

Half-Life: Lambda Security

Artëm Tsvetkov • SENIOR SECURITY ENGINEER, SKYSCANNER



What's a **serverless** ?

Serverless

- It's called serverless, but there is a server
- Completely managed by Amazon
- Upload your code, configure event sources, permissions, and you're good to go!

What's a Lambda ?

What's a Lambda?

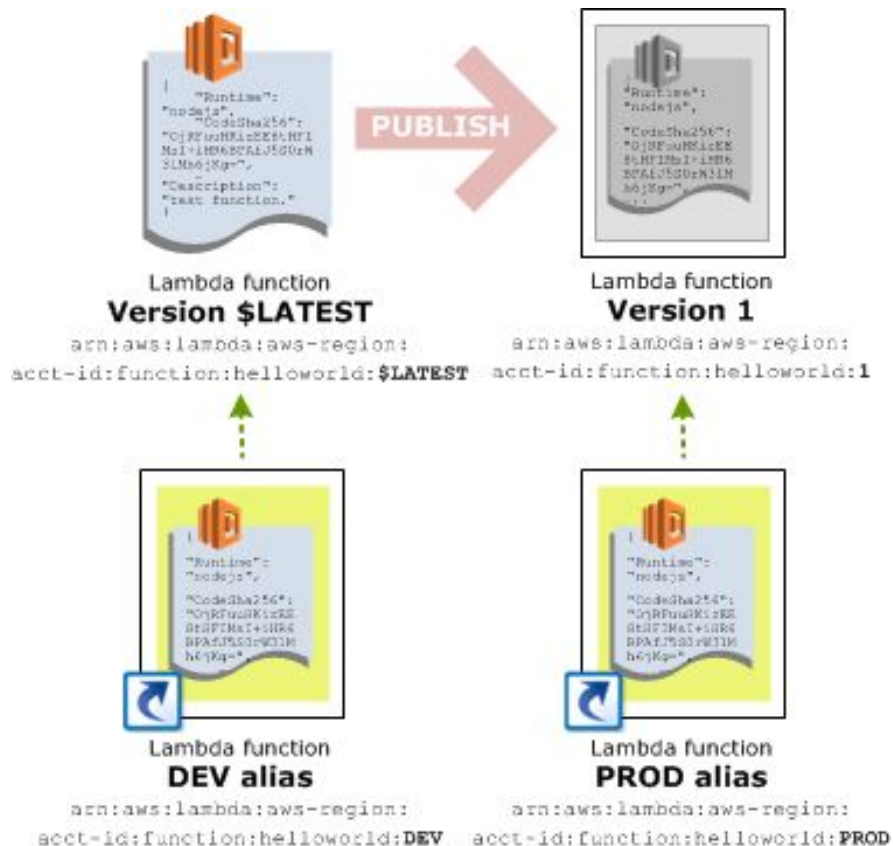
Event-driven serverless computing platform

Lambda

- Runs code in response to an event
- Scales with high availability automatically
- Isolated environment
- Read-only filesystem
- One execution per request
- Typically runs for a few seconds
- Limited to 15 minutes of runtime

