

**DevSecOps : add security to my
DevOps**

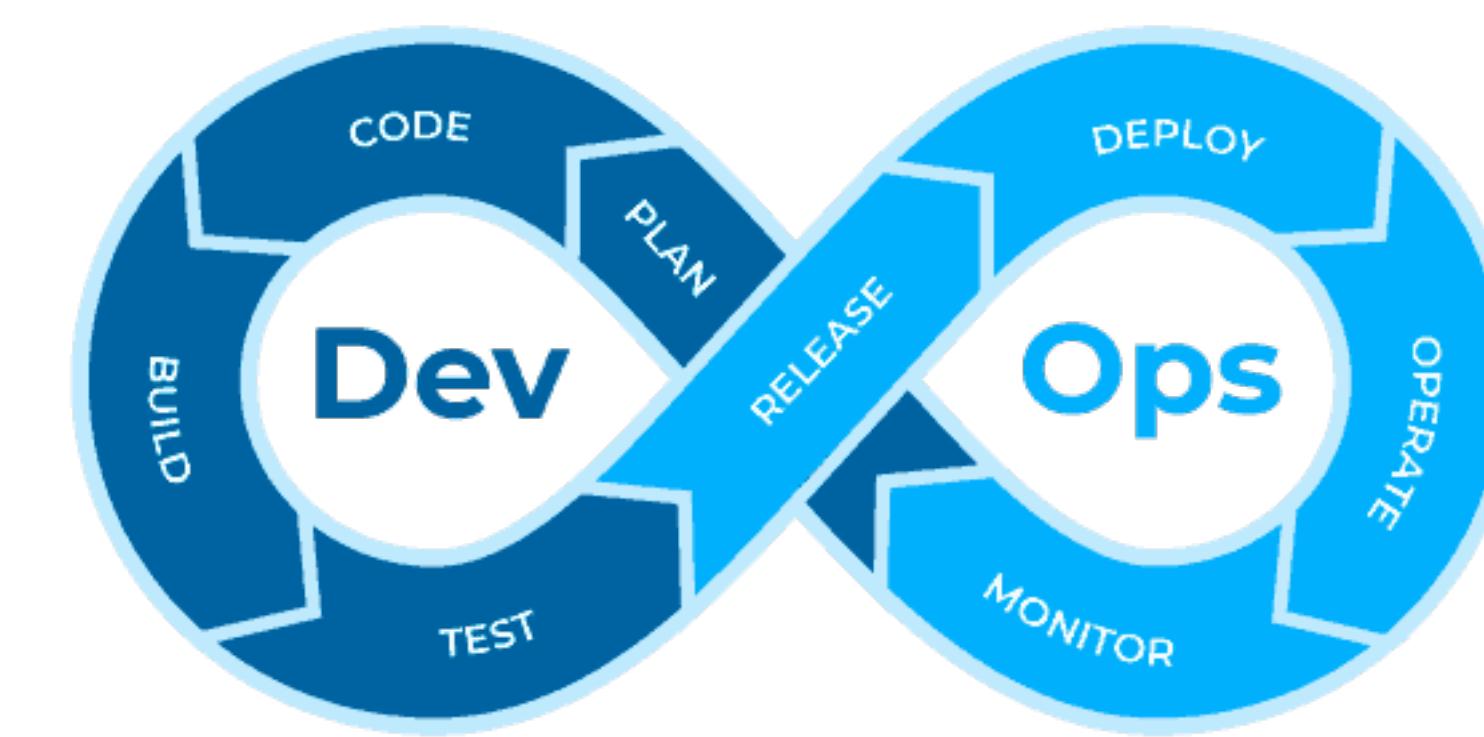
Introduction



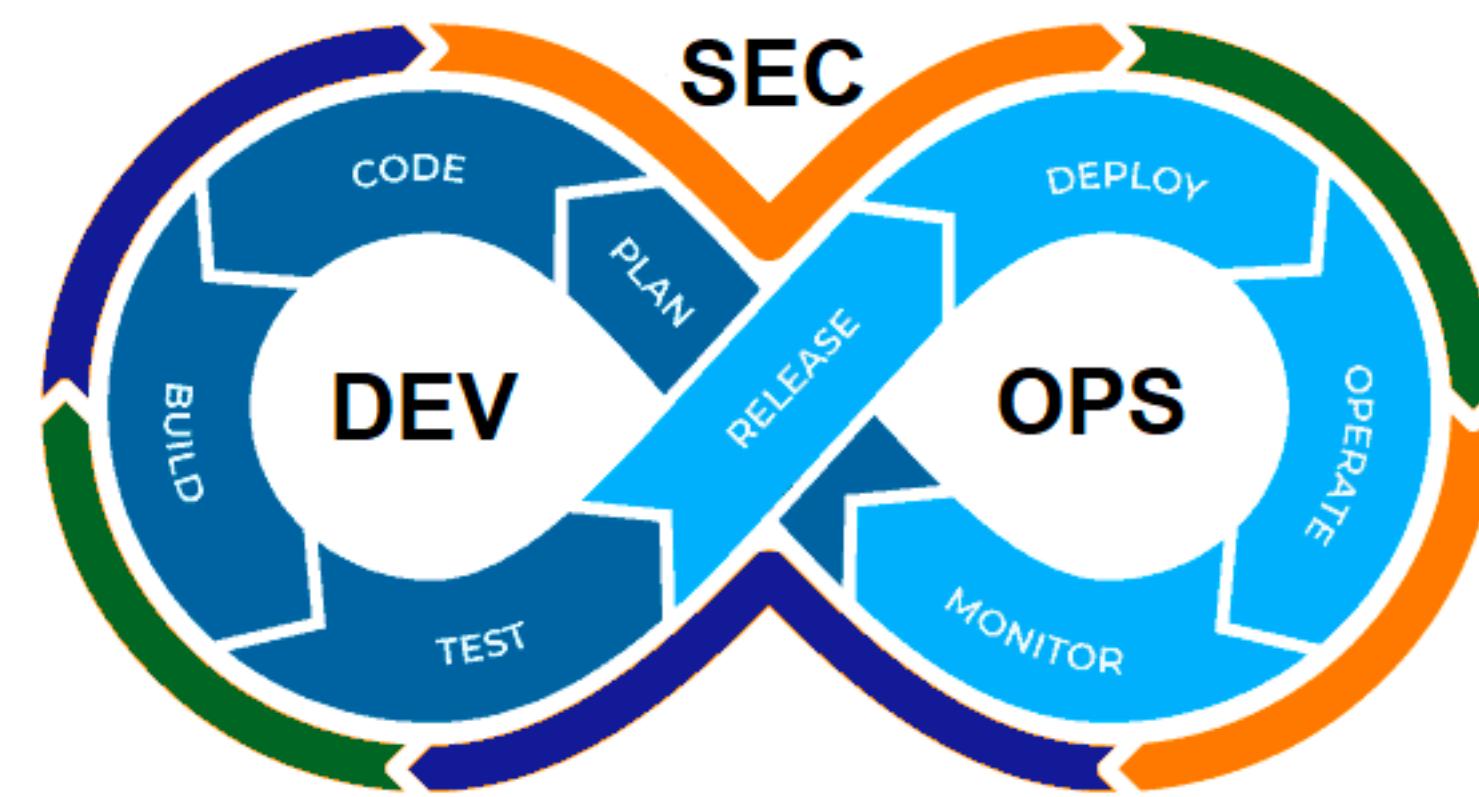
Introduction



Introduction



Introduction



Introduction

Oublier la cybersécurité, c'est "rouler à 200 km/h à moto sans casque"

Forget about cybersecurity, it's ride a motorcycle at 200 km/h without helmet

Guillaume Poupart, (futur) ex-director of the French Anssi

Introduction



@adrienpessu

SAST (STATIC APPLICATION SECURITY TESTING)

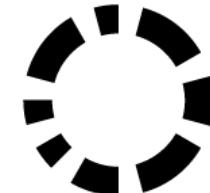
