



La sécurité dès le début de la conception d'un projet

David Aparicio

Meetup Café DevOps
Jeudi 12 Décembre 2024, 18h30


[@dadideo](#)

David Aparicio

15/ DD INSA de Lyon / UNICAMP (Brésil)

Facebook Open Academy / MIT AppInventor

17/ Dev(Sec)Ops @ AMADEUS (Nice, 2 ans)

19/ Data(Sec)Ops @ OVHcloud (Lyon, 5 ans)

24/ Senior Dev(Sec)Ops @ Sopht (Lyon, 1 mois)





Une solution pensée pour un pilotage centralisé de votre écosystème IT

Collecte automatisée

Sur toute la chaîne de valeur d'un
écosystème IT

Observabilité à 360°

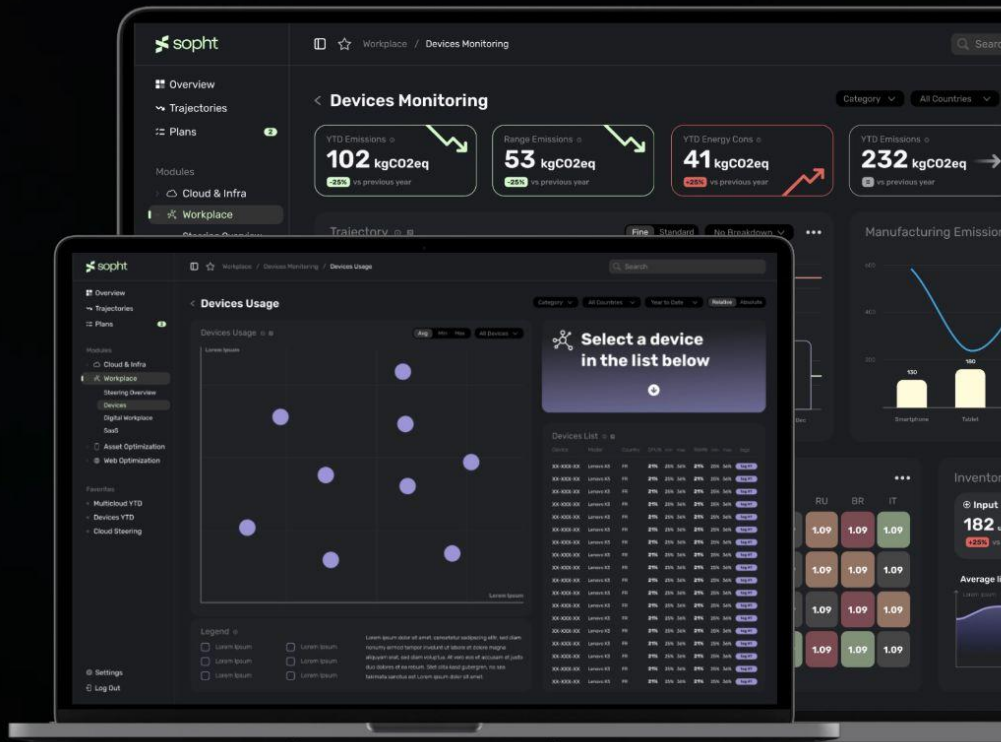
sur les scopes 1, 2 et 3
avec des données
granulaires et dynamiques

Actionnabilité guidée

Au moyen de simulations et
recommandations
contextualisées

Suivi d'impact

Avec l'incidence de vos actions
sur votre trajectoire en surveillant
l'impact CO2e





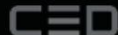
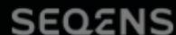
Observabilité

- Mesure complète de l'écosystème IT
- Couverture des scopes 1, 2 et 3
- Facteurs d'émission multicritères
- Exploration dynamique des données
- Projection et prévision d'impact
- Filtrage des données par entité

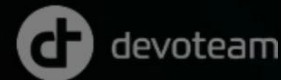




Nos principales références



Nos partenaires



Intégrations aux plateformes ESG





Témoignages

“

Évaluer et comprendre nos principaux facteurs d'émission est évidemment un enjeu en soi, mais les piloter de manière dynamique avec des plans d'actions concrets, c'est ce que nous permet la plateforme Sopht.

