



DevSecOps : de la sécurité dans mon DevOps

Introduction



@tgrall

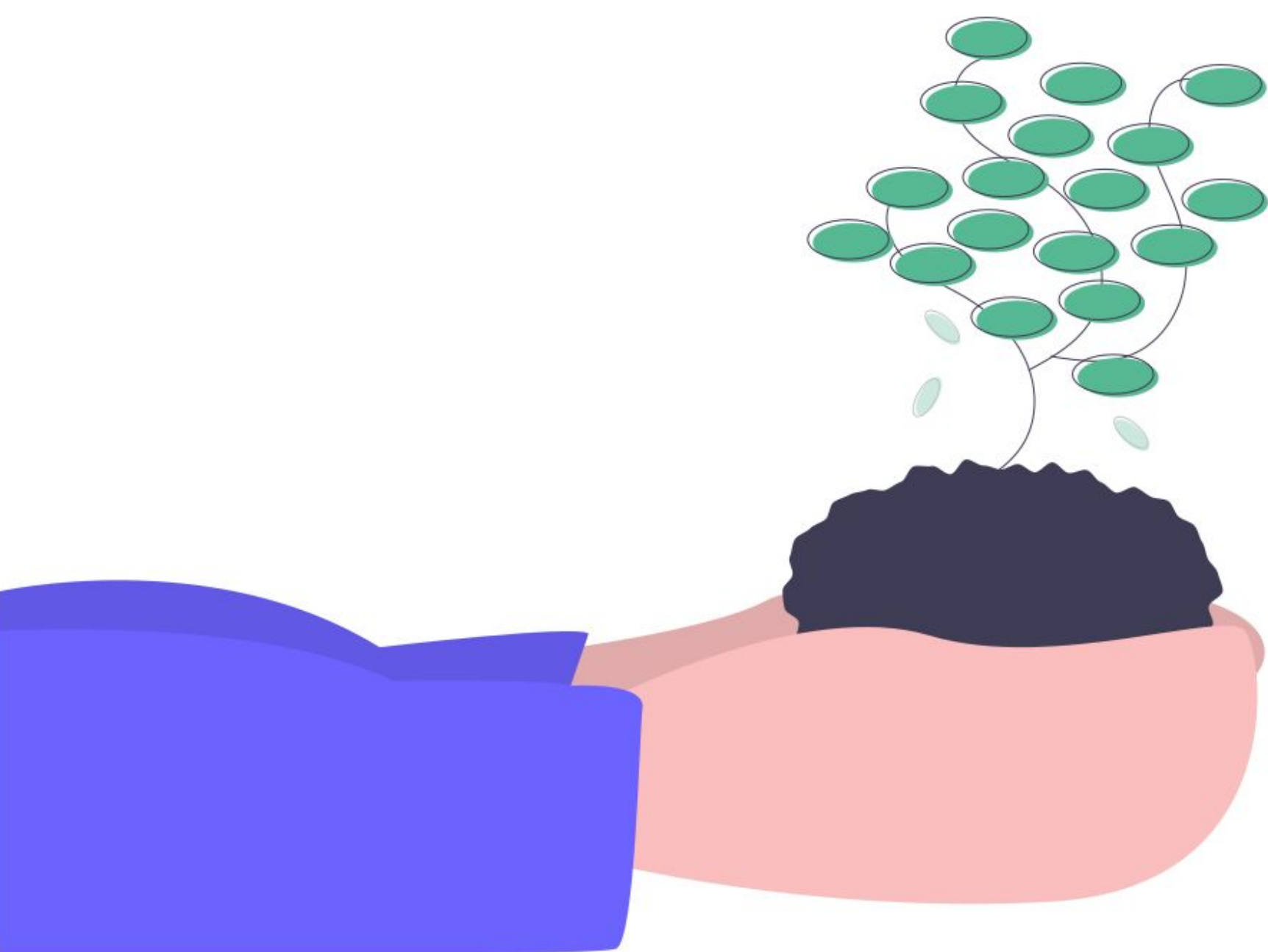


