corley

HACK IN BO
Spring 2023 Edition
20ª EDIZIONE

Anomaly Detection and IP Insights

#HIB23

HACK IN BO
Spring 2023 Edition
20ª EDIZIONE

Alessandra Bilardi

Data & Automation Specialist

aws certified Database SPECIALTY
aws certified Machine Learning SPECIALTY

alessandra.bilardi@corley.it
@abilardi
bilardi

corley

aws partner network
Advanced Consulting Partner

SUMMARY

Web Application Security Risks

Our Best Friends

Monitoring with Machine Learning

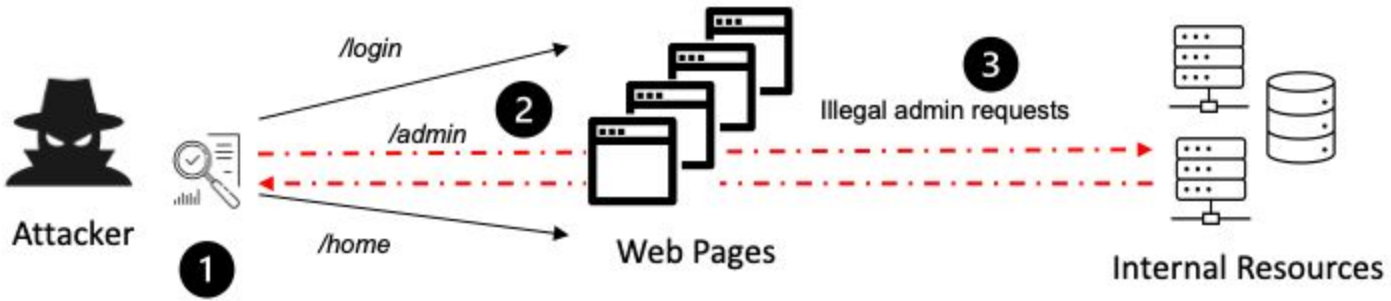
Web Application Security Risks

OWASP Top 10

1. Broken access control
2. Cryptographic failures
3. Injection
4. Insicure design
5. Security misconfiguration
6. Vulnerable and outdated components
7. Identification and authentication failures
8. Software and data integrity failures
9. Security logging and monitoring failures
10. Server-side request forgery

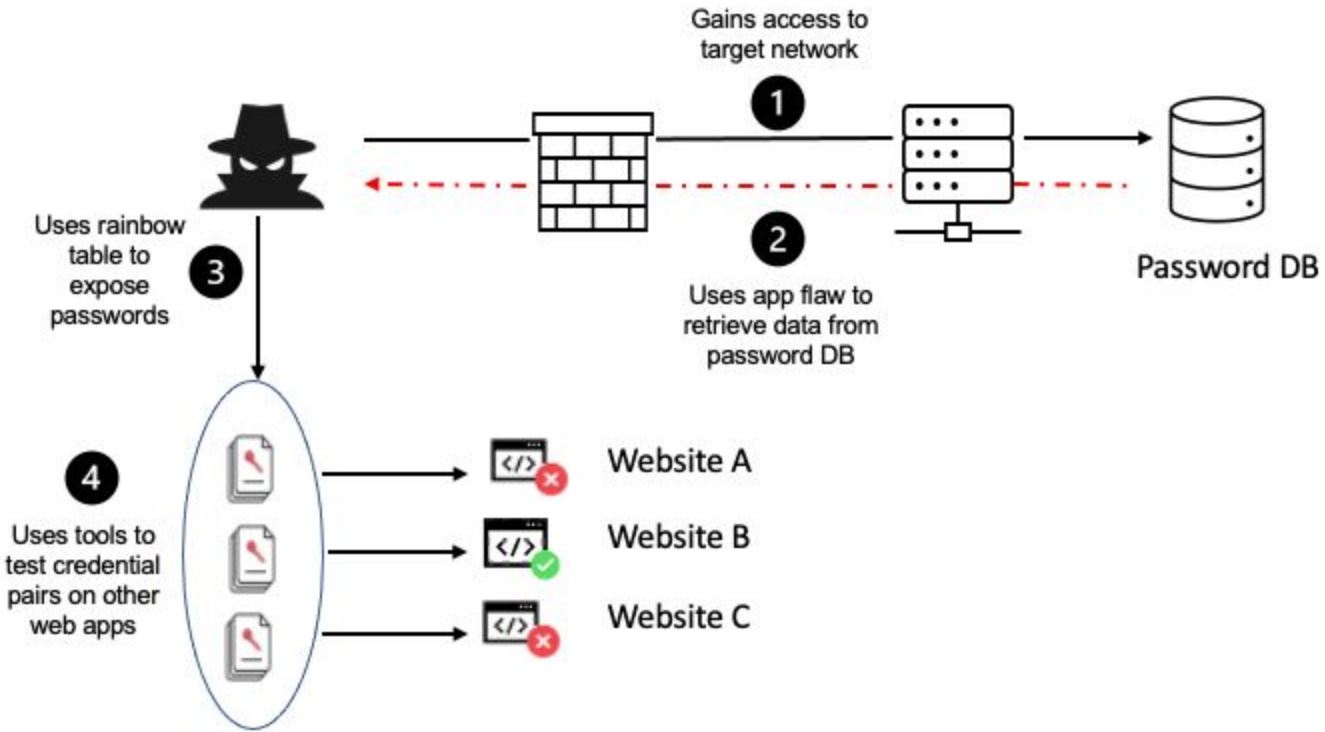
https://owasp.org/Top10/

Web Application Security Risks



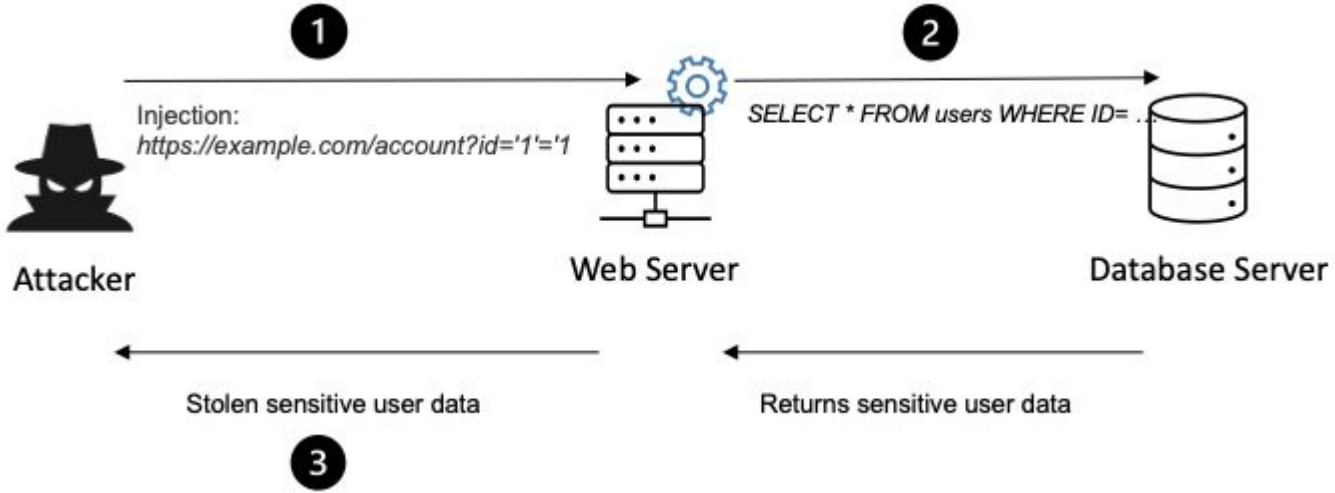
https://my.f5.com/manage/s/article/K45215395

Web Application Security Risks



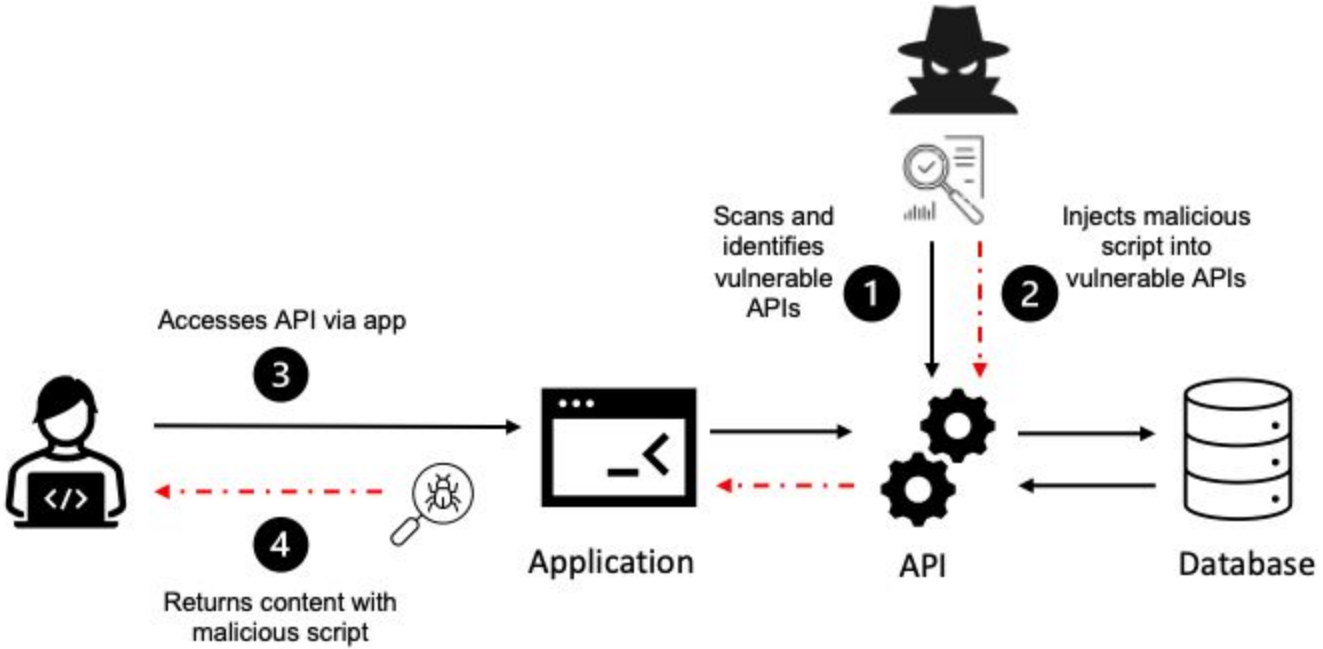
https://my.f5.com/manage/s/article/K45215395

Web Application Security Risks



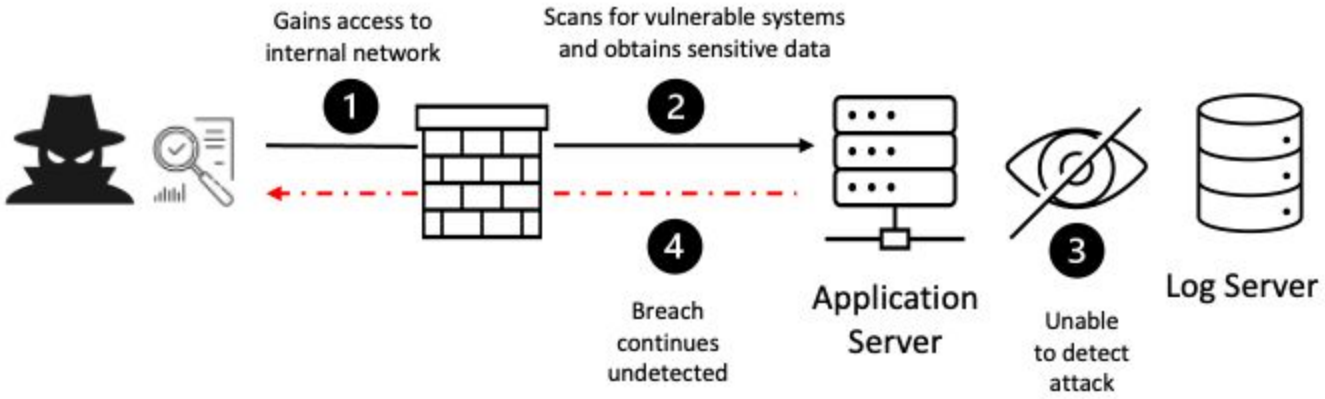
https://my.f5.com/manage/s/article/K45215395