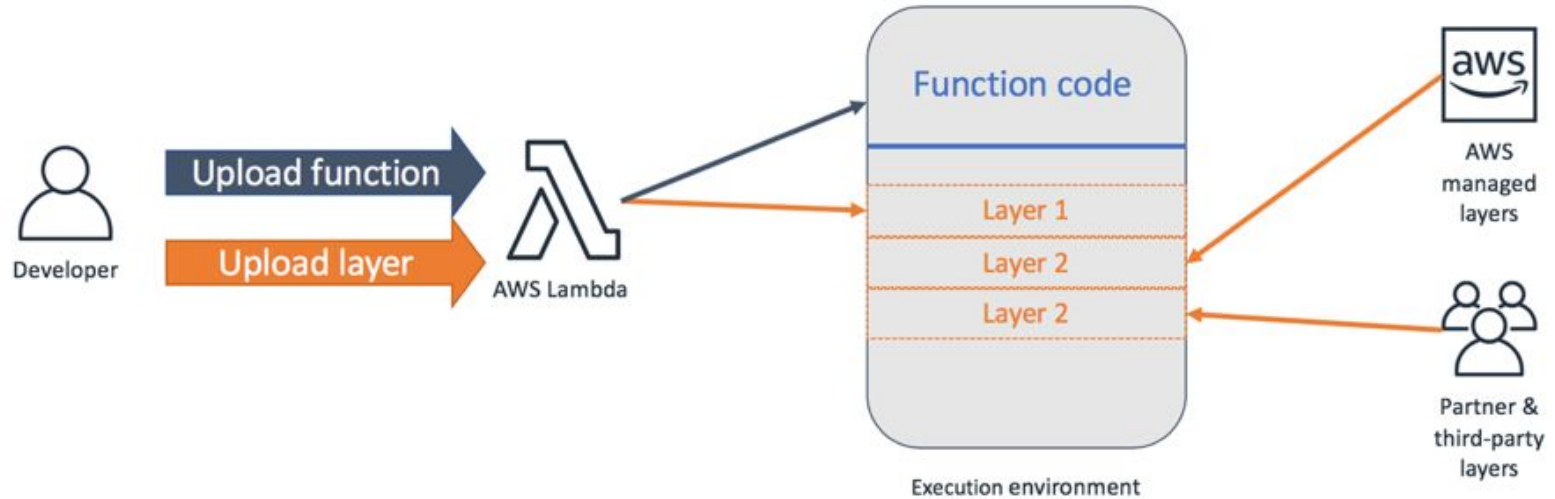
Versions and Aliases

<https://docs.aws.amazon.com/lambda/latest/dg/versioning-aliases.html>



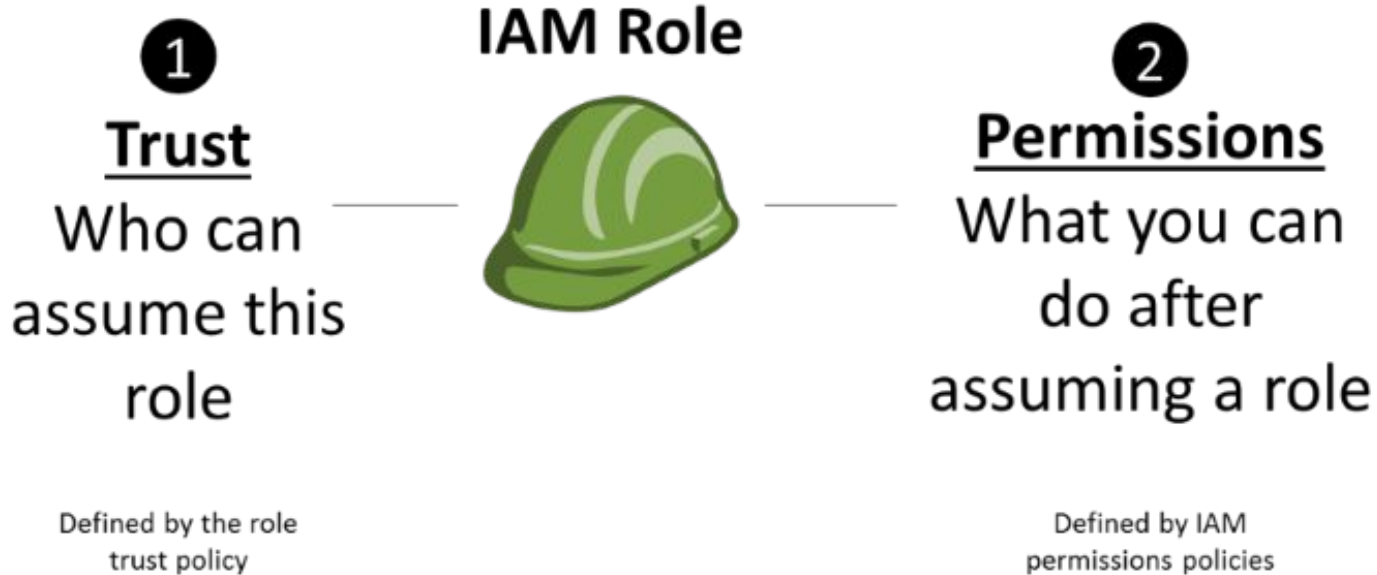
Layers

<https://aws.amazon.com/blogs/compute/working-with-aws-lambda-and-lambda-layers-in-aws-sam/>



