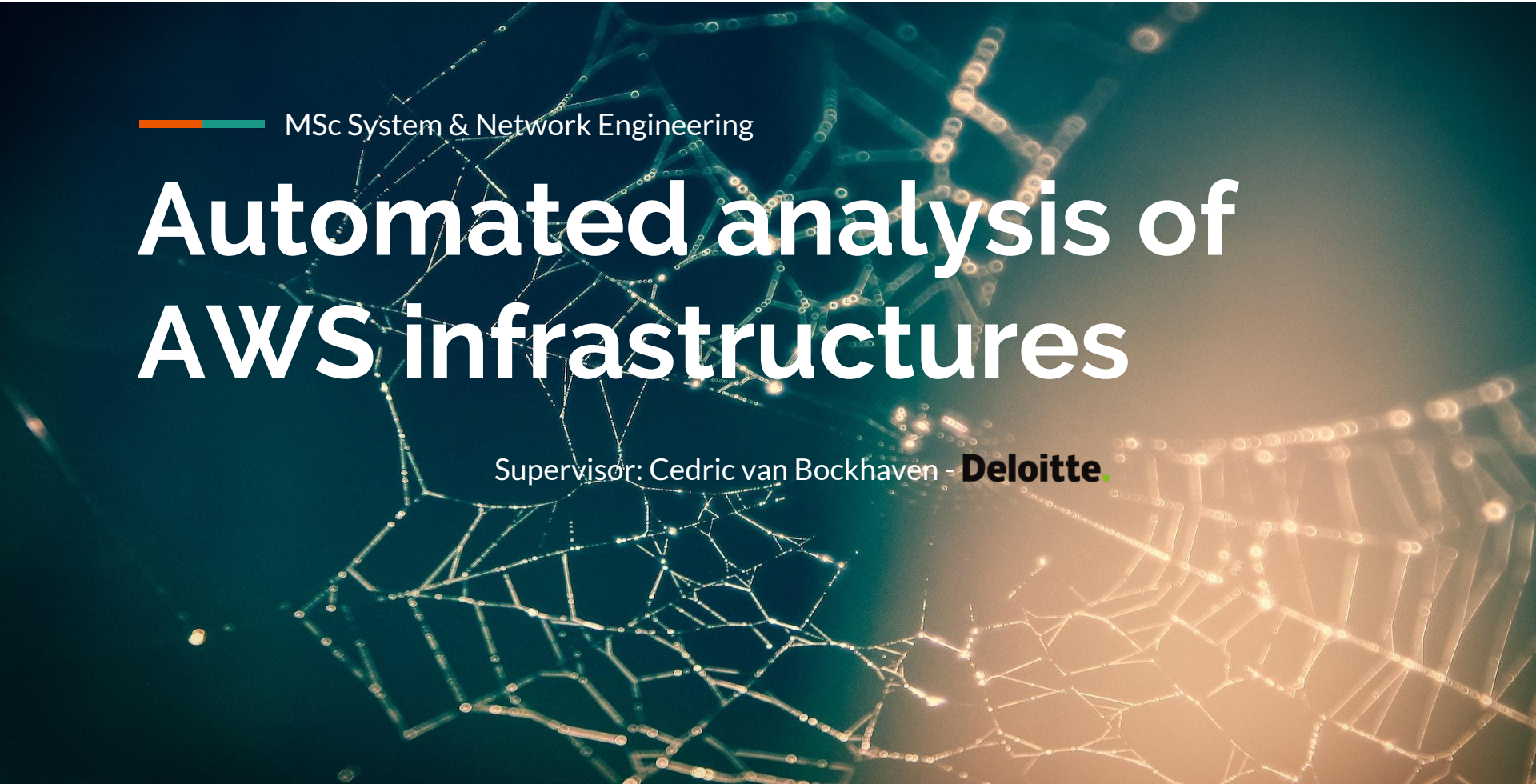


MSc System & Network Engineering

Automated analysis of AWS infrastructures

Supervisor: Cedric van Bockhaven - Deloitte.

Background

"... a secure cloud services platform, offering compute power, database storage, content delivery and other functionality …"

Background

EC2 (Elastic Compute Cloud)

RDS (Relational Database Service)

S3 (Simple Storage Service)

Background

VPC

Security groups

IAM

Background

VPC

Security groups

IAM

Background

IAM

- Access keys
- Policies
- Users
- Groups
- Roles

Background

IAM > Policies

- Effect (Allow/Deny)
- Action
- Resource

Introduction

- You've infiltrated an AWS infrastructure, **now what?**
- Expanding access
- Knowledge of inaccessible components
- Visualization

Background

Bloodhound

Active Directory

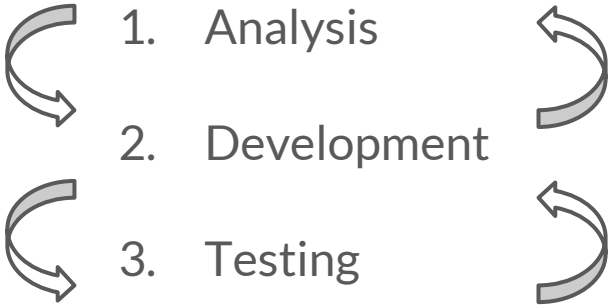
Research question

Given an infiltrated AWS component, what part of the related infrastructure would an automated tool be able to index?