@adrienpessu

Introduction



Introduction



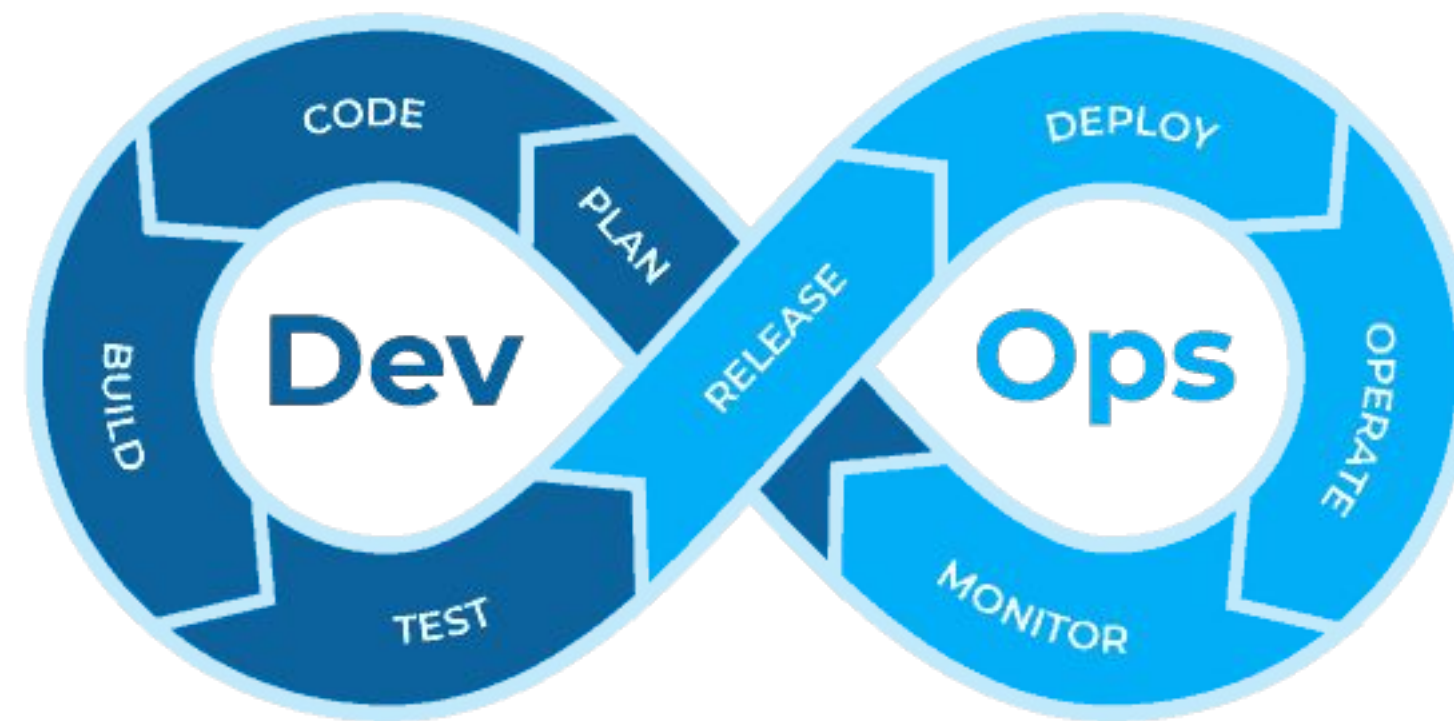
Introduction