Web Application Security Risks



https://my.f5.com/manage/s/article/K45215395

Web Application Security Risks

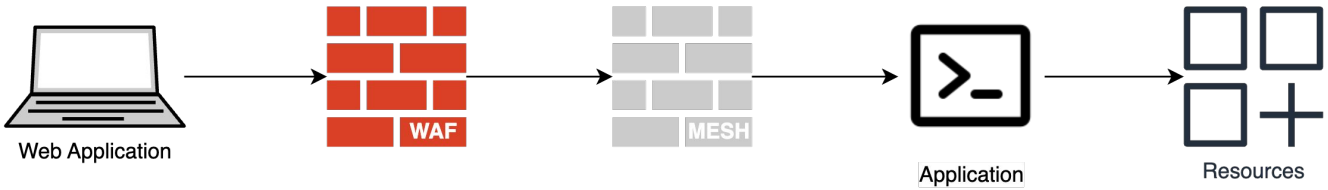


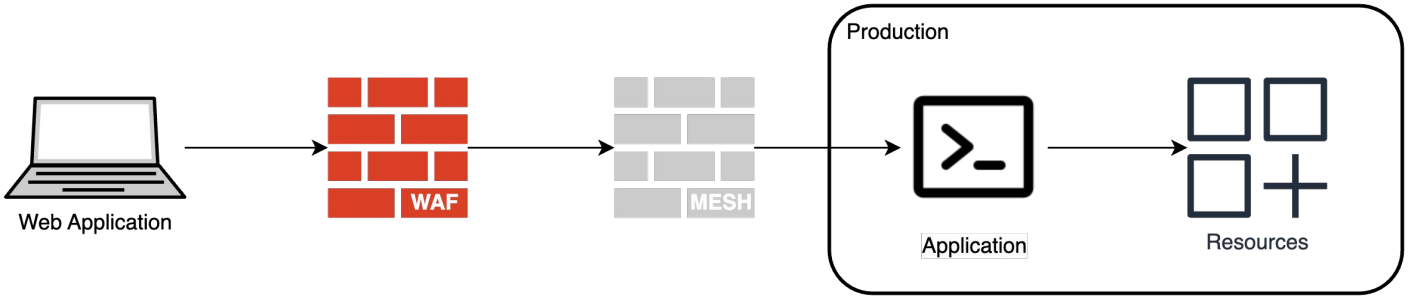
https://my.f5.com/manage/s/article/K45215395