Execution Role

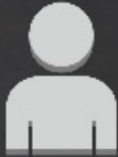
<https://aws.amazon.com/blogs/security/now-create-and-manage-aws-iam-roles-more-easily-with-the-updated-iam-console/>



Resource-based Policy

<https://www.slideshare.net/AmazonWebServices/become-an-iam-policy-ninja>

Identity-based Permissions



user



group



role

Trust Policies

Resource-based Permissions



Amazon
SNS



Amazon
SQS



Amazon
Glacier



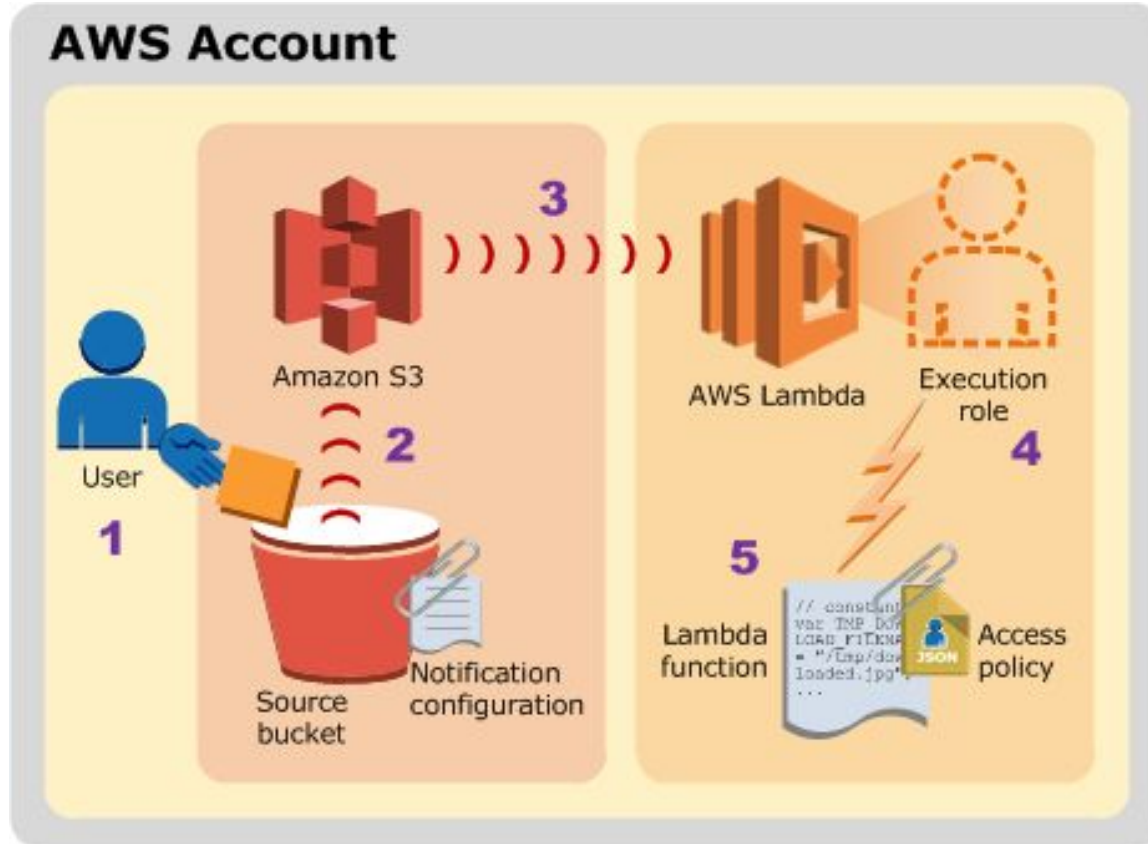
Amazon
S3



AWS KMS

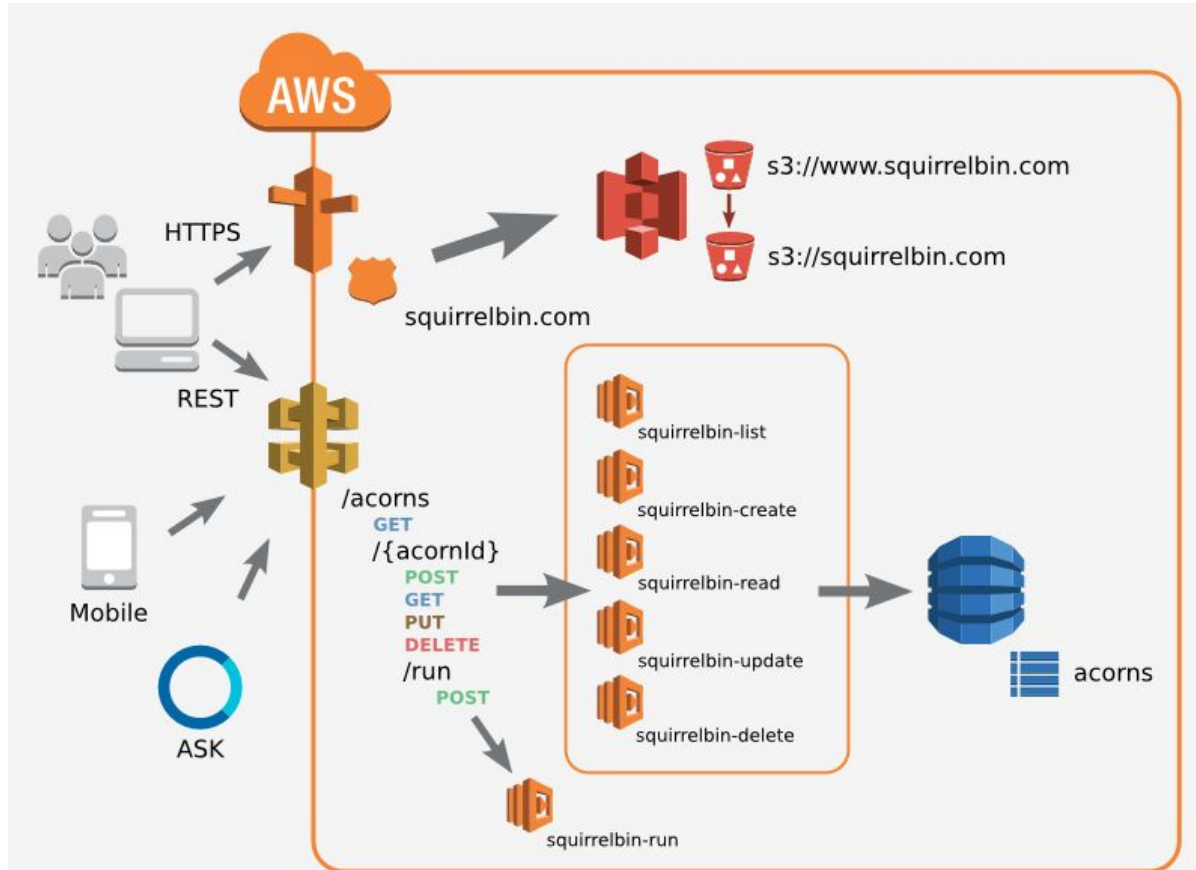
Example: File Upload

<https://docs.aws.amazon.com/lambda/latest/dg/with-s3.html>



