

# ADD0

## ALL DAY DEVOPS

NOVEMBER 6, 2019

Reliable and Automated  
Cloud Native Security  
Operations

Akash Mahajan

APPSECCO



ADD0  
ALL DAY DEVOPS

**ADD0**  
ALL DAY DEVOPS



**TRACK:**  
**DEVSECOPS**

**AKASH MAHAJAN**



**Reliable and Automated  
Cloud Native Security  
Operations**

**NOV. 6, 2019**  
**24 HOURS**  
**5 TRACKS**  
**150 SESSIONS**  
**FREE • ONLINE**  
**ALLDAYDEVOPS.COM**

# Akash Mahajan – About Me

- Co-Founder of Appsecco (appsecco.com)
- Co-Founder of null.co.in – India's largest open security community
- Speaker at ADDO twice
- Cool fact – I had one of my talks featured in FeedbackLoops 😊
- Author of Security Books
  - Burp Suite Essentials
  - Security Automation using Ansible2
- Security Trainer c0c0n, nullcon, BlackHat US



# Agenda for the next 20 minutes

1. Briefly describe what is reliable, automated & cloud native
2. Make a strong case for why unintentional public S3 buckets are bad for security
3. Demo – A security response against public S3 buckets
4. Elaborate on why we want reliability
5. Conclusion on why cloud native SecOps
6. A simplified client case study – If we have time remaining

# Disclaimer

- There are many-many ways to meet our security objectives.
  - From my experience for the cloud native workloads, Security Operations need to be cloud native
- Some of the audience of this conference may think that I am preaching to the choir
  - I feel that there is still a lot of merit in discussing specific use cases and drive home this point
- I have security expertise, not running large scale prod systems expertise
  - That is what all of you viewers bring to the table

# Words and What I mean

Num	Word	What I mean
1.	Reliable	Our system will work without fail and with minimal MTTR
2.	Automated	Work done which has removed toil. Removed repetition, reduces human error and will scale as per the need
3.	Cloud Native	Leveraging services of that specific public IaaS cloud (AWS)
4.	Security	Specifically related to operational security. Runtime once deployed to production



# A hacker gained access to 100 million Capital One credit card applications and accounts

540 Mllion Facebook Records Leaked by Public Amazon S3 Buckets

GoDaddy Leaks 'Map of the Internet' via Amazon S3 Cloud Bucket Misconfig

198 million Americans hit by 'largest ever' voter records leak

Personal data on 198 million voters, including analytics data that suggests who a person is likely to vote for and why, was stored on an unsecured Amazon server.

Dow Jones Data Leak Results from an AWS Configuration Error

Security pros expect to see more incidents like the Dow Jones leak, which exposed customers' personal information following a public cloud configuration error.

Defense contractor stored intelligence data in Amazon cloud unprotected [Updated]

Booz Allen Hamilton engineer posted geospatial intelligence to Amazon S3 bucket.

Accenture left a huge trove of highly sensitive data on exposed servers

Data on 150,000 patients exposed in another misconfigured AWS bucket

Patient Home Monitoring failed to lock down public access to its online server, exposing personal data of 150,000 patients.

Verizon partner data breach exposes millions of customer records

Accessed through an unprotected Amazon S3 storage server

# Not just an alarming news headline

**GRAYHAT WARFARE**  
cause white is boring

Home Buckets Files API Top Packages Contact Us

Files 358 of 952 million (?)

Buckets 84942 of 217279 (?)

Last Update 08-September-2019

A website that  
downloads files from  
public S3 buckets

Access to data for  
free or 20 Euros per  
month!

Free	Registered	Premium
No account	Registered account	Registered
Free	Free	€20.00/month
<ul style="list-style-type: none"><li>✗ Search in: 357 million files</li><li>✓ Max Number of Files in Listing: 500</li><li>✓ Max number of Buckets in Listing: 1000</li><li>✓ Short Filename matching (Only filename - no directory): Searching for <b>Metallica</b> will return: ✓ (http://....amazonaws.com/files/<b>Metallica</b> - Outlaw Torn.mp3) But will not return: ✗</li></ul>	<ul style="list-style-type: none"><li>✗ Search in: 357 million files</li><li>✓ Max Number of Files in Listing: 1000</li><li>✓ Max number of Buckets in Listing: 2000</li><li>✓ Short Filename matching (Only filename - no directory): Searching for <b>Metallica</b> will return: ✓ (http://....amazonaws.com/files/<b>Metallica</b> - Outlaw Torn.mp3) But will not return: ✗</li></ul>	<ul style="list-style-type: none"><li>✓ Search in: 951 million files</li><li>✓ Max Number of Files in Listing: Unlimited</li><li>✓ Max number of Buckets in Listing: Unlimited</li><li>✓ Full Filename matching (Filename + Directory): Searching for <b>Metallica</b> will return both: ✓ (http://....amazonaws.com/files/<b>Metallica</b> - Outlaw Torn.mp3)</li></ul>



