DevSecOps
Cloud-Native

BROUGHT TO YOU BY
CODESHIELD.IO

DR. JOHANNES SPÄTH
CEO

TRANSYLVANIA CLOUD
2021

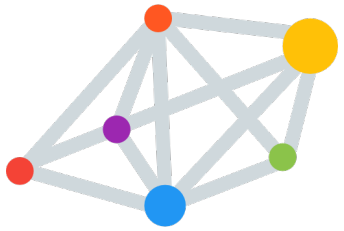
Security in the Cloud

01 RECENT BREACHES

02 WHO IS RESPONSIBLE?

03 WHAT SHOULD WE DO?

04 WHAT CAN WE DO?



200+ Cloud-Resources

"To understand security, we need to consider the big picture, i.e., the full application stack."

About Me

Johannes Späth, PhD

Co-Founder of CodeShield

Fraunhofer — 5+ years experience in applied research (IT-Security & program analysis / SAST)

ORACLE — Research Intern 2016, Brisbane, Australia

HEINZ NIXDORF INSTITUT UNIVERSITÄT PADERBORN — PhD in Computer Science

aws — AWS Community Builder 2021

01 SECURITY IN THE CLOUD RECENT BREACHES

01 Recent Cloud-Security Breaches

BHIM 04/2020

personal and payment information of 7 Mio. were exposed, due to a misconfigured S3 bucket.

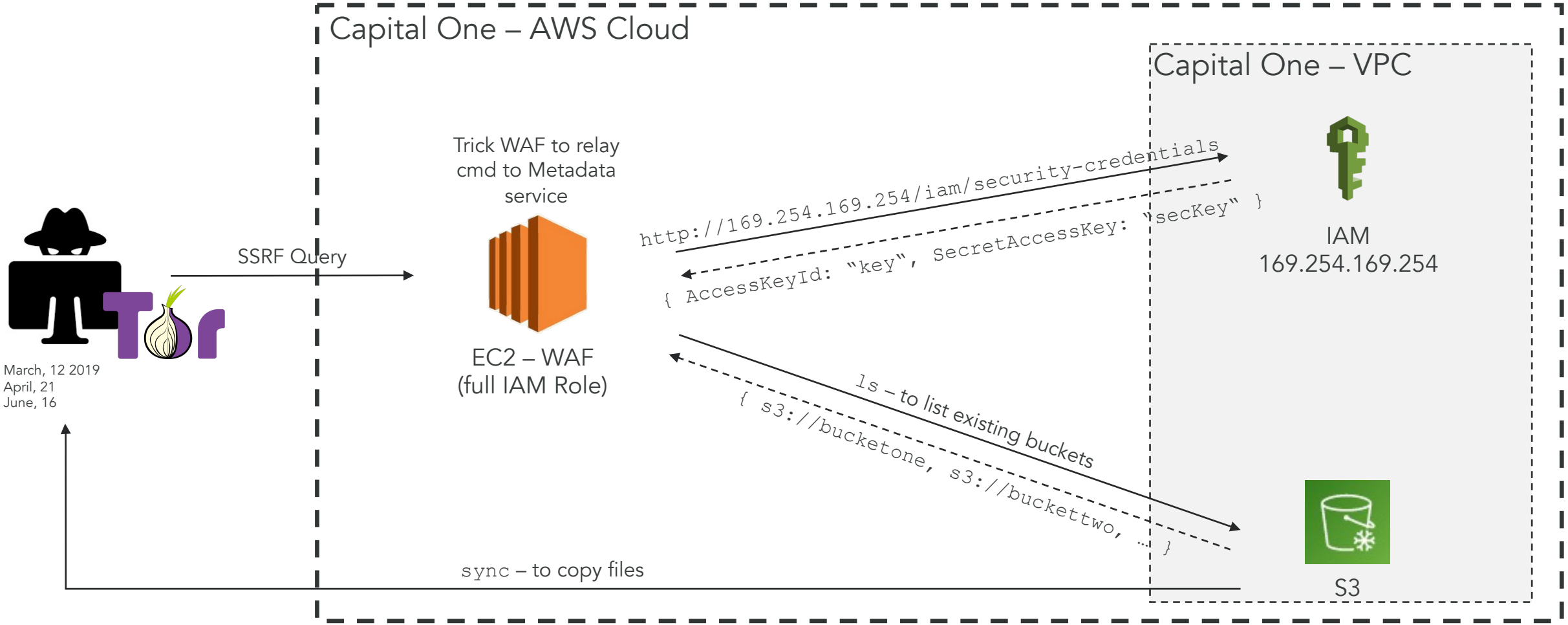
AutoClerk 10/2019

personal data of thousands of hotel guests and members of the US government, military exposed, due to an open elasticsearch database.

