Security for Cloud-Native Applications

BROUGHT TO YOU BY
CODESHIELD.IO

Andreas Dann

AWS User Group
Cologne 2022

About Me

Andreas Dann

HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN
Fraunhofer

4+ years research
(IT-Security, program analysis, SCA)

SAP

Research Intern 2019
Mougins, France

code_shield

Co-Founder 2020
Paderborn

AWS community builders

AWS Community Builder 2021
in the security track

Soot

Maintainer static analysis framework

Contributor to Eclipse Steady

Cloud-Native Security

01 CLOUD SECURITY BREACHES – Capital One Hack

02 LATERAL MOVEMENTS IN THE CLOUD – IAM Privilege Escalation

03 WHAT CAN WE DO – Checklist

01 SECURITY IN THE CLOUD PROMINENT BREACHES

01 Prominent Cloud Breaches

BHIM 04/2020

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

AutoClerk 10/2019

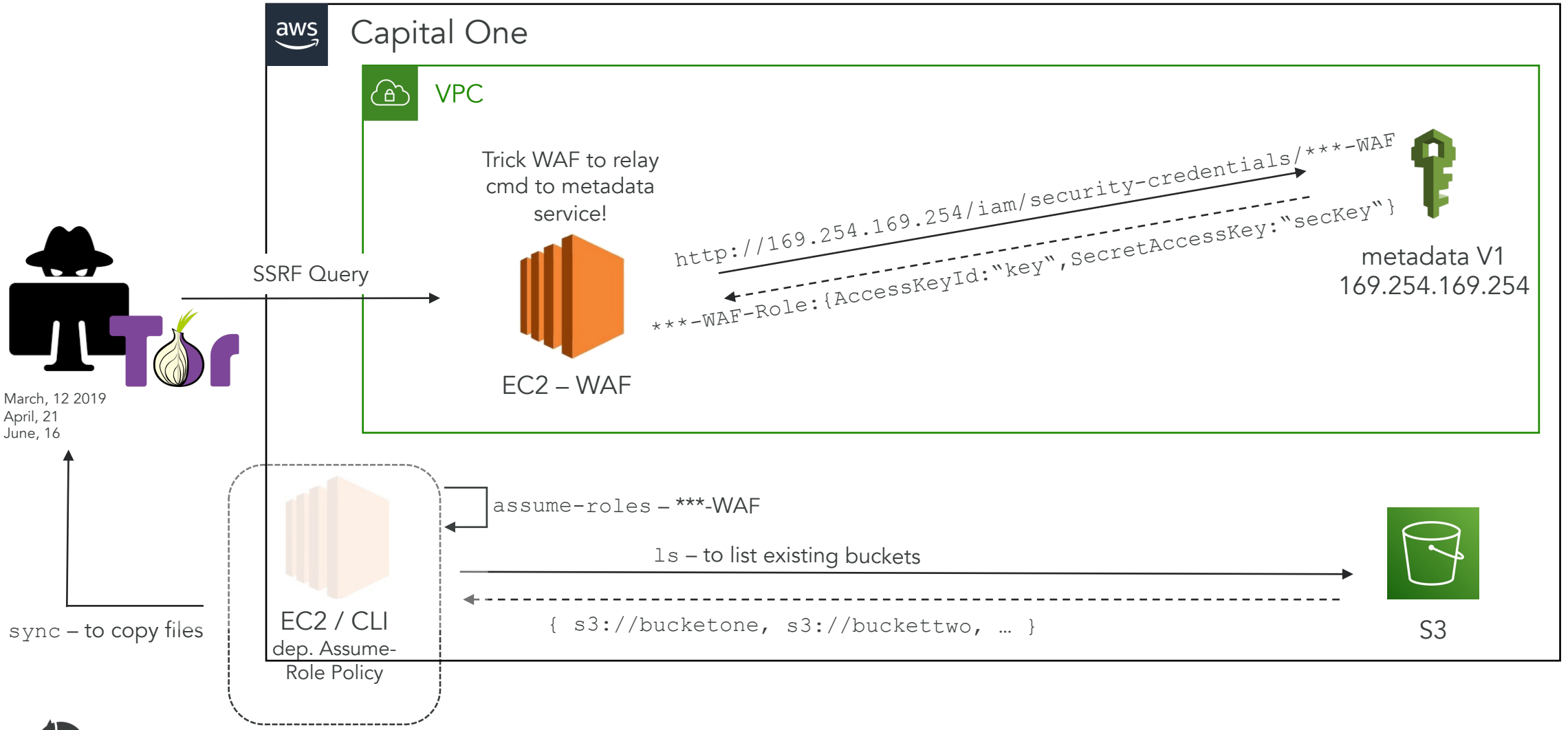
personal data of thousands of hotel guests and members of the US government, military exposed, due to an open elasticsearch database.