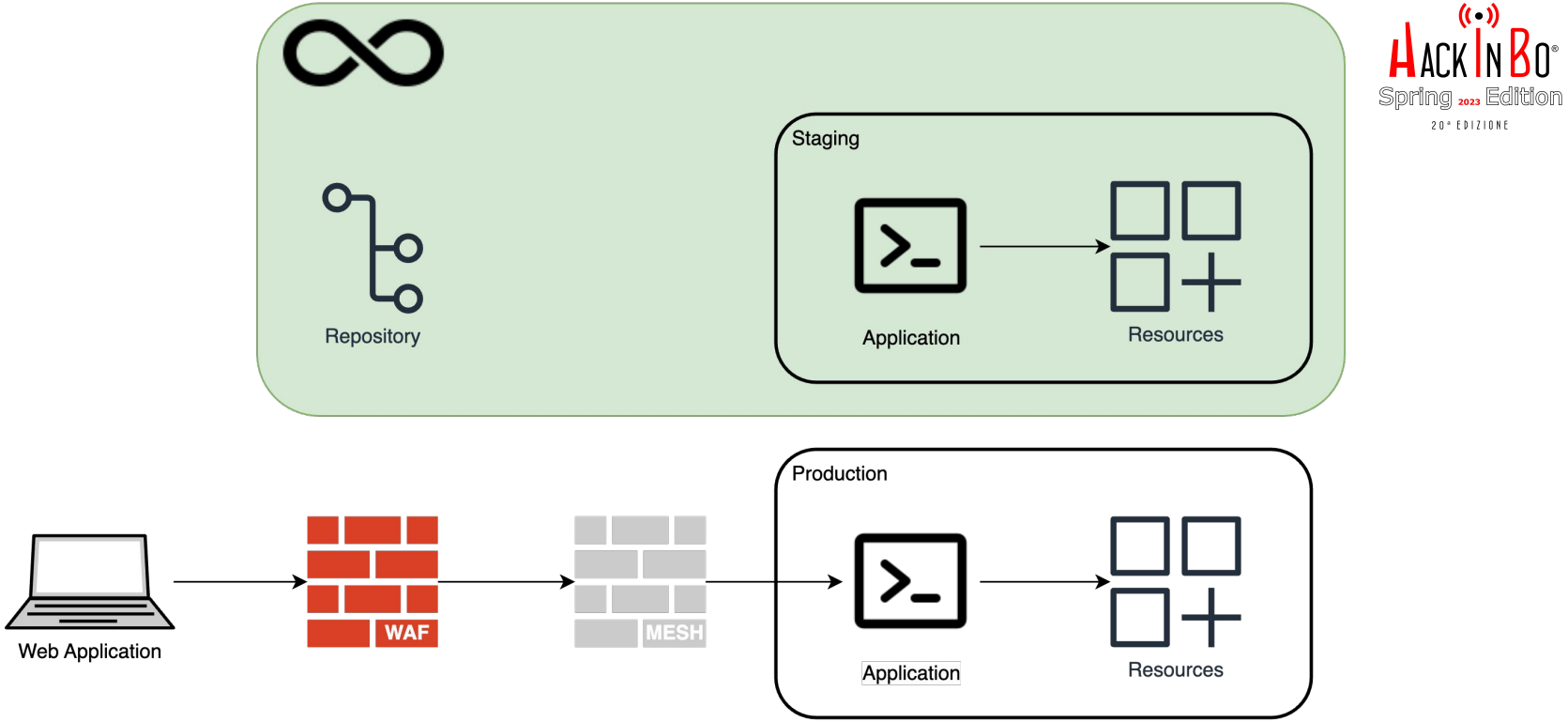
Our Best Friends

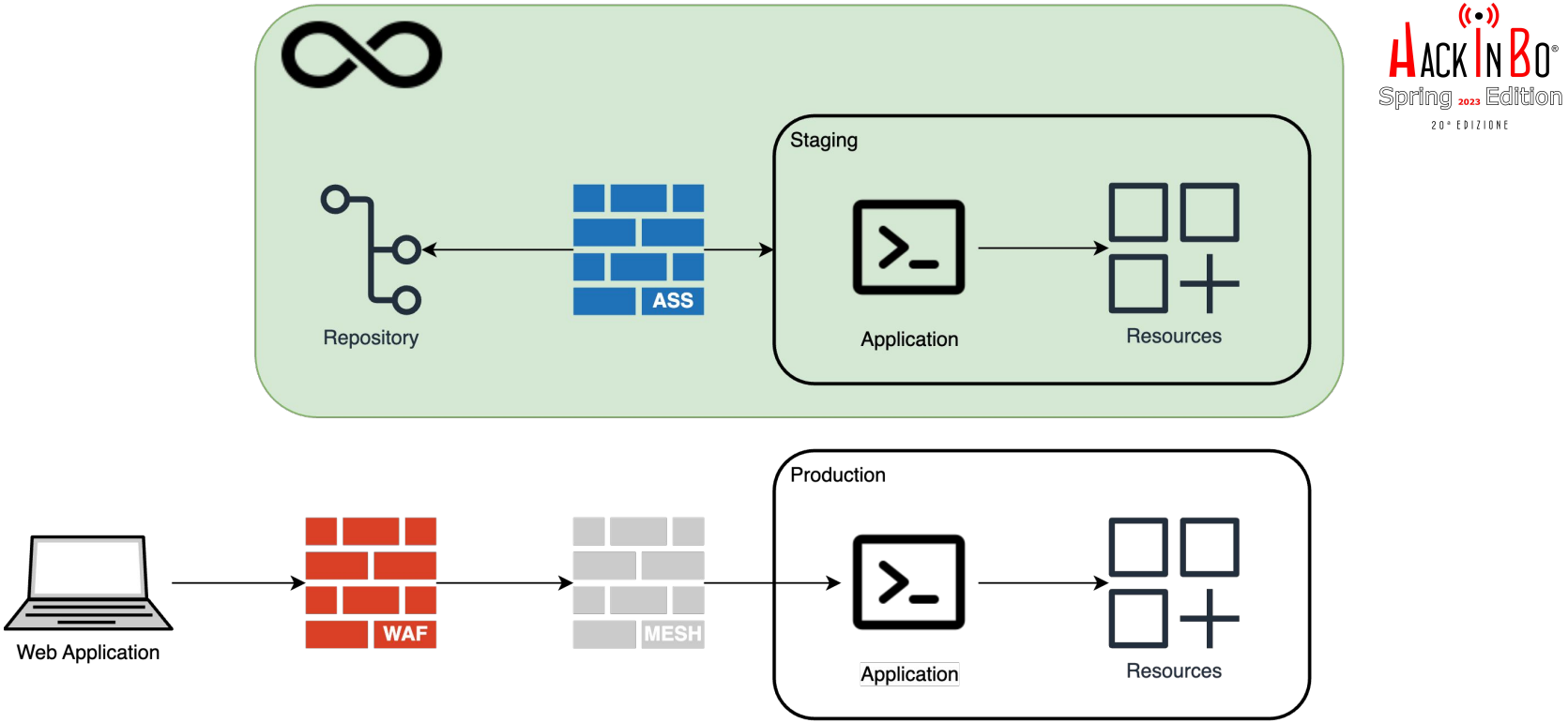

Web Application
Application
Resources

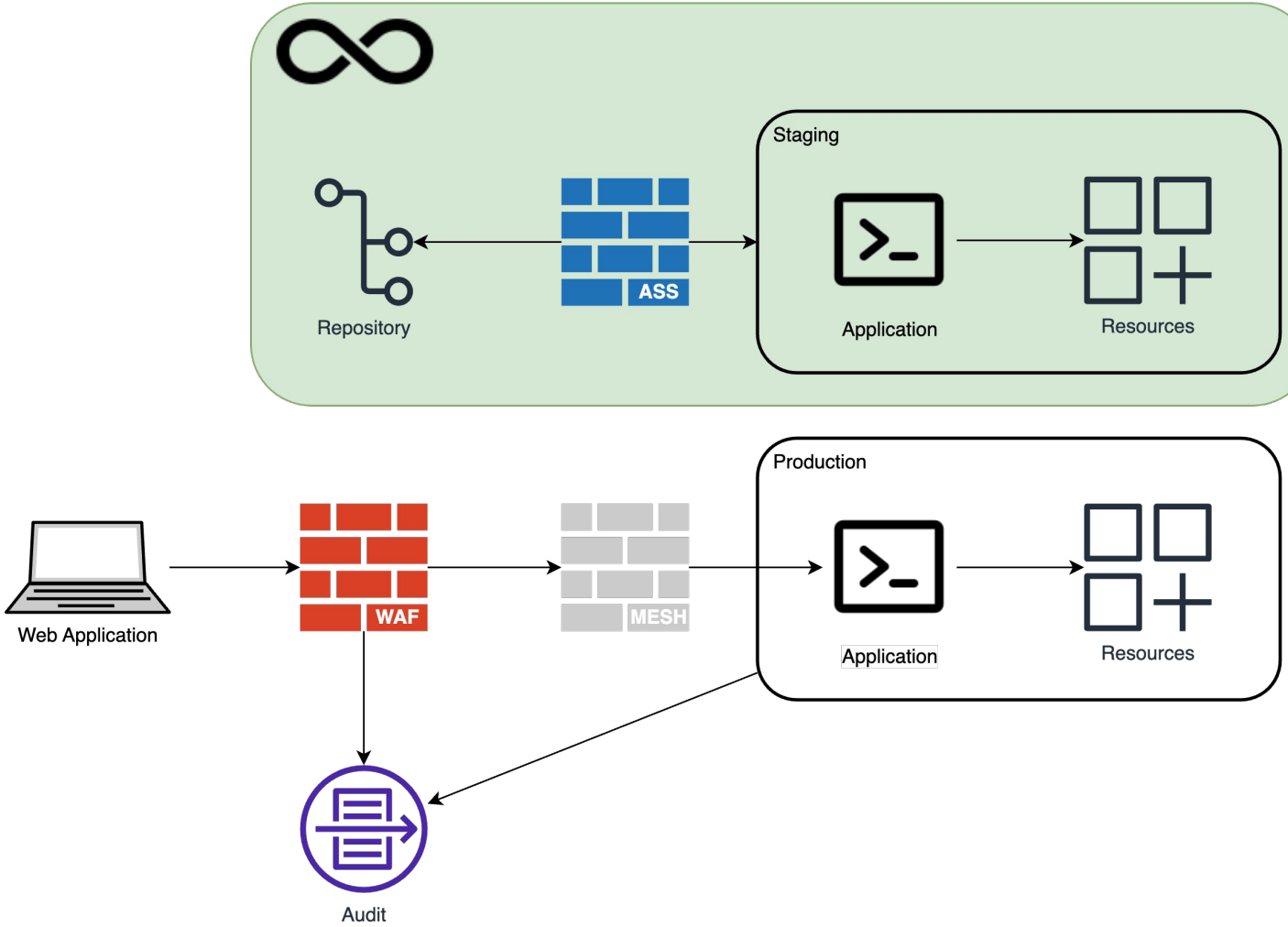

Web Application
WAF
Application
Resources

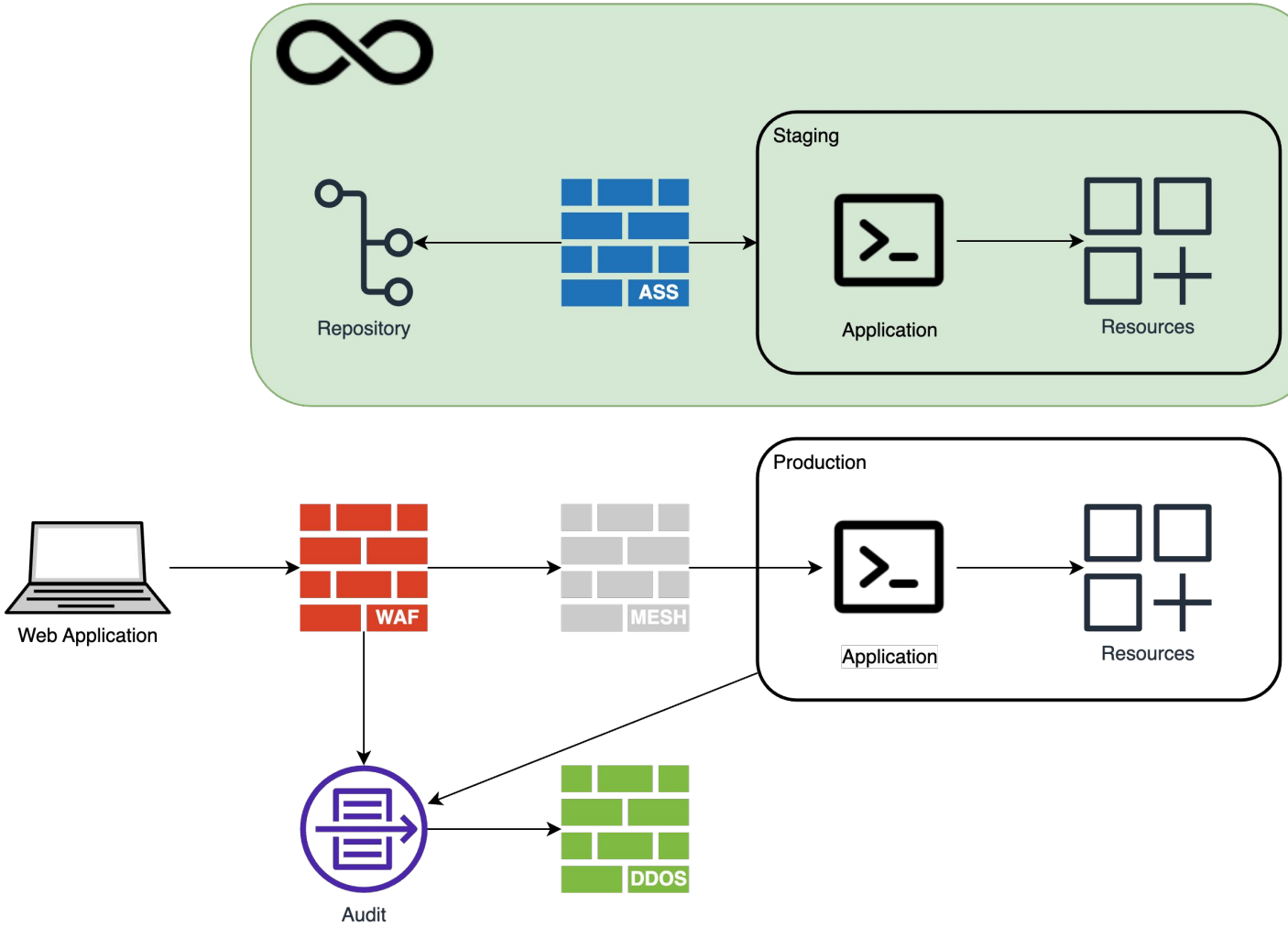

Web Application
WAF
MESH
Application
Resources

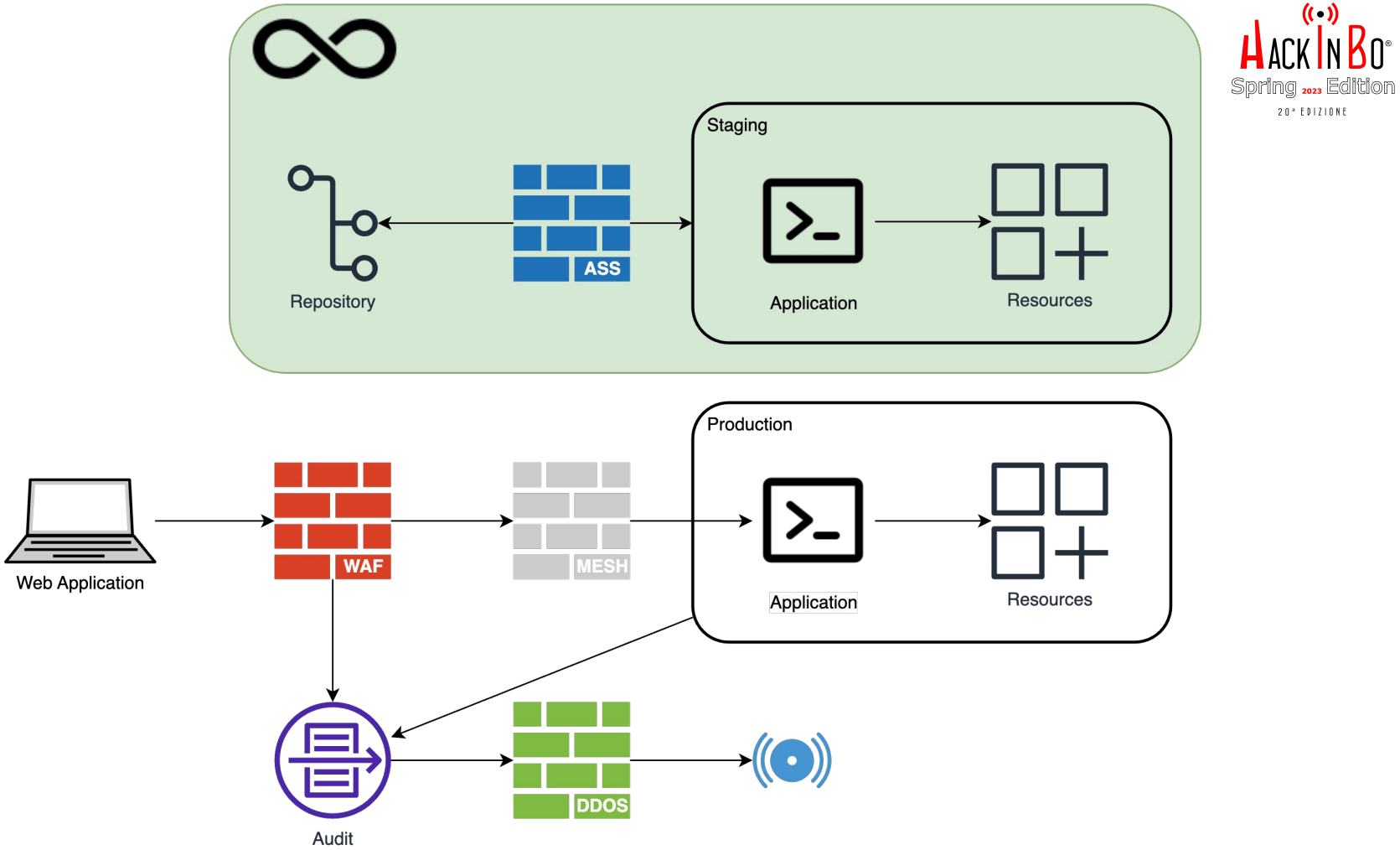

Production
WAF
MESH
Web Application
Application
Resources

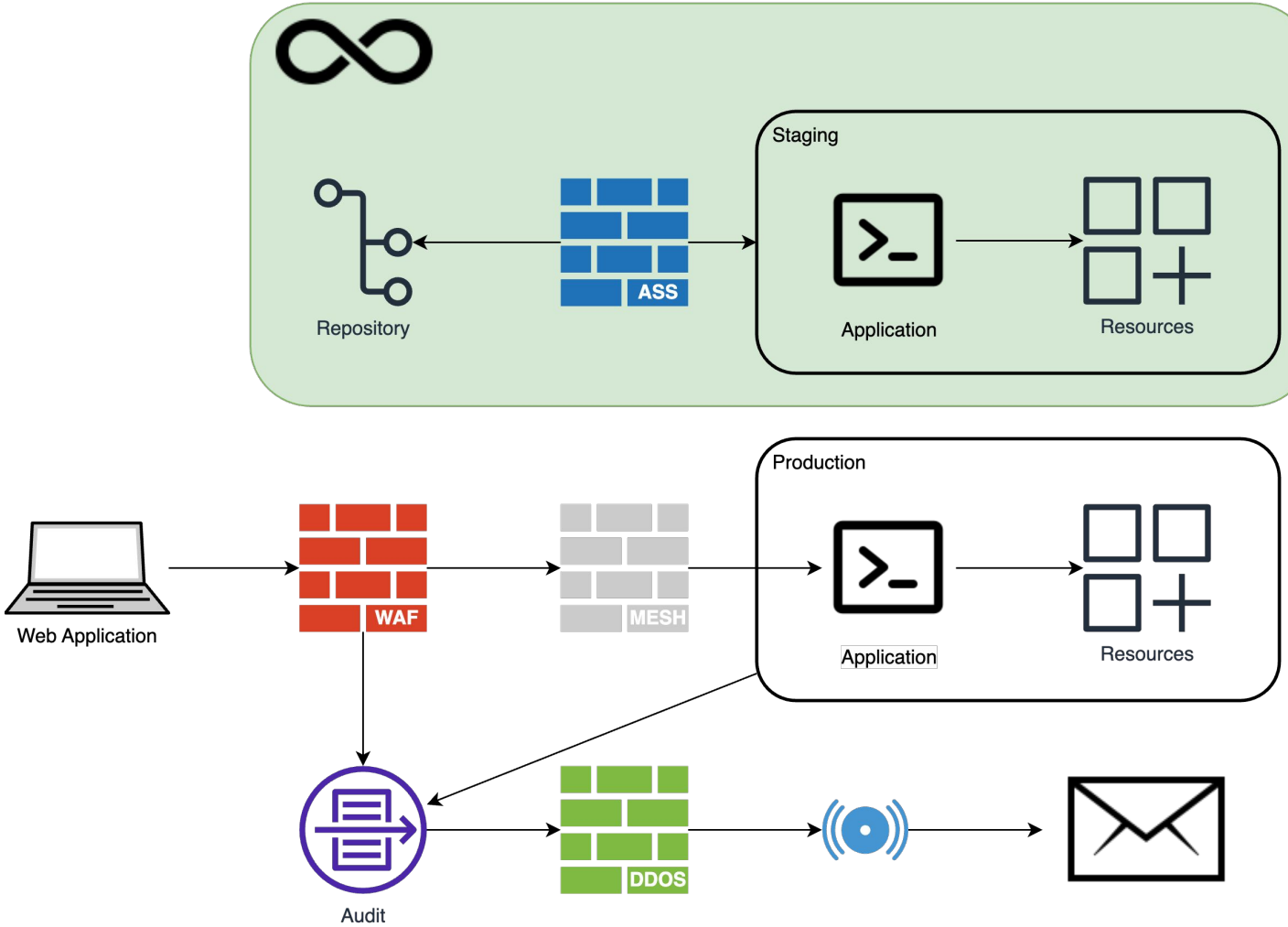

Repository
Staging
Application
Resources
Web Application
WAF
MESH
Production
Application
Resources


Staging
Repository
ASS
Application
Resources
Production
Web Application
WAF
MESH
Application
Resources