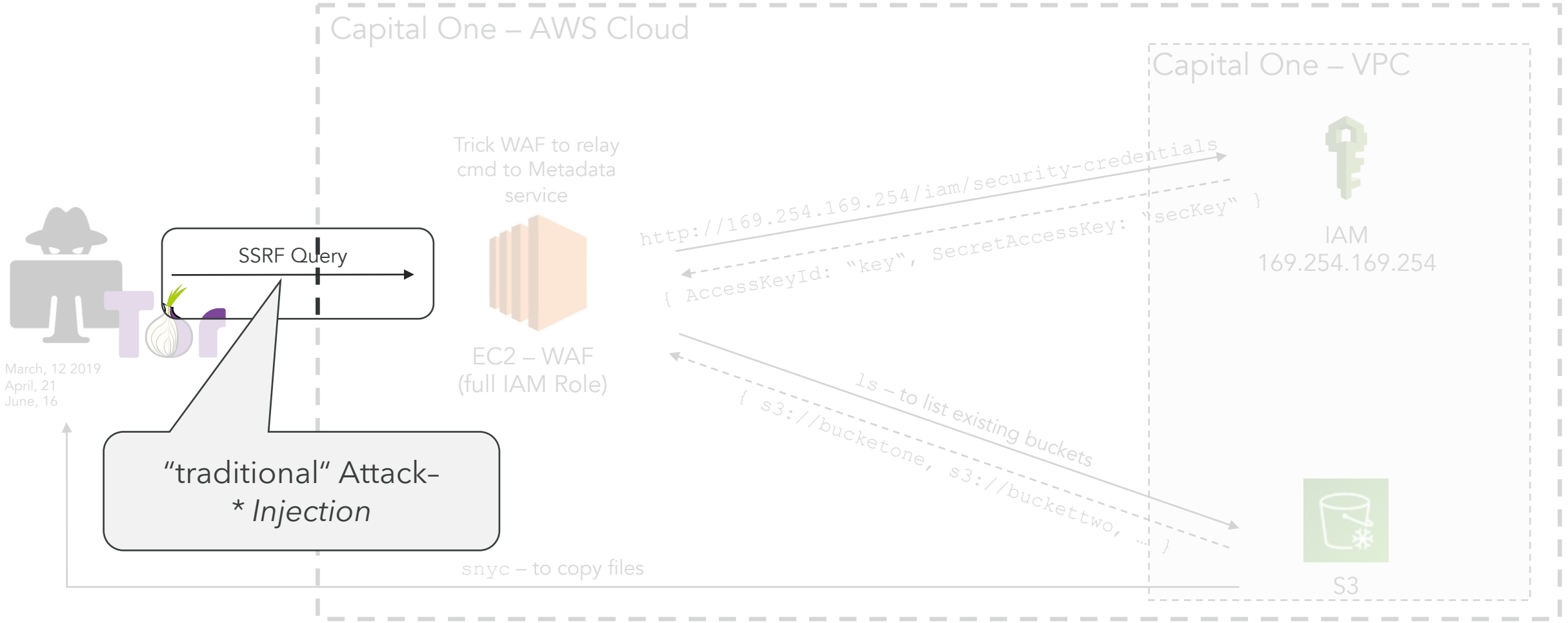
CAPITAL ONE 07/2019

80,000 account numbers, 140,000 Social Security numbers, 1 million Canadian Social Insurance Numbers exposed, due to a Server-Side-Request Forgery attack.

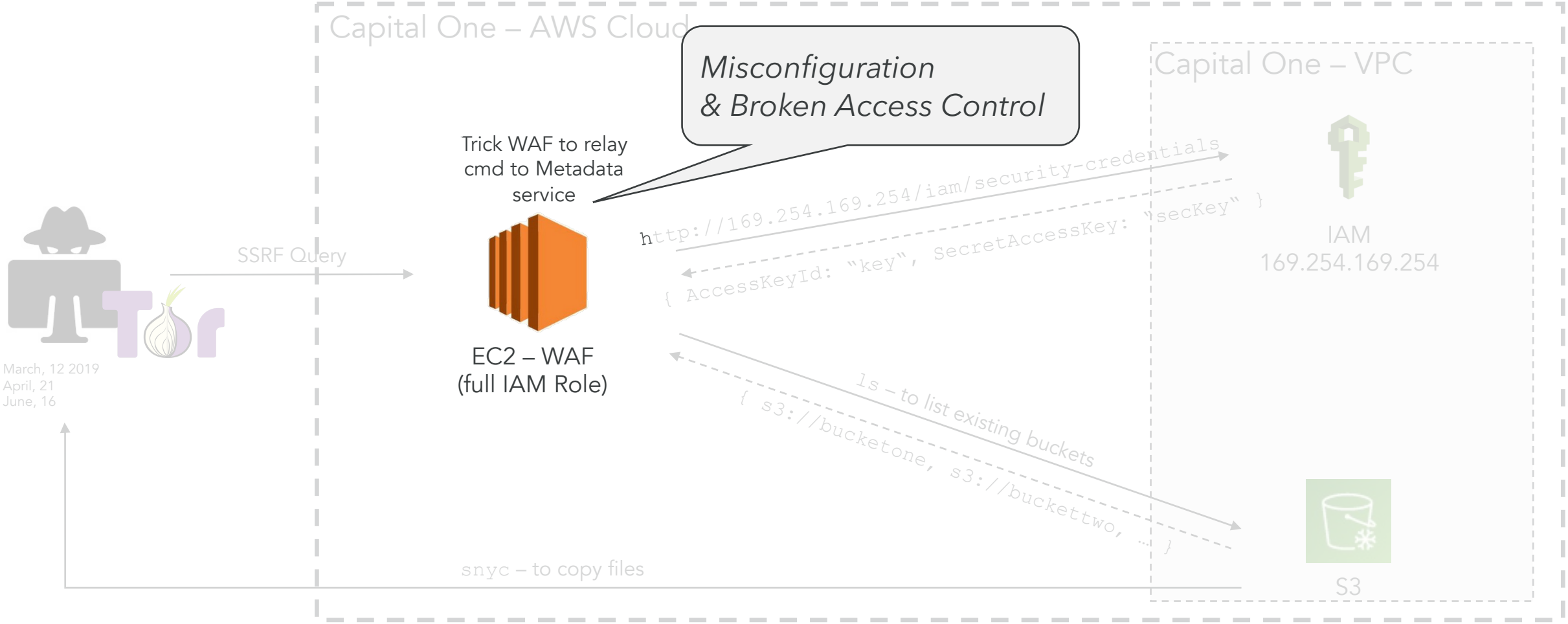
01 Capital One Hack - What happened?