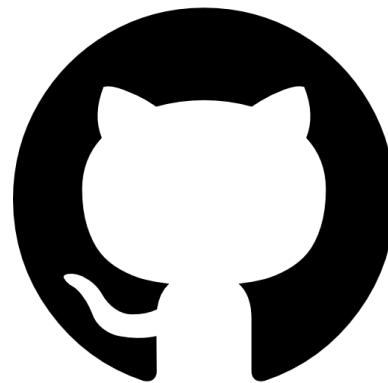


phpcs-security-audit v3

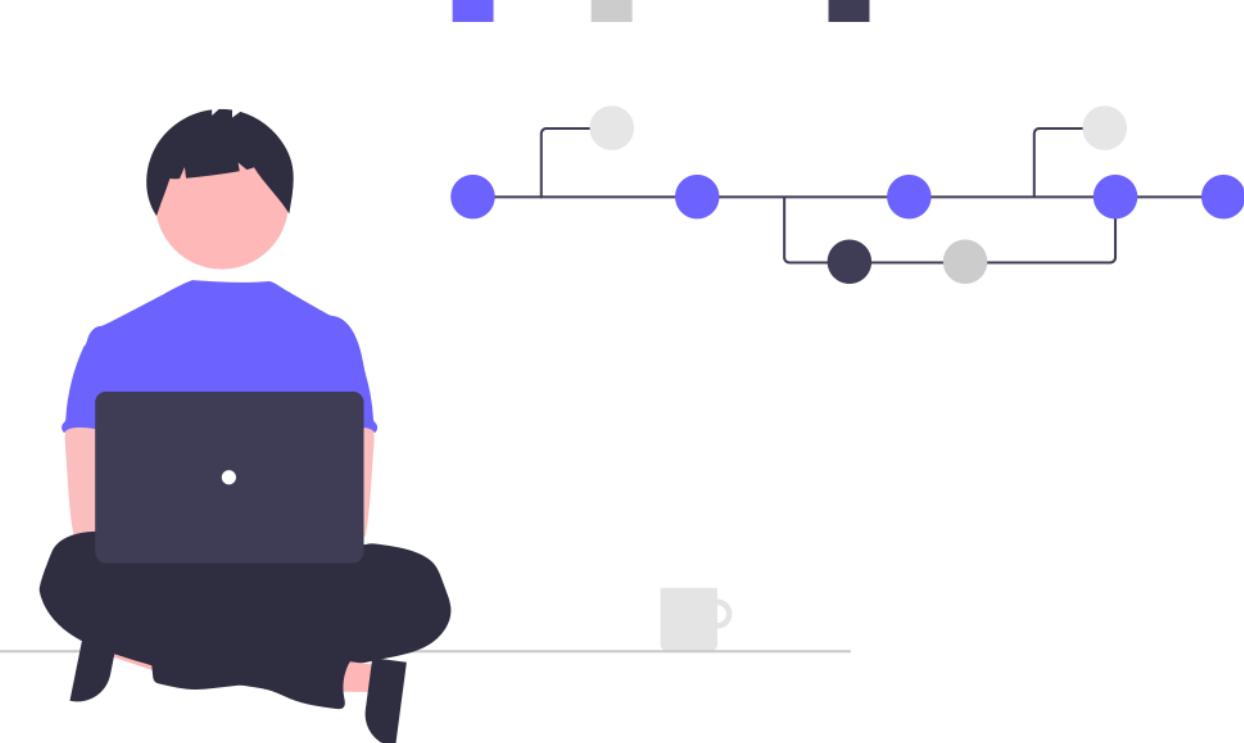
{ } Find Security Bugs



sonarQube



C O D A C Y



SAST (STATIC APPLICATION SECURITY TESTING)

```
<div text [innerHTML] = "greeting.translate.key' I translate:{name: name}"></div>
```

Hello {{ name }}, welcome to Voxxed Days

Hello Adrien, welcome to Voxxed Days

SCA (SOFTWARE COMPOSITION ANALYSIS)



sonatype



Checkmarx

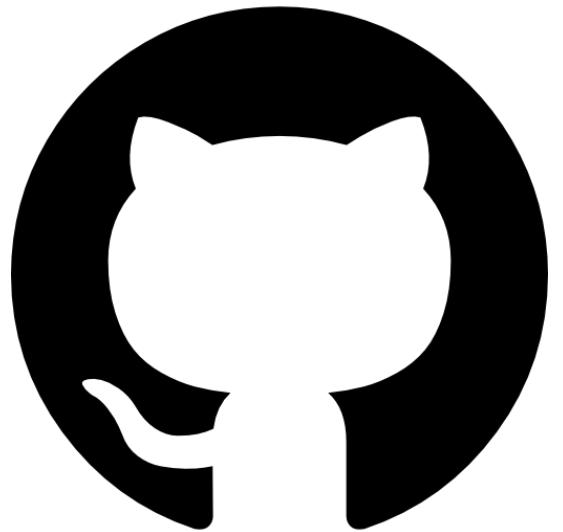
VERACODE



npm-audit



DEPENDENCY-TRACK



SCA (SOFTWARE COMPOSITION ANALYSIS)