Staging
Repository
ASS
Application
Resources
Production
Web Application
WAF
MESH
Application
Resources
Audit


Staging
Repository
ASS
Application
Resources
Production
Web Application
WAF
MESH
Application
Resources
Audit
DDOS


Staging
Repository
ASS
Application
Resources
Production
Web Application
WAF
MESH
Application
Resources
Audit
DDOS


Staging
Repository
ASS
Application
Resources
Production
Web Application
WAF
MESH
Application
Resources
Audit
DDOS

Our Best Friends

1. **WAF**
   Filtering by IP, country, headers, requests
   SQL injection & Cross-Site scripting,
   Intrusion Prevention System,
   Deep Packet inspection

2. **Mesh**
   S2S communication management
   Implement custom traffic routing rules, and configure and standardize how traffic moves between your services

3. **CI / CD**
   Application Security Testing
   SAST, DAST, IAST, SCA, API

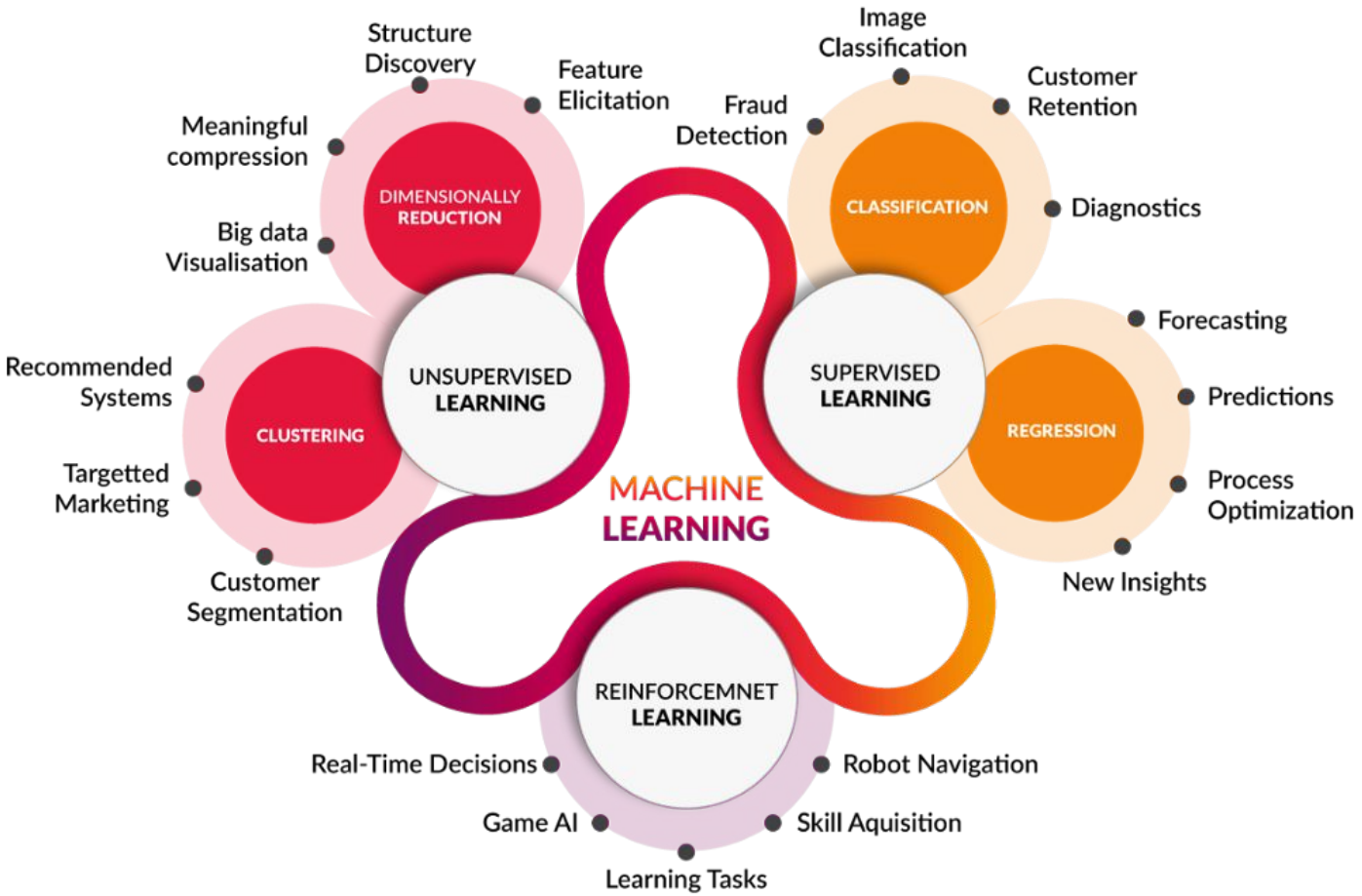
4. **DDoS mitigation**
   DDoS attacks at the network (L3), transport (L4), and application (L7) layers in data centers around the world

Monitoring with Machine Learning

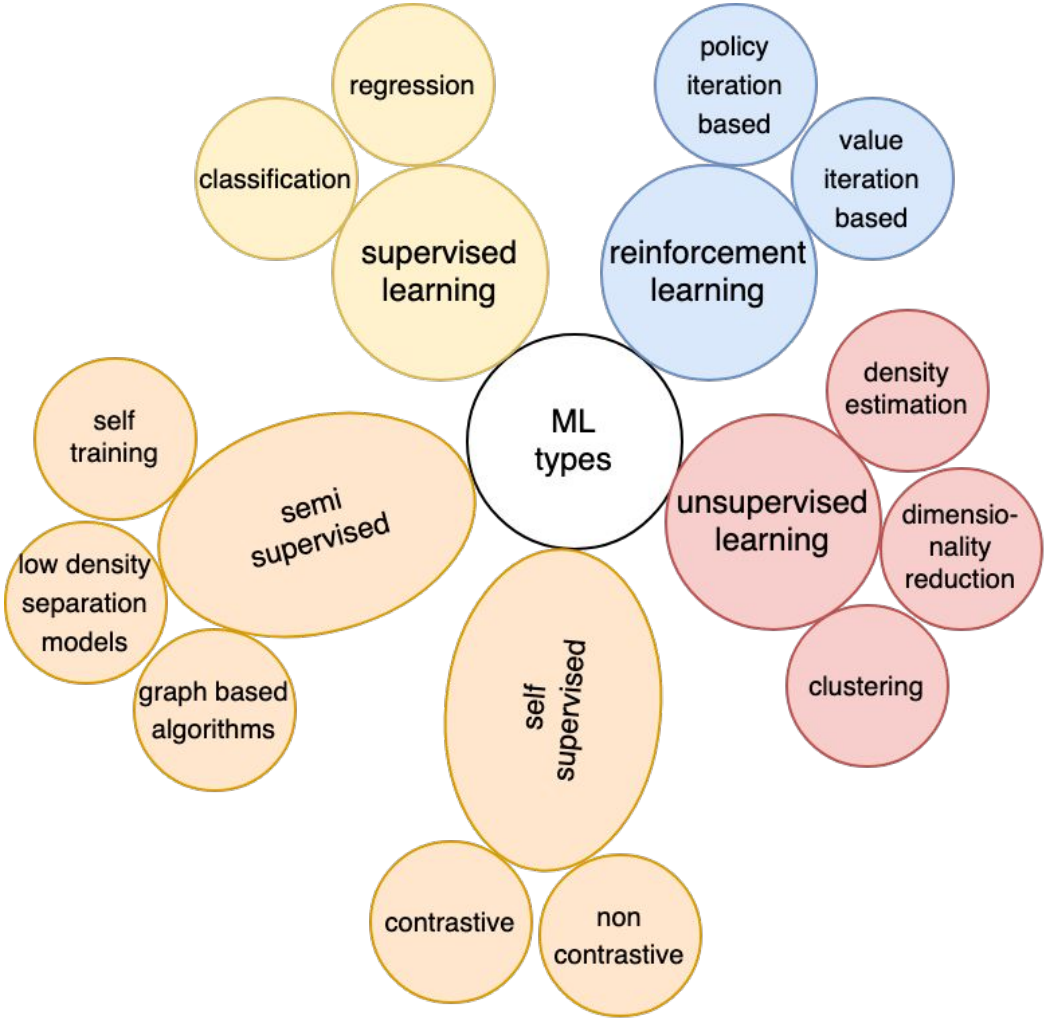
HackInBo Spring 2023 Edition
20ª EDIZIONE

"Machine learning is a branch of artificial intelligence which focuses on the use of data and algorithms to imitate the way that human learn, gradually improving its accuracy"

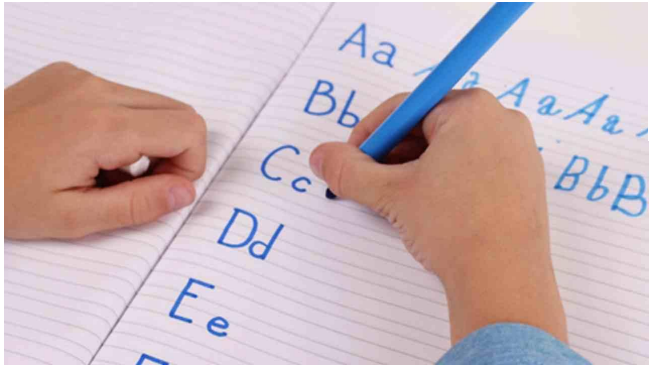
https://www.ibm.com/topics/machine-learning



https://cdn-images-1.medium.com/max/1024/1*onFQ6R6jSrUI9QzDNPZqQA.png


ML types
supervised learning
regression
classification
reinforcement learning
policy iteration based
value iteration based
unsupervised learning
density estimation
dimensio-nality reduction
clustering
semi supervised
self training
low density separation models
graph based algorithms
self supervised
contrastive
non contrastive

ML types

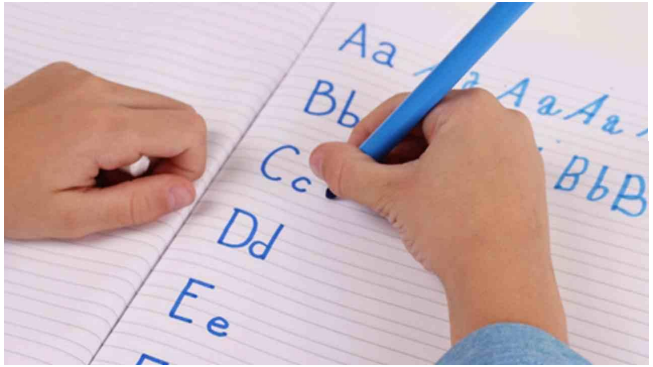


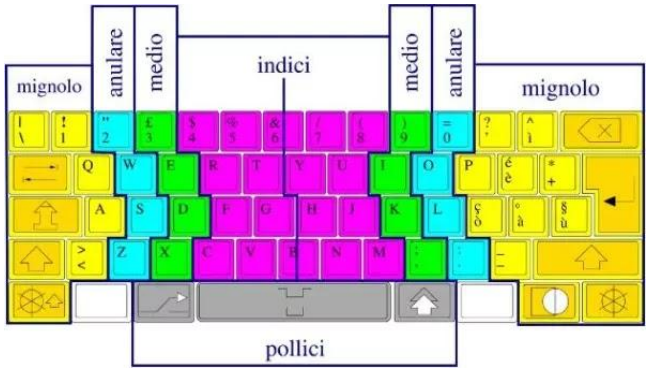
- Supervised Learning
- Unsupervised Learning
- Reinforcement Learning

Images: supervised, unsupervised, reinforcement

ML types

- Supervised Learning
- Unsupervised Learning
- Reinforcement Learning





Images: supervised, unsupervised, reinforcement

ML types

- Supervised Learning
- Unsupervised Learning
- Reinforcement Learning

Images: supervised, unsupervised, reinforcement

ML steps

1. Preparation
2. Training
3. Testing
4. Prediction

1. Il dato potrebbe arrivare già pronto per l'apprendimento, ma spesso è necessaria una elaborazione
2. L'apprendimento del modello potrebbe essere demandato ad un sistema di AI, eccetto per custom step
3. La valutazione è una predizione per la quale conosciamo i valori attesi, per i quali possiamo calcolare l'accuratezza
4. La predizione lavora su nuovi dati elaborati con il punto 1 con il modello migliore salvato nel punto 3