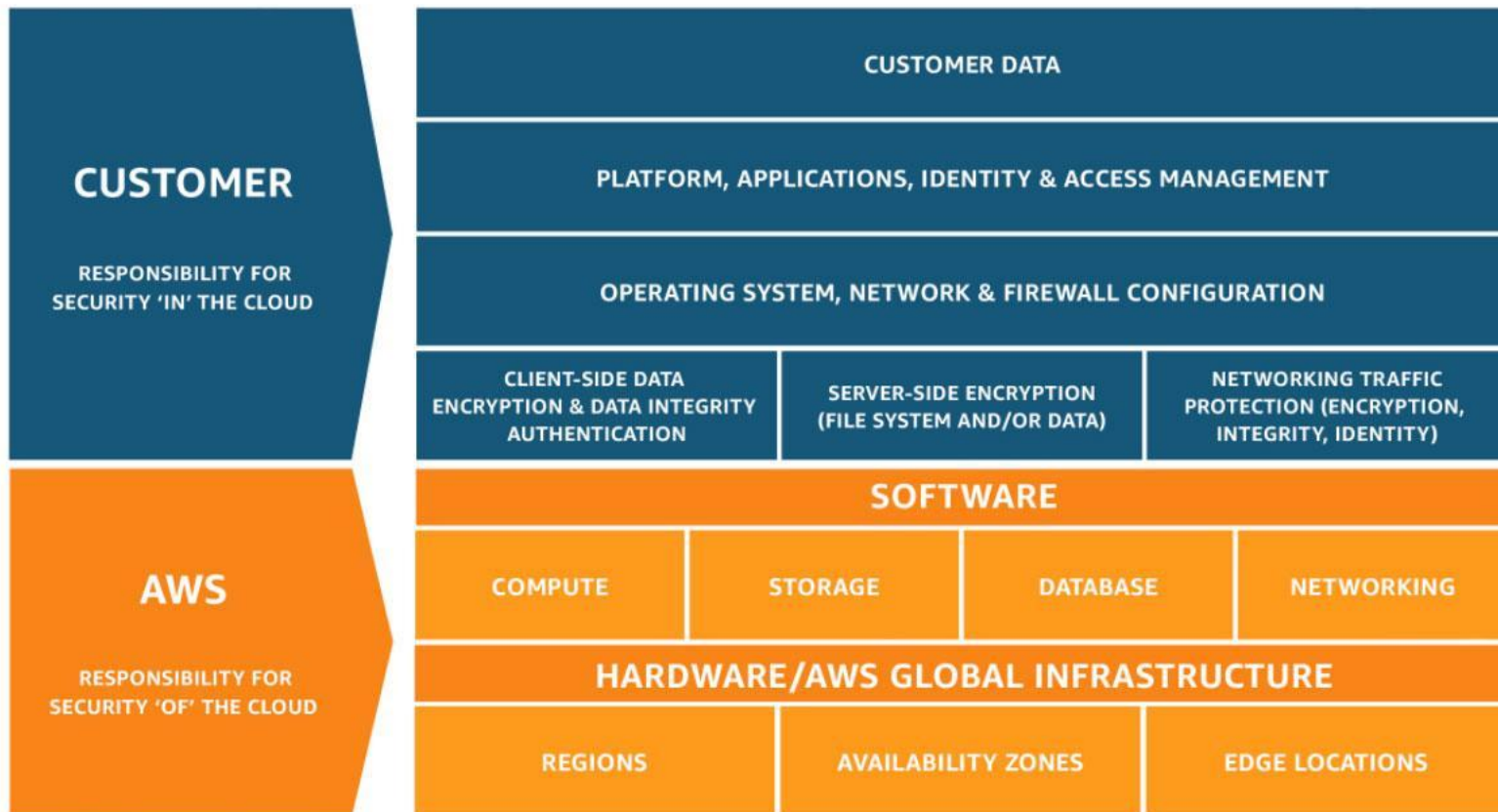
Example: Microservice

<https://aws.amazon.com/blogs/compute/the-squirrelbin-architecture-a-serverless-microservice-using-aws-lambda/>



AWS Shared Responsibility Model




<https://aws.amazon.com/compliance/shared-responsibility-model/>



Permissions are hard

- Users
- Roles
- Trusted Entities
- Access Control Lists
- Resource-based policies
- Managed policies
- Inline policies

Example: SQS Permissions

 Services ▾ Resource Groups ▾  EC2 

Create New Queue Queue Actions ▾

Filter by Prefix: X

☐ Name

☒ testq

1 SQS Queue selected

Details Permissions Redrive Policy Monitoring Tags Encryption Lambda Triggers

Add a Permission Edit Policy Document (Advanced) [What's an SQS Queue Access Policy?](#)


Effect	Principals	Actions	Conditions
This queue has an empty SQS Queue Access Policy . This means that only the queue owner is allowed to use it. You can Add a Permission to grant another account access to this queue.			


Example: SQS Permissions

Add a Permission to testq


×

Permissions enable you to control which operations a user can perform on a queue. [Click here](#) to learn more about access control concepts.

Effect  ☒ Allow
☐ Deny

Principal  ☒ Everybody (*)

Use commas between multiple values.