**Marie Ait-Daoud**

Green IT manager

Vinci Groupe



Agenda

Introduction

Outils

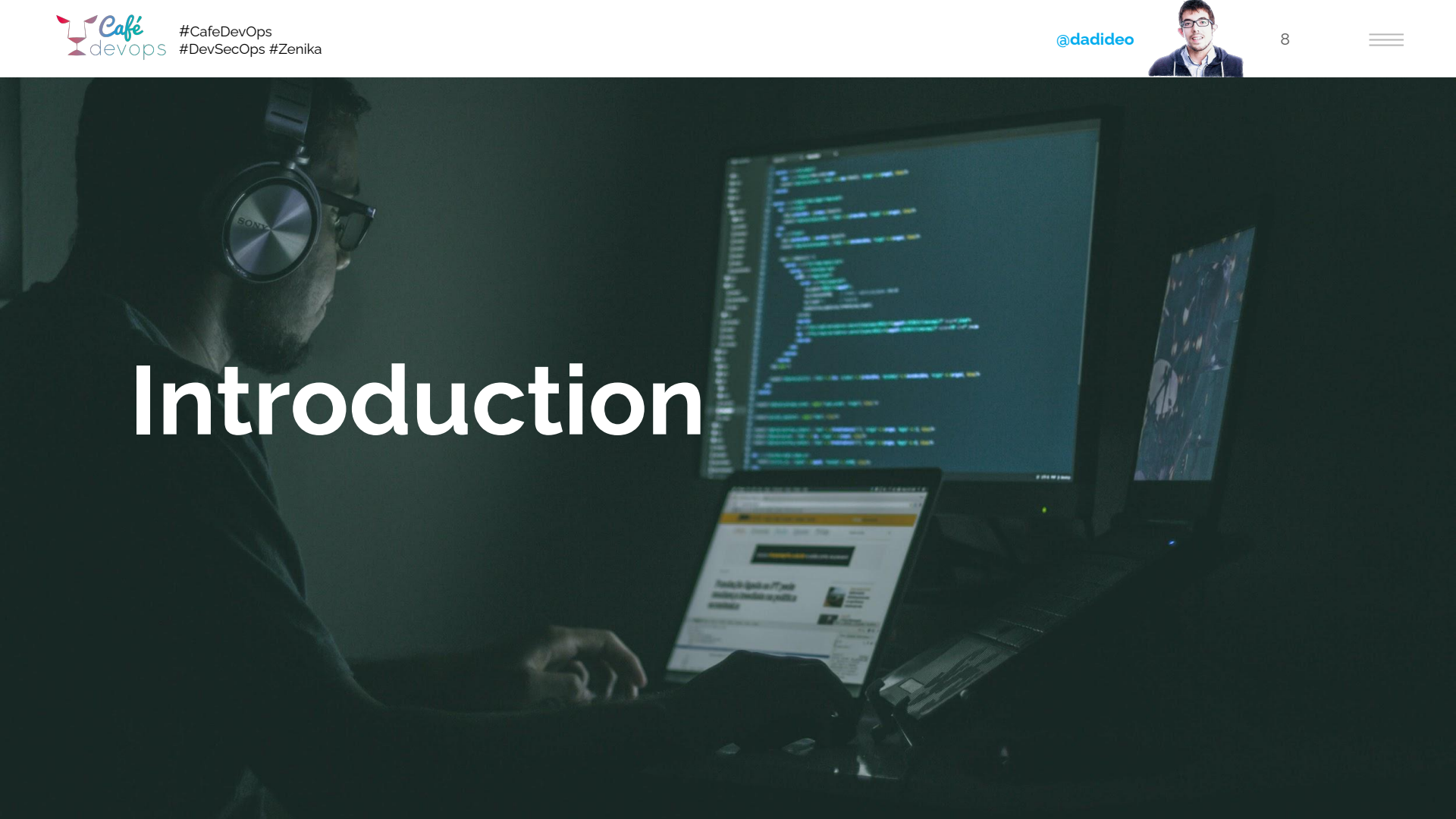
Conseils

Demo

Conclusion

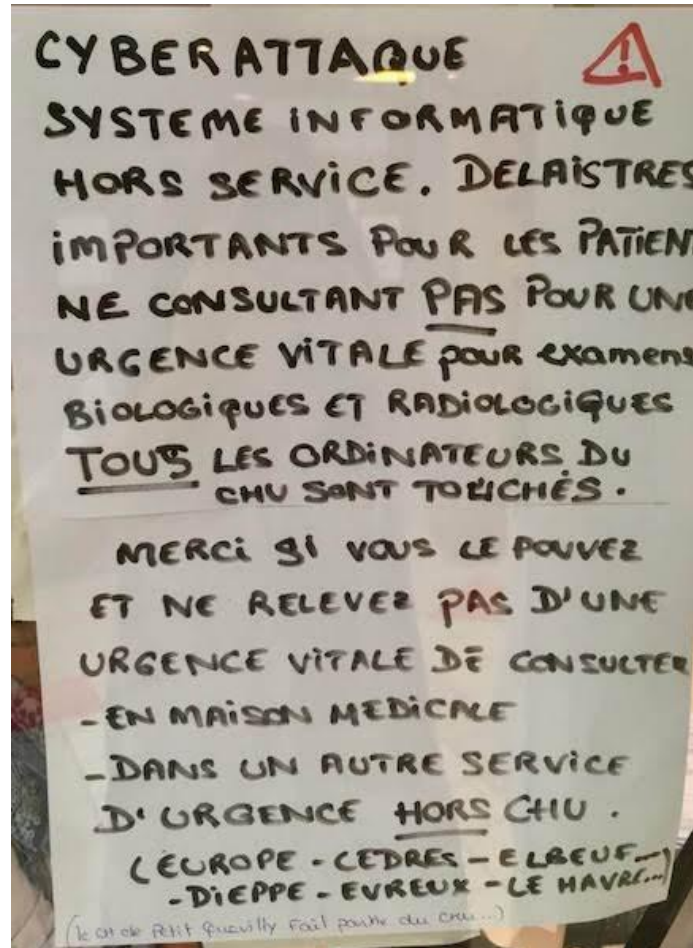


Introduction





Pourquoi ce talk ?



[Thread @zigazou](#)

Agir.. Avant la PROD!

Y a-t-il un pilote à jour dans l'avion?

En 2015, les autorités états-uniennes de l'aviation alertaient les compagnies aériennes: le Boeing 787 Dreamliner devait être redémarré tous les 248 jours pour contourner un bogue pouvant entraîner une coupure de courant généralisée dont on peut imaginer les conséquences en vol. Cette fois, elles ont

annoncé qu'il faut éteindre et rallumer ces mêmes avions tous les 51 jours pour éviter des problèmes informatiques catastrophiques en raison d'une mémoire saturée de données sinon. Mesdames et Messieurs, veuillez regagner vos places et attacher vos ceintures de sécurité, nous allons bientôt rebouter!



Octobre 2020.

Le Virus Informatique
n°44 (papier/en ligne)



Pourquoi ?

2013	2017 (new, * from the community)	2021 (new, * from the survey)
A1 - Injection	A1 - Injection	A1 - Broken Access Control
A2 - Broken Authentication & Session Management	A2 - Broken Authentication	A2 - Cryptographic Failures
A3 - Cross-Site Scripting (XSS)	A3 - Sensitive Data Exposure	A3 - Injection
A4 - Insecure Direct Object References	A4 - XML External Entities (XXE)	A4 - Insecure Design
A5 - Security Misconfiguration	A5 - Broken Access Control [MERGED A4+A7]	A5 - Security Misconfiguration
A6 - Sensitive Data Exposure	A6 - Security Misconfiguration	A6 - Vulnerable and Outdated Components
A7 - Missing Function Level Access Control	A7 - Cross-Site Scripting (XSS)	A7 - Identification and Authentication Failures
A8 - Cross-Site Request Forgery (CSRF)	A8 - Insecure Deserialization *	A8 - Software and Data Integrity Failures
A9 - Using Components with Known Vulnerabilities	A9 - Using Components with Known Vulnerabilities	A9 - Security Logging and Monitoring Failures *
A10 - Unvalidated Redirects and Forwards	A10 - Insufficient Logging & Monitoring *	A10 - Server-Side Request Forgery (SSRF) *
OWASP TOP 10		





Bonjour ChatGPT! Peux-tu me donner des actions concrètes pour sécuriser mon code ?



Bonjour! Voici quelques actions concrètes pour sécuriser votre code :

1. Effectuer des tests d'intrusion réguliers pour détecter les vulnérabilités dans votre code.
2. Utiliser des mots de passe forts et un stockage sécurisé des mots de passe.
3. Valider toutes les entrées utilisateur pour éviter les attaques par injection SQL ou d'autres types d'injection.
4. Utiliser des autorisations d'accès appropriées pour limiter l'accès aux fonctionnalités sensibles de votre application.
5. Utiliser des bibliothèques et des frameworks de sécurité réputés pour ajouter des couches supplémentaires de sécurité à votre code.
6. Assurez-vous que vos dépendances et bibliothèques utilisées sont à jour et sécurisées.
7. Utilisez des outils pour détecter les vulnérabilités de sécurité automatiquement.
8. Utilisez des mécanismes de chiffrement pour protéger les données sensibles.
9. Utilisez des certificats SSL pour sécuriser les communications réseau.
10. Utilisez une stratégie de gestion des vulnérabilités pour gérer efficacement les vulnérabilités de sécurité détectées.



Sécurité dès la conception

Du domaine du **Génie Logiciel**

Souvent associé à **Privacy By Design**

Considérer la sécurité comme une **partie intégrante**

Conception d'architecture **robuste**

Résistant aux attaques **bien connues**

Utilisant des techniques **réutilisables**

Minimiser l'impact **en prévision** des vulnérabilités

Exigences dans de **multiples domaines** (auth., intégrité, confidentialité, etc...)

Même lorsque le système est attaqué

Préserver l'architecture pendant l'évolution du logiciel

Mise en oeuvre durant tout le **cycle de vie**, jusqu'à la fin du support, et donc une date de **décommissionnement**