CAPITAL ONE 07/2019

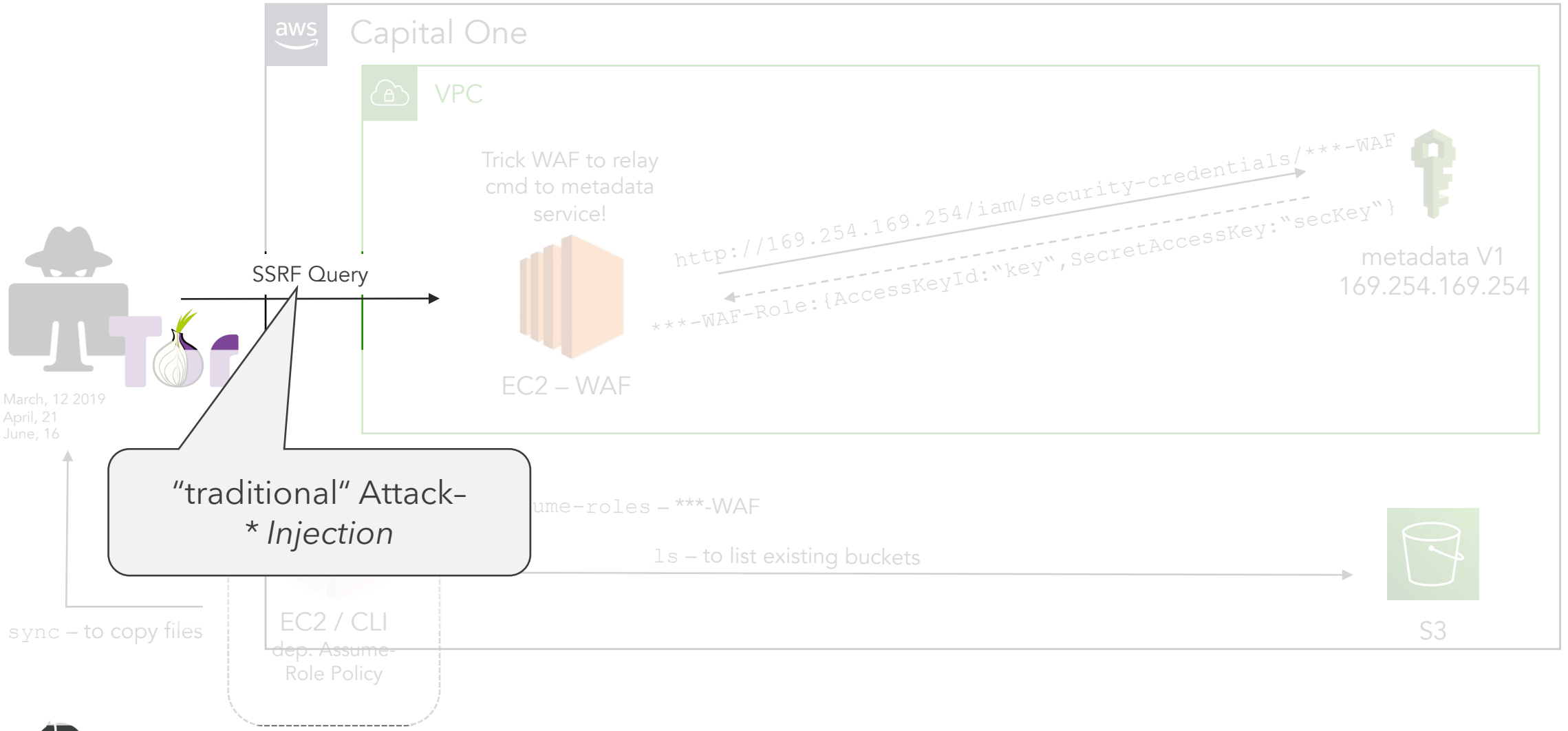
80,000 account numbers, 140,000 Social Security numbers, 1 million Canadian Social Insurance Numbers exposed, due to a Server-Side-Request Forgery attack.