VULNERABILITIES

CVE-2020-7774 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

This affects the package y18n before 3.2.2, 4.0.1 and 5.0.5. PoC by po6ix: const y18n = require('y18n'); y18n.setLocale('__proto__'); y18n.updateLocale({polluted: true}); console.log(polluted); // true

[+View Analysis Description](#)

Severity

CVSS Version 3.x

CVSS Version 2.0

CVSS 3.x Severity and Metrics:



NIST: NVD

Base Score: N/A

NVD score not yet provided.

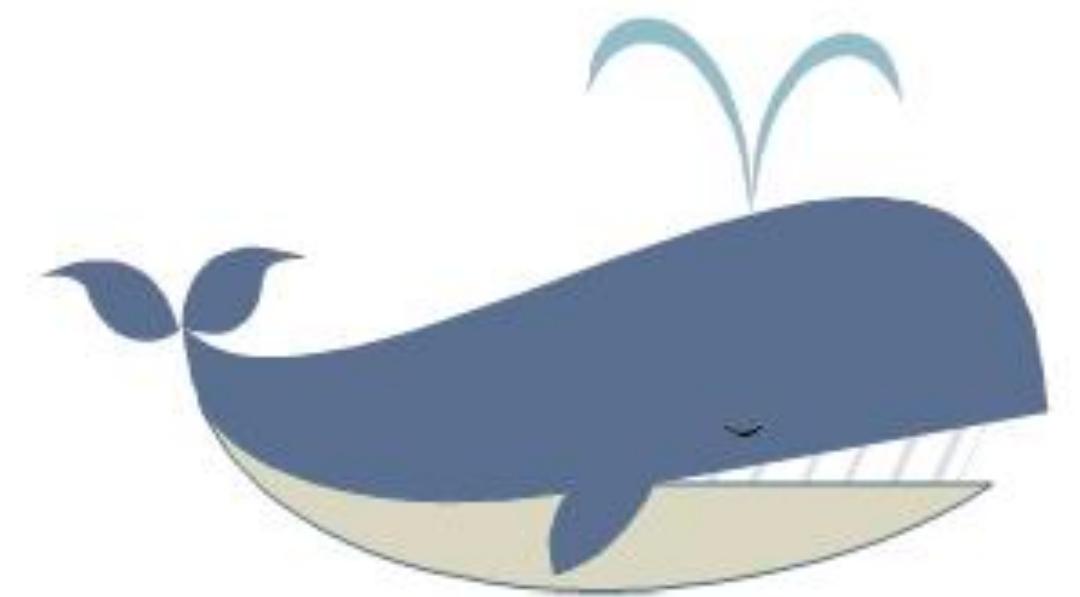


CNA: Snyk

Base Score: 7.3 HIGH

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Docker



Docker

```
$ docker scan --file Dockerfile docker-scan:e2e
Testing docker-scan:e2e
...
x High severity vulnerability found in perl
  Description: Integer Overflow or Wraparound
  Info: https://snyk.io/vuln/SNYK-DEBIAN10-PERL-570802
  Introduced through: git@1:2.20.1-2+deb10u3, meta-common-packages@meta
  From: git@1:2.20.1-2+deb10u3 > perl@5.28.1-6
  From: git@1:2.20.1-2+deb10u3 > liberror-perl@0.17027-2 > perl@5.28.1-6
  From: git@1:2.20.1-2+deb10u3 > perl@5.28.1-6 > perl/perl-modules-5.28@5.28.1-6
  and 3 more...
  Introduced by your base image (golang:1.14.6)

Organization:      docker-desktop-test
Package manager:   deb
Target file:       Dockerfile
Project name:     docker-image|99138c65ebc7
Docker image:      99138c65ebc7
Base image:        golang:1.14.6
Licenses:          enabled

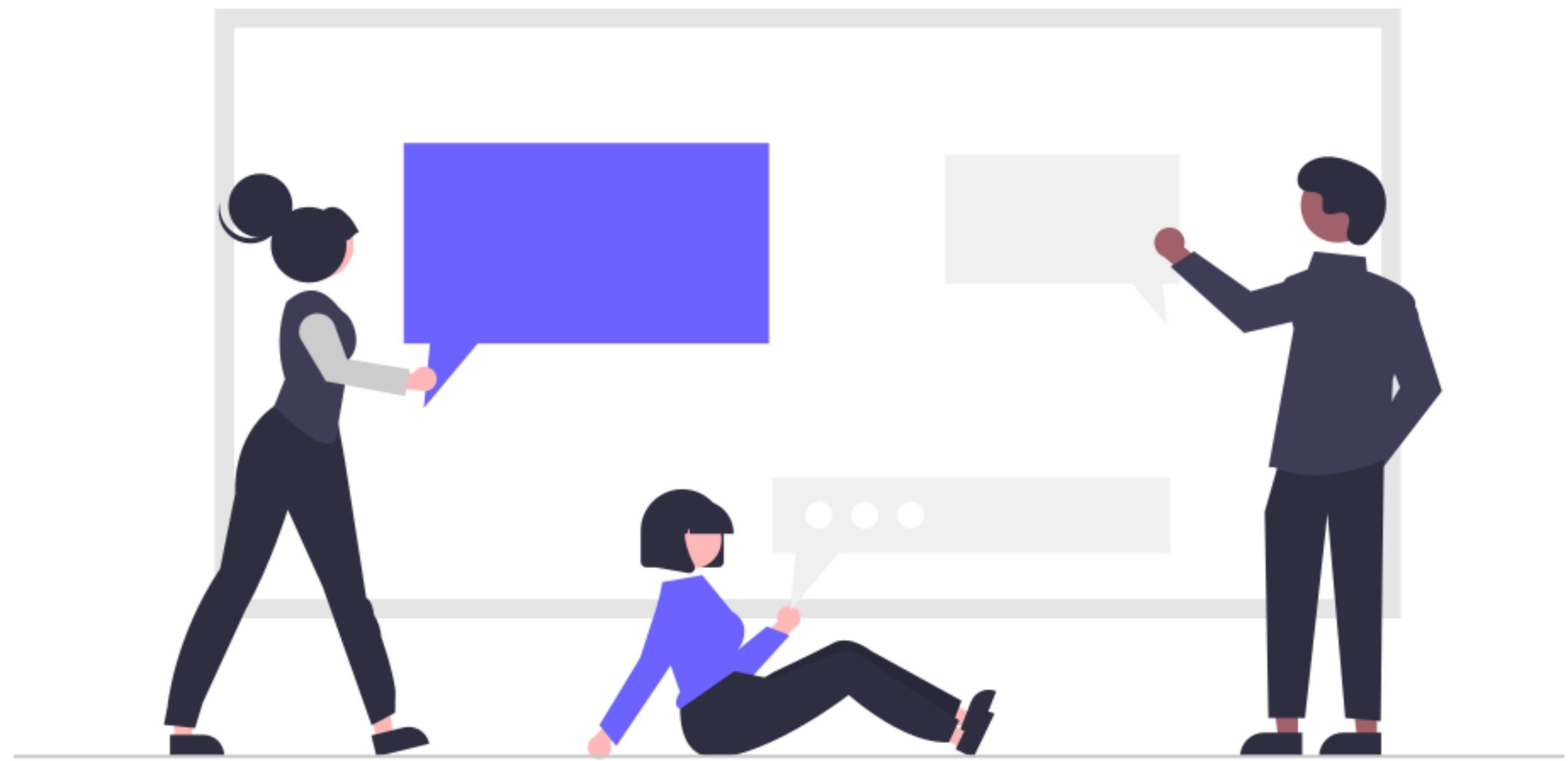
Tested 200 dependencies for known issues, found 157 issues.

According to our scan, you are currently using the most secure version of the selected base image
```

