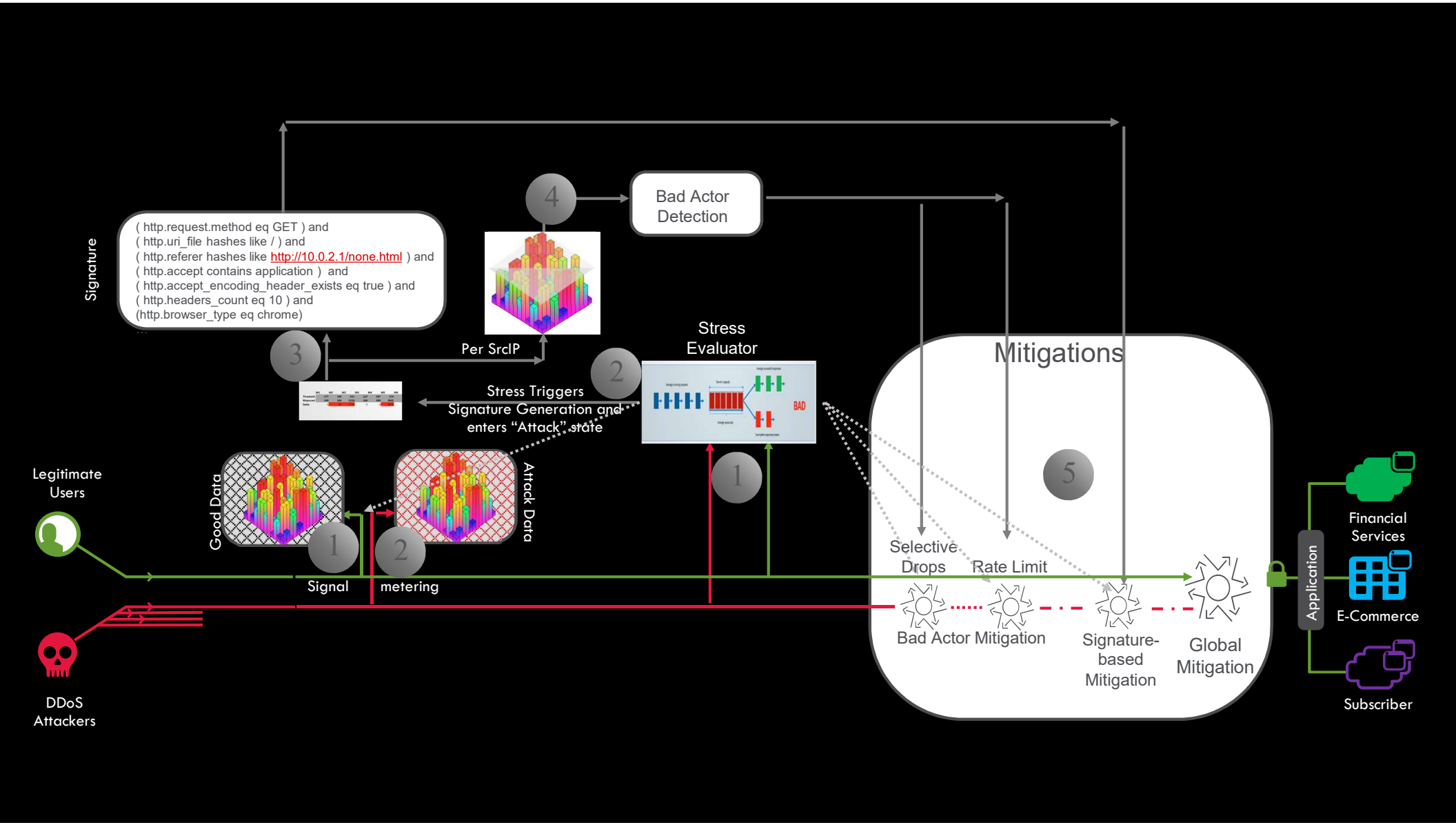
Stress = DoS

Opposite of DoS = Availability of Service

Our Spirit: Fight to the death to keep service alive for legitimate users!


tN+1
Server
Health
Frequency (PPS)
Browser
Types
Safari
Firefox
IE / Cortana
Opera
Chrome
Threshold Fixed
during attack
Current Value
Chrome
Opera
IE / Cortana
Firefox
Safari
Max (Chrome)
Min (Chrome)
Load (PPS)


tN>t
Server Health
URI
Referrer
Headers
Other L7 Predicates
Val min
Val max
Frequency (PPS)
Browser Types
Safari
Firefox
IE / Cortana
Opera
Chrome
Threshold Fixed during attack
Current Value
Min (Chrome)
Max (Chrome)
Load (PPS)
Threshold
VR-N
VR-D
VR-C
VR-B
VR-A
Max (Chrome)
Min (Chrome)
Load (EPS)


Signature
(http.request.method eq GET) and
(http.uri_file hashes like /) and
(http.referer hashes like http://10.0.2.1/none.html) and
(http.accept contains application) and
(http.accept_encoding_header_exists eq true) and
(http.headers_count eq 10) and
(http.browser_type eq chrome)
4
Bad Actor Detection
Per SrcIP
3
Stress Evaluator
2
Stress Triggers
Signature Generation and enters "Attack" state
BAD
Mitigations
5
1
Legitimate Users
Good Data
Attack Data
1
2
Signal
metering
Selective Drops
Rate Limit
Bad Actor Mitigation
Signature-based Mitigation
Global Mitigation
Application
Financial Services
E-Commerce
Subscriber
DDoS Attackers

What do you think?