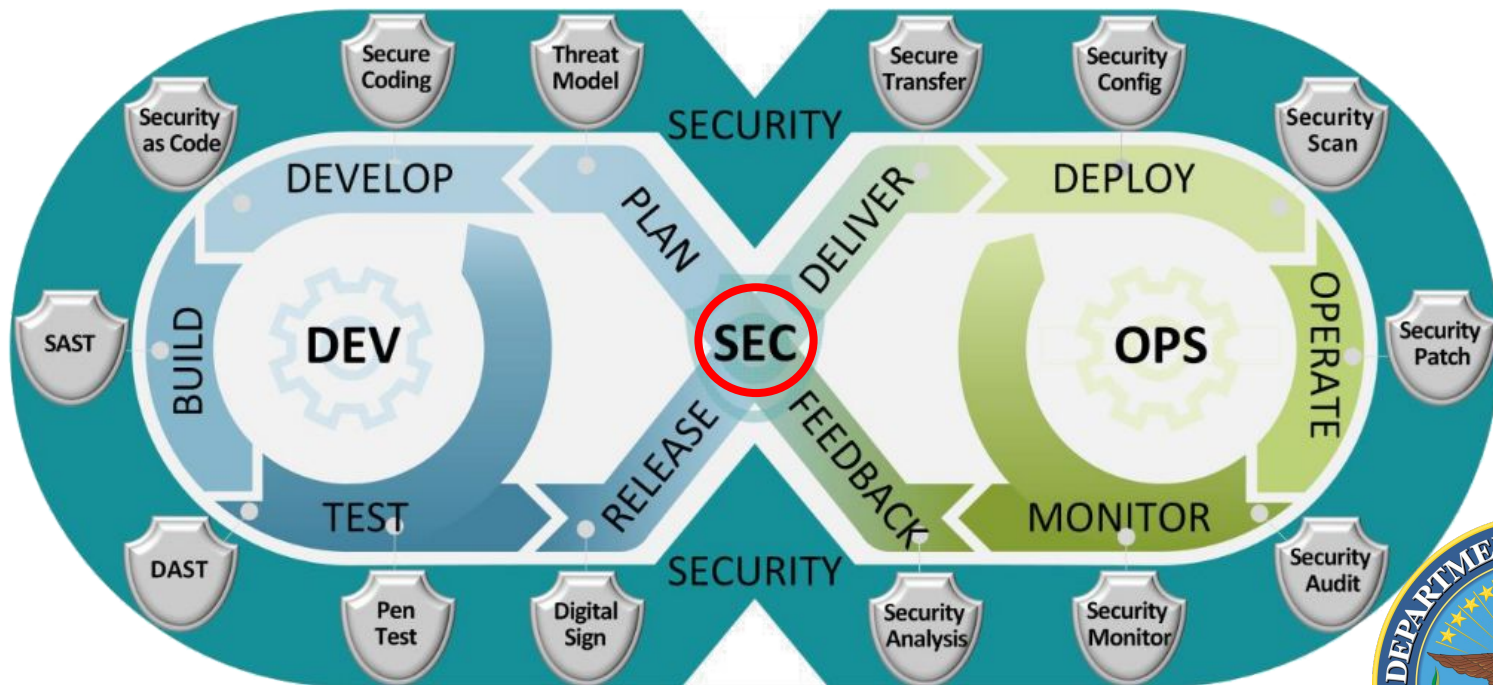


Voici quelques actions concrètes pour sécuriser votre chaîne d'intégration et de déploiement (CI/CD) :

1. Utiliser des outils de gestion de code source pour gérer les autorisations d'accès aux dépôts de code.
2. Automatiser les tests de sécurité dans le pipeline de CI/CD pour détecter les vulnérabilités dans le code avant le déploiement.
3. Utiliser des outils de chiffrement pour protéger les données sensibles stockées dans les conteneurs ou les images de conteneur.
4. Utiliser des outils de gestion de configuration pour s'assurer que les paramètres de sécurité sont correctement configurés dans les environnements de déploiement.
5. Utiliser des outils de surveillance pour surveiller les activités de la chaîne d'intégration et de déploiement pour détecter les anomalies et les comportements suspects.
6. Utiliser des outils de gestion des accès pour contrôler qui peut déployer des applications et dans quels environnements.
7. Utiliser des outils de gestion des vulnérabilités pour suivre les vulnérabilités de sécurité dans les dépendances et les bibliothèques utilisées dans le pipeline CI/CD.
8. Automatiser les mises à jour de sécurité pour les dépendances et les bibliothèques utilisées dans le pipeline CI/CD.
9. Utiliser des outils pour automatiser les audits de sécurité pour les environnements de production.
10. Utiliser des outils pour automatiser le déploiement d'applications dans des environnements sécurisés.