01 Capital One Hack – What (likely) happened?

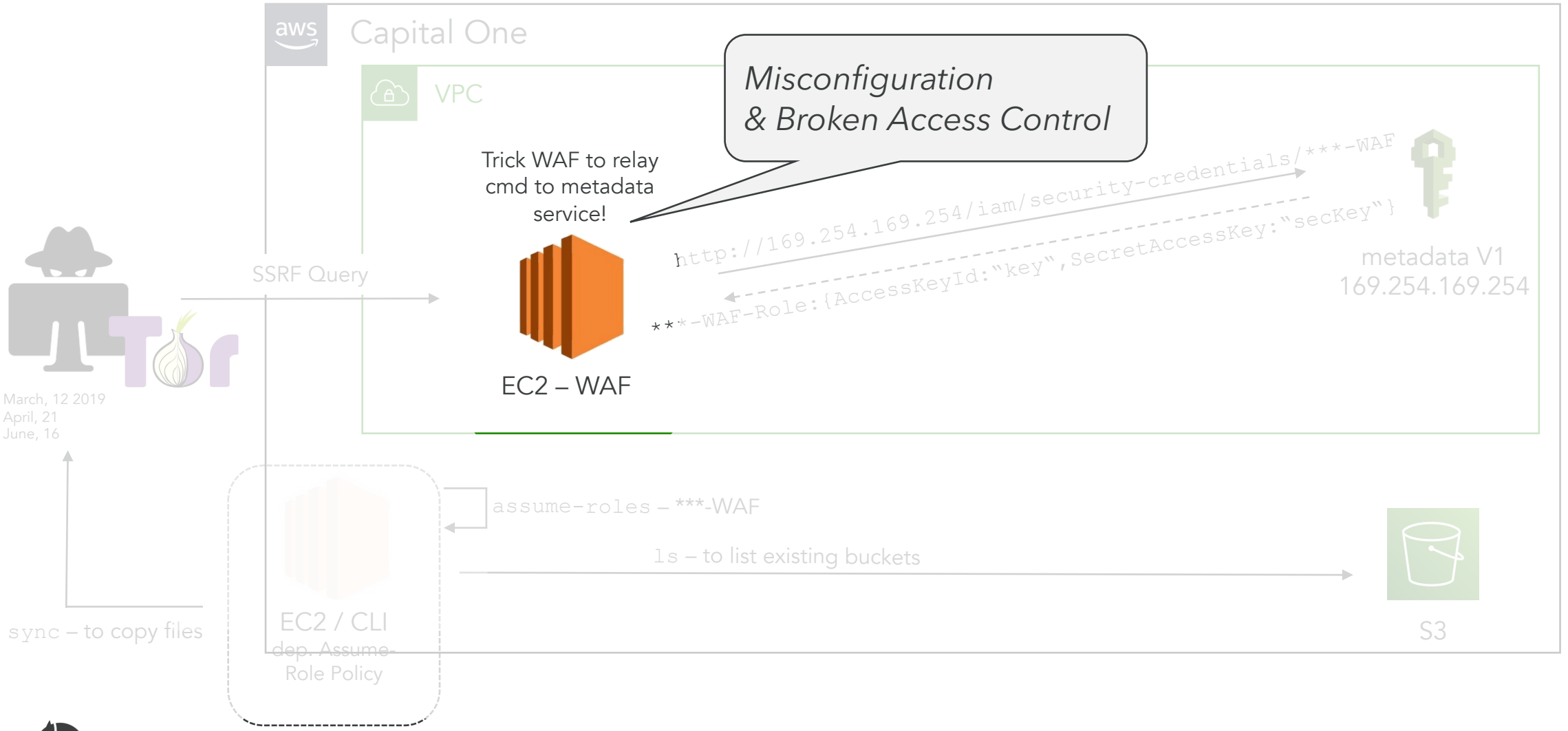
MIT Report Extended



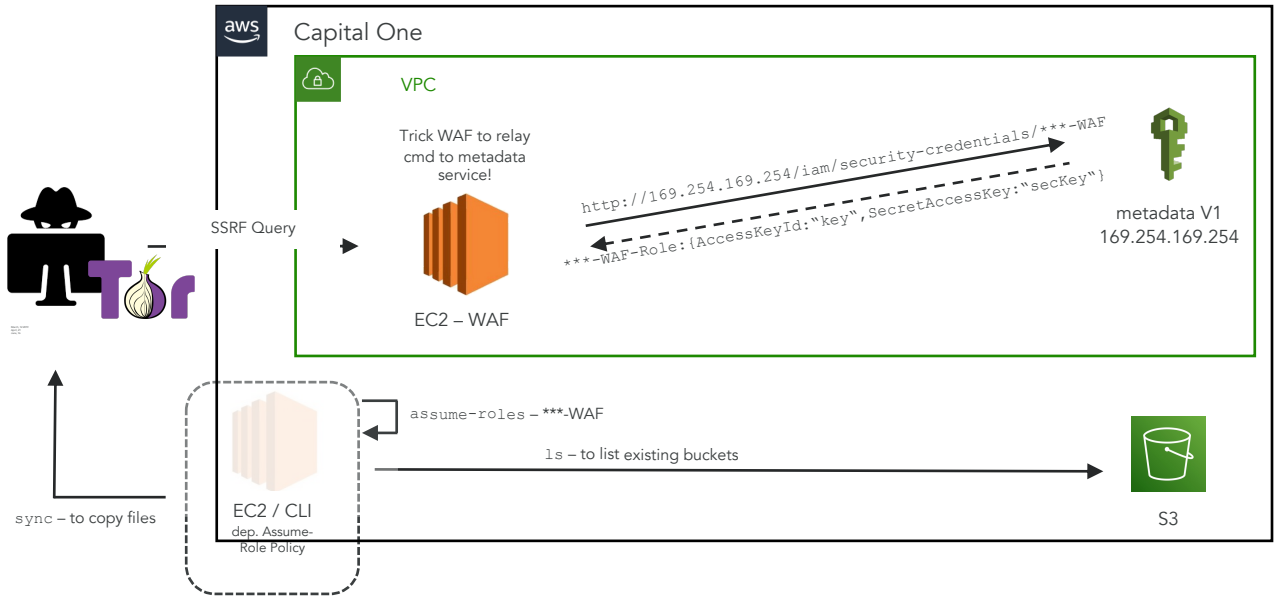
01 Capital One Hack – What (likely) happened?



01 Capital One Hack – What happened?

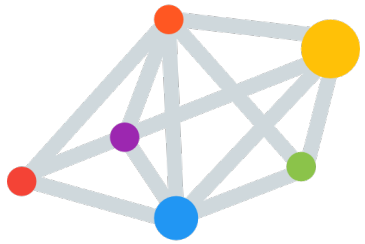


01 Capital One Hack – Learnings: Network vs. IAM Policies



Even if EC2 instance would not have a IAM role with access to S3, but with permissions to *list* and *attach* policies an attacker could go policy shopping.

IAM permissions can "jump" to private resources, forming an alternative network.

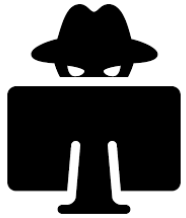


02 LATERAL MOVEMENT AND WHY THEY MATTER?

02 Lateral Movements

*„**Lateral Movement** refers to the techniques that cyber attackers use to progressively move through a network as they search for the key data and assets“*