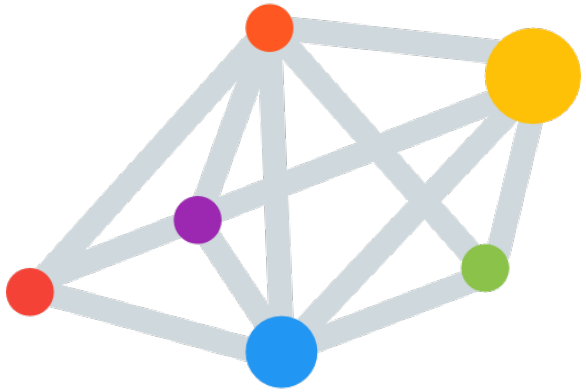
01 Capital One Hack - What happened?



01 Capital One Hack – What happened?



01 Capital One Hack – Lessons Learned



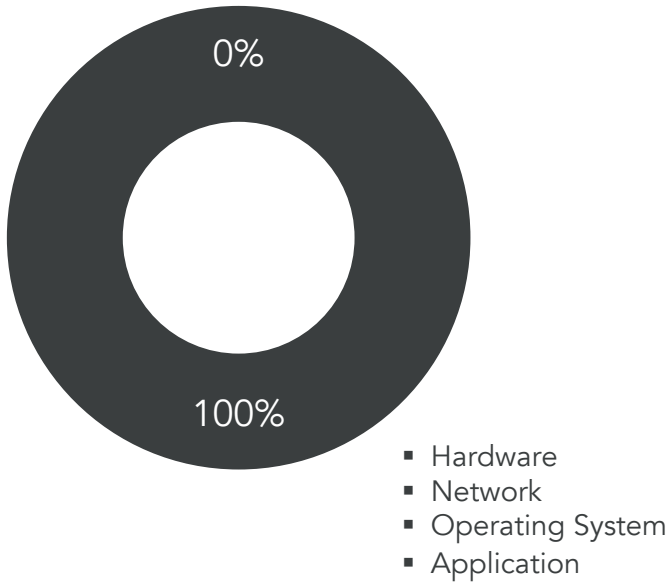
Security must be considered across all components