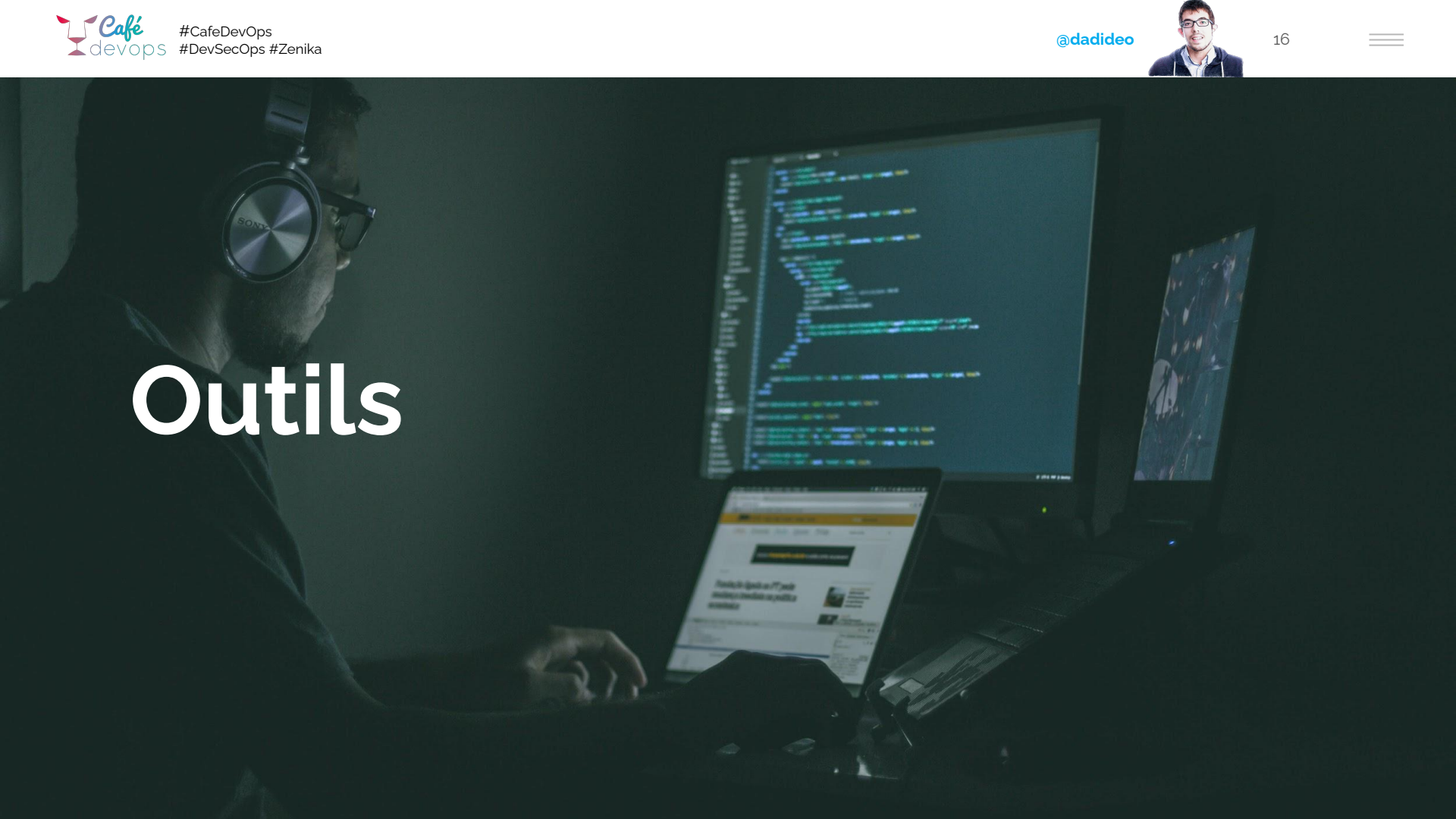


Shift-left Security



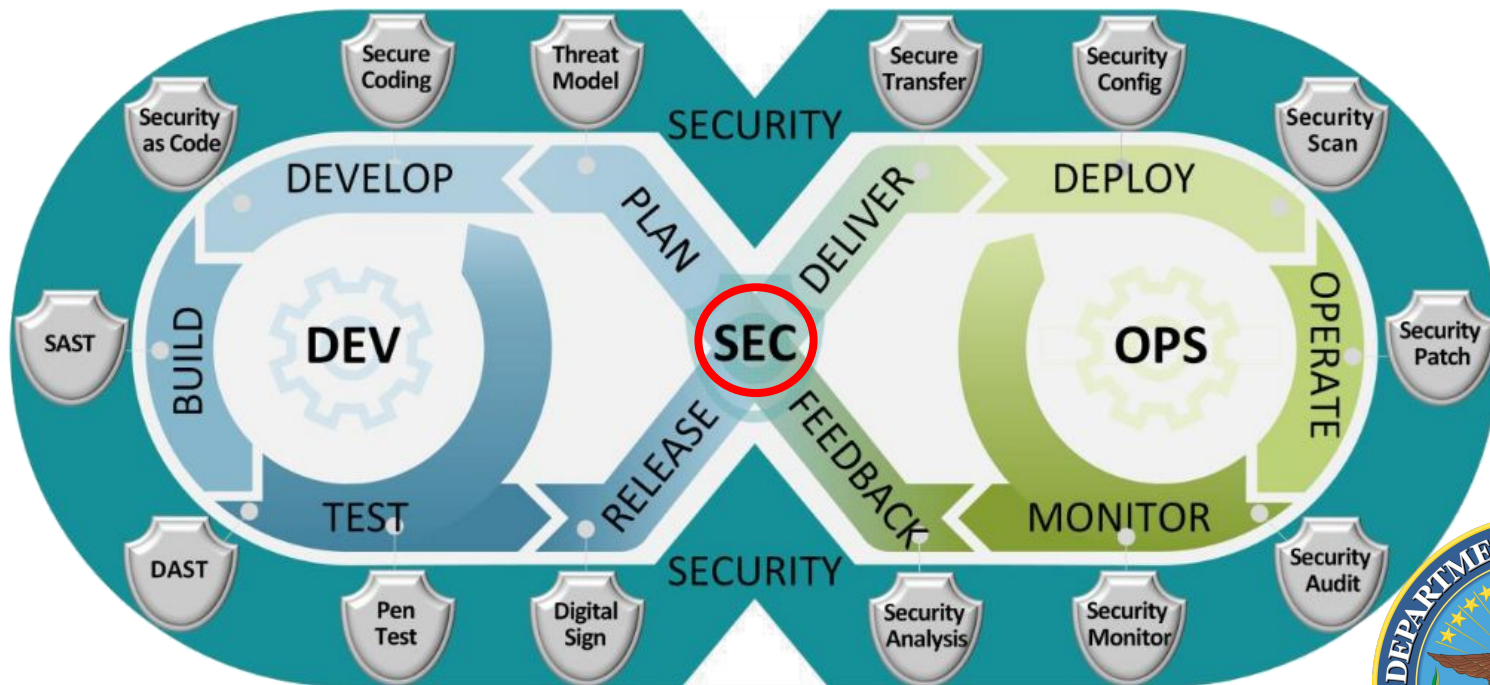


Outils





Shift-left Security





DevOps



CI/CD

Pipeline Jobs 5



[Philippe Charrière \(Twitter\)](#)



Plan: Threat Model



Bonnes pratiques ANSSI

Se documenter, se former

Lire les guides de l'ANSSI

Comparer les technologies, les langages de programmation

Effectuer l'analyse des risques

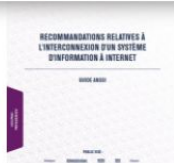
Identifier le modèle de l'attaquant pour ce produit en particulier

Préparer des spécifications / des ateliers

Participer à des conférences Sécurité

Choix du système hôte ([OS hardening](#))

Veille technologique ([Feedly/RSS](#))

**ANSSI**Agence nationale de la sécurité des
systèmes d'information**RECOMMANDATIONS RELATIVES À L'INTERCONNEXION D'UN SYSTÈME D'INFORMATION À INTERNET**

Réseaux

19/06/2020

architecture

interconnexion

Internet

messagerie

passerelle

**RÈGLES DE PROGRAMMATION POUR LE DÉVELOPPEMENT D'APPLICATIONS SÉCURISÉES EN RUST**

09/06/2020

application sécurisée

bonne pratique

développement sécurisé

langage Rust

règle

**RECOMMANDATIONS DE SÉCURITÉ RELATIVES À TLS**

Cryptographie Réseaux

26/03/2020

chiffrement

HTTPS

TLS

**RECOMMANDATIONS SUR LA SÉCURISATION DES SYSTÈMES DE CONTRÔLE D'ACCÈS VIDÉOPROTECTION**Bonnes pratiques de sécurité numérique (ANSSI)



Dev: Secure Coding/SaC



Linters

Go

Un linter est un outil d'analyse statique de code source. Il sert à détecter : des erreurs (très utile sur des langages interprétés comme JavaScript qui n'ont pas de phase de compilation) ; des problèmes de syntaxe et de non-respect de style (tabulation vs espaces, indentation, etc.)

STATIC LINTS WITH GOLANG-CI



Customize: linters list, values...

In few situations you can bypass the linters with nolint directive.

//nolint

```
linters:  
  disable-all: true  
  enable:  
    - bodyclose  
    - deadcode  
    - depguard  
    - dogsled  
    - dupl  
    - errcheck  
    - funlen  
    - goconst  
    - gocritic  
    - gocyclo  
    - gofmt  
    - goimports  
    - golint  
    - gomnd  
    - goprintffuncname  
    - gosec  
    - gosimple  
    - govet  
    - ineffassign  
    - interfacer  
    - misspell  
    - nakedret  
    - rowserrcheck  
    - scopelint  
    - staticcheck  
# ...
```



"Common mistakes" en Go, Aurélie Vache
(Async 2021)



Linters

Shell

Il permet d'avoir un code avec moins d'effets de bord
Disponible dans (quasiment) tous les langages

```
$ shellcheck myscript

Line 4:
if ! grep -q backup=true.* "~/.myconfig"
      ^-- SC2062: Quote the grep pattern so the
          ^-- SC2088: Tilde does not

Line 6:
echo 'Backup not enabled in $HOME/.myconfig, exiting
     ^-- SC2016: Expressions don't expand in single

Line 10:
if [[ $1 =~ "-v(erbos)e?" ]]
      ^-- SC2076: Don't quote right-hand side of

Line 12:
verbose='-printf "Copying %f\n"'
      ^-- SC2089: Quotes/backslashes will be treat

Line 16:
-iname *.tar.gz \
      ^-- SC2061: Quote the parameter to -iname so
      ^-- SC2035: Use ./*glob* or -- *glob* so name
```



[ShellCheck, finds bugs in your shell scripts](#)

Docker CLI



Guillaume 🐻
@glours



Replying to @glours @silvin_docker and 2 others

With a better Gif and a link to the documentation
docs.docker.com/engine/scan/

```
~/docker/scan (zsh) 361 ..an-cli-plugin (zsh) 362
100%
docker scan hello-world

Testing hello-world...

Organization:    docker-desktop-test
Package manager: linux
Project name:    docker-image|hello-world
Docker image:   hello-world
Licenses:       enabled

/ Tested hello-world for known issues, no vulnerable paths found.

Note that we do not currently have vulnerability data for your image.
```

12:11 PM · Sep 2, 2020 · TweetDeck



[Vulnerability scanning - Docker Documentation](https://docs.docker.com/engine/scan/)



19/10/20

→ ↺ 🏠 🔒 https://securite.developpez.com/actu/309772/Quatre-packages-npm-trouves-en-train-d-ou... 📄 ⋮ 🌟 ⬇

Quatre packages npm trouvés en train d'ouvrir des shells sur des systèmes Linux et Windows.

Tout ordinateur avec l'un de ces packages installés « doit être considéré comme totalement compromis »

Le 19 octobre 2020 à 12:27, par [Stan Adkens](#) 6 commentaires



364 PARTAGES

👍 15 🗨 0



L'équipe de sécurité de npm a supprimé la semaine dernière quatre packages hébergés sur son dépôt, découverts en train d'ouvrir des shells afin d'établir une connexion à des serveurs distants pour exfiltrer les données des utilisateurs à partir des systèmes Linux et Windows infectés. Selon l'équipe de sécurité, chaque bibliothèque a été téléchargée des centaines de fois depuis son chargement sur le portail npm.

Les noms des quatre packages npm sont : plutov-slack-client, nodetest199, nodetest1010 et nmpubman. Les packages ont été mis en ligne sur le portail npm en mai 2018 (en ce qui concerne le premier) et en septembre de la même année (pour le reste). Jeudi dernier, le personnel du npm a retiré les quatre paquets JavaScript du portail npm parce qu'ils contenaient du code malveillant.



npm est le plus grand dépôt de packages pour tous les langages de programmation. L'équipe de sécurité de npm scanne régulièrement sa collection de bibliothèques JavaScript, considérée comme le plus important dépôt. Bien que les paquets malveillants soient régulièrement supprimés, la suppression de la semaine dernière est la troisième grande mesure de répression de ces trois derniers mois.