https://en.wikipedia.org/wiki/Network_Lateral_Movement

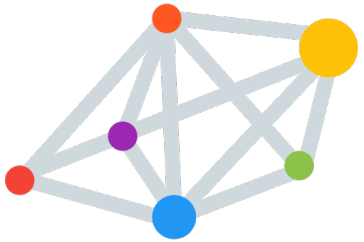


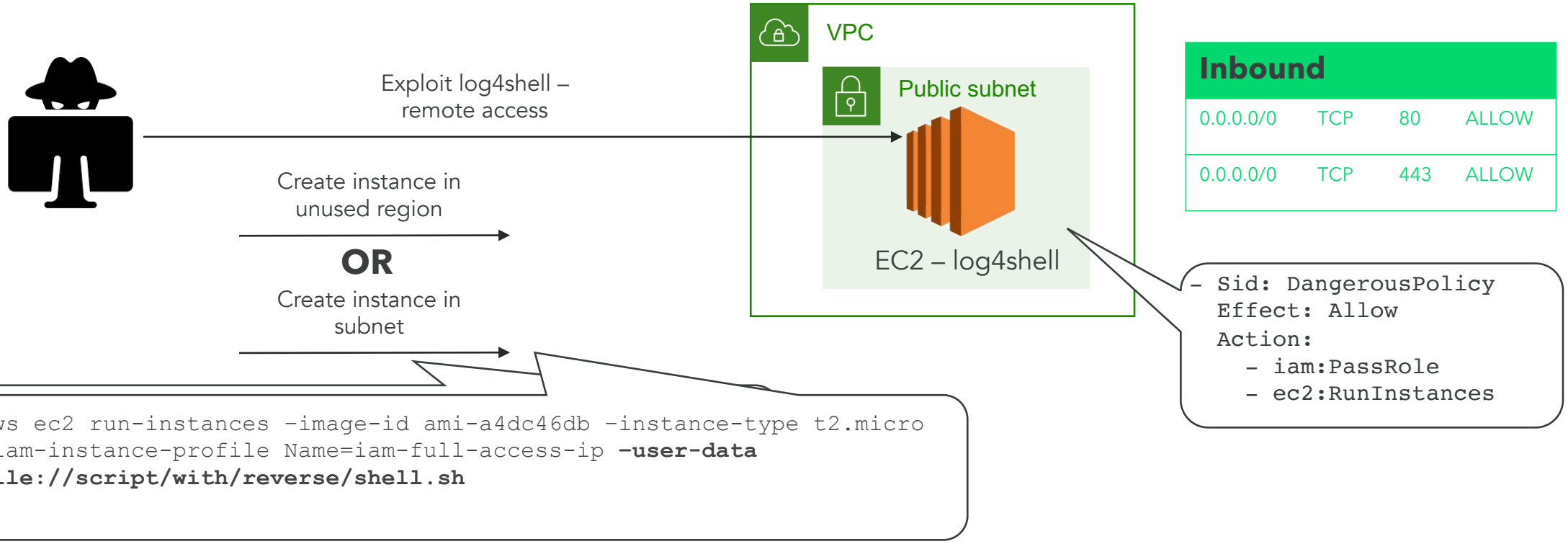
NOT looking at vulnerabilities and misconfigurations in isolation!

Attacker’s perspective - how to chain weaknesses to an attack.

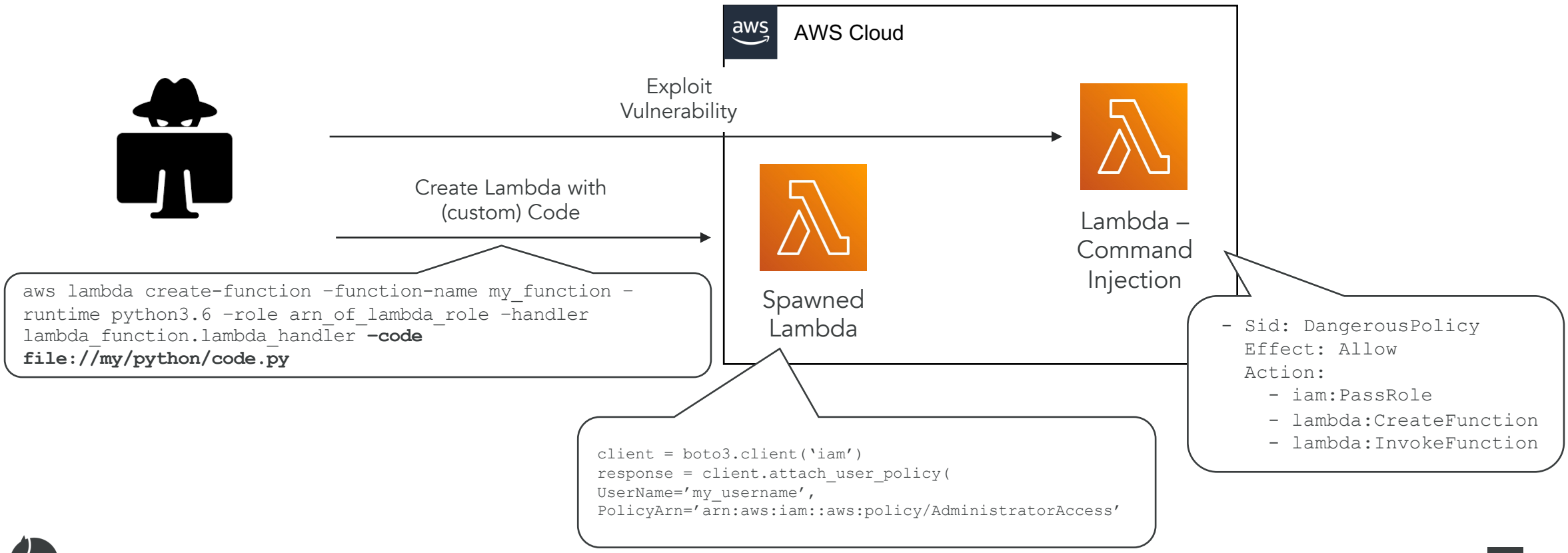
02 Lateral Movements - Example

IAM permissions form an alternative network that attackers can abuse by chaining policies.