DAST (DYNAMIC APPLICATION SECURITY TESTING)



IAST (INTERACTIVE APPLICATION SECURITY TESTING)





```
● ● ●

> terraform plan | scenery
+ aws_cLOUDTRAIL.main
  id: <computed>
  arn: <computed>
  enable_log_file_validation: "true"
  enable_logging: "true"
  home_region: <computed>
  include_global_service_events: "true"
  is_multi_region_trail: "true"
  kms_key_id: "arn:aws:kms:us-west-2:123456789123:key/c6c7f815-5c3c-42b8-a0f8-e93e61b42215"
  name: "main"
  s3_bucket_name: "cloudtrail-logs"
  tags.%: "2"
  tags.Name: "audit-log-trail"
  tags.Service: "auditing"

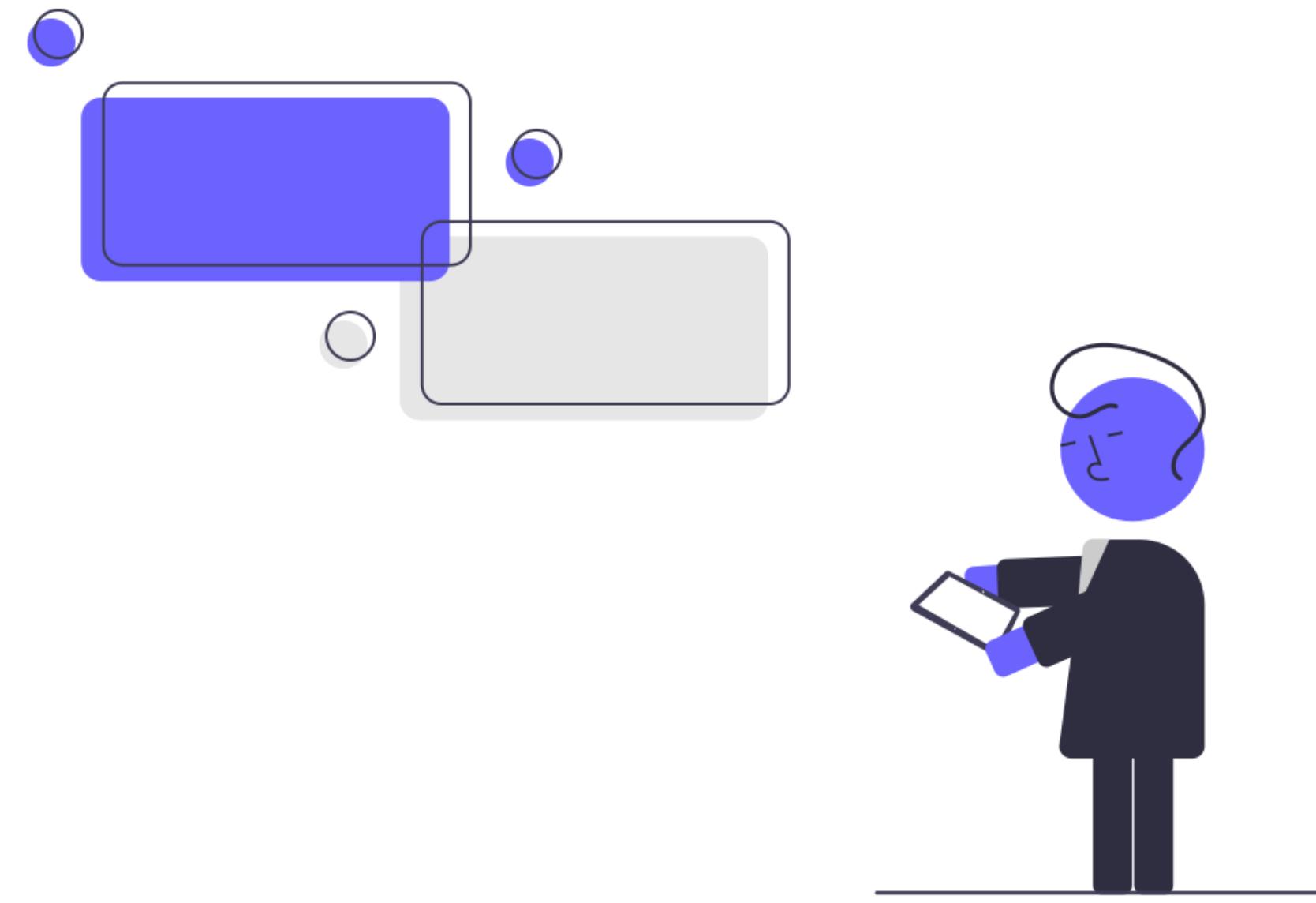
- aws_iam_policy.demo_service
  policy: {
    "Version": "2012-10-17",
    "Statement": [
      + {
        + "Sid": "",
        + "Effect": "Allow",
        + "Action": "s3:GetObject",
        + "Resource": "arn:aws:s3:::demo-bucket/*"