Selon les avis publiés par l'équipe de sécurité de npm, les quatre bibliothèques JavaScript ont ouvert des shells sur les ordinateurs des développeurs qui ont importé ces packages dans leurs projets. Les shells permettaient aux acteurs de la



[4 packages npm ouvrent des shells \[Linux/Windows\]](#)



npm-audit Javascript

Auditer les vulnérabilités connues des librairies et des dépendances associées

```
High | Arbitrary File Overwrite
Package | tar
Patched in | >=4.4.2
Dependency of | libnpm
Path | libnpm > npm-lifecycle > node-gyp > tar
More info | https://npmjs.com/advisories/803

High | Arbitrary File Overwrite
Package | tar
Patched in | >=4.4.2
Dependency of | npm-lifecycle
Path | npm-lifecycle > node-gyp > tar
More info | https://npmjs.com/advisories/803

Found 19 vulnerabilities (8 moderate, 11 high) in 11360 scanned packages
run 'npm audit fix' to fix 4 of them.
12 vulnerabilities require semver-major dependency updates.
3 vulnerabilities require manual review. See the full report for details.
```



[npm-audit | npm Docs](#)



Github Code Scanning

Il permet d'avoir un retour rapide
directement dans son code
(sur les failles)



[Github Code Scanning](#) / [Démonstration TelecomValley](#)



Pas copier-coller depuis StackOverFlow

98% snippets sécu/crypto sont insecure



Fisher et al., 2017; Nadi et al., 2016; Das et al., 2014, Prevent cryptographic pitfalls by design



GitHub Copilot Security Study: 'Developers Should Remain Awake' in View of 40% Bad Code Rate

By David Ramel 08/26/2021

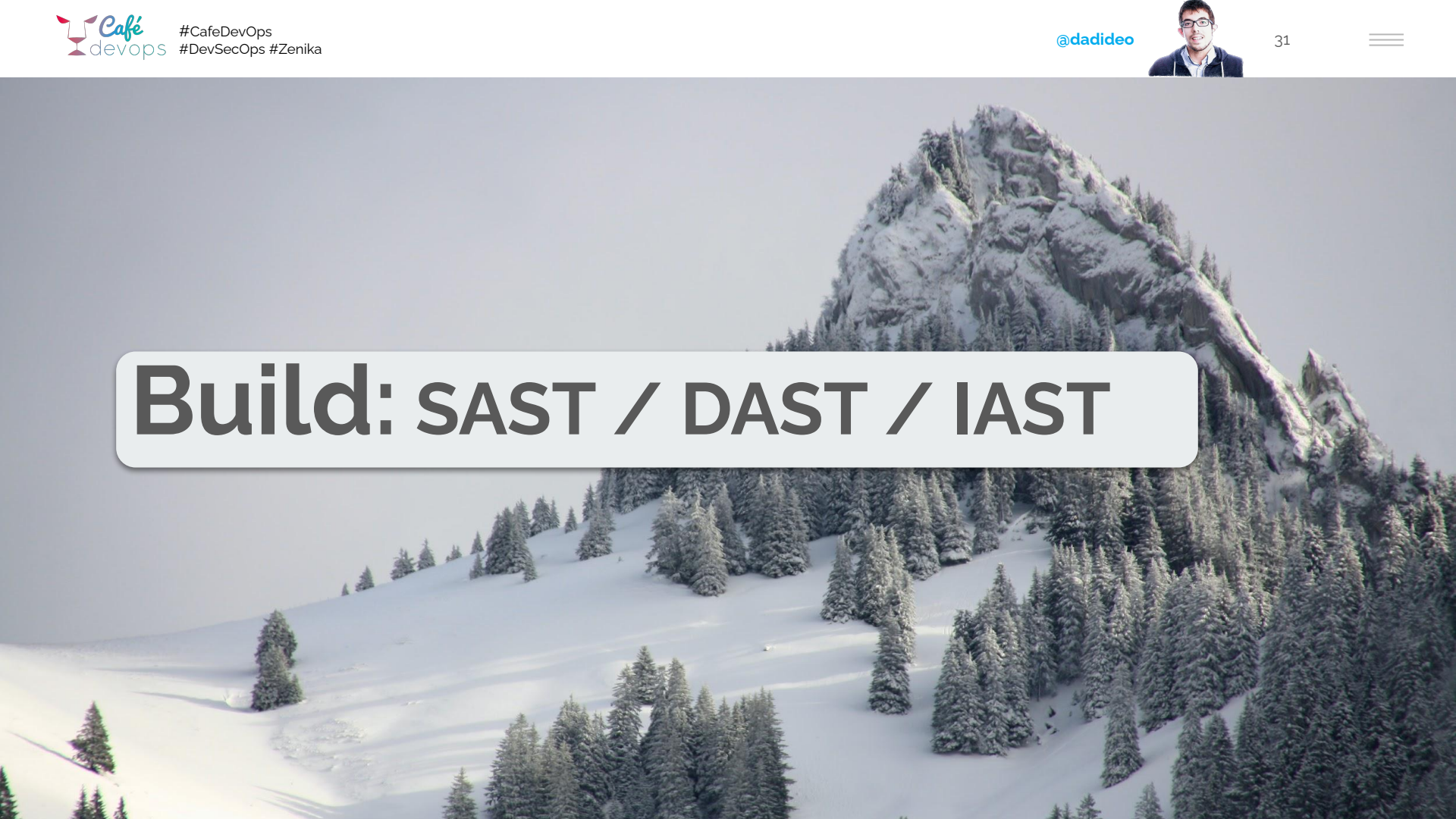
Researchers published a scholarly paper looking into security implications of GitHub Copilot, an advanced AI system now being used for code completion in Visual Studio Code and possibly headed for Visual Studio after its current preview period ends.

In multiple scenario testing, some 40 percent of tested projects were found to include security vulnerabilities.

GitHub Copilot is described as an "**AI pair programmer**" whose advanced AI



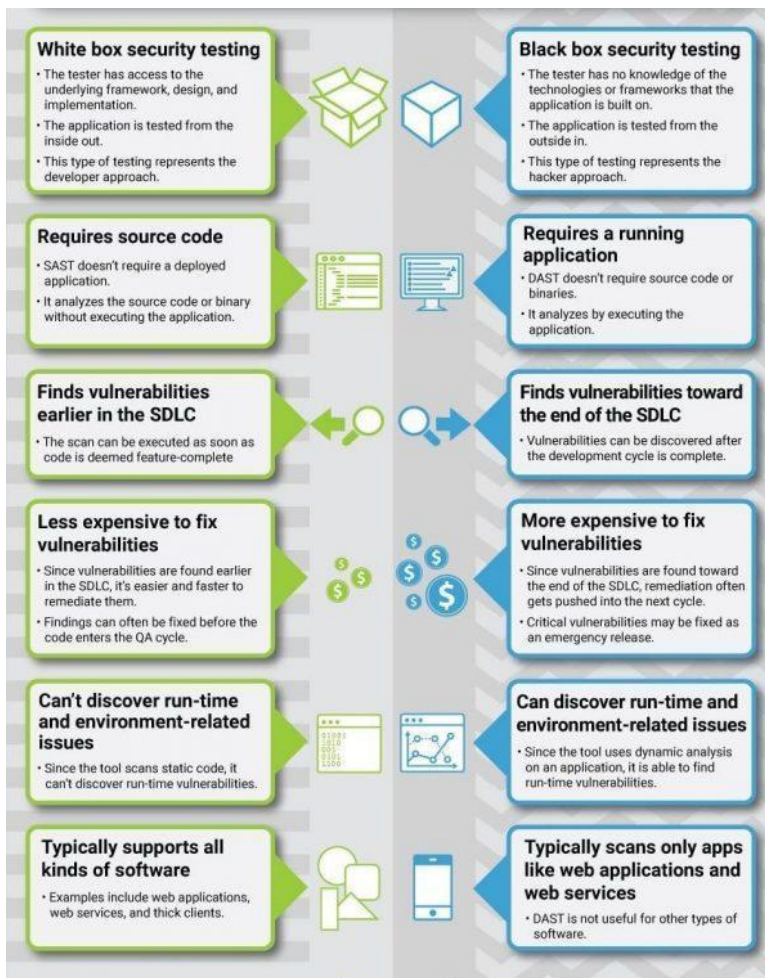
[40% of Code Produced by GitHub Copilot Vulnerable to Threats](#)



Build: SAST / DAST / IAST



SAST DAST IAST App Security Test





AWS git-secrets / GitGuardian



1 policy break detected!

ca-certificates.crt – FILE EXTENSIONS

2022-10-11 10:35:19 pm (UTC)

 davidaparicio/namecheck

See on GitGuardian

SEE ON GITHUB

[GitGuardian](#) is an automated secrets detection service.