Examples

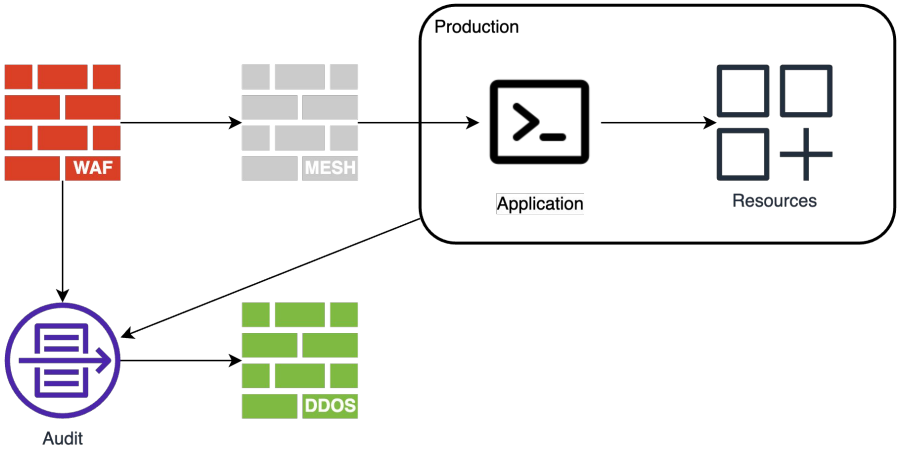
```
>>> import numpy as np
>>> from sklearn.dummy import DummyClassifier
>>> X_train = np.array([-1, 1, 1, 1])
>>> y_train = np.array([0, 1, 1, 1])
>>> X_test = np.array([-1, 0, 1, 2])
>>> y_test = np.array([0, 1, 1, 1])
>>> model = DummyClassifier(strategy="most_frequent").fit(X_train, y_train)
>>> model.score(X_test, y_test)
0.75
>>> model.predict(= np.array([-2,-1, 0, 1, 2])))
array([0, 0, 0, 1, 1])
```

https://scikit-learn.org/stable/modules/generated/sklearn.dummy.DummyClassifier.html

“With great power comes great responsibility.”

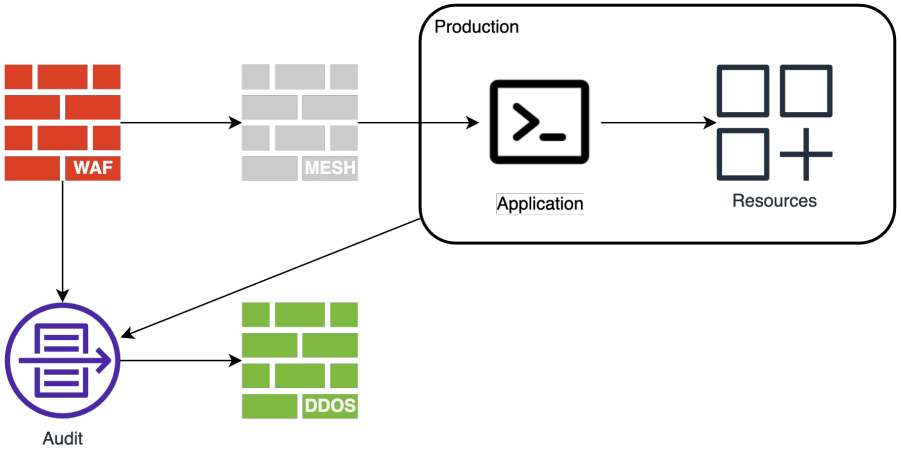
STAN LEE

DDoS mitigation



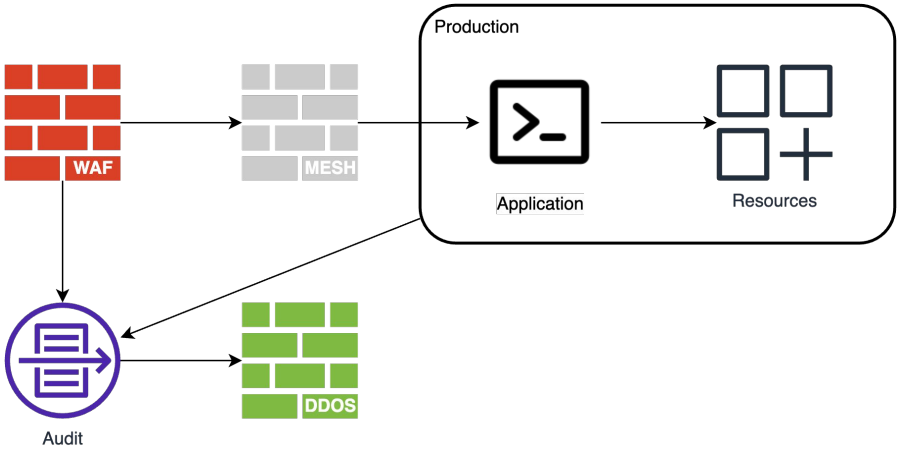
DDoS mitigation

- Anomaly Detection



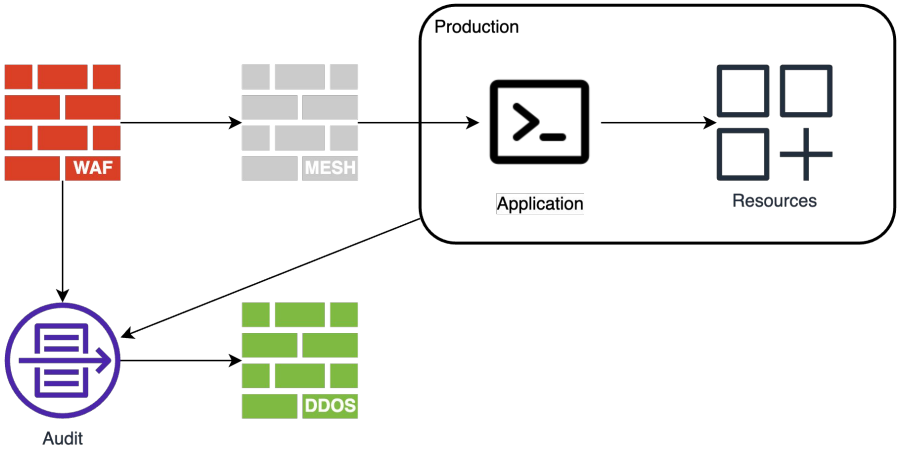
DDoS mitigation

- Anomaly Detection
- IP Insights



DDoS mitigation

- Anomaly Detection
- Network Intrusion Detection



Anomaly Detection

```
[13:05:29] ~ (master)$ head -n 12 Downloads/alb-access-log-sample2
http 2029-03-04T06:55:01.047920Z app/wordpress/d3fad233572a26a0 54.92.151.53:50337 172.31.0.241:80 0.001 0.113 0.000 400 400 152 13911 "GET http://wordpress-1604126382.us-east-2.elb.amazonaws.com:80/ HTTP/1.1" "Apache-HttpClient/4.5.6 (Java/1.8.0_191)" - - arn:aws:elasticloadbalancing:us-east-2:272056417722:targetgroup/wordpress/ea0b820008fed4b6 "Root=1-5c7ccbc4-dae3f75a278b6263e93521cb" "-" "-" 0 2029-03-04T06:55:00.933000Z "waf,forward" "-" "-"
http 2029-03-04T06:55:01.047920Z app/wordpress/d3fad233572a26a0 54.92.151.53:50337 172.31.0.241:80 0.001 0.113 0.000 400 400 152 13911 "GET http://wordpress-1604126382.us-east-2.elb.amazonaws.com:80/ HTTP/1.1" "Apache-HttpClient/4.5.6 (Java/1.8.0_191)" - - arn:aws:elasticloadbalancing:us-east-2:272056417722:targetgroup/wordpress/ea0b820008fed4b6 "Root=1-5c7ccbc4-dae3f75a278b6263e93521cb" "-" "-" 0 2029-03-04T06:55:00.933000Z "waf,forward" "-" "-"
..
http 2029-03-04T06:55:00.865092Z app/wordpress/d3fad233572a26a0 54.92.151.53:50284 172.31.0.241:80 0.001 0.001 0.000 200 200 202 4265 "GET http://wordpress-1604126382.us-east-2.elb.amazonaws.com:80/wp-content/themes/twentynineteen/print.css?ver=1.1 HTTP/1.1" "Apache-HttpClient/4.5.6 (Java/1.8.0_191)" - - arn:aws:elasticloadbalancing:us-east-2:272056417722:targetgroup/wordpress/ea0b820008fed4b6 "Root=1-5c7ccbc4-2586401e126054371b10b5f2" "-" "-" 0 2029-03-04T06:55:00.862000Z "waf,forward" "-" "-"
http 2029-03-04T06:55:00.881515Z app/wordpress/d3fad233572a26a0 54.92.151.53:50296 172.31.0.241:80 0.001 0.001 0.000 200 200 192 1713 "GET http://wordpress-1604126382.us-east-2.elb.amazonaws.com:80/wp-includes/js/wp-embed.min.js?ver=5.0.3 HTTP/1.1" "Apache-HttpClient/4.5.6 (Java/1.8.0_191)" - - arn:aws:elasticloadbalancing:us-east-2:272056417722:targetgroup/wordpress/ea0b820008fed4b6 "Root=1-5c7ccbc4-5ed5fe462050aee48d063de2" "-" "-" 0 2029-03-04T06:55:00.879000Z "waf,forward" "-" "-"
http 2029-03-04T06:55:00.882187Z app/wordpress/d3fad233572a26a0 54.92.151.53:50299 172.31.0.241:80 0.001 0.001 0.000 200 200 205 1981 "GET http://wordpress-1604126382.us-east-2.elb.amazonaws.com:80/bitnami/images/xclose.png.pagespeed.ic.Zei43eohAv.png HTTP/1.1" "Apache-HttpClient/4.5.6 (Java/1.8.0_191)" - - arn:aws:elasticloadbalancing:us-east-2:272056417722:targetgroup/wordpress/ea0b820008fed4b6 "Root=1-5c7ccbc4-29efe2c0a09dbf92f38ab919" "-" "-" 0 2029-03-04T06:55:00.879000Z "waf,forward" "-" "-"
http 2029-03-04T06:55:00.890093Z app/wordpress/d3fad233572a26a0 54.92.151.53:50282 172.31.0.241:80 0.001 0.001 0.000 200 200 202 111744 "GET http://wordpress-1604126382.us-east-2.elb.amazonaws.com:80/wp-content/themes/twentynineteen/style.css?ver=1.1 HTTP/1.1" "Apache-HttpClient/4.5.6 (Java/1.8.0_191)" - - arn:aws:elasticloadbalancing:us-east-2:272056417722:targetgroup/wordpress/ea0b820008fed4b6 "Root=1-5c7ccbc4-f117677afa4a43e46622eef1" "-" "-" 0 2029-03-04T06:55:00.862000Z "waf,forward" "-" "-"
http 2029-03-04T06:55:00.896191Z app/wordpress/d3fad233572a26a0 54.92.151.53:50308 172.31.0.241:80 0.001 0.001 0.000 200 200 211 17575 "GET http://wordpress-1604126382.us-east-2.elb.amazonaws.com:80/bitnami/images/xcorner-logo.png.pagespeed.ic.6TukXqDtLV.png HTTP/1.1" "Apache-HttpClient/4.5.6 (Java/1.8.0_191)" - - arn:aws:elasticloadbalancing:us-east-2:272056417722:targetgroup/wordpress/ea0b820008fed4b6 "Root=1-5c7ccbc4-0edcd60096615f4c2f32c0a1" "-" "-" 0 2029-03-04T06:55:00.894000Z "waf,forward" "-" "-"
http 2029-03-04T06:55:00.914126Z app/wordpress/d3fad233572a26a0 54.92.151.53:50313 172.31.0.241:80 0.001 0.001 0.000 200 200 210 25956 "GET http://wordpress-1604126382.us-east-2.elb.amazonaws.com:80/wp-includes/css/dist/block-library/style.min.css?ver=5.0.3 HTTP/1.1" "Apache-HttpClient/4.5.6 (Java/1.8.0_191)" - - arn:aws:elasticloadbalancing:us-east-2:272056417722:targetgroup/wordpress/ea0b820008fed4b6 "Root=1-5c7ccbc4-1a945d976de42f0dd3d483c2" "-" "-" 0 2029-03-04T06:55:00.911000Z "waf,forward" "-" "-"
http 2029-03-04T06:55:00.927609Z app/wordpress/d3fad233572a26a0 54.92.151.53:50326 172.31.0.241:80 0.001 0.001 0.000 200 200 192 1713 "GET http://wordpress-1604126382.us-east-2.elb.amazonaws.com:80/wp-includes/js/wp-embed.min.js?ver=5.0.3 HTTP/1.1" "Apache-HttpClient/4.5.6 (Java/1.8.0_191)" - - arn:aws:elasticloadbalancing:us-east-2:272056417722:targetgroup/wordpress/ea0b820008fed4b6 "Root=1-5c7ccbc4-013333ec24dda0d3f4fed376" "-" "-" 0 2029-03-04T06:55:00.925000Z "waf,forward" "-" "-"
..
```