      },
      {
        "Sid": "",
        "Effect": "Allow",
        "Action": "ssm:GetParametersByPath",
        "Resource": "arn:aws:ssm:us-west-2:123456789123:parameter/demo/*"
      }
    ]
  }

- aws_route53_record.record
  allow_overwrite: "" => "true"

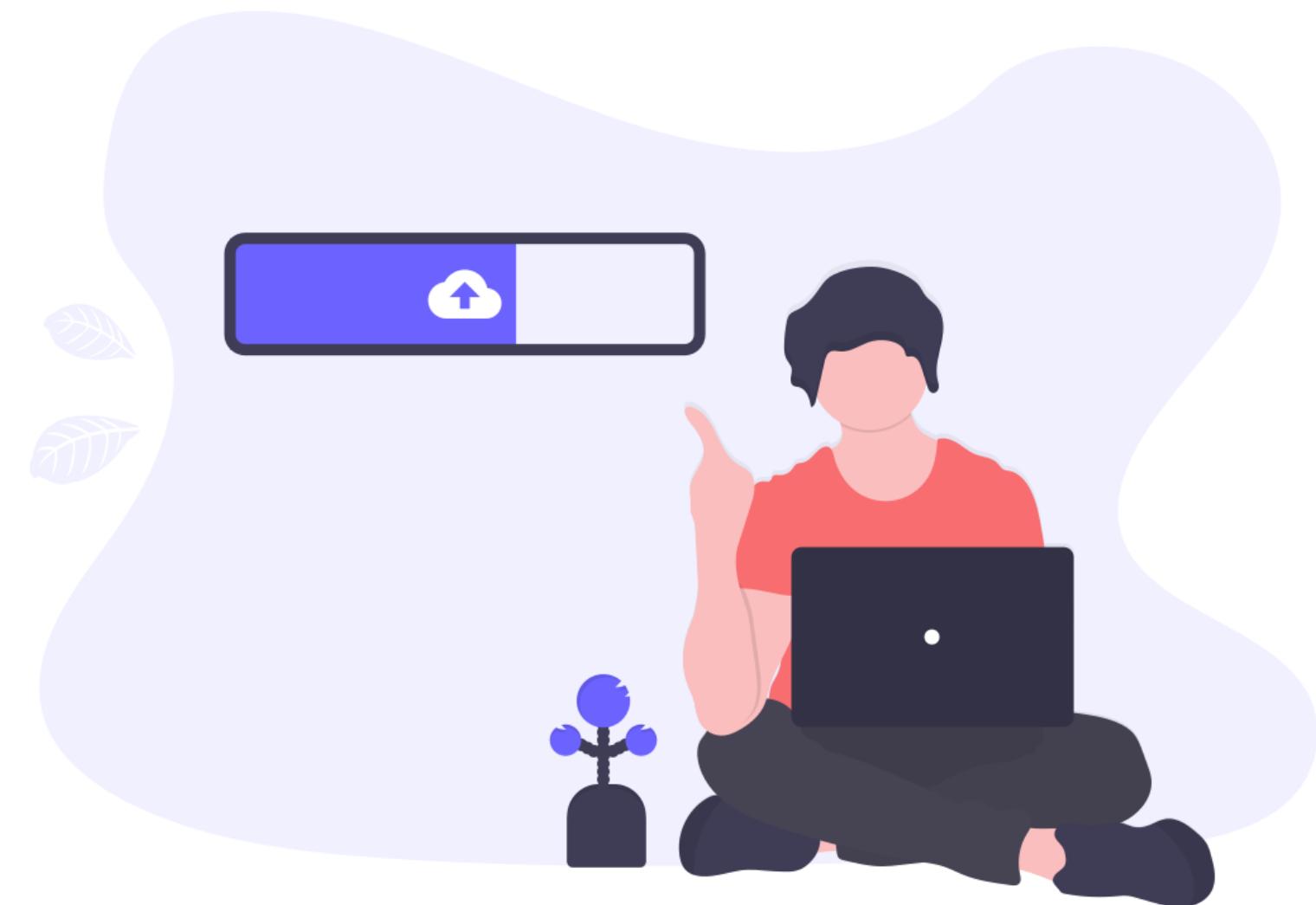
-/+ module.replica.aws_security_group_rule.whitelists[1] (new resource required)
  id: "sgrule-2762726406" => <computed> (forces new resource)
  from_port: "5432" => "5432"
  protocol: "tcp" => "tcp"
  security_group_id: "sg-abcdef12" => "sg-abcdef12"
  self: "false" => "false"
  source_security_group_id: "sg-12345678" => "sg-87654321" (forces new resource)
  to_port: "5432" => "5432"
  type: "ingress" => "ingress"

Plan: 1 to add, 3 to change, 0 to destroy.
>
```

WAF (WEB APPLICATION FIREWALL)