02 SECURITY IN THE CLOUD WHO IS RESPONSIBLE?

02 „Shared Responsibilty“ Security Model

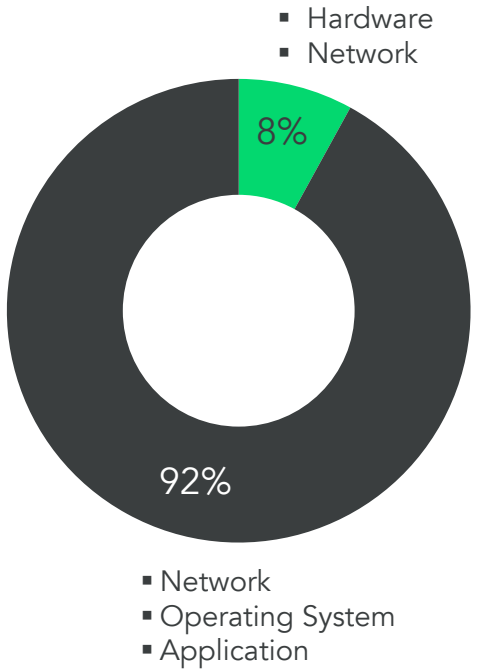
2010

Self-Hosted



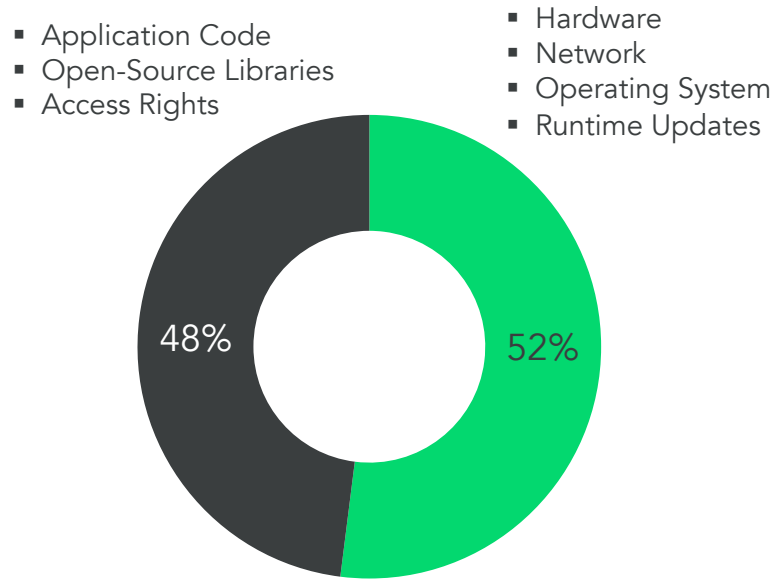
2015

Cloud-Hosted



2020

Cloud-Native

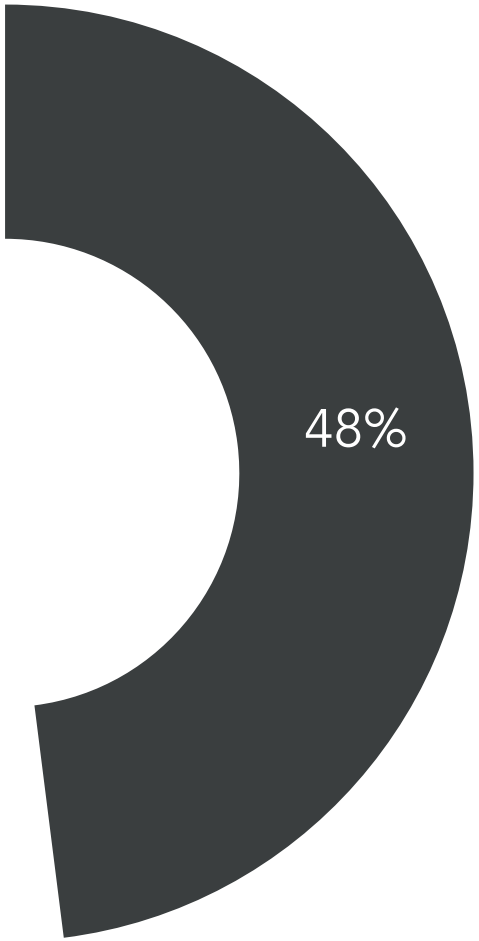


Software Provider‘s Responsibility

Cloud Provider‘s Responsibility

https://securityboulevard.com/2019/01/serverless-and-the-evolution-in-cloud-security-how-faas-differs-from-iaas/

02 Cloud-Native Application



Infrastructure-as-Code

Detect data-flows in architecture and misconfiguration in infrastructure

Open-Source Dependencies

Detect known CVEs in unknown Code

Application / Lambda / "Function" Code

Detect unknown vulnerabilities in own code

03 SECURITY IN THE CLOUD
WHAT SHOULD WE DO?

2010

Self-Hosted

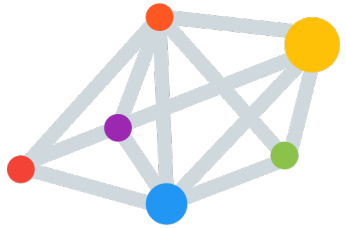
Monolith

1-3 Components

2020

Cloud-Native

Everything-as-Function



200+ Cloud-Resources

03 Security Audit

2010

Self-Hosted

Monolith

1-3 Components

01 Is the software documented?

02 What is the general architecture of the software?

03 Which assets does your software process?

04 Which sensitive data does your software handle?

05 Which security mechanisms are in place?

06 Is the infrastructure correctly configured?

07 Does the code contain existing vulnerabilities (CVEs)?

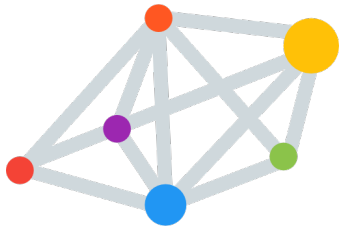
08 Is the custom code written in a secure manner?

03 Security Audit

2020

Cloud-Native

Everything-as-Function



200+ Cloud-Resources

01 Is the software documented?

02 What is the general architecture of the software?

03 Which assets does your software process?

04 Which sensitive data does your software handle?

05 Which security mechanisms are in place?

06 Is the infrastructure correctly configured?

07 Does the code contain existing vulnerabilities (CVEs)?

08 Is the custom code written in a secure manner?

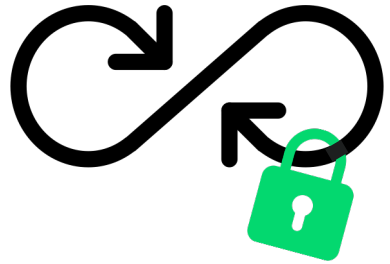
04 SECURITY IN THE CLOUD
WHAT CAN WE DO?