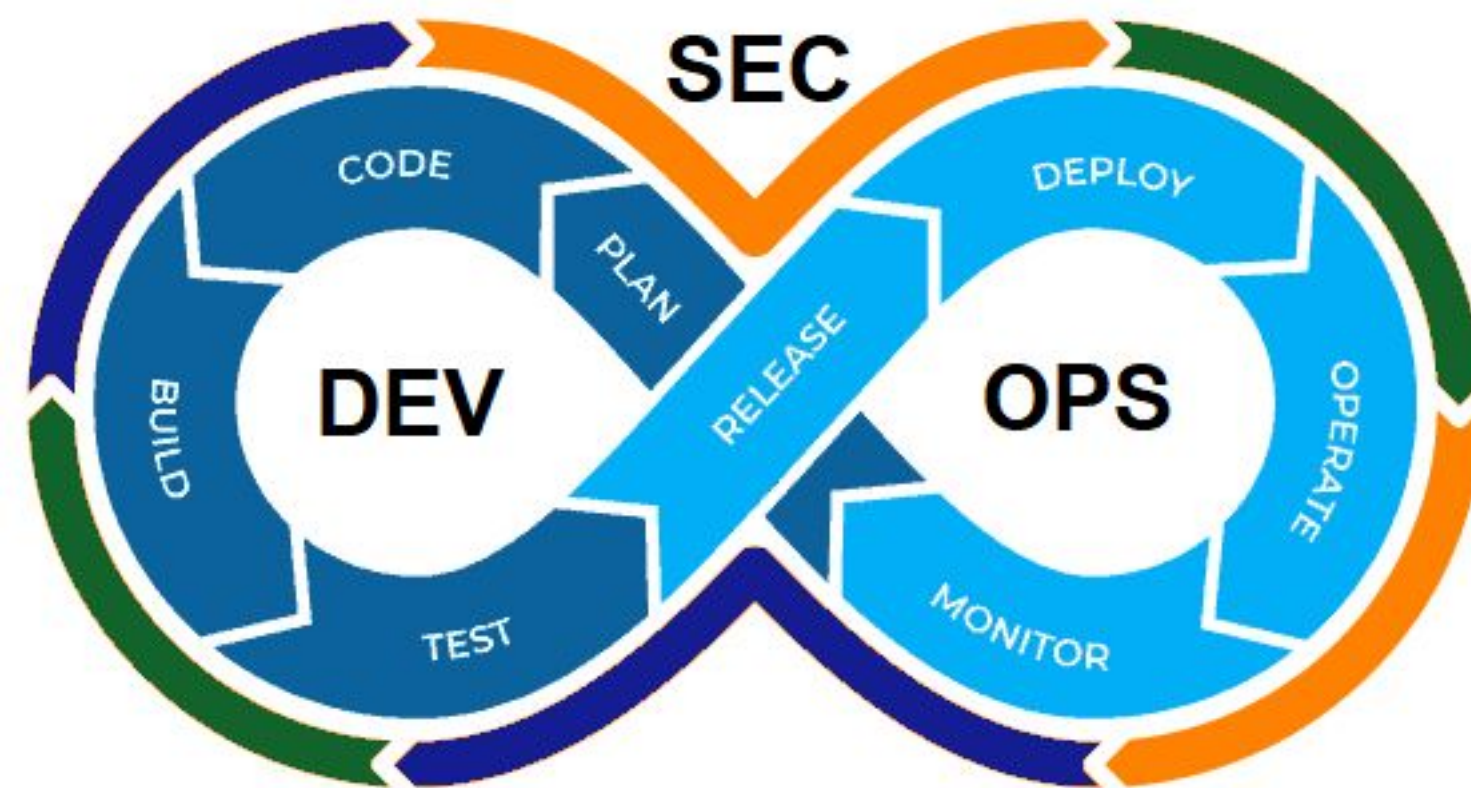
Oublier la cybersécurité, c'est "rouler à 200 km/h à
moto sans casque”