We help developers and security teams secure the modern software development process.



Sonar

```
246  if (Provider.class == roleTypeClass) {  
247      Type providedType = ReflectionUtils.getLastTypeGenericArgument(dependen  
248      2 Class providedClass = 1 ReflectionUtils.getTypeClass(providedType);  
249  
250      if (this.componentManager.hasComponent(providedType, dependencyDescript  
251      || 3 providedClass.isAssignableFrom(List.class) || providedClass.
```

A "NullPointerException" could be thrown; "providedClass" is nullable here.



Bug



Major



cert, cwe

```
252      continue;  
253  }
```

Reliability



Bugs

2

B

1

B

Security



Security Vulnerabilities

0

A

0

A



Security Hotspots

39

-

0

-

Maintainability



Technical Debt

6 days

C

0

A



Code Smells

319

-

0

-

New code

Since last release



Sonar Dashboard



Snyk



davidaparicio's weekly report

2nd of September – 9th of September 2020

Status of all 4 active projects

1 known vulnerability 1 H 0 M 0 L	49 total dependencies
--	---

Review the status of your projects on your dashboard.

[View on Snyk](#)

If you have any questions, [we're happy to help](#).

Stay secure!
The Snyk team



DAST (Gitlab)

Language (package managers) / framework	Scan tool
.NET Core	Security Code Scan
C/C++	Flawfinder
Go	Gosec
Helm Charts	Kubesecc
Java (Ant , Gradle , Maven , SBT)	SpotBugs with find-sec-bugs
Java / Kotlin (Android)	MobSF (beta)
JavaScript	ESLint security plugin
Kubernetes manifests	Kubesecc
Node.js	NodeJsScan
PHP	phpcs-security-audit
Python (pip)	bandit

Available rules

- G101: Look for hard coded credentials
- G102: Bind to all interfaces
- G103: Audit the use of unsafe block
- G104: Audit errors not checked
- G106: Audit the use of ssh.InsecureIgnoreHostKey
- G107: Url provided to HTTP request as taint input
- G108: Profiling endpoint automatically exposed on /debug/pprof
- G109: Potential Integer overflow made by strconv.Atoi result conversion to int16/32
- G110: Potential DoS vulnerability via decompression bomb
- G201: SQL query construction using format string
- G202: SQL query construction using string concatenation
- G203: Use of unescaped data in HTML templates
- G204: Audit use of command execution
- G301: Poor file permissions used when creating a directory
- G302: Poor file permissions used with chmod
- G303: Creating tempfile using a predictable path
- G304: File path provided as taint input
- G305: File traversal when extracting zip/tar archive
- G306: Poor file permissions used when writing to a new file
- G307: Deferring a method which returns an error
- G401: Detect the usage of DES, RC4, MD5 or SHA1
- G402: Look for bad TLS connection settings
- G403: Ensure minimum RSA key length of 2048 bits
- G404: Insecure random number source (rand)
- G501: Import blacklist: crypto/md5
- G502: Import blacklist: crypto/des
- G503: Import blacklist: crypto/rc4
- G504: Import blacklist: net/http/cgi
- G505: Import blacklist: crypto/sha1
- G601: Implicit memory aliasing of items from a range statement

Retired rules

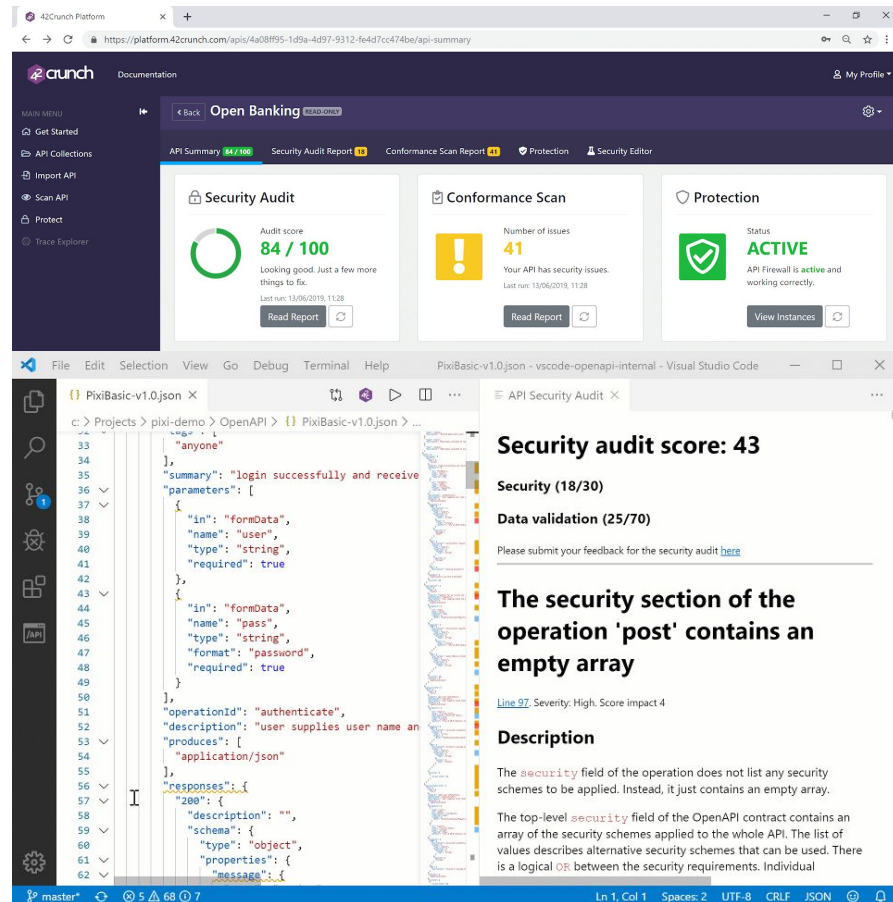
- G105: Audit the use of math/big.Int.Exp - [CVE is fixed](#)

42Crunch Scanner d'API

Utilise la spécification OpenAPI / Swagger pour identifier les faiblesses de votre API



Protection contre le Top 10 de la sécurité de l'API de l'OWASP

The screenshot displays the 42Crunch Platform interface for an API security audit. The top section shows the 'Open Banking' API with a Security Audit score of 84/100, a Conformance Scan score of 41, and a Protection status of ACTIVE. Below this, the VS Code editor shows the OpenAPI specification for 'PixiBasic-v1.0.json'. The right sidebar highlights a security issue: 'Security audit score: 43' with a severity of High. The issue description states: 'The security section of the operation 'post' contains an empty array'. The top-level security field of the OpenAPI contract contains an array of the security schemes applied to the whole API. The list of values describes alternative security schemes that can be used. There is a logical OR between the security requirements. Individual



Test: PenTest



Proxy

Method **Origin** **Path** **Status**

GET	https://juice-shop.herokuapp.com	/rest/products/search?q=	200 OK
GET	https://juice-shop.herokuapp.com	/rest/admin/application-configuration	304 Not Modified
GET	https://juice-shop.herokuapp.com	/assets/118n/en.json	200 OK
GET	https://juice-shop.herokuapp.com	/rest/admin/application-configuration	200 OK
GET	https://juice-shop.herokuapp.com	/main.js	200 OK
GET	https://juice-shop.herokuapp.com	/vendor.js	200 OK