04 „Shift Left“

DevOps

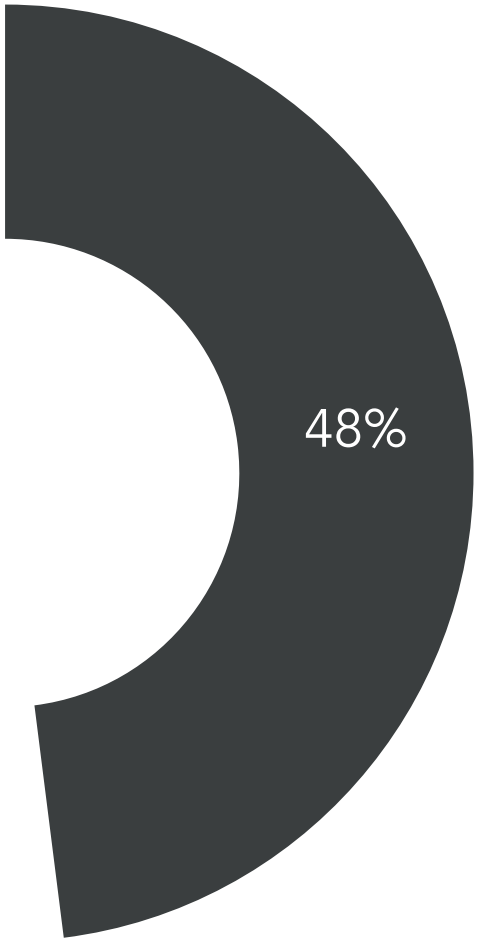
- Continous Testing
- Continous Delivery
- Continous Deployment

DevSecOps



- Continous Security
  - Static Application Security Testing
  - Software Composition Analysis
  - Infrastructure-as-Code Security Testing

04 DevSecOps Solution Space



Infrastructure-as-Code

Infrastructure-as-Code Security Testing

LambdaGuard bc KICS ...

Open-Source Dependencies

Software Composition Analysis

DEPENDENCY-TRACK WhiteSource snyk ...

Application / Lambda / "Function" Code

Static Application Security Testing

Fortify coverity sonarqube ...

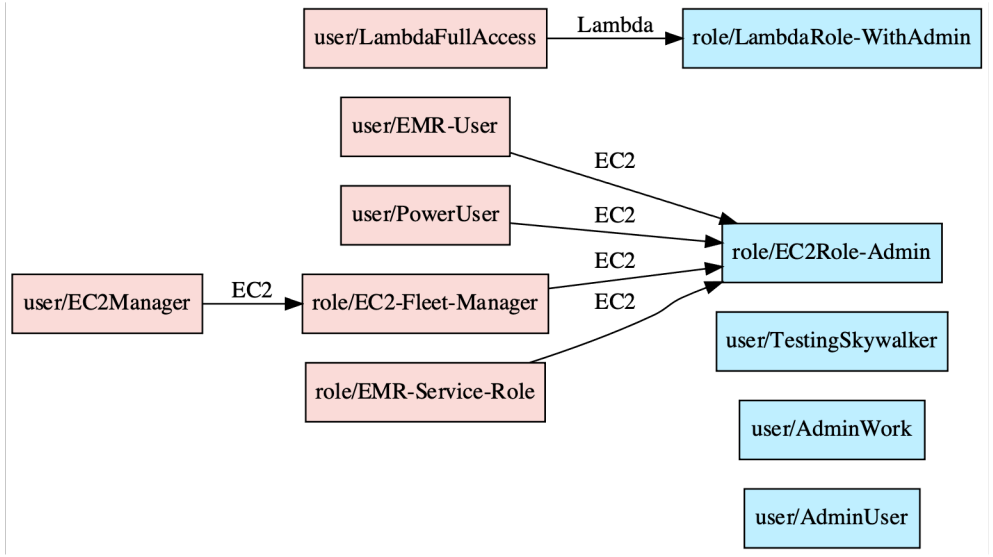
04 Principal Mapper

Benefits

- Visualizes IAM and AWS Identities as Graph
- Detects Privilege Escalation
- Detects Identity Misconfiguration

Shortcomings

- No Fix Recommendations
- No Code-Level Analysis

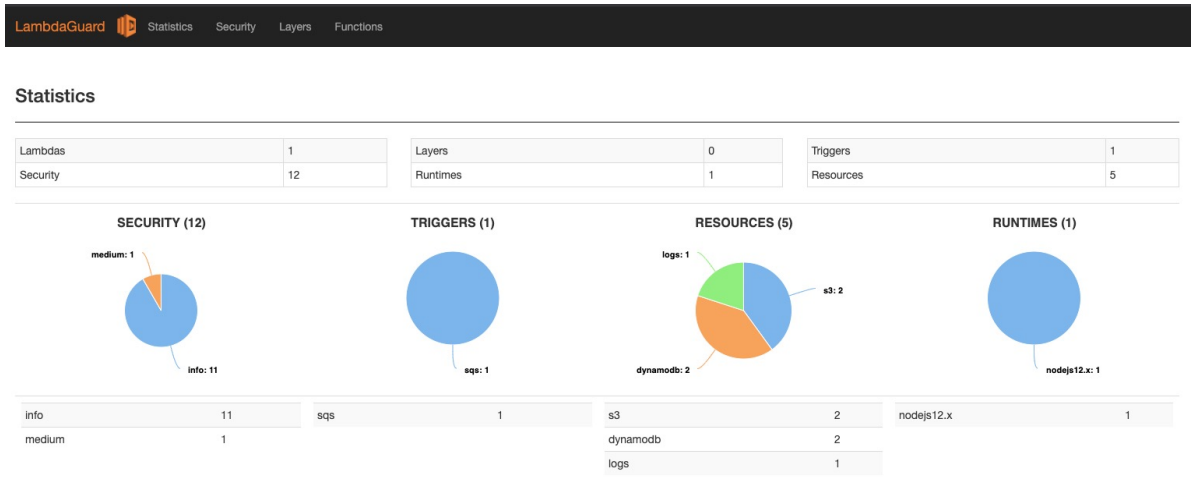


GitHub https://github.com/nccgroup/PMapper

04 LambdaGuard

Benefits

- Inspects CloudFormation Templates
- Displays triggers & resources
- Potential security issues
  (based on CloudFormation Template)