Guillaume Poupard, (futur ex-)patron de l'Anssi

Introduction

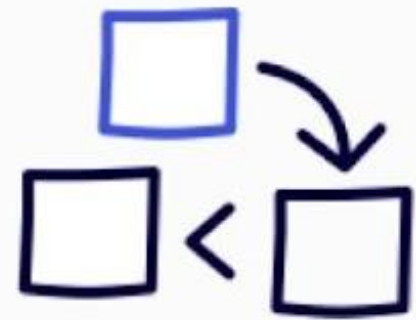


Introduction





Backlog



Code



Test



Deploy



Monitor



Threat
Modeling



SAST/SCA



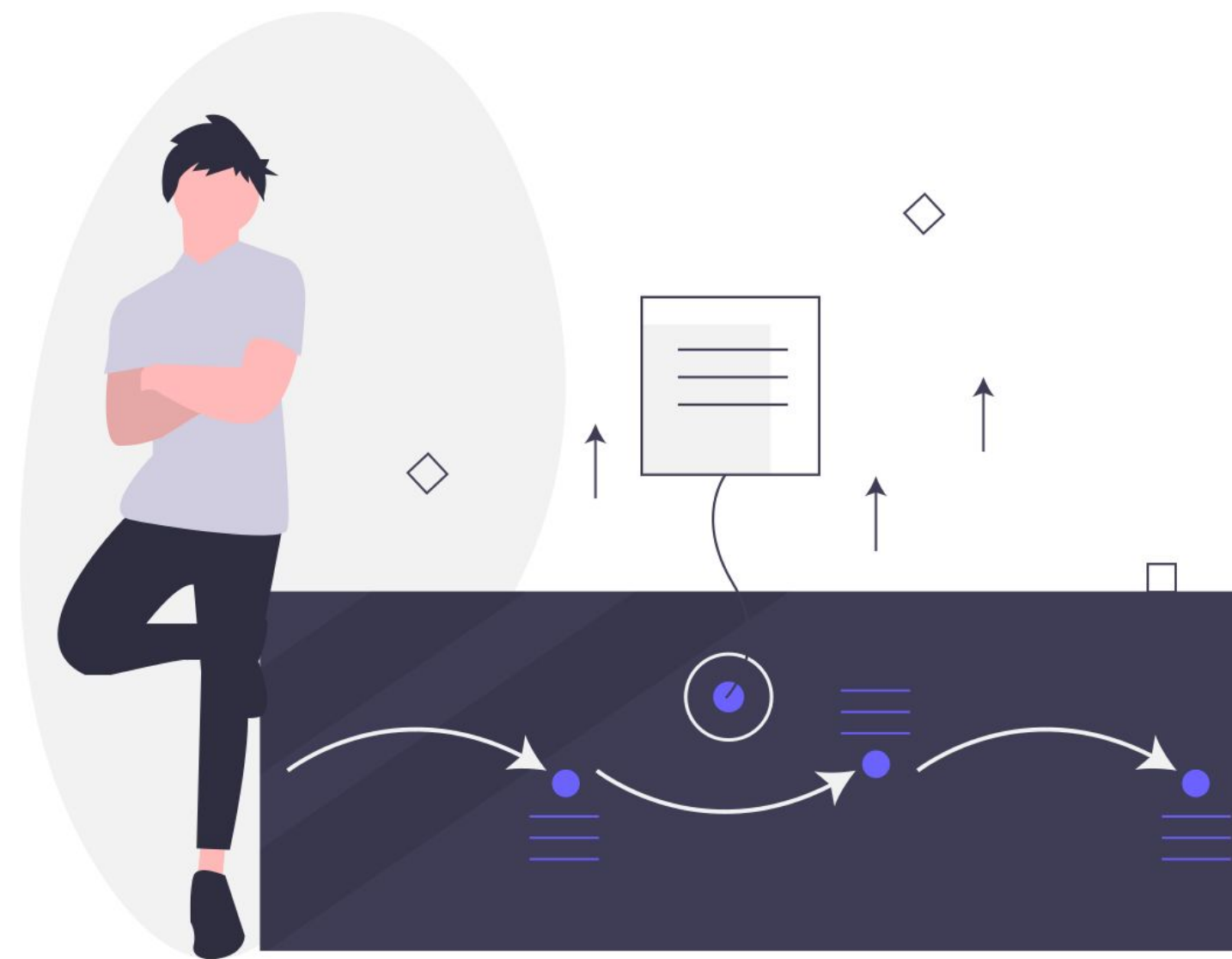
DAST



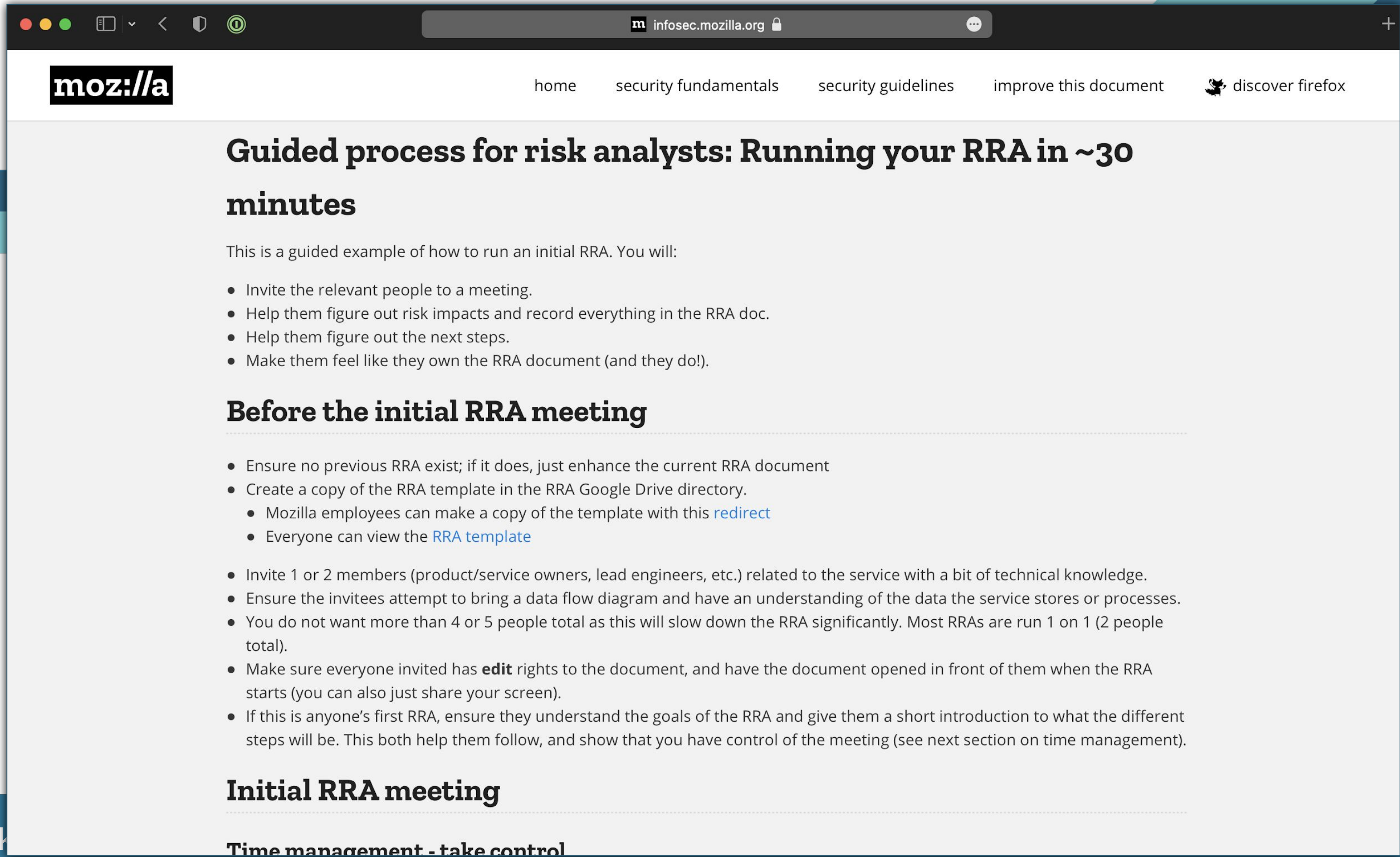
IAST



Penetration
test



Risk assessment



The screenshot shows a web browser window with the address bar displaying 'infosec.mozilla.org'. The page features the Mozilla logo and a navigation menu with links to 'home', 'security fundamentals', 'security guidelines', 'improve this document', and 'discover firefox'. The main heading is 'Guided process for risk analysts: Running your RRA in ~30 minutes'. Below this, a paragraph states: 'This is a guided example of how to run an initial RRA. You will:'. This is followed by a bulleted list of four steps: '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.', and 'Make them feel like they own the RRA document (and they do!)'. The next section is 'Before the initial RRA meeting', which includes a bulleted list of seven items: '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' (with sub-points for Mozilla employees using a 'redirect' and everyone viewing 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).', and '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)'. The final section is 'Initial RRA meeting', and the bottom of the page shows the start of a section titled 'Time management - take control'.

moz://a

home security fundamentals security guidelines improve this document discover firefox

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!).