RAISE YOUR HAND IF YOU THINK THAT THE DEMO I GAVE IS AN EXAMPLE OF UNSUPERVISED MACHINE LEARNING.

RAISE YOUR HAND IF YOU THINK THE DEMO I GAVE IS AN EXAMPLE OF SUPERVISED MACHINE LEARNING.

HOW MANY OF YOU THINK WE HAVE A COMBINATION OF BOTH?

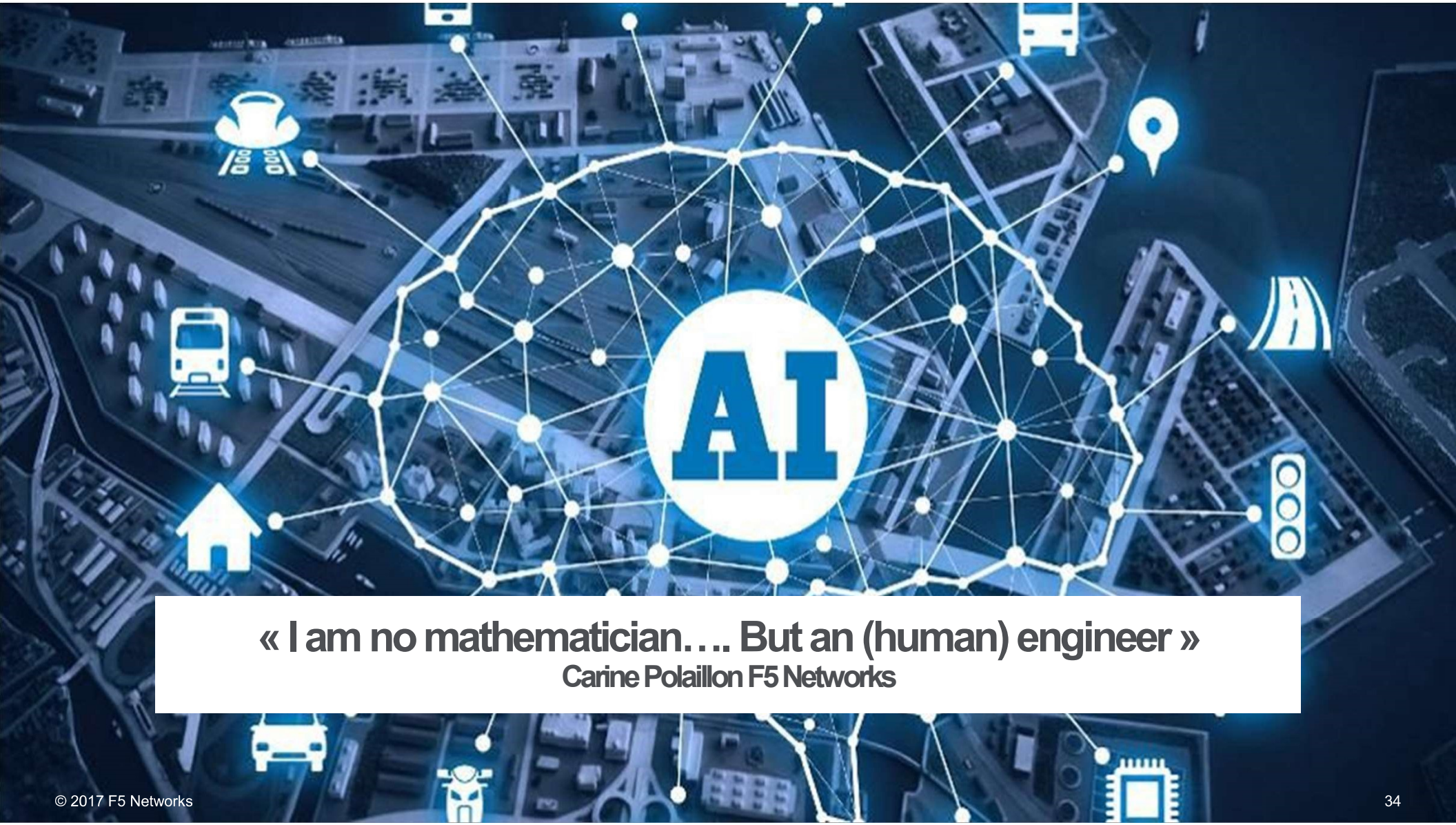
WHO THINKS THERE IS NO MACHINE LEARNING INVOLVED AT ALL?

What I think….

WE HAVE HERE 2 ALGORITHMS

The algorithm that does baseline is mostly an unsupervised statistical machine learning mechanism

There is a second algorithm that acts like a supervisor (but note, it is a machine learning algorithm and not a human) during attack time, and does not interact with the first algorithm during peace time.



« I am no mathematician…. But an (human) engineer »

Carine Polaillon F5 Networks