Anomaly Detection

```
[13:05:29] ~ (master)$ head -n 12 Downloads/alb-access-log-sample2
http 2029-03-04T06:55:01.047920Z app/wordpress/d3fad233572a26a0 54.92.151.53:50337 172.31.0.241:80 0.001 0.113 0.000 400 400 152 13911 "GET http://wordpress-1604126382.us-east-2.elb.amazonaws.com:80/ HTTP/1.1" "Apache-HttpClient/4.5.6 (Java/1.8.0_191)" - - arn:aws:elasticloadbalancing:us-east-2:272056417722:targetgroup/wordpress/ea0b820008fed4b6 "Root=1-5c7ccbc4-dae3f75a278b6263e93521cb" "-" "-" 0 2029-03-04T06:55:00.933000Z "waf,forward" "-" "-"
http 2029-03-04T06:55:01.047920Z app/wordpress/d3fad233572a26a0 54.92.151.53:50337 172.31.0.241:80 0.001 0.113 0.000 400 400 152 13911 "GET http://wordpress-1604126382.us-east-2.elb.amazonaws.com:80/ HTTP/1.1" "Apache-HttpClient/4.5.6 (Java/1.8.0_191)" - - arn:aws:elasticloadbalancing:us-east-2:272056417722:targetgroup/wordpress/ea0b820008fed4b6 "Root=1-5c7ccbc4-dae3f75a278b6263e93521cb" "-" "-" 0 2029-03-04T06:55:00.933000Z "waf,forward" "-" "-"
..
http 2029-03-04T06:55:00.865092Z app/wordpress/d3fad233572a26a0 54.92.151.53:50284 172.31.0.241:80 0.001 0.001 0.000 200 200 202 4265 "GET http://wordpress-1604126382.us-east-2.elb.amazonaws.com:80/wp-content/themes/twentynineteen/print.css?ver=1.1 HTTP/1.1" "Apache-HttpClient/4.5.6 (Java/1.8.0_191)" - - arn:aws:elasticloadbalancing:us-east-2:272056417722:targetgroup/wordpress/ea0b820008fed4b6 "Root=1-5c7ccbc4-2586401e126054371b10b5f2" "-" "-" 0 2029-03-04T06:55:00.862000Z "waf,forward" "-" "-"
http 2029-03-04T06:55:00.881515Z app/wordpress/d3fad233572a26a0 54.92.151.53:50296 172.31.0.241:80 0.001 0.001 0.000 200 200 192 1713 "GET http://wordpress-1604126382.us-east-2.elb.amazonaws.com:80/wp-includes/js/wp-embed.min.js?ver=5.0.3 HTTP/1.1" "Apache-HttpClient/4.5.6 (Java/1.8.0_191)" - - arn:aws:elasticloadbalancing:us-east-2:272056417722:targetgroup/wordpress/ea0b820008fed4b6 "Root=1-5c7ccbc4-5ed5fe462050aee48d063de2" "-" "-" 0 2029-03-04T06:55:00.879000Z "waf,forward" "-" "-"
http 2029-03-04T06:55:00.882187Z app/wordpress/d3fad233572a26a0 54.92.151.53:50299 172.31.0.241:80 0.001 0.001 0.000 200 200 205 1981 "GET http://wordpress-1604126382.us-east-2.elb.amazonaws.com:80/bitnami/images/xclose.png.pagespeed.ic.Zei43eohAv.png HTTP/1.1" "Apache-HttpClient/4.5.6 (Java/1.8.0_191)" - - arn:aws:elasticloadbalancing:us-east-2:272056417722:targetgroup/wordpress/ea0b820008fed4b6 "Root=1-5c7ccbc4-29efe2c0a09dbf92f38ab919" "-" "-" 0 2029-03-04T06:55:00.879000Z "waf,forward" "-" "-"
http 2029-03-04T06:55:00.890093Z app/wordpress/d3fad233572a26a0 54.92.151.53:50282 172.31.0.241:80 0.001 0.001 0.000 200 200 202 111744 "GET http://wordpress-1604126382.us-east-2.elb.amazonaws.com:80/wp-content/themes/twentynineteen/style.css?ver=1.1 HTTP/1.1" "Apache-HttpClient/4.5.6 (Java/1.8.0_191)" - - arn:aws:elasticloadbalancing:us-east-2:272056417722:targetgroup/wordpress/ea0b820008fed4b6 "Root=1-5c7ccbc4-f117677afa4a43e46622eef1" "-" "-" 0 2029-03-04T06:55:00.862000Z "waf,forward" "-" "-"
http 2029-03-04T06:55:00.896191Z app/wordpress/d3fad233572a26a0 54.92.151.53:50308 172.31.0.241:80 0.001 0.001 0.000 200 200 211 17575 "GET http://wordpress-1604126382.us-east-2.elb.amazonaws.com:80/bitnami/images/xcorner-logo.png.pagespeed.ic.6TukXqDtLV.png HTTP/1.1" "Apache-HttpClient/4.5.6 (Java/1.8.0_191)" - - arn:aws:elasticloadbalancing:us-east-2:272056417722:targetgroup/wordpress/ea0b820008fed4b6 "Root=1-5c7ccbc4-0edcd60096615f4c2f32c0a1" "-" "-" 0 2029-03-04T06:55:00.894000Z "waf,forward" "-" "-"
http 2029-03-04T06:55:00.914126Z app/wordpress/d3fad233572a26a0 54.92.151.53:50313 172.31.0.241:80 0.001 0.001 0.000 200 200 210 25956 "GET http://wordpress-1604126382.us-east-2.elb.amazonaws.com:80/wp-includes/css/dist/block-library/style.min.css?ver=5.0.3 HTTP/1.1" "Apache-HttpClient/4.5.6 (Java/1.8.0_191)" - - arn:aws:elasticloadbalancing:us-east-2:272056417722:targetgroup/wordpress/ea0b820008fed4b6 "Root=1-5c7ccbc4-1a945d976de42f0dd3d483c2" "-" "-" 0 2029-03-04T06:55:00.911000Z "waf,forward" "-" "-"
http 2029-03-04T06:55:00.927609Z app/wordpress/d3fad233572a26a0 54.92.151.53:50326 172.31.0.241:80 0.001 0.001 0.000 200 200 192 1713 "GET http://wordpress-1604126382.us-east-2.elb.amazonaws.com:80/wp-includes/js/wp-embed.min.js?ver=5.0.3 HTTP/1.1" "Apache-HttpClient/4.5.6 (Java/1.8.0_191)" - - arn:aws:elasticloadbalancing:us-east-2:272056417722:targetgroup/wordpress/ea0b820008fed4b6 "Root=1-5c7ccbc4-013333ec24dda0d3f4fed376" "-" "-" 0 2029-03-04T06:55:00.925000Z "waf,forward" "-" "-"
..
```

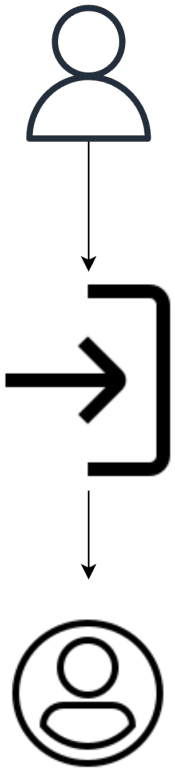
Anomaly Detection

```
[13:05:29] ~ (master)$ head -n 12 Downloads/alb-access-log-sample2
http 2029-03-04T06:55:01.047920Z app/wordpress/d3fad233572a26a0 54.92.151.53:50337 172.31.0.241:80 0.001 0.113 0.000 400 400 152 13911 "GET http://wordpress-1604126382.us-east-2.elb.amazonaws.com:80/ HTTP/1.1" "Apache-HttpClient/4.5.6 (Java/1.8.0_191)" - - arn:aws:elasticloadbalancing:us-east-2:272056417722:targetgroup/wordpress/ea0b820008fed4b6 "Root=1-5c7ccbc4-dae3f75a278b6263e93521cb" "-" "-" 0 2029-03-04T06:55:00.933000Z "waf,forward" "-" "-"
http 2029-03-04T06:55:01.047920Z app/wordpress/d3fad233572a26a0 54.92.151.53:50337 172.31.0.241:80 0.001 0.113 0.000 400 400 152 13911 "GET http://wordpress-1604126382.us-east-2.elb.amazonaws.com:80/ HTTP/1.1" "Apache-HttpClient/4.5.6 (Java/1.8.0_191)" - - arn:aws:elasticloadbalancing:us-east-2:272056417722:targetgroup/wordpress/ea0b820008fed4b6 "Root=1-5c7ccbc4-dae3f75a278b6263e93521cb" "-" "-" 0 2029-03-04T06:55:00.933000Z "waf,forward" "-" "-"
..
http 2029-03-04T06:55:00.865092Z app/wordpress/d3fad233572a26a0 54.92.151.53:50284 172.31.0.241:80 0.001 0.001 0.000 200 200 202 4265 "GET http://wordpress-1604126382.us-east-2.elb.amazonaws.com:80/wp-content/themes/twentynineteen/print.css?ver=1.1 HTTP/1.1" "Apache-HttpClient/4.5.6 (Java/1.8.0_191)" - - arn:aws:elasticloadbalancing:us-east-2:272056417722:targetgroup/wordpress/ea0b820008fed4b6 "Root=1-5c7ccbc4-2586401e126054371b10b5f2" "-" "-" 0 2029-03-04T06:55:00.862000Z "waf,forward" "-" "-"
http 2029-03-04T06:55:00.881515Z app/wordpress/d3fad233572a26a0 54.92.151.53:50296 172.31.0.241:80 0.001 0.001 0.000 200 200 192 1713 "GET http://wordpress-1604126382.us-east-2.elb.amazonaws.com:80/wp-includes/js/wp-embed.min.js?ver=5.0.3 HTTP/1.1" "Apache-HttpClient/4.5.6 (Java/1.8.0_191)" - - arn:aws:elasticloadbalancing:us-east-2:272056417722:targetgroup/wordpress/ea0b820008fed4b6 "Root=1-5c7ccbc4-5ed5fe462050aee48d063de2" "-" "-" 0 2029-03-04T06:55:00.879000Z "waf,forward" "-" "-"
http 2029-03-04T06:55:00.882187Z app/wordpress/d3fad233572a26a0 54.92.151.53:50299 172.31.0.241:80 0.001 0.001 0.000 200 200 205 1981 "GET http://wordpress-1604126382.us-east-2.elb.amazonaws.com:80/bitnami/images/xclose.png.pagespeed.ic.Zei43eohAv.png HTTP/1.1" "Apache-HttpClient/4.5.6 (Java/1.8.0_191)" - - arn:aws:elasticloadbalancing:us-east-2:272056417722:targetgroup/wordpress/ea0b820008fed4b6 "Root=1-5c7ccbc4-29efe2c0a09dbf92f38ab919" "-" "-" 0 2029-03-04T06:55:00.879000Z "waf,forward" "-" "-"
http 2029-03-04T06:55:00.890093Z app/wordpress/d3fad233572a26a0 54.92.151.53:50282 172.31.0.241:80 0.001 0.001 0.000 200 200 202 111744 "GET http://wordpress-1604126382.us-east-2.elb.amazonaws.com:80/wp-content/themes/twentynineteen/style.css?ver=1.1 HTTP/1.1" "Apache-HttpClient/4.5.6 (Java/1.8.0_191)" - - arn:aws:elasticloadbalancing:us-east-2:272056417722:targetgroup/wordpress/ea0b820008fed4b6 "Root=1-5c7ccbc4-f117677afa4a43e46622eef1" "-" "-" 0 2029-03-04T06:55:00.862000Z "waf,forward" "-" "-"
http 2029-03-04T06:55:00.896191Z app/wordpress/d3fad233572a26a0 54.92.151.53:50308 172.31.0.241:80 0.001 0.001 0.000 200 200 211 17575 "GET http://wordpress-1604126382.us-east-2.elb.amazonaws.com:80/bitnami/images/xcorner-logo.png.pagespeed.ic.6TukXqDtLV.png HTTP/1.1" "Apache-HttpClient/4.5.6 (Java/1.8.0_191)" - - arn:aws:elasticloadbalancing:us-east-2:272056417722:targetgroup/wordpress/ea0b820008fed4b6 "Root=1-5c7ccbc4-0edcd60096615f4c2f32c0a1" "-" "-" 0 2029-03-04T06:55:00.894000Z "waf,forward" "-" "-"
http 2029-03-04T06:55:00.914126Z app/wordpress/d3fad233572a26a0 54.92.151.53:50313 172.31.0.241:80 0.001 0.001 0.000 200 200 210 25956 "GET http://wordpress-1604126382.us-east-2.elb.amazonaws.com:80/wp-includes/css/dist/block-library/style.min.css?ver=5.0.3 HTTP/1.1" "Apache-HttpClient/4.5.6 (Java/1.8.0_191)" - - arn:aws:elasticloadbalancing:us-east-2:272056417722:targetgroup/wordpress/ea0b820008fed4b6 "Root=1-5c7ccbc4-1a945d976de42f0dd3d483c2" "-" "-" 0 2029-03-04T06:55:00.911000Z "waf,forward" "-" "-"
http 2029-03-04T06:55:00.927609Z app/wordpress/d3fad233572a26a0 54.92.151.53:50326 172.31.0.241:80 0.001 0.001 0.000 200 200 192 1713 "GET http://wordpress-1604126382.us-east-2.elb.amazonaws.com:80/wp-includes/js/wp-embed.min.js?ver=5.0.3 HTTP/1.1" "Apache-HttpClient/4.5.6 (Java/1.8.0_191)" - - arn:aws:elasticloadbalancing:us-east-2:272056417722:targetgroup/wordpress/ea0b820008fed4b6 "Root=1-5c7ccbc4-013333ec24dda0d3f4fed376" "-" "-" 0 2029-03-04T06:55:00.925000Z "waf,forward" "-" "-"
..
```