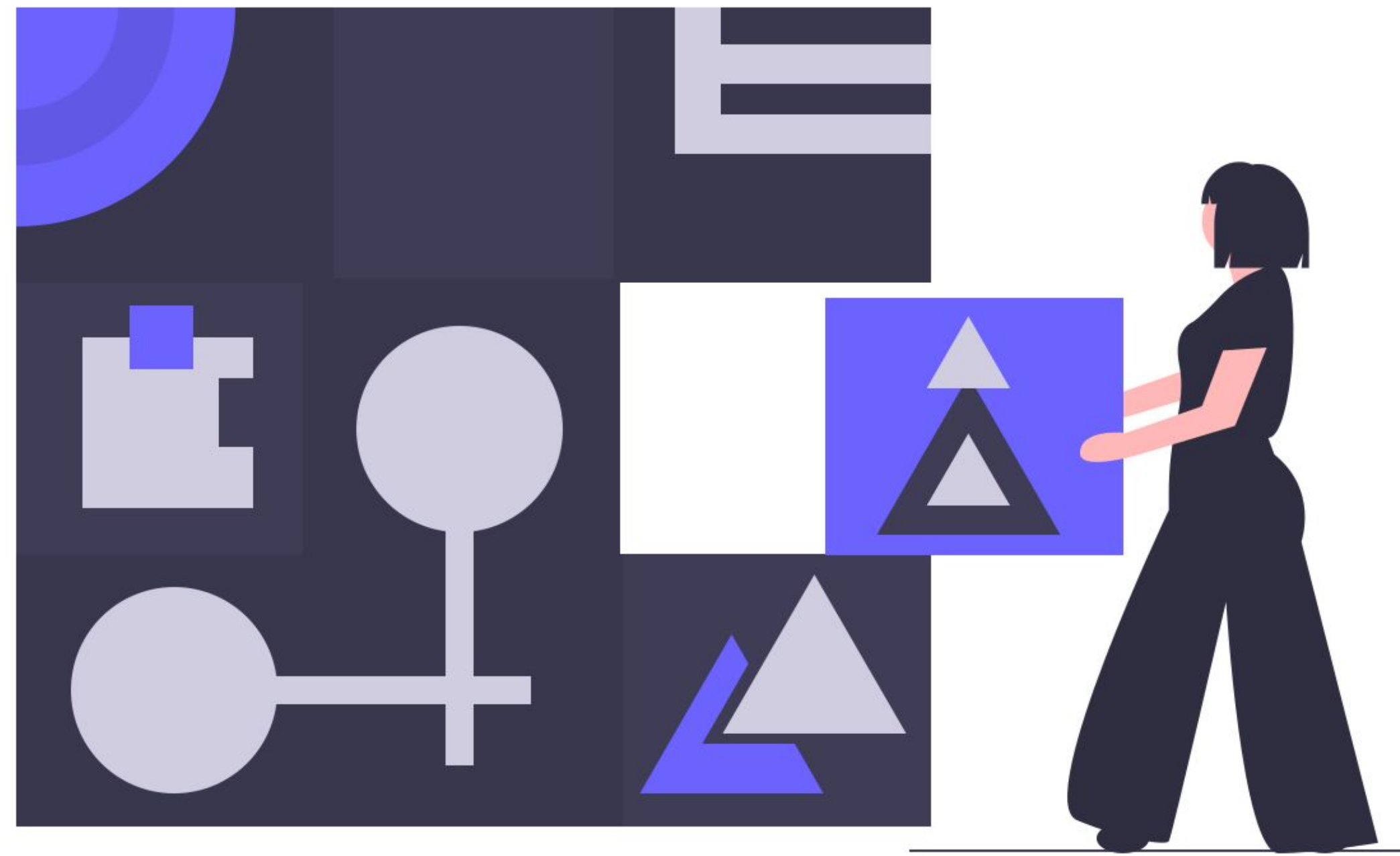
Before the initial RRA meeting

- 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

Threat modelling



SCA (SOFTWARE COMPOSITION ANALYSIS)

[GitHub Advisory Database](#) / [GitHub Reviewed](#) / CVE-2021-44228

Remote code injection in Log4j

Critical severity [GitHub Reviewed](#) Published on 10 Dec 2021 • Updated 27 days ago

Vulnerability details [Dependabot alerts](#) [0](#)

Package	Affected versions	Patched versions
 org.apache.logging.log4j:log4j-core (Maven)	>= 2.13.0, < 2.15.0 < 2.3.1 >= 2.4, < 2.12.2	2.15.0 2.3.1 2.12.2

Description

Summary

Log4j versions prior to 2.16.0 are subject to a remote code execution vulnerability via the ldap JNDI parser. As per [Apache's Log4j security guide](#): Apache Log4j2 <=2.14.1 JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.16.0, this behavior has been disabled by default.

Log4j version 2.15.0 contained an earlier fix for the vulnerability, but that patch did not disable attacker-controlled JNDI lookups in all situations. For more information, see the [Updated advice for version 2.16.0](#) section of this advisory.

Impact

Logging untrusted or user controlled data with a vulnerable version of Log4J may result in Remote Code Execution (RCE) against your application. This includes untrusted data included in logged errors such as exception traces, authentication failures, and other unexpected vectors of user controlled input.

Affected versions

Any Log4J version prior to v2.15.0 is affected to this specific issue.

The v1 branch of Log4J which is considered End Of Life (EOL) is vulnerable to other RCE vectors so the recommendation is to still update to 2.16.0 where possible.

Security releases

Additional backports of this fix have been made available in versions 2.3.1, 2.12.2, and 2.12.3

Affected packages

Only the `org.apache.logging.log4j:log4j-core` package is directly affected by this vulnerability. The `org.apache.logging.log4j:log4j-api` should be kept at the same version as the `org.apache.logging.log4j:log4j-core` package to ensure compatability if in use.