GET /rest/admin/application-configuration REQUEST

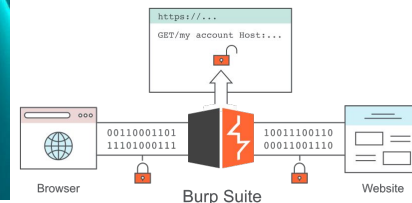
Query Params	Headers (12)	Body														
	<table border="1"> <thead> <tr> <th>Key</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>User-Agent</td> <td>Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.109 Safari/537.36</td> </tr> <tr> <td>Referer</td> <td>https://juice-shop.herokuapp.com/</td> </tr> <tr> <td>Sec-Fetch-Dest</td> <td>empty</td> </tr> <tr> <td>Accept-Language</td> <td>en-US,en;q=0.9</td> </tr> <tr> <td>Accept-Encoding</td> <td>gzip, deflate, br</td> </tr> <tr> <td>Accept</td> <td>application/json, text/plain, */*</td> </tr> </tbody> </table>	Key	Value	User-Agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.109 Safari/537.36	Referer	https://juice-shop.herokuapp.com/	Sec-Fetch-Dest	empty	Accept-Language	en-US,en;q=0.9	Accept-Encoding	gzip, deflate, br	Accept	application/json, text/plain, */*	
Key	Value															
User-Agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.109 Safari/537.36															
Referer	https://juice-shop.herokuapp.com/															
Sec-Fetch-Dest	empty															
Accept-Language	en-US,en;q=0.9															
Accept-Encoding	gzip, deflate, br															
Accept	application/json, text/plain, */*															

Body (18690 bytes) Headers (11) HTTP/1.1 200 OK RESPONSE

```
1 [{"config":{"server":{"port":3000,"basePath":"","application":{"domain":"juice-sh.op","name":"OWASP Juice Shop","logo":"JuiceShop_Logo.png","favicon":"favicon.ico","theme":"bluegrey-lightgreen","showVersionNumber":true,"showGitHubLinks":true,"localBackupEnabled":true,"numberOfRandomFakeUsers":0,"altcoinName":"Juicycoin","privacyContactEmail":"donotreply@owasp-juice-shop","customMetricsPrefix":"juiceshop","chatBot":{"name":"Juicy","greeting":"Nice to meet you <customer-name>, I'm <bot-name>","trainingData":{"botDefaultTrainingData.json","defaultResponse":"Sorry I couldn't understand what you were trying to say","avatar":"JuicyChatBot.png"},"social":{"twitterUrl":"https://twitter.com/owasp_juiceshop","facebookUrl":"https://www.facebook.com/owasp.juiceshop","slackUrl":"https://owasp.org/slack/invite","redditUrl":"https://www.reddit.com/r/owasp_juiceshop","pressKitUrl":"https://github.com/OWASP/owasp-swig/tree/master/projects/juice-shop","questionnaireUrl":null},"recyclePage":{"topProductImage":"fruit_press.jpg"}}
```

Security Bug Hunting with Proxies (Black Box)

Hetty, Burp Suite, OWASP ZAP, mitmproxy, charles



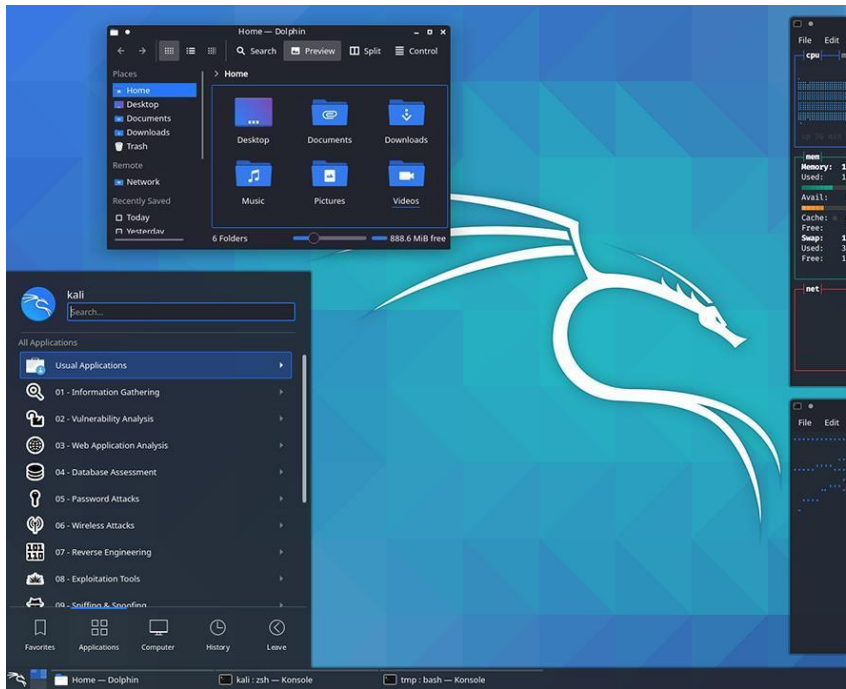


Kali Linux / Parrot OS

Boîte à outils

Les tests d'intrusion sont un moyen de trouver et de colmater des brèches. Objectif: Simuler des attaques pour tester la robustesse de la plate-forme

- Nmap
- Metasploit
- Wireshark
- John The Ripper
- Hashcat
- Hydra
- Burp Suite
- Zed Attack Proxy (ZAP)
- sqlmap
- aircrack-ng