Methodology

1. Analysis
2. Development
3. Testing

Methodology



Analysis

IAM

- Resource-level permissions
  - *:Describe*
  - *:List*

Background

IAM > Policies

- Effect (Allow/Deny)
- Action
- Resource

Analysis

IAM

- Resource-level permissions
  - *:Describe*
  - *:List*

Analysis

Metadata server

- EC2
- 169.254.169.254

Functionality

Metadata crawler

Captures everything on the metadata server…

… including security credentials

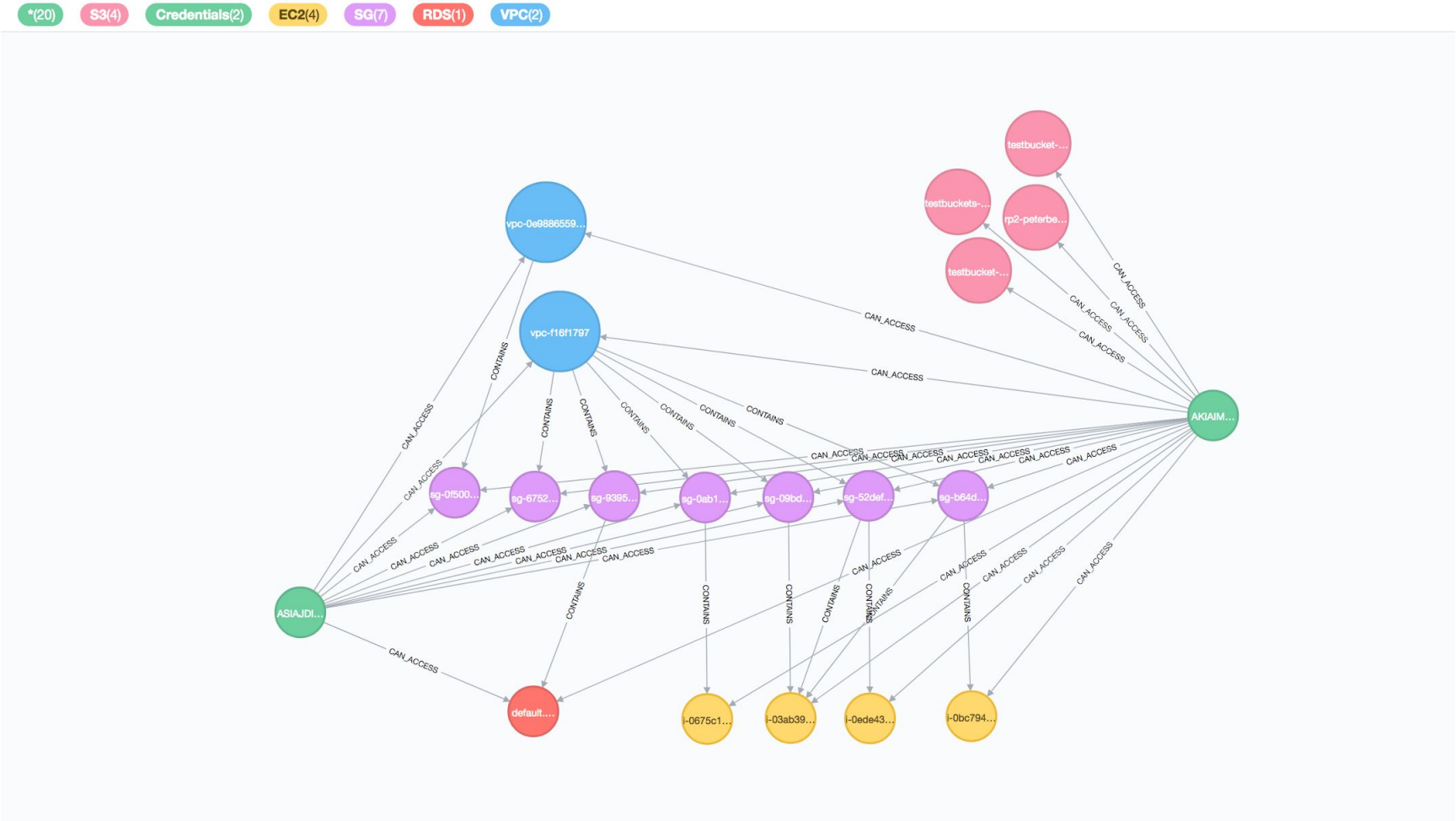
Functionality

Permission bruteforcer

Checks what commands access keys can use

Infrastructure analyser

Uses access of key(s) to create mapping of infrastructure


*(20)
S3(4)
Credentials(2)
EC2(4)
SG(7)
RDS(1)
VPC(2)
testbucket-...
testbuckets-...
rp2-peterbe...
testbucket-...
vpc-0e9886559...
vpc-f16f1797
AKIAIM...
sg-0f500...
sg-6752...
sg-9395...
sg-0ab1...
sg-09bd...
sg-52def...
sg-b64d...
ASIAJDI...
default....
i-0675c1...
i-03ab39...
i-0ede43...
i-0bc794...
CAN_ACCESS
CONTAINS