Remediation Advice

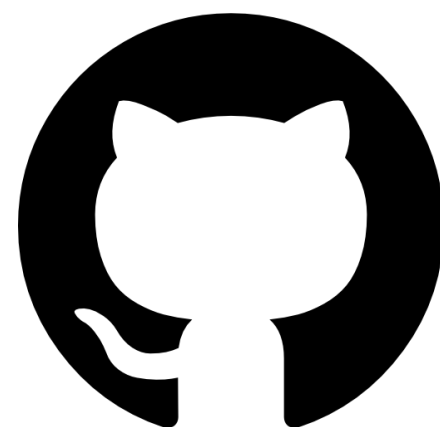
Updated advice for version 2.16.0

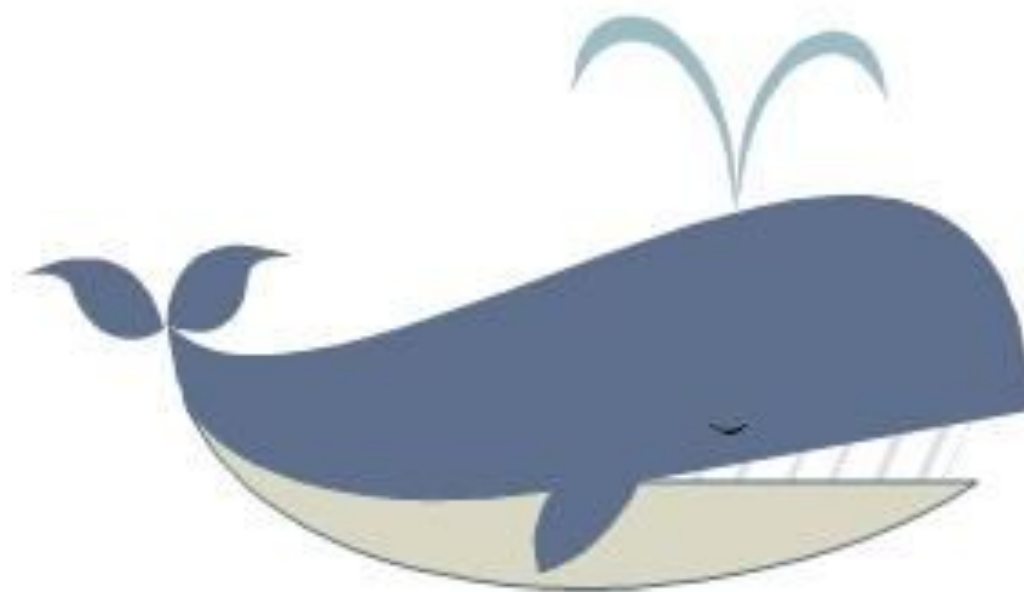
The Apache Logging Services team provided updated mitigation advice upon the release of version 2.16.0, which [disables JNDI by](#)

SCA (SOFTWARE COMPOSITION ANALYSIS)

Checkmarx

npm-audit





```
$ 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.

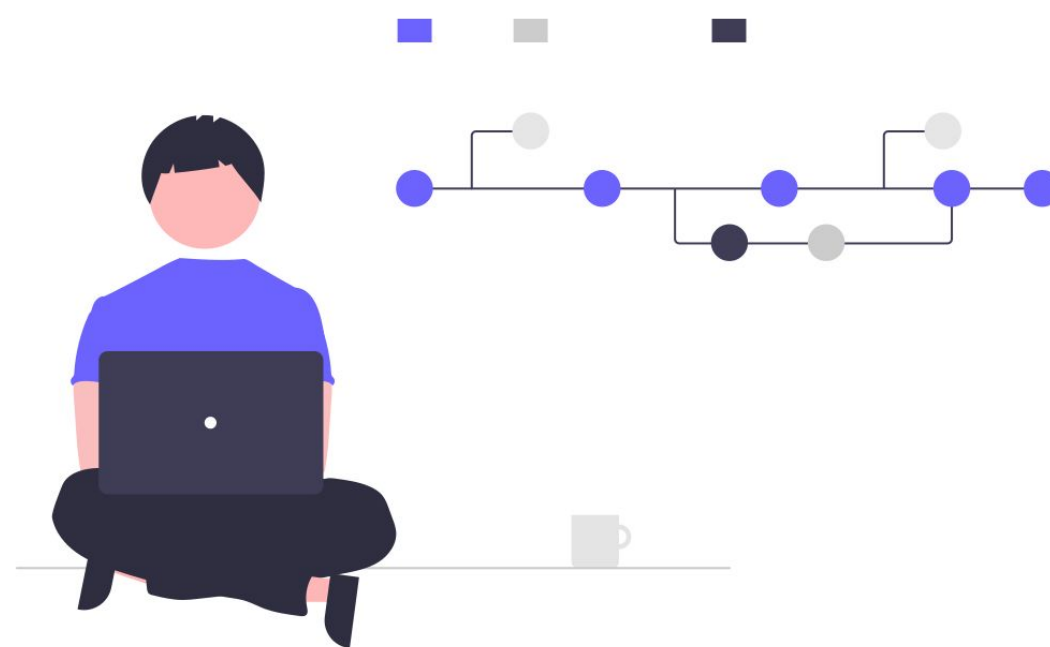
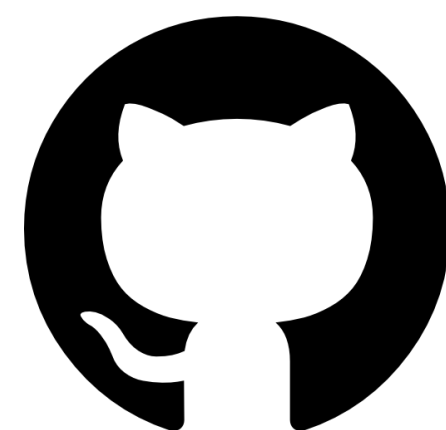
According to our scan, you are currently using the most secure version of the selected base image
```