### 3 Steps to finding our public S3 buckets & securing them

1. List S3 buckets which are public in an AWS account
2. Remediate this security misconfiguration using automation
3. I lied, only two steps as once we have remediated, we can go back and list the buckets again 😎 😊

# Demo - Step 1 – Listing Public Buckets using Slurp



**ADDO**  
ALL DAY DEVOPS



TRACK:  
DEVSECOPS

APPSECCO

**AKASH MAHAJAN**



Reliable and Automated  
Cloud Native Security  
Operations

NOV. 6, 2019  
**24 HOURS**  
**5 TRACKS**  
**150 SESSIONS**  
FREE • ONLINE  
**ALLDAYDEVOPS.COM**



# Demo – Step 1 - Confirming the contents of the public buckets



**ADDO**  
ALL DAY DEVOPS



TRACK:  
DEVSECOPS

APPSECCO

**AKASH MAHAJAN**



Reliable and Automated  
Cloud Native Security  
Operations

NOV. 6, 2019

**24 HOURS**

**5 TRACKS**

**150 SESSIONS**



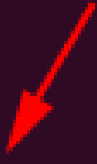
FREE • ONLINE

**ALLDAYDEVOPS.COM**



## Demo – Step 2 – Remediation for public buckets

**filters:**

- **type:** global-grants
- **type:** value
  - key:** "tag:createdby" 
  - value:** "automation"
- **not:** 
  - **type:** value
    - key:** "tag:type" 
    - value:** "static-site"

**ADDO**  
ALL DAY DEVOPS



TRACK:  
DEVSECOPS

APPSECCO

**AKASH MAHAJAN**



Reliable and Automated  
Cloud Native Security  
Operations

NOV. 6, 2019  
**24 HOURS**  
**5 TRACKS**  
**150 SESSIONS**  
FREE • ONLINE  
**ALLDAYDEVOPS.COM**





# Demo – Step 3 – Confirming it worked for us



**ADDO**  
ALL DAY DEVOPS



TRACK:  
DEVSECOPS

APPSECCO

**AKASH MAHAJAN**



Reliable and Automated  
Cloud Native Security  
Operations

NOV. 6, 2019

**24 HOURS**

**5 TRACKS**

**150 SESSIONS**

FREE • ONLINE

**ALLDAYDEVOPS.COM**



# Why do we want reliability?

- Security choices will be made based on output of service that we automated for discovery of buckets
- The service will become the primary interface, SecOps team members will be trained to respond to this instead of manual discovery.
  - Over time this will become the way
- Beyond a certain scale, only automation will ensure timely coverage

# Why become Cloud Native for our security operations?

*Small agile teams can focus on creating and fulfilling business aligned security objectives and key results instead of managing the infrastructure around it*

# Secure Operations for our Cloud Native Security Operations

- Focus on solving issues that matter to business first
  - One less server is one less target for attackers
- Infra as code, configuration managed as code
  - Secure defaults backed in
- Automation to some extent is inherent
  - Newer security features can be rolled out
- Scale our scope

## Challenges that you may face

- Major reskilling, capability building, and capacity building required
- Compliance, legal challenges around data, privacy etc.
- Already existing security costs in software, hardware and training – (anchoring bias, sunken cost)

# What we would like to achieve from SecOps PoV

- Bring in near real time detection and blocking of security attacks
- Analyse incidents quickly and with automation
- Remediate potential security holes before they become a problem



## A client case study

1. Developers create public buckets all the time
2. While awareness and security training is on-going (enforcement), this automated monitoring is finding public buckets daily
3. Public bucket which violate the tagging policy reported as security issues (via API) to their vulnerability management dashboard
4. Even though there is a gap in finding reported and remediation, the team has real data now.
5. *This makes it easy for the secops to have relevant conversations with the team members*

# Any Questions or thoughts?

Akash Mahajan | [akash@appsecco.com](mailto:akash@appsecco.com) | [@makash](https://twitter.com/makash)

## APPSECCO