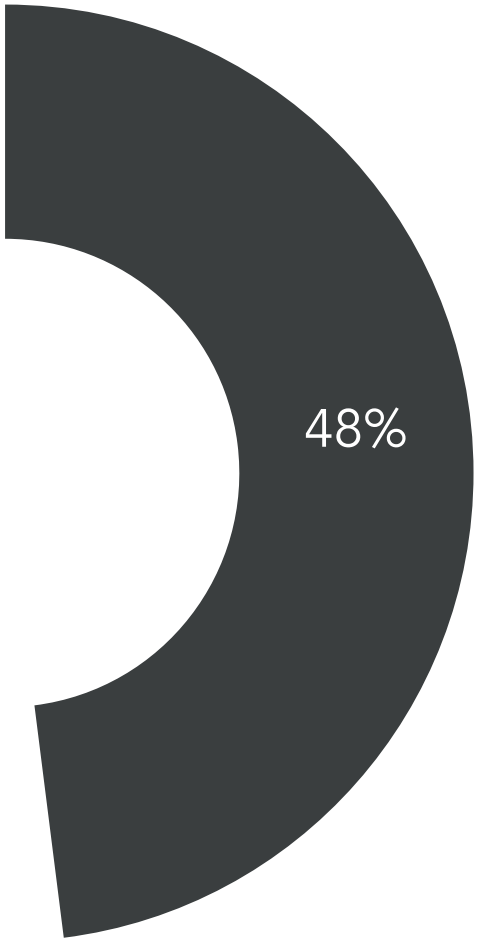


Shortcomings

- Views Resources individually
- „Big Picture“ Missing
- No Code Analysis

GitHub https://github.com/Skyscanner/LambdaGuard

04 DevSecOps Solution Space



Infrastructure-as-Code

Infrastructure-as-Code Security Testing

LambdaGuard bc KICS ...

Open-Source Dependencies

Software Composition Analysis

DEPENDENCY-TRACK WhiteSource snyk ...

Application / Lambda / "Function" Code

Static Application Security Testing

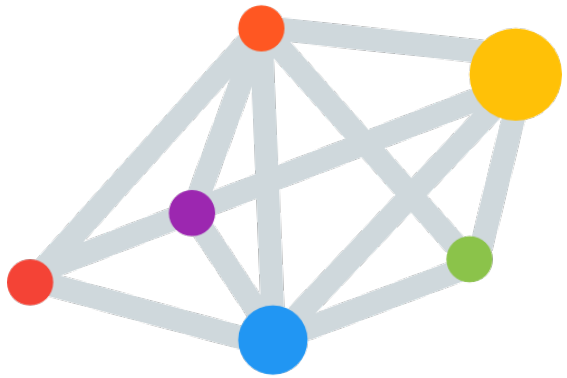
Fortify coverity sonarqube ...

Tools **miss the big picture** and produce irrelevant results (False Positives / False Negatives)

04 Provides the „Big Picture“, dives down to Details

code_shield

- Connect your Git Repositories
- Connect your AWS Account
- Visualizes infrastructure data-flows based on CloudFormation Template
- Detects security vulnerabilities
  - Least privilege (IaC + SAST)
  - SCA results with prioritization



04 “Everything-as-Code”

Cloud-Native Application

Task for Security

Infrastructure-as-Code

Ease of Attack: Easy

Detect data-flows and misconfiguration in architecture

Graph Visualization + IaC-Analysis

Manuel Benz
M.Sc. IT-Security
4+ yrs research

Open-Source Code

Ease of Attack: Medium

Detect known CVEs in unknown Code

Bytecode Analysis + “Fingerprinting”

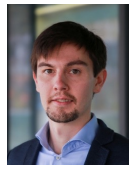
Andreas Dann
M.Sc. Computer Science
4+ yrs research