02 Lateral Movements - IAM Permissions



03 WHAT CAN WE DO AND WHAT TOOLS EXISTS?

03 We have tools in place to continuously secure our...

Application / Lambda / Function Code

Detect unknown vulnerabilities in known code

Static Application Security Testing

Fortify coverity sonarqube ...

Open-Source Dependencies

Detect known CVEs in unknown Code

Software Composition Analysis

DEPENDENCY-TRACK WhiteSource snyk ...

Infrastructure-as-Code

Detect misconfiguration in architecture

Infrastructure-as-Code Security Testing

LambdaGuard bc KICS ...

03 tfsec

```
Problem 2

  [AWS004] Resource 'aws_alb_listener.my-alb-listener' uses plain HTTP instead of HTTPS.
  /Users/liamg/example/main.tf:9

       6 |
       7 | resource "aws_alb_listener" "my-alb-listener"{
       8 |     port     = "80"
       9 |     protocol = "HTTP"
      10 | }
      11 |
      12 | resource "aws_db_security_group" "my-group" {
```

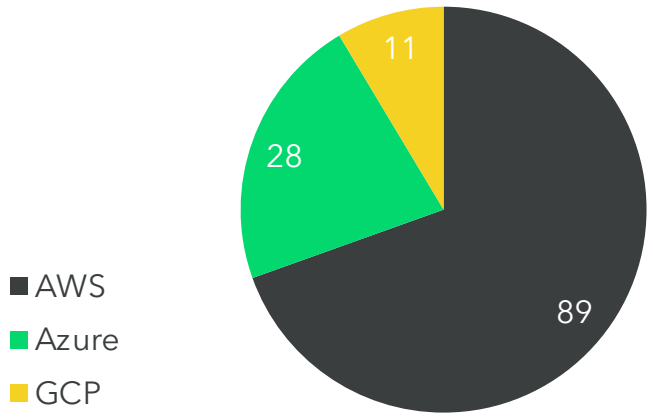
Benefits

- Inspects Terraform Templates
- 129 Rules for AWS, Azure, GCP
- Example Rules
  - HTTP should instead be HTTPS
  - Data encrypted at rest
  - Public write disabled for buckets

Shortcomings

- Context within application is missing
- No Code Analysis

#Rules



GitHub https://github.com/tfsec/tfsec

03 checkov

Benefits

- Inspects CloudFormation, Kubernetes, docker, Serverless
- Example Rules
  - Data encrypted at rest
  - No hard-coded secrets

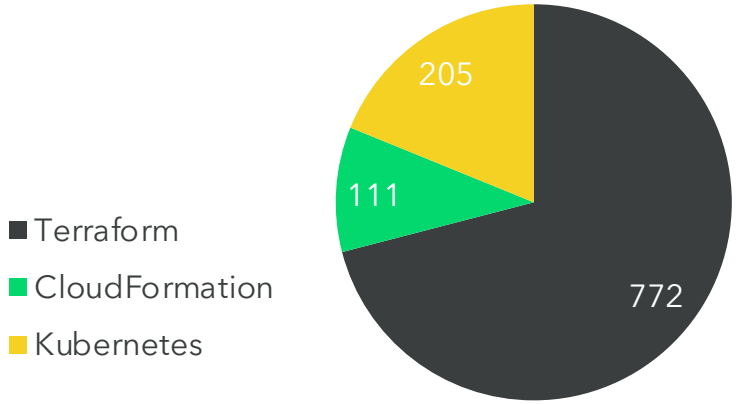
Shortcomings

- Context within application is missing
- No Code Analysis

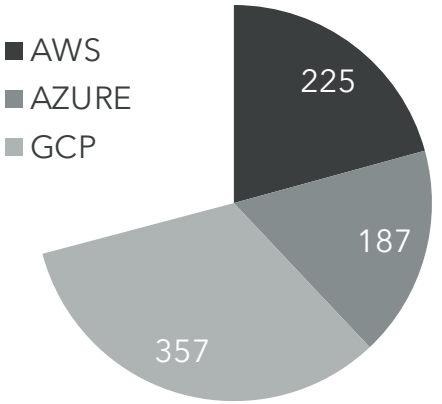
```
Check: CKV_AWS_19: "Ensure all data stored in the S3 bucket is securely en
rypted at rest"
        FAILED for resource: aws_s3_bucket.data
        File: /aws/s3.tf:1-9
        Guide: https://docs.bridgecrew.io/docs/s3_14-data-encrypted-at-res

                1 | resource "aws_s3_bucket" "data" {
                2 |   bucket        = "${local.resource_prefix.value}-data
                3 |   acl           = "public-read"
                4 |   force_destroy = true
                5 |   tags = {
                6 |     Name        = "${local.resource_prefix.value}-data
                7 |     Environment = local.resource_prefix.value
                8 |   }
                9 | }
```

#Rules



Terraform Rules by Provider



GitHub https://github.com/bridgecrewio/checkov

03 In our projects, we have tools in place to continuously secure our...

Application / Lambda / Function Code

Detect unknown vulnerabilities in known code

Static Application Security Testing

Fortify coverity sonarqube ...