Actions  ☒ All SQS Actions (SQS:*)

[Add Conditions \(optional\)](#)

Cancel

Add Permission

Unique Serverless challenge

Policy Configuration Management

Key Policy Elements

Policy defines permissions for an associated identity or resource

Key	Value
Effect	Allow or Deny
Principal	Users, roles or trusted entities affected by the policy
Action	Permissions that are allowed or denied
Resource	Resources that can or cannot be used
Condition	When policy is in effect (OPTIONAL)

Common pitfalls

Unrestricted Action

Actions specify permissions

```
"Action": "s3:GetObject"
```

```
"Action": "s3:*"
```

Unrestricted Principal

Principal specifies who is affected by the policy

```
"Principal": { "AWS": "arn:aws:iam::account:user/name" }
```

```
"Principal": "*" 
```

Undefined Condition

Conditions specify when policy takes effect

```
"Condition": {  
  "IpAddress": {  
    "aws:SourceIp": ["192.0.2.0/24"]  
  }  
}
```

Other pitfalls

- Allow NotPrincipal
- Allow NotAction
- S3 ACLs
- Wildcard everywhere
- ...
- ...
- ...

Half-Life: Lambda Security

Half-Life: Lambda Security

Asset visibility & security

Half-Life: Lambda Security

```
pip3 install halflife
```

```
https://github.com/Skyscanner/halflife
```

Half-Life

- Takes Lambda function ARNs as input
- Maps event sources that trigger function execution
- Maps resources used by the function
- Tracks demographics (runtimes, regions, etc.)
- Checks Resource-based and Execution Role policies
- Checks event source policy and configuration
- Checks resource policy and configuration
- Optionally runs static code analysis on function source code (using SonarQube)
- Provides JSON and HTML reports

Running Half-Life

Made to run from CLI or as CRON

```

      `.::////:.`
    ./ossssssoosssso/.
  -oss/-`      .-/ssso-
`oss-` .++++:  -oss-`
`oss/   .//oss-   /sss`
+ss+    -sss.     /sso
.sss`    .ssso`    sss.   Half-Life: Lambda Security
-ssso    :ssoss+    oss-
.sss`    /ss+`oss/   sss.
+ss+    `oss/   .sss/// /sso
`oss/`.oso-    -ssso+./sso`
`+ssso:      .` -oss+`
  -ossst-`    .-+ssso-
    ./osssssssssso/.
      `.::////:.`

  UserId.....[REDACTED]
  Account.....[REDACTED]
  Arn.....arn:aws:iam::[REDACTED]

  Lambdas.....3
  Security.....19
  Triggers.....2
  Resources.....5
  Runtimes.....2
  Regions.....1
  Report.....halflife_output/report.html
```

Reporting

JSON

```
"runtimes": {  
  "count": 256,  
  "items": {  
    "python3.6": 199,  
    "python2.7": 17,  
    "nodejs8.10": 11,  
    "nodejs6.10": 13,  
    "nodejs4.3": 9,  
    "java8": 7  
  }  
},
```

```
"security": {  
  "count": 19,  
  "items": {  
    "info": 10,  
    "low": 4,  
    "high": 4,  
    "medium": 1  
  }  
}
```

Reporting

JSON

```
{
  "index": "3a4a0bce3e1a8103d987bdf268a929ac",
  "lambda": "arn:aws:lambda:eu-west-1:██████████:function:██████████",
  "where": "arn:aws:s3:::██████████\n\nhttp://██████████.s3.amazonaws.com\
",
  "level": "high",
  "text": "Public Bucket ACL: FULL_CONTROL access for Authenticated AWS users"
},
```

Reporting

JSON

```
"arn": "arn:aws:lambda:eu-west-1: [REDACTED] :function:[REDACTED]",
"name": "[REDACTED]",
"description": "",
"region": "eu-west-1",
"runtime": "python3.7",
"handler": "lambda_function.lambda_handler",
"codeURL": "https://awslambda-eu-west-1-tasks.s3.eu-west-1.amazonaws.com/snapshots/25[REDACTED]",
"role": "arn:aws:iam:: [REDACTED] :role/service-role/[REDACTED]",
"policy": {
  "function": {
    "Version": "2012-10-17",
    "Id": "default",
    "Statement": [
      {
        "Sid": "lambda-bf183417-a83e-49d0-a2fc-de6af7f61286",
        "Effect": "Allow",
        "Principal": {
          "Service": "s3.amazonaws.com"
        },
        "Action": "lambda:InvokeFunction",
        "Resource": "arn:aws:lambda:eu-west-1: [REDACTED] :function:[REDACTED]",
        "Condition": {
          "StringEquals": {
            "AWS:SourceAccount": "[REDACTED]"
          }
        }
      }
    ]
  }
}
```