Application Code

Ease of Attack: Difficult

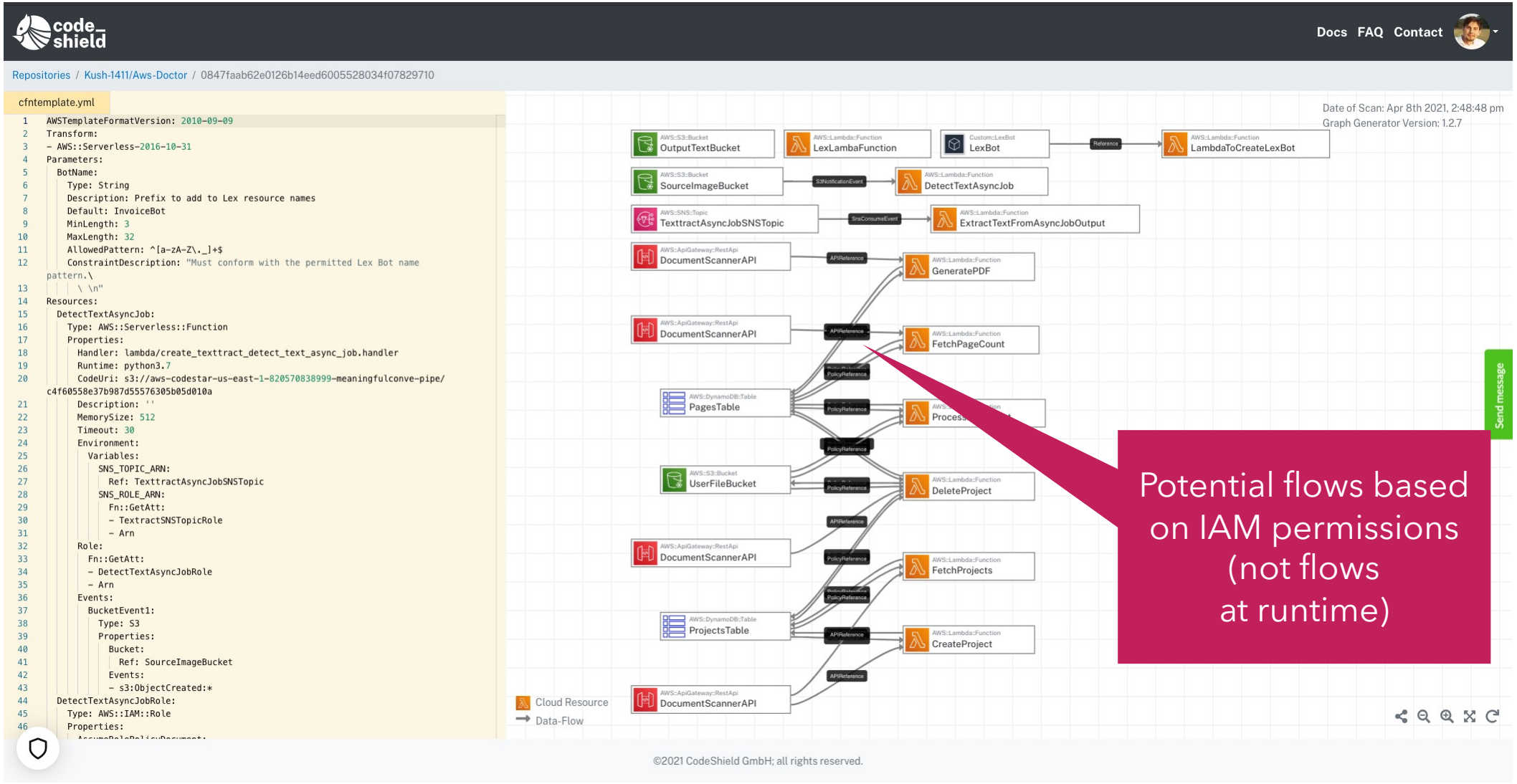
Detect unknown vulnerabilities in known code