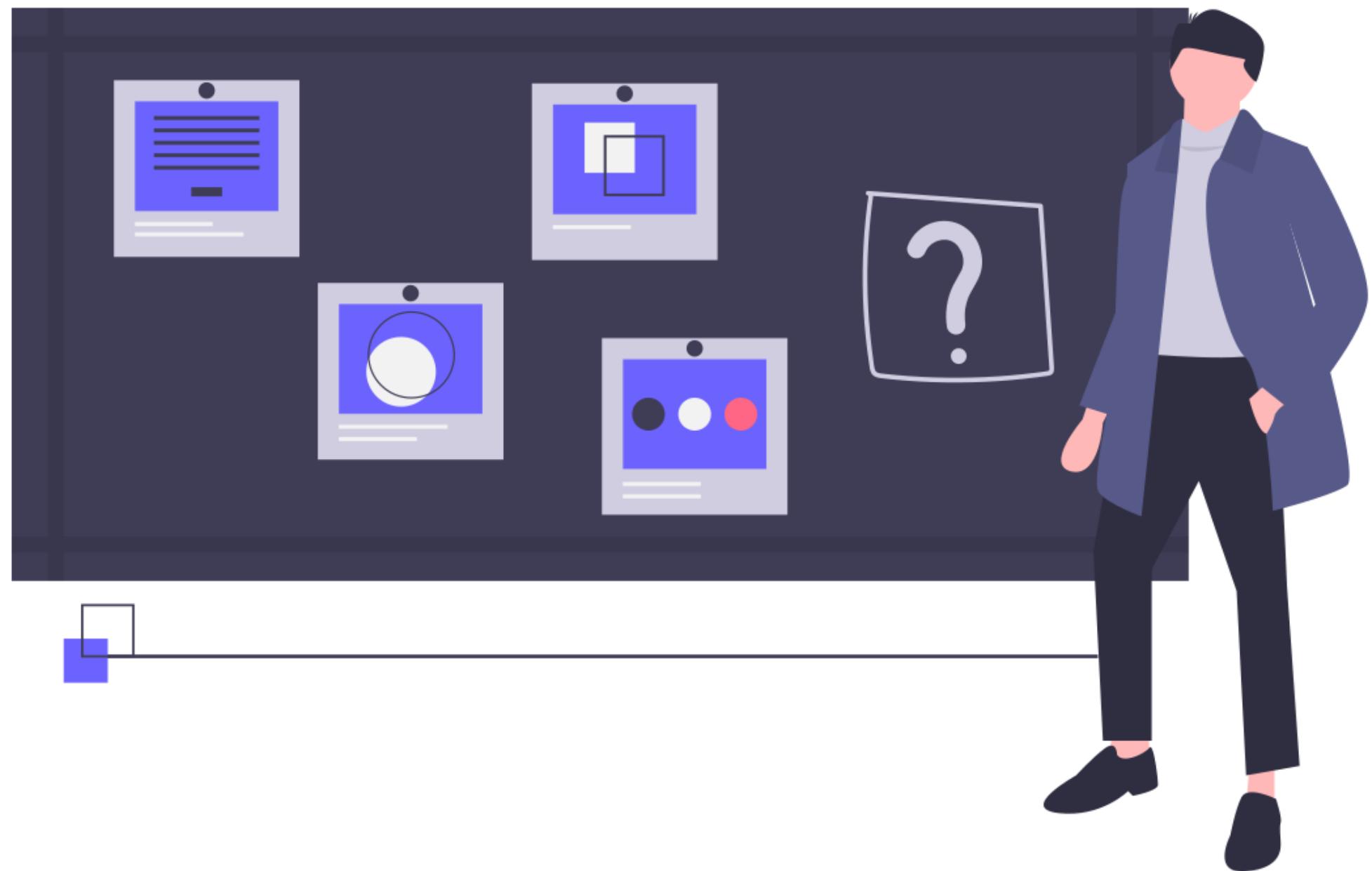
RASP (RUN-TIME APPLICATION SECURITY PROTECTION)