Reporting

HTML

Half-Life

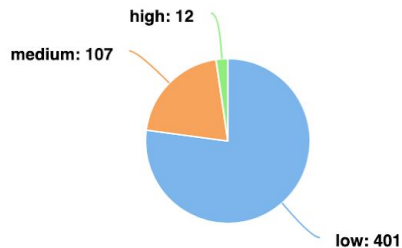


Statistics

Security

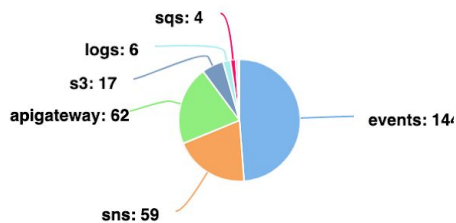
Functions

SECURITY (520)



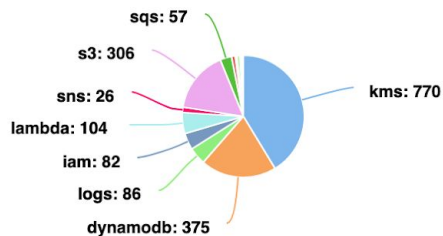
low	401
medium	107
high	12

TRIGGERS (295)



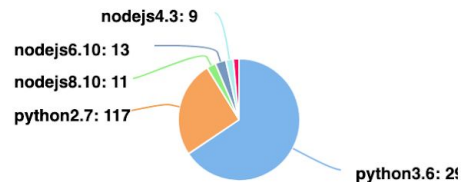
events	144
sns	59
apigateway	62
s3	17
logs	6
sqs	4
dynamodb	2

RESOURCES (1864)



kms	770
dynamodb	375
logs	86
iam	82
lambda	104
sns	26
s3	306

RUNTIMES (456)



python3.6	299
python2.7	117
nodejs8.10	11
nodejs6.10	13
nodejs4.3	9
java8	7

Reporting

HTML

Half-Life



Statistics

Security

Functions

high

Public Bucket ACL: FULL_CONTROL access for Authenticated AWS users

high

Service is publicly accessible due to unrestricted Principal and undefined Condition in Policy Statement Sid Stmt1551884083153 https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_principal.html

high

Hardcoded secrets can be abused to gain unauthorized access and compromise the security perimeter.
index.js on line 4.

medium

Objects are stored without encryption

Reporting

HTML

arn:aws:lambda:eu-west-1::[REDACTED] eu-west-1 python3.7

ARN arn:aws:lambda:eu-west-1::[REDACTED]

Name [REDACTED]

Description

Region eu-west-1

Runtime python3.7

Handler lambda_function.lambda_handler

Role arn:aws:iam::[REDACTED]:role/service-role/[REDACTED]

Triggers (2) s3, sqs

Resources (4) s3, ec2, ses, elasticloadbalancing

Security (7)

Level	Text	Where
high	Service is publicly accessible due to unrestricted Principal and undefined Condition in Policy Statement Sid Sid1553283872211 https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_principal.html	arn:aws:sqs:eu-west-1::[REDACTED] https://eu-west-1.queue.amazonaws.com/[REDACTED]
high	Public Bucket ACL: FULL_CONTROL access for Authenticated AWS users	arn:aws:s3:::[REDACTED] http://[REDACTED].s3.amazonaws.com

Improvements

- Analyze Lambda layers
- Identify third-party dependencies in code
- More rules and services
- Extend static code analysis with more rules and potentially other scanning engines
- HTML reporting
- Extend vulnerability descriptions
- Fix bugs
- ...

Thank you.

Artëm Tsvetkov • SENIOR SECURITY ENGINEER, SKYSCANNER