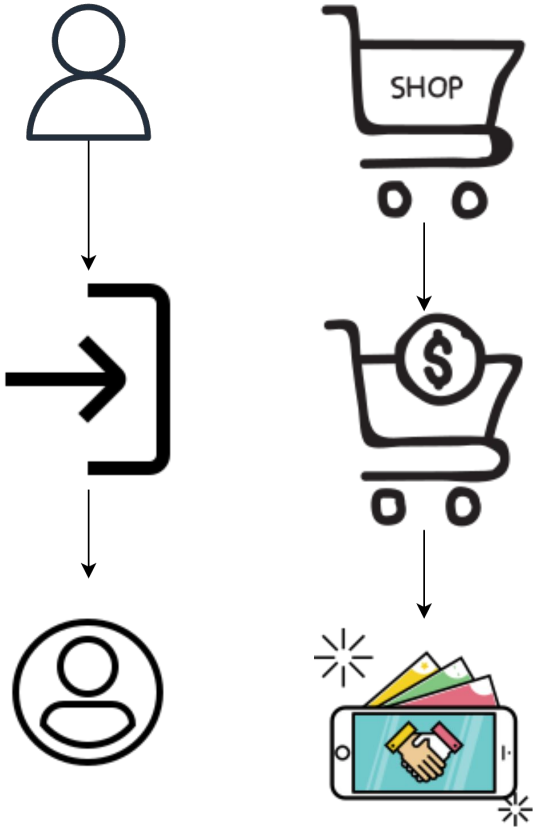
Anomaly Detection

```
[13:05:29] ~ (master)$ head -n 12 Downloads/alb-access-log-sample2
http 2029-03-04T06:55:01.047920Z app/wordpress/d3fad233572a26a0 54.92.151.53:50337 172.31.0.241:80 0.001 0.113 0.000 400 400 152 13911 "GET http://wordpress-1604126382.us-east-2.elb.amazonaws.com:80/ HTTP/1.1" "Apache-HttpClient/4.5.6 (Java/1.8.0_191)" - - arn:aws:elasticloadbalancing:us-east-2:272056417722:targetgroup/wordpress/ea0b820008fed4b6 "Root=1-5c7ccbc4-dae3f75a278b6263e93521cb" "-" "-" 0 2029-03-04T06:55:00.933000Z "waf,forward" "-" "-"
http 2029-03-04T06:55:01.047920Z app/wordpress/d3fad233572a26a0 54.92.151.53:50337 172.31.0.241:80 0.001 0.113 0.000 400 400 152 13911 "GET http://wordpress-1604126382.us-east-2.elb.amazonaws.com:80/ HTTP/1.1" "Apache-HttpClient/4.5.6 (Java/1.8.0_191)" - - arn:aws:elasticloadbalancing:us-east-2:272056417722:targetgroup/wordpress/ea0b820008fed4b6 "Root=1-5c7ccbc4-dae3f75a278b6263e93521cb" "-" "-" 0 2029-03-04T06:55:00.933000Z "waf,forward" "-" "-"
..
http 2029-03-04T06:55:00.865092Z app/wordpress/d3fad233572a26a0 54.92.151.53:50284 172.31.0.241:80 0.001 0.001 0.000 200 200 202 4265 "GET http://wordpress-1604126382.us-east-2.elb.amazonaws.com:80/wp-content/themes/twentynineteen/print.css?ver=1.1 HTTP/1.1" "Apache-HttpClient/4.5.6 (Java/1.8.0_191)" - - arn:aws:elasticloadbalancing:us-east-2:272056417722:targetgroup/wordpress/ea0b820008fed4b6 "Root=1-5c7ccbc4-2586401e126054371b10b5f2" "-" "-" 0 2029-03-04T06:55:00.862000Z "waf,forward" "-" "-"
http 2029-03-04T06:55:00.881515Z app/wordpress/d3fad233572a26a0 54.92.151.53:50296 172.31.0.241:80 0.001 0.001 0.000 200 200 192 1713 "GET http://wordpress-1604126382.us-east-2.elb.amazonaws.com:80/wp-includes/js/wp-embed.min.js?ver=5.0.3 HTTP/1.1" "Apache-HttpClient/4.5.6 (Java/1.8.0_191)" - - arn:aws:elasticloadbalancing:us-east-2:272056417722:targetgroup/wordpress/ea0b820008fed4b6 "Root=1-5c7ccbc4-5ed5fe462050aee48d063de2" "-" "-" 0 2029-03-04T06:55:00.879000Z "waf,forward" "-" "-"
http 2029-03-04T06:55:00.882187Z app/wordpress/d3fad233572a26a0 54.92.151.53:50299 172.31.0.241:80 0.001 0.001 0.000 200 200 205 1981 "GET http://wordpress-1604126382.us-east-2.elb.amazonaws.com:80/bitnami/images/xclose.png.pagespeed.ic.Zei43eohAv.png HTTP/1.1" "Apache-HttpClient/4.5.6 (Java/1.8.0_191)" - - arn:aws:elasticloadbalancing:us-east-2:272056417722:targetgroup/wordpress/ea0b820008fed4b6 "Root=1-5c7ccbc4-29efe2c0a09dbf92f38ab919" "-" "-" 0 2029-03-04T06:55:00.879000Z "waf,forward" "-" "-"
http 2029-03-04T06:55:00.890093Z app/wordpress/d3fad233572a26a0 54.92.151.53:50282 172.31.0.241:80 0.001 0.001 0.000 200 200 202 111744 "GET http://wordpress-1604126382.us-east-2.elb.amazonaws.com:80/wp-content/themes/twentynineteen/style.css?ver=1.1 HTTP/1.1" "Apache-HttpClient/4.5.6 (Java/1.8.0_191)" - - arn:aws:elasticloadbalancing:us-east-2:272056417722:targetgroup/wordpress/ea0b820008fed4b6 "Root=1-5c7ccbc4-f117677afa4a43e46622eef1" "-" "-" 0 2029-03-04T06:55:00.862000Z "waf,forward" "-" "-"
http 2029-03-04T06:55:00.896191Z app/wordpress/d3fad233572a26a0 54.92.151.53:50308 172.31.0.241:80 0.001 0.001 0.000 200 200 211 17575 "GET http://wordpress-1604126382.us-east-2.elb.amazonaws.com:80/bitnami/images/xcorner-logo.png.pagespeed.ic.6TukXqDtLV.png HTTP/1.1" "Apache-HttpClient/4.5.6 (Java/1.8.0_191)" - - arn:aws:elasticloadbalancing:us-east-2:272056417722:targetgroup/wordpress/ea0b820008fed4b6 "Root=1-5c7ccbc4-0edcd60096615f4c2f32c0a1" "-" "-" 0 2029-03-04T06:55:00.894000Z "waf,forward" "-" "-"
http 2029-03-04T06:55:00.914126Z app/wordpress/d3fad233572a26a0 54.92.151.53:50313 172.31.0.241:80 0.001 0.001 0.000 200 200 210 25956 "GET http://wordpress-1604126382.us-east-2.elb.amazonaws.com:80/wp-includes/css/dist/block-library/style.min.css?ver=5.0.3 HTTP/1.1" "Apache-HttpClient/4.5.6 (Java/1.8.0_191)" - - arn:aws:elasticloadbalancing:us-east-2:272056417722:targetgroup/wordpress/ea0b820008fed4b6 "Root=1-5c7ccbc4-1a945d976de42f0dd3d483c2" "-" "-" 0 2029-03-04T06:55:00.911000Z "waf,forward" "-" "-"
http 2029-03-04T06:55:00.927609Z app/wordpress/d3fad233572a26a0 54.92.151.53:50326 172.31.0.241:80 0.001 0.001 0.000 200 200 192 1713 "GET http://wordpress-1604126382.us-east-2.elb.amazonaws.com:80/wp-includes/js/wp-embed.min.js?ver=5.0.3 HTTP/1.1" "Apache-HttpClient/4.5.6 (Java/1.8.0_191)" - - arn:aws:elasticloadbalancing:us-east-2:272056417722:targetgroup/wordpress/ea0b820008fed4b6 "Root=1-5c7ccbc4-013333ec24dda0d3f4fed376" "-" "-" 0 2029-03-04T06:55:00.925000Z "waf,forward" "-" "-"
..
```

Anomaly Detection



Anomaly Detection



Anomaly Detection

Anomaly Detection

Dataset

- client ID / cookies → entity hash ❗
- method, uri, http code, ..
- received bytes
- sent bytes

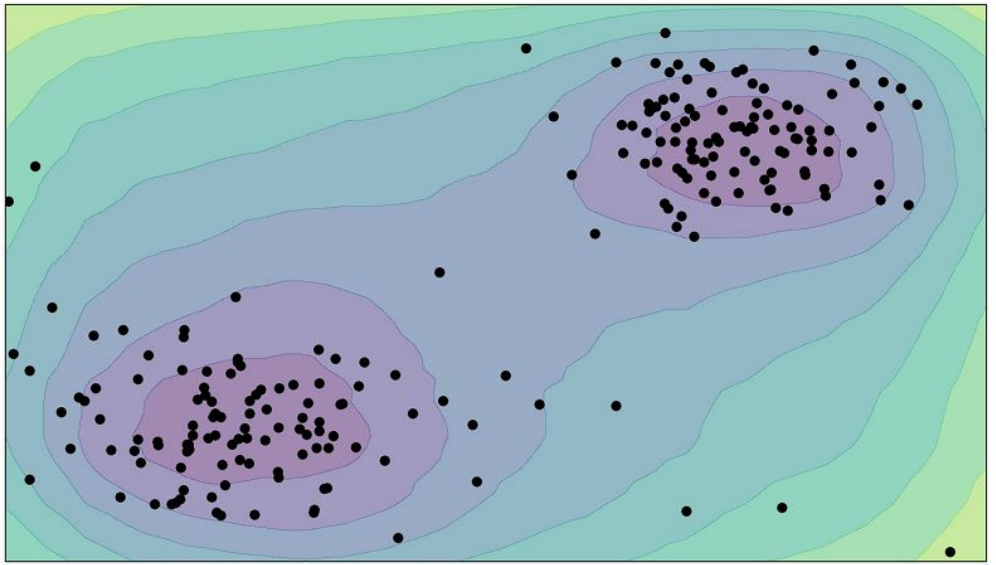
Anomaly Detection

Dataset

- client ID / cookies → entity hash ❗
- method, uri, http code, ..
- received bytes
- sent bytes