SAST (STATIC APPLICATION SECURITY TESTING)

Checkmarx

{🐛} Find Security Bugs

🔗 [phpcs-security-audit v3](#)



SAST (STATIC APPLICATION SECURITY TESTING)

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

Bonjour {{ name }}, bienvenue à Rennes

Bonjour Adrien, bienvenue à Rennes



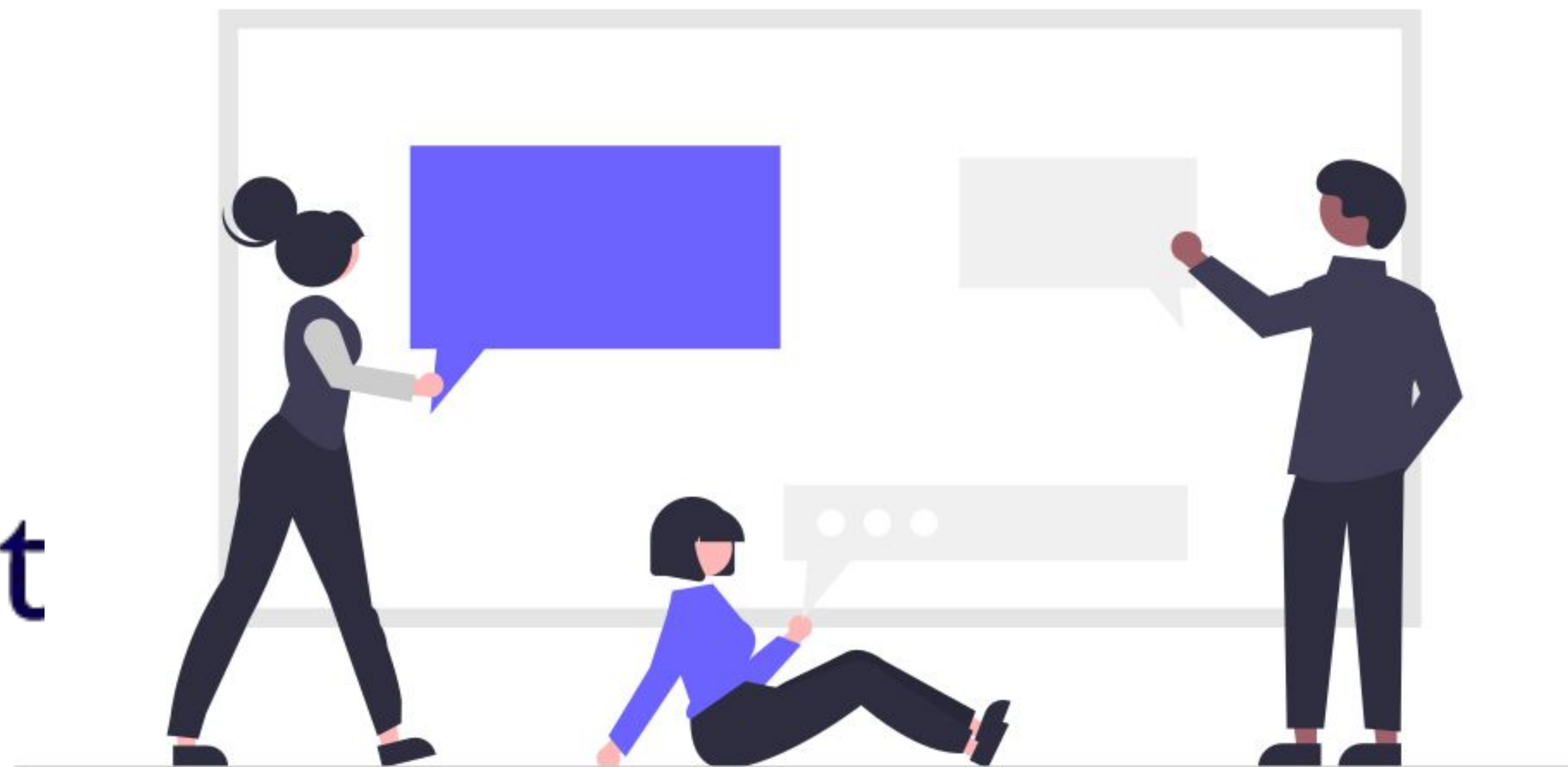
DAST (DYNAMIC APPLICATION SECURITY TESTING)



IAST (INTERACTIVE APPLICATION SECURITY TESTING)

SYNOPSYS®

 **Contrast**
SECURITY





Conclusion