Development

- Neo4j
- boto3
- py2neo

Conclusion

- Very useful for expanding access & escalating privilege
- Resource-level permissions
- Diversity of keys more important than privilege in terms of enumeration

Discussion/Future work

Expandable in an infinite number of ways

- Linkurious (visualization)

Discussion/Future work

Expandable in an infinite number of ways

Discussion/Future work

- Linkurious (visualization)
- STS

Expandable in an infinite number of ways

Discussion/Future work

- Linkurious (visualization)
- STS
  - More AWS services/commands

Expandable in an infinite number of ways

Discussion/Future work

Expandable in an infinite number of ways

- Linkurious (visualization)
- STS
  - More AWS services/commands
- Automated infiltration

Discussion/Future work

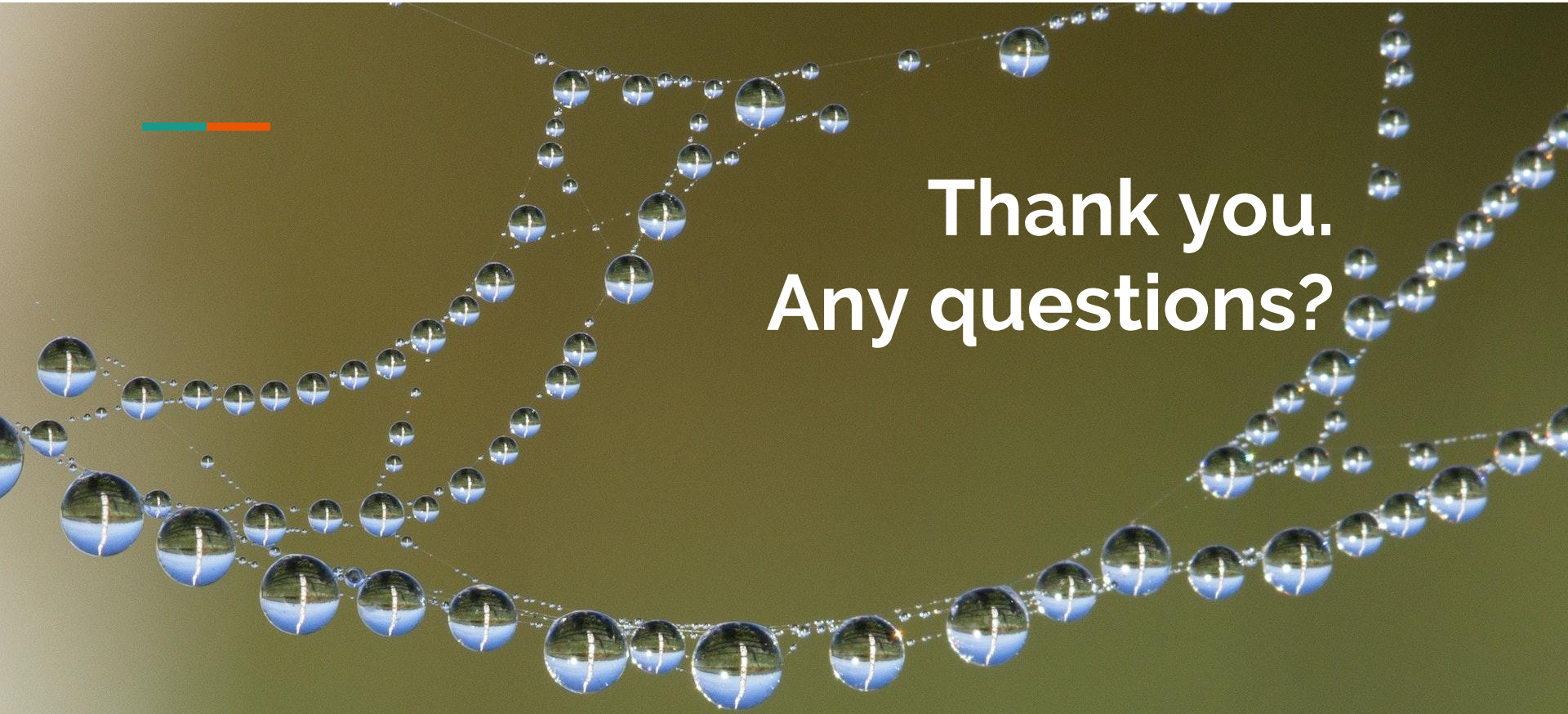
Expandable in an infinite number of ways

- Linkurious (visualization)
- STS
  - More AWS services/commands
- Automated infiltration
- Nmapping subnets

Discussion/Future work

Expandable in an infinite number of ways

- Linkurious (visualization)
- STS
  - More AWS services/commands
- Automated infiltration
- Nmapping subnets
- Resource-level permission bruteforcer



Thank you.
Any questions?

https://gitlab.com/PeterBennink/aws-infrastructure-analysis