Machine Learning Algorithm

- outliers detection
- anomaly scoring
- random cut forest



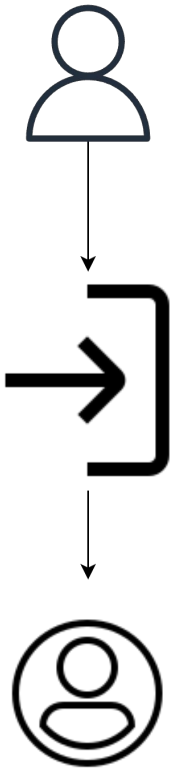
https://aws.amazon.com/blogs/big-data/using-random-cut-forests-for-real-time-anomaly-detection-in-amazon-opensearch-service/

Network Intrusion Detection

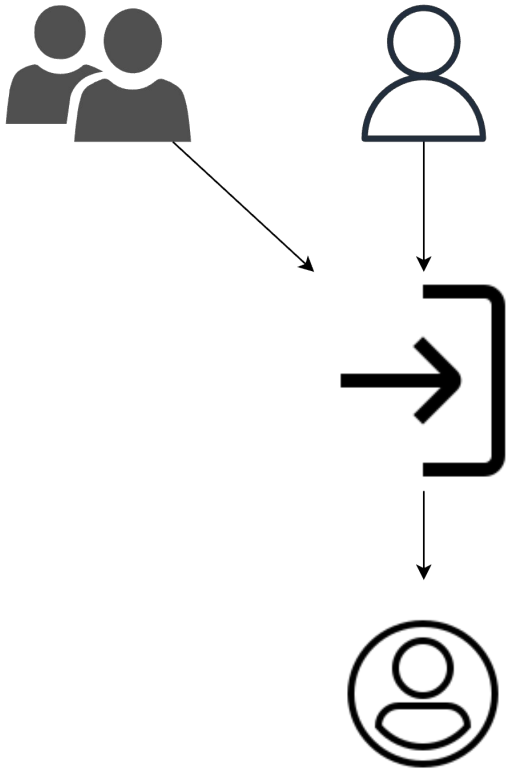
```
[15:33:07] ~ (master)$ head -n 12 Downloads/sample-cloudfront-access-logs2
#Fields: date time x-edge-location sc-bytes c-ip cs-method cs(Host) cs-uri-stem sc-status cs(Referer) cs(User-Agent) cs-uri-query cs(Cookie) x-edge-result-type x-edge-reque
st-id x-host-header cs-protocol cs-bytes time-taken x-forwarded-for ssl-protocol ssl-cipher x-edge-response-result-type cs-protocol-version fle-status fle-encrypted-fields
2018-11-07      00:12:08        FRA53   376     3.120.138.129   GET     d345qc258n54ge.cloudfront.net   /notavailable.json      302     -       Mozilla/5.0%2520(compatible;
%2520bingbot/2.0;%2520+http://www.bing.com/bingbot.htm) -       -       LambdaGeneratedResponse PsDv-_qwCLPFx4CUU0cHWEmaH72tmUZkj70pPiTS-8KQBa616MpB1Q==        d345qc258n54
ge.cloudfront.net       https   337     0.394   -       TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256     LambdaGeneratedResponse HTTP/1.1        -       -
2018-11-07      00:12:15        FRA53   376     3.120.138.129   GET     d345qc258n54ge.cloudfront.net   /notavailable.json      302     -       Mozilla/5.0%2520(compatible;
%2520bingbot/2.0;%2520+http://www.bing.com/bingbot.htm) -       -       LambdaGeneratedResponse wmWvz0x5vh0LtvPxX1UcZLfjDLnUnKtMfxeiLcmT8FUNqYUwE5--MQ==        d345qc258n54
ge.cloudfront.net       https   337     0.387   -       TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256     LambdaGeneratedResponse HTTP/1.1        -       -
2018-11-07      00:11:29        BOM52   965     13.233.35.131   GET     d345qc258n54ge.cloudfront.net   /index.html     200     -       Mozilla/5.0%2520(Windows%2520NT%2520
10.0;%2520Win64;%2520x64;%2520rv:61.0)%2520Gecko/20100101%2520Firefox/61.0      -       -       Hit     myPa1eZJ2BTEssoRDwy1bm2eVRMNPpA4V_zcmhk6GaM9uNoenklnDg==        d345
qc258n54ge.cloudfront.net       https   337     1.047   -       TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256     Hit     HTTP/1.1        -       -
2018-11-07      00:12:20        DUB2    966     52.209.5.129    GET     d345qc258n54ge.cloudfront.net   /index.html     200     -       Mozilla/5.0%2520(iPhone;%2520CPU%252
0iPhone%2520OS%252011_0%2520like%2520Mac%2520OS%2520X)%2520AppleWebKit/604.1.38%2520(KHTML,%2520like%2520Gecko)%2520Version/11.0%2520Mobile/15A372%2520Safari/604.1      -       -
Hit     7jLJcHNNYD188OhFVANOXxpMJ4NHfWVOcej8Px4SMMIaJEIoeXZ7Fg==        d345qc258n54ge.cloudfront.net   https   394     0.417   -       TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256H
it      HTTP/1.1        -       -
2018-11-07      00:12:06        FRA53   376     3.120.138.129   GET     d345qc258n54ge.cloudfront.net   /notavailable.json      302     -       Mozilla/5.0%2520(compatible;
%2520bingbot/2.0;%2520+http://www.bing.com/bingbot.htm) -       -       LambdaGeneratedResponse JIsS5JwjGFPfHUO7A4YMtCpuBZ9kQX1Z0oxomj2ElRt6dbZXsxrnHw==        d345qc258n54
ge.cloudfront.net       https   337     2.066   -       TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256     LambdaGeneratedResponse HTTP/1.1        -       -
..
2018-11-07      00:13:08        FRA53   379     3.120.138.129   GET     d345qc258n54ge.cloudfront.net   /notavailable.json      302     -       Mozilla/5.0%2520(Windows%252
0NT%25206.1;%2520WOW64;%2520Trident/7.0;%2520rv:11.0)%2520like%2520Gecko        -       -       Hit     APo0h4RqJrzeR5iQ8MC7KQ5FIYOzD3yUTi4Z_XzWLL6Hk8IHMcHS2g==        d345
qc258n54ge.cloudfront.net       https   334     0.380   -       TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256     Hit     HTTP/1.1        -       -
2018-11-07      00:13:11        FRA53   379     3.120.138.129   GET     d345qc258n54ge.cloudfront.net   /notavailable.json      302     -       Mozilla/5.0%2520(Windows%252
0NT%25206.1;%2520WOW64;%2520Trident/7.0;%2520rv:11.0)%2520like%2520Gecko        -       -       Hit     nWdC8u7Pdv7Mbhj0xsk7oPaLhv8VhisxKF8zt2J2NWGSneKf-E5zVQ==        d345
qc258n54ge.cloudfront.net       https   334     0.390   -       TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256     Hit     HTTP/1.1        -       -
2018-11-07      00:13:32        BOM52   376     13.233.35.131   GET     d345qc258n54ge.cloudfront.net   /notavailable.json      302     -       Mozilla/5.0%2520(compatible;
%2520bingbot/2.0;%2520+http://www.bing.com/bingbot.htm) -       -       LambdaGeneratedResponse XJPKNRx5TBn7LRbzH-JPZczPSgVoZyJfbPOFcKJa0fN3USx756oz5g==        d345qc258n54
ge.cloudfront.net       https   337     0.768   -       TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256     LambdaGeneratedResponse HTTP/1.1        -       -
2018-11-07      00:13:39        BOM52   376     13.233.35.131   GET     d345qc258n54ge.cloudfront.net   /notavailable.json      302     -       Mozilla/5.0%2520(compatible;
%2520bingbot/2.0;%2520+http://www.bing.com/bingbot.htm) -       -       LambdaGeneratedResponse NFsTgQ7kMID3GQssxvObN-CiTL0K1YuP2X3SI8HpYF99nzaYxn93hg==        d345qc258n54
ge.cloudfront.net       https   337     0.779   -       TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256     LambdaGeneratedResponse HTTP/1.1        -       -
2018-11-07      00:13:33        BOM52   376     13.233.35.131   GET     d345qc258n54ge.cloudfront.net   /notavailable.json      302     -       Mozilla/5.0%2520(compatible;
```

Network Intrusion Detection

Network Intrusion Detection



Network Intrusion Detection



Network Intrusion Detection

Dataset

- client IP → 4-tuple
- client ID / cookies → entity hash ❗

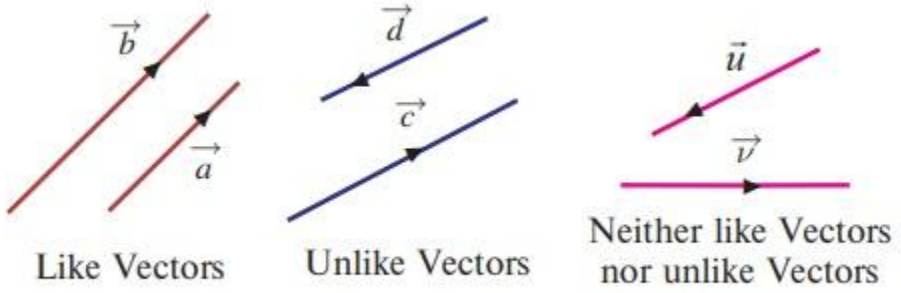
Network Intrusion Detection

Dataset

- client IP → 4-tuple
- client ID / cookies → entity hash ❗

Machine Learning Algorithm

- vector representation
- similarity scoring
- multiclass classification

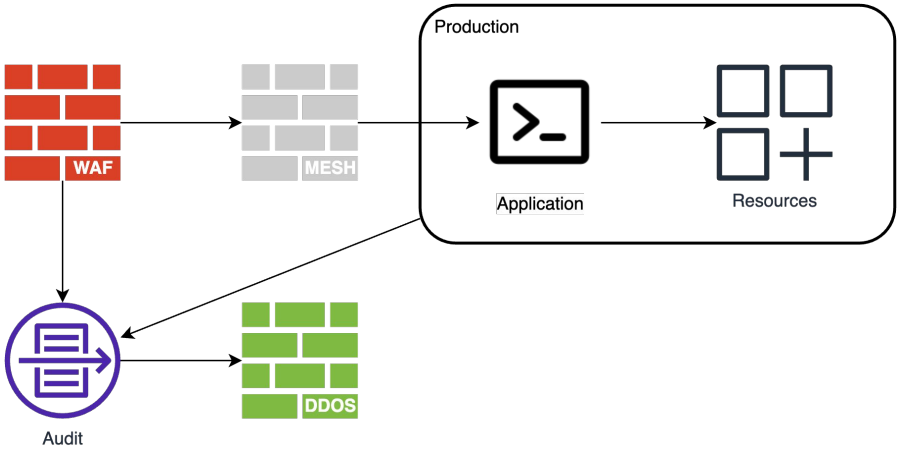


https://img.brainkart.com/imagebk37/Nuk6cVa.jpg

related: https://www.sciencedirect.com/science/article/abs/pii/S0950705121001507

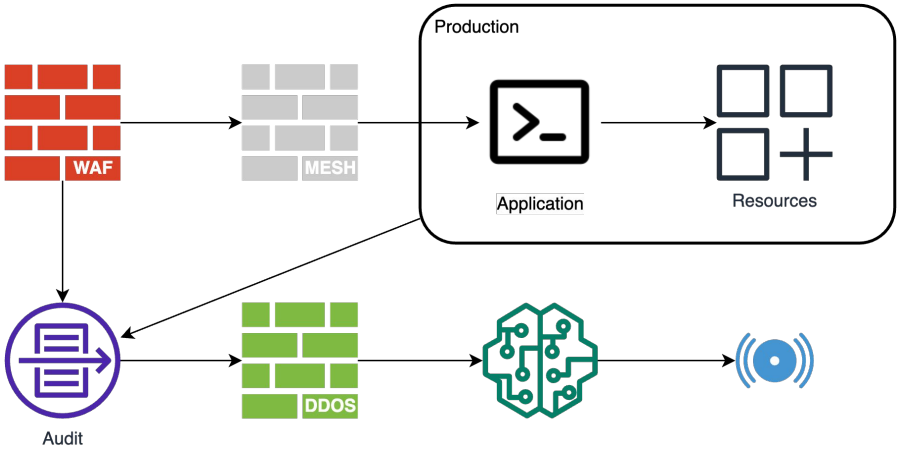
DDoS mitigation

- Anomaly Detection
- Network Intrusion Detection



DDoS mitigation

- Anomaly Detection
- Network Intrusion Detection



HACK IN BO
Spring 2023 Edition
20ª EDIZIONE

Thanks for listening.

#HIB23

corley

Contacts