Open-Source Dependencies

Detect known CVEs in unknown Code

Software Composition Analysis

DEPENDENCY-TRACK WhiteSource snyk ...

Infrastructure-as-Code

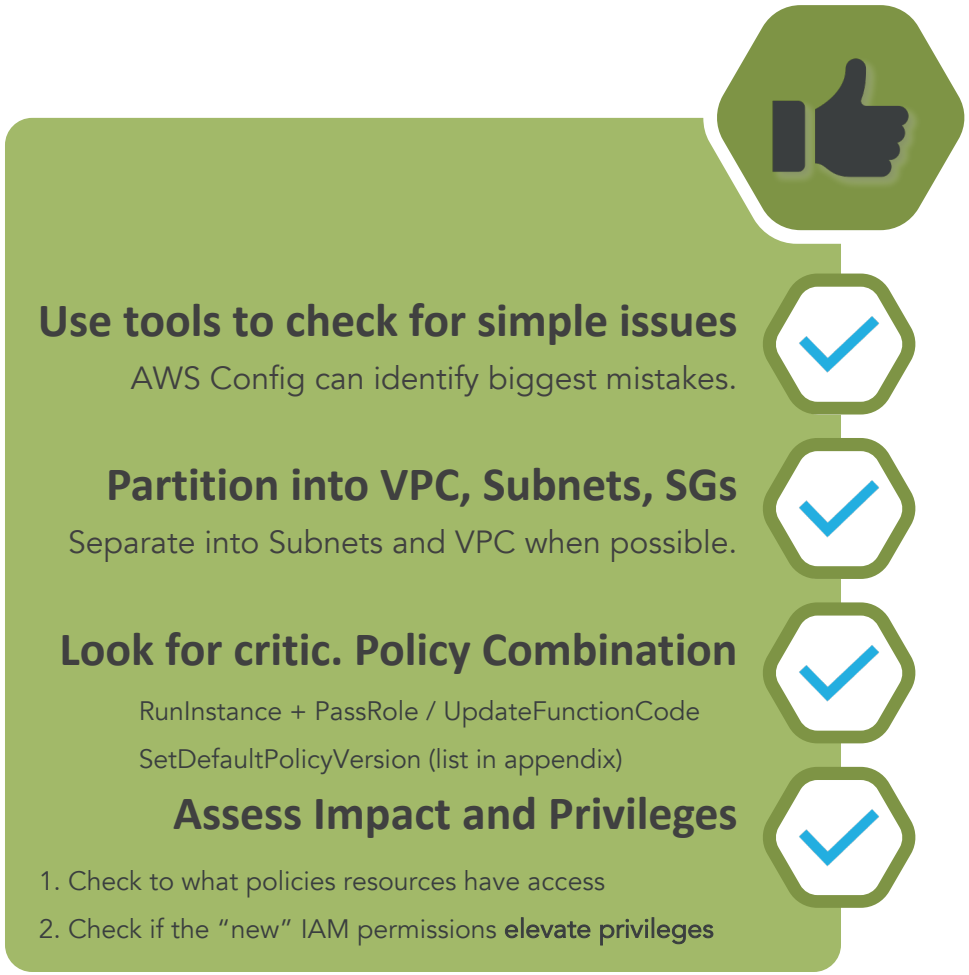
Detect misconfiguration in architecture

Infrastructure-as-Code Security Testing

LambdaGuard bc KICS ...

Tools focus on single aspect, and thus **miss lateral movements.**
However, they can detect single critical issues.

03 Still manual effort required



Use tools to check for simple issues

AWS Config can identify biggest mistakes.

Partition into VPC, Subnets, SGs

Separate into Subnets and VPC when possible.