Precise & Efficient Data-Flow Engine

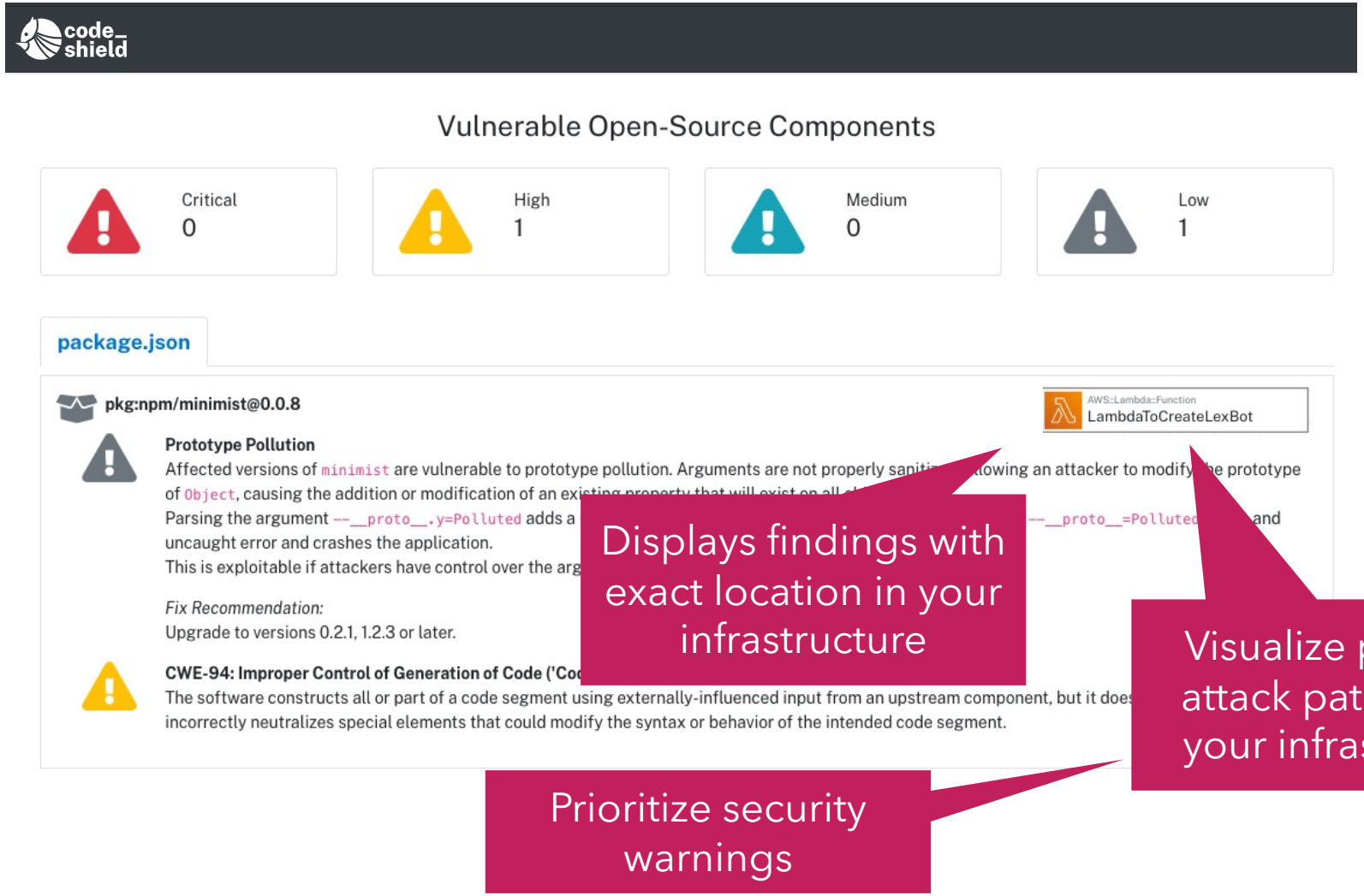


Johannes Späth
PhD Computer Science
5+ yrs research

04 Architecture Overview



04 Reachability Analysis for Software Composition Analysis



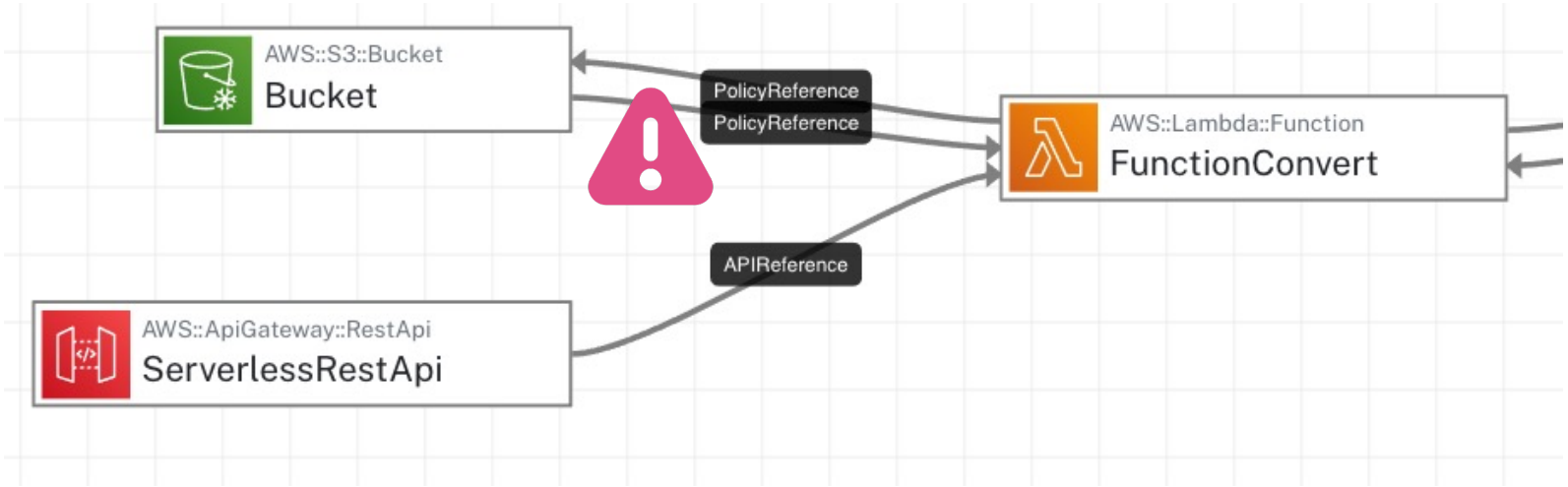
04 Combining SAST + IaC: Violation of Least Privilege

CloudFormation

```
Policies:
  - DynamoDBCrudPolicy:
      TableName: !Ref Table
  - S3FullAccessPolicy:
      BucketName: !Ref Bucket
```

Lambda's Source Code

```
s3Client.putObject(
        new PutObjectRequest(System.getenv("BUCKET_NAME"), key, txt,
objectMetadata)
                .withCannedAcl(CannedAccessControlList.PublicRead));
```



Book a Demo!

Dr. Johannes Späth
CEO & Co-Founder

johannes.spaeth@codeshield.io

Technologiepark 8, 33100 Paderborn