Pentesting



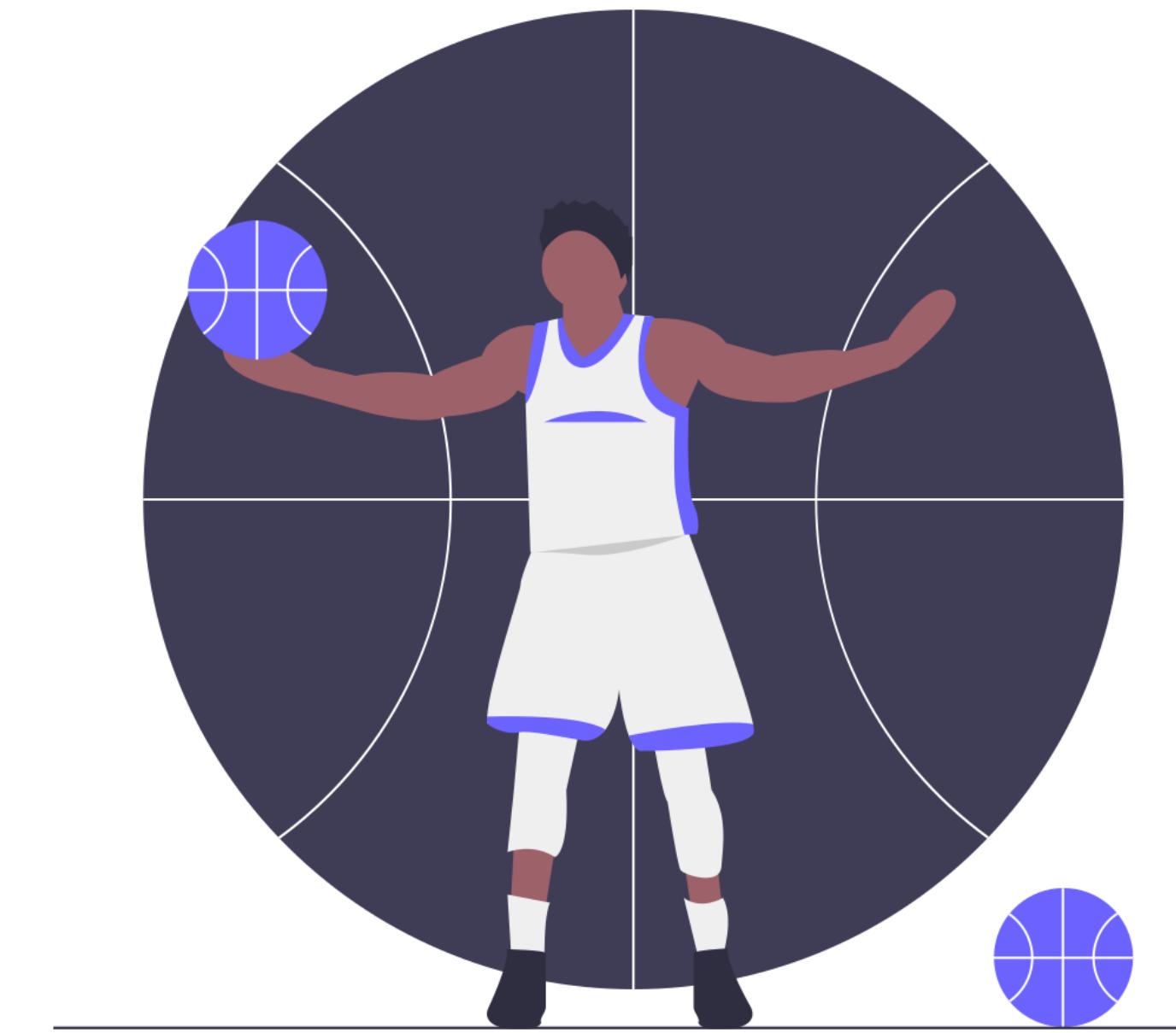
Training



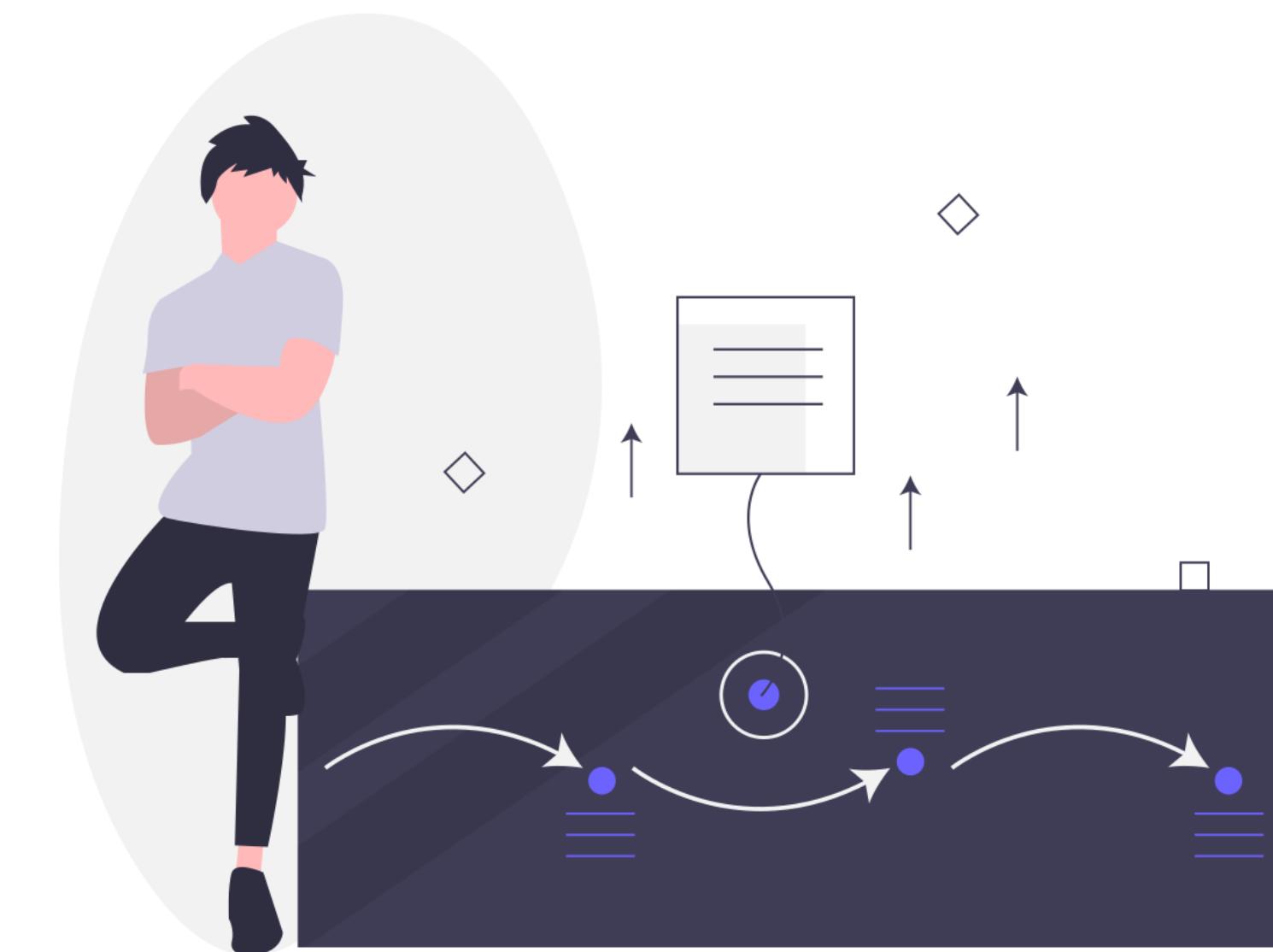
Documentation



Security champion



Risk assessment



Risk assessment

The screenshot shows a Firefox browser window with the following details:

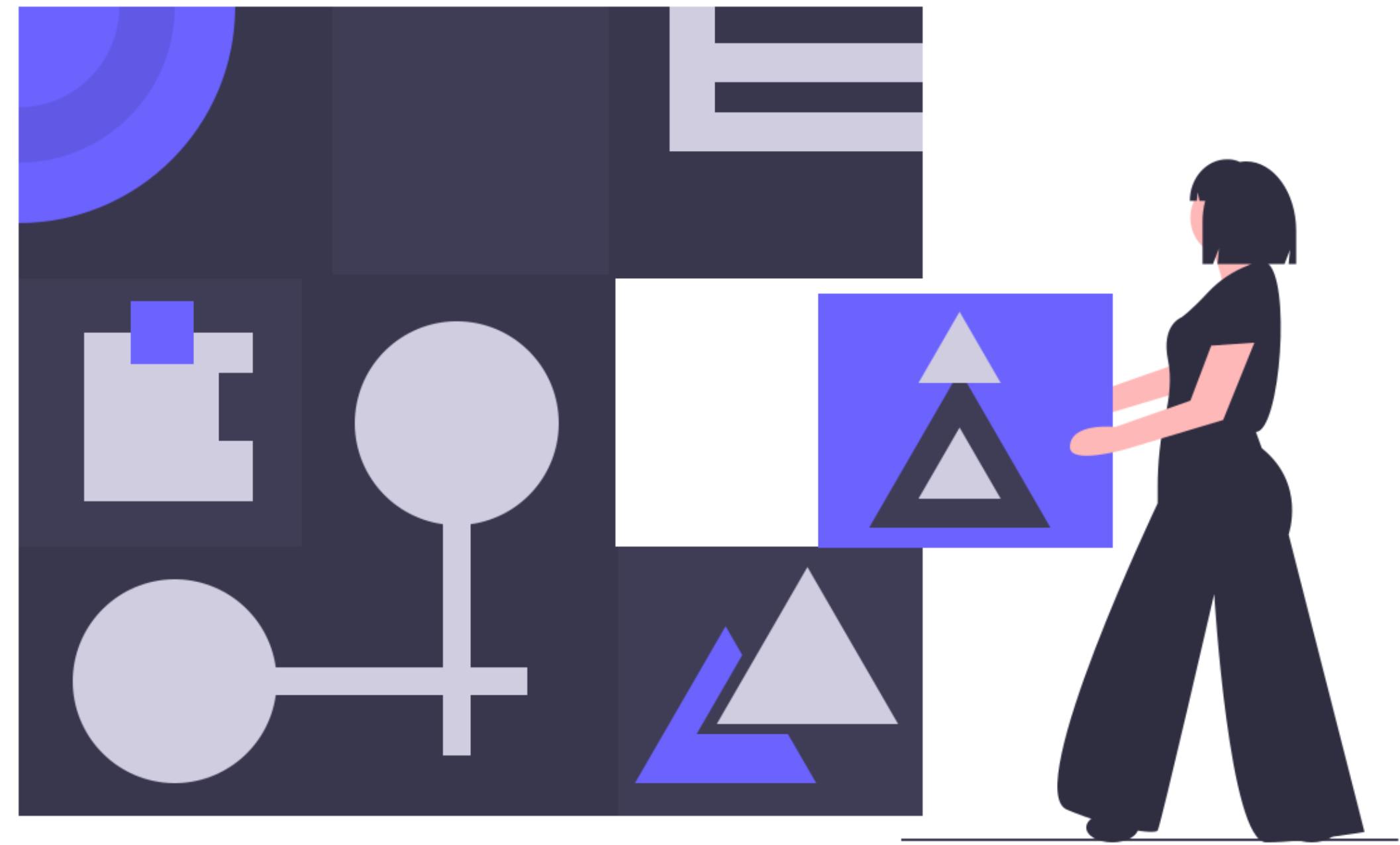
- Address Bar:** infosec.mozilla.org
- Page Title:** moz://a
- Page Content:**
 - ## Guided process for risk analysts: Running your RRA in ~30 minutes
 - This is a guided example of how to run an initial RRA. You will:

 - Invite the relevant people to a meeting.
 - Help them figure out risk impacts and record everything in the RRA doc.
 - Help them figure out the next steps.
 - Make them feel like they own the RRA document (and they do!).
 - ### Before the initial RRA meeting

 - Ensure no previous RRA exist; if it does, just enhance the current RRA document
 - Create a copy of the RRA template in the RRA Google Drive directory.
 - Mozilla employees can make a copy of the template with this [redirect](#)
 - Everyone can view the [RRA template](#)
 - Invite 1 or 2 members (product/service owners, lead engineers, etc.) related to the service with a bit of technical knowledge.
 - Ensure the invitees attempt to bring a data flow diagram and have an understanding of the data the service stores or processes.
 - You do not want more than 4 or 5 people total as this will slow down the RRA significantly. Most RRAs are run 1 on 1 (2 people total).
 - Make sure everyone invited has **edit** rights to the document, and have the document opened in front of them when the RRA starts (you can also just share your screen).
 - If this is anyone's first RRA, ensure they understand the goals of the RRA and give them a short introduction to what the different steps will be. This both help them follow, and show that you have control of the meeting (see next section on time management).
 - ### Initial RRA meeting

 - [Time management - take control](#)
- Page Navigation:** Home, security fundamentals, security guidelines, improve this document, discover firefox

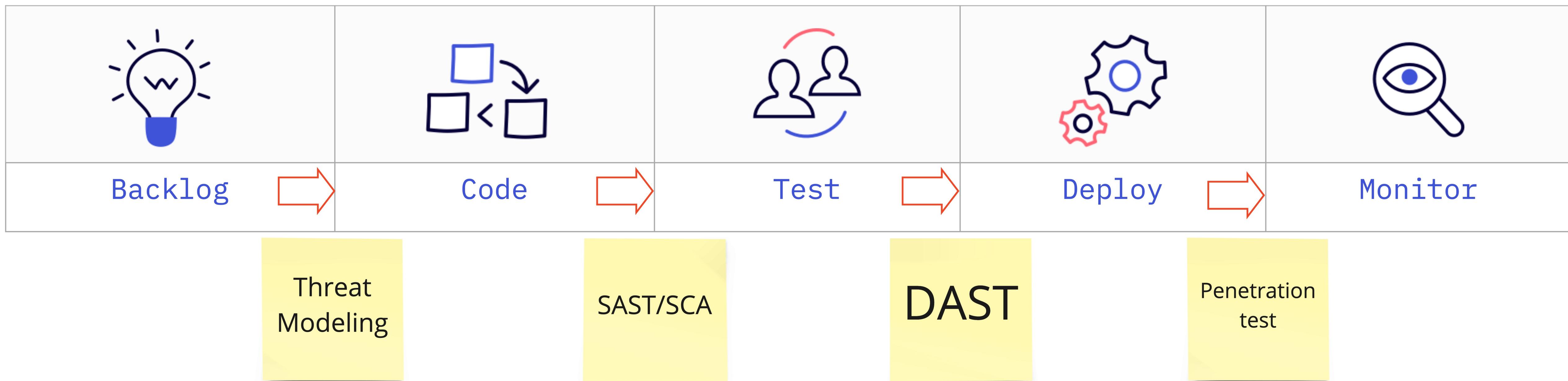
Threat modelling



KPI (Key performance indicator)



Conclusion



Conclusion