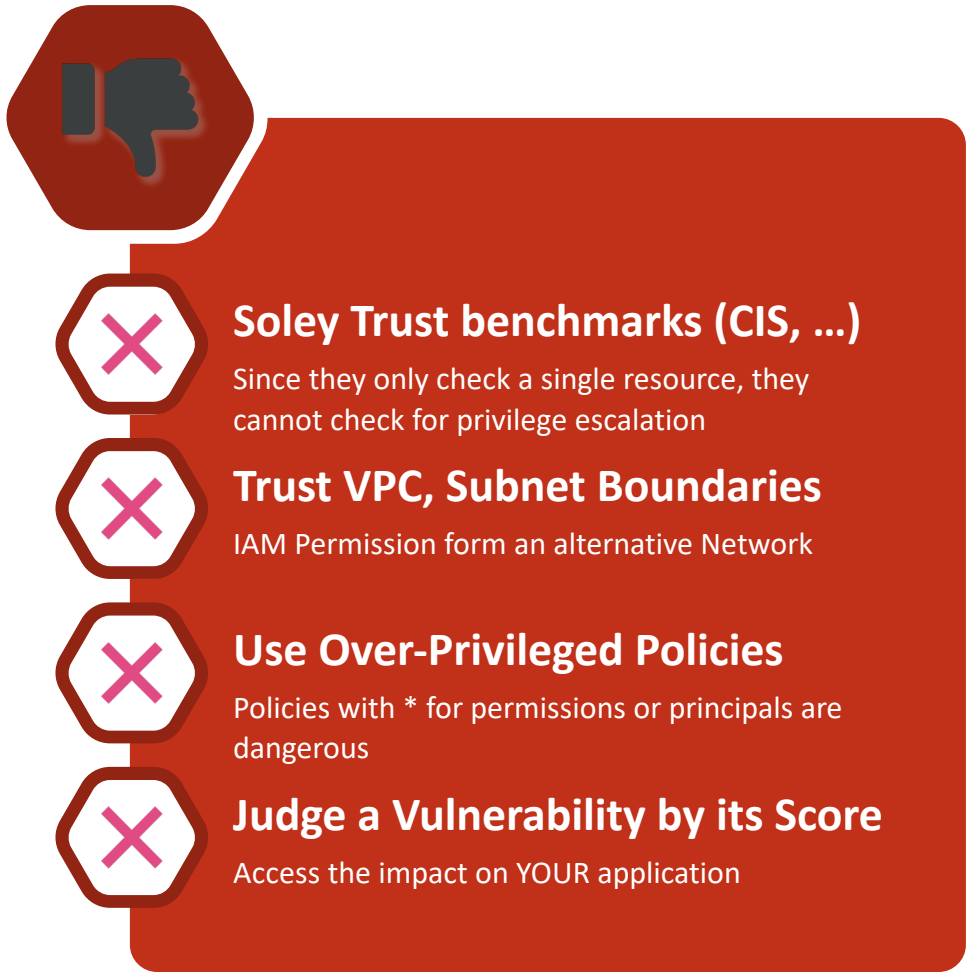
Look for critic. Policy Combination

RunInstance + PassRole / UpdateFunctionCode

SetDefaultPolicyVersion (list in appendix)

Assess Impact and Privileges

1. Check to what policies resources have access
2. Check if the "new" IAM permissions **elevate privileges**



Soley Trust benchmarks (CIS, …)

Since they only check a single resource, they cannot check for privilege escalation

Trust VPC, Subnet Boundaries

IAM Permission form an alternative Network

Use Over-Privileged Policies

Policies with * for permissions or principals are dangerous

Judge a Vulnerability by its Score

Access the impact on YOUR application

02 Tip: Overview of Open-Source Cloud Security Tools

Privilege Escalation Examples

https://github.com/RhinoSecurityLabs/AWS-IAM-Privilege-Escalation

Cloud Security Checklist

https://tldrsec.com/blog/cloud-security-orienteering/

Overview of Tools

https://github.com/toniblyx/my-arsenal-of-aws-security-tools

01 Tip: Exploiting Code Injection, SSRF

Interactive Capital One Hack Tutorial

https://application.security/free-application-security-training/server-side-request-forgery-in-capital-one

OWASP Serverless Goat Application updated and migrated to Java

https://github.com/CodeShield-Security/Serverless-Goat-Java

Exploit Serverless Goat Tutorial

https://medium.com/all-about-modern-application-security-testing-a/how-to-prevent-code-injection-vulnerabilities-in-serverless-applications-part-1-2-5b17fb343395

Exploit Confused Deputy (SAR) Tutorial

https://codeshield.io/blog/2021/08/26/sar_confused_deputy/

Andreas Dann
COO & Co-Founder

andreas.dann@codeshield.io

Technologiepark 8, 33100 Paderborn