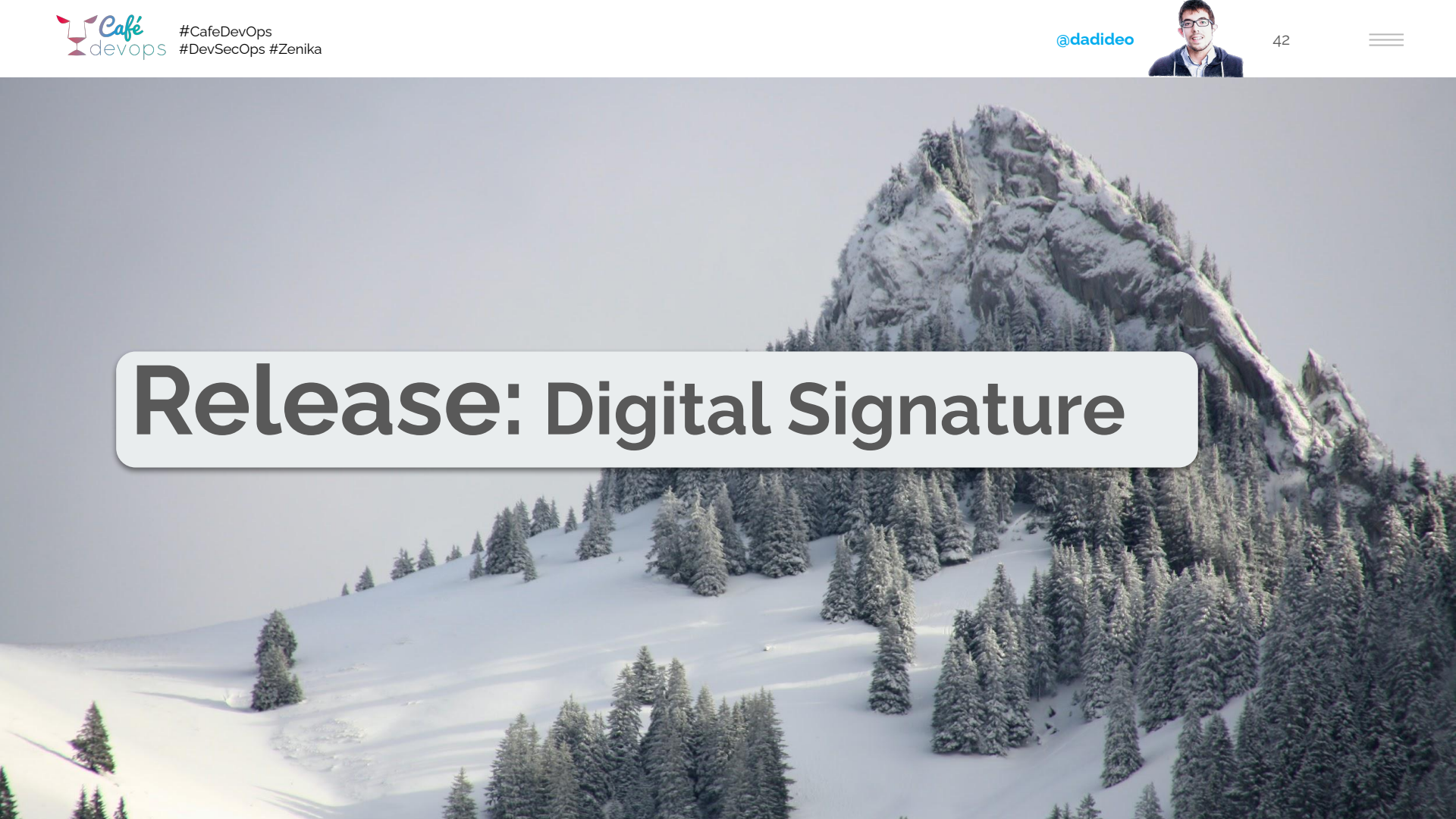


11 outils pour s'initier au pentest



Hackers as a Service





Release: Digital Signature



Docker Notary

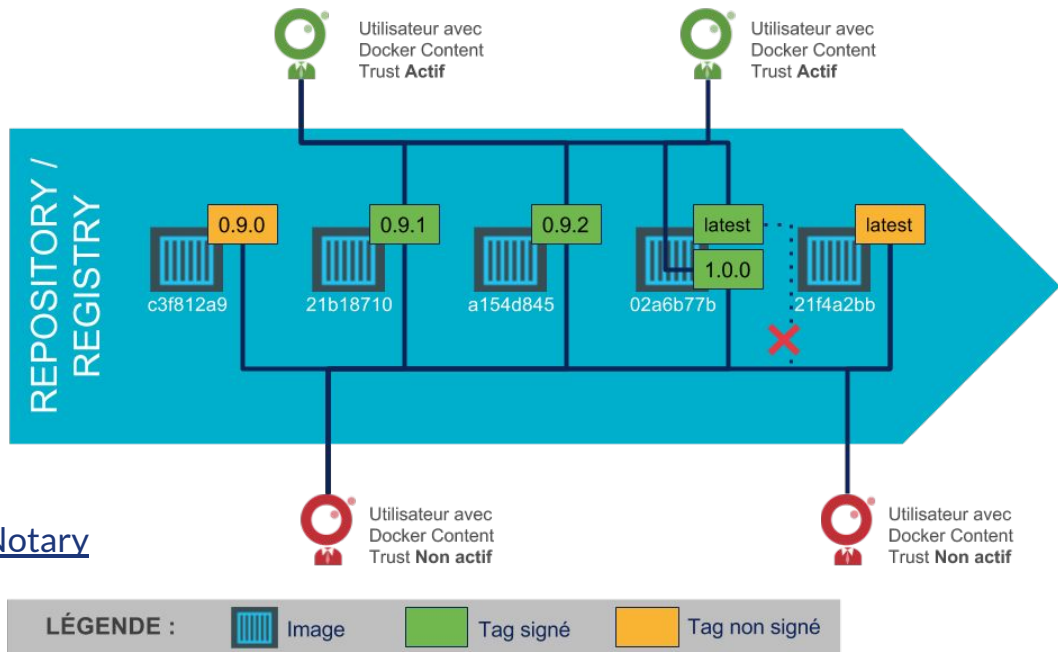
Ready for PROD

Signer pour certifier et être avoir la garantie sur la provenance (non-altération)



[Documentation Docker Notary \[EN\]](#)

La signature d'images Docker sur une Registry avec Notary





Deliver: Secure Transfer



JFrog Artifactory

Repository

Signer pour certifier, être avoir la garantie sur la provenance (non-altération), archiver et faciliter les rollbacks

The screenshot displays the JFrog Artifactory web interface. The top navigation bar is green with the JFrog Artifactory logo, a search icon, and user information 'Welcome, admin' and 'Help'. The main content area is titled 'Artifact Repository Browser' and includes links for 'Set Me Up' and 'Deploy'. On the left, a sidebar shows a tree view of repositories: 'docker' (expanded), 'docker-local', 'hello-world', 'uploads', 'v1.0', 'bintray-docker-remote-cache', and 'docker-remote-cache'. The right pane shows the 'docker' repository details under the 'General' tab. The 'Info' section lists: Name: docker (1), Package Type: Docker, Repository Path: docker/ (2), and Repository Layout: simple-default. The 'Included Repositories' section lists: docker-local, bintray-docker-r..., and docker-remote.

JFrog Artifactory

Artifact Repository Browser

Tree Simple

- docker
 - docker-local
 - hello-world
 - uploads
 - v1.0
 - bintray-docker-remote-cache
 - docker-remote-cache

docker

General

Info

Name:	docker (1)
Package Type:	Docker
Repository Path:	docker/ (2)
Repository Layout:	simple-default

Included Repositories

- docker-local
- bintray-docker-r...
- docker-remote



Deploy: Security Conf/Scan



Argo CI + Vault

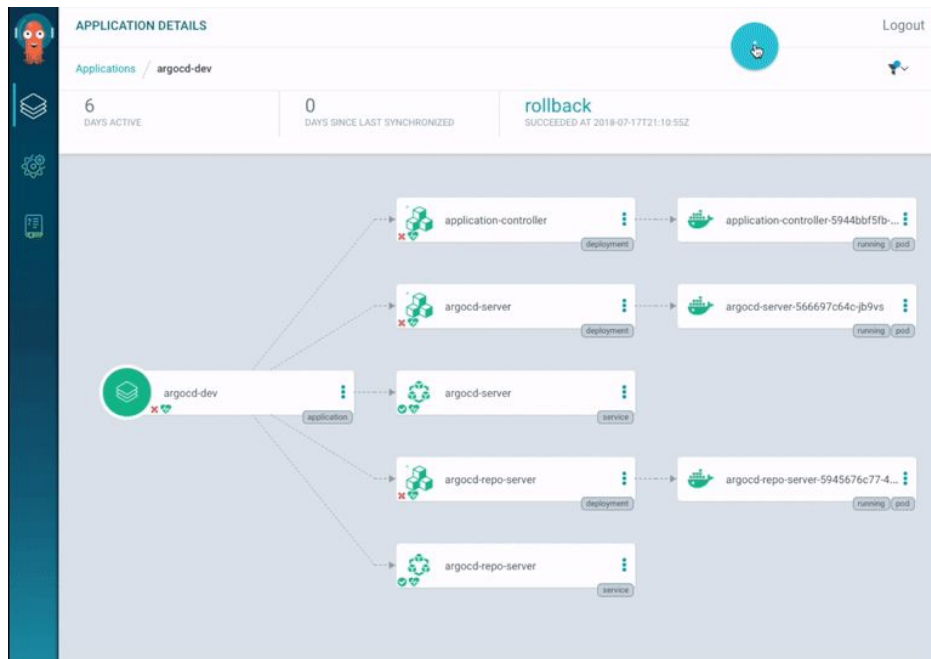
Keep immutable

Les définitions, configurations et environnements des applications doivent être déclaratifs et contrôlés par version. Le déploiement et la gestion du cycle de vie des applications doivent être automatisés, contrôlables et faciles à comprendre

-> Maintenir un système iso aux specs



[Why Argo CD? \[EN\]](#)





Operate: Secu. Patch/Audit



Ansible / Chef / Puppet Patch & Reboot

Maintenir un système à jour en installant les patches de sécurité

- Linux
- Windows
- Mac OS
- iOS
- Android
- /e/
- etc...



[Playbook: apply patches & perform a reboot if required](#)

```
---
- name: Patch and reboot servers
  hosts: all
  vars:
    yum_name: "*"
    yum_state: latest
    yum_securityrepo: yes
    yum_enablerepo: "rhel?-server-rpms,rhel?-server-satellite-tools-6.?-rpms"
    yum_disablerepo: "*"
    yum_exclude: ""
  tasks:
    - name: upgrade packages via yum
      yum:
        name={{ yum_name }}
        state={{ yum_state }}
        security={{ yum_securityrepo }}
        become: "yes"
        register: yumcommandout
      when:
        - (ansible_facts['distribution_major_version'] == '6') or
          (ansible_facts['distribution_major_version'] == '7')

    - name: display security packages
      debug:
        msg: "security patches for: {{ yumcommandout.changes.updated }}"
      when: yumcommandout.changes is defined

    - name: check to see if we need a reboot
      command: needs-restarting -r
      register: result
      ignore_errors: yes
      changed_when: false #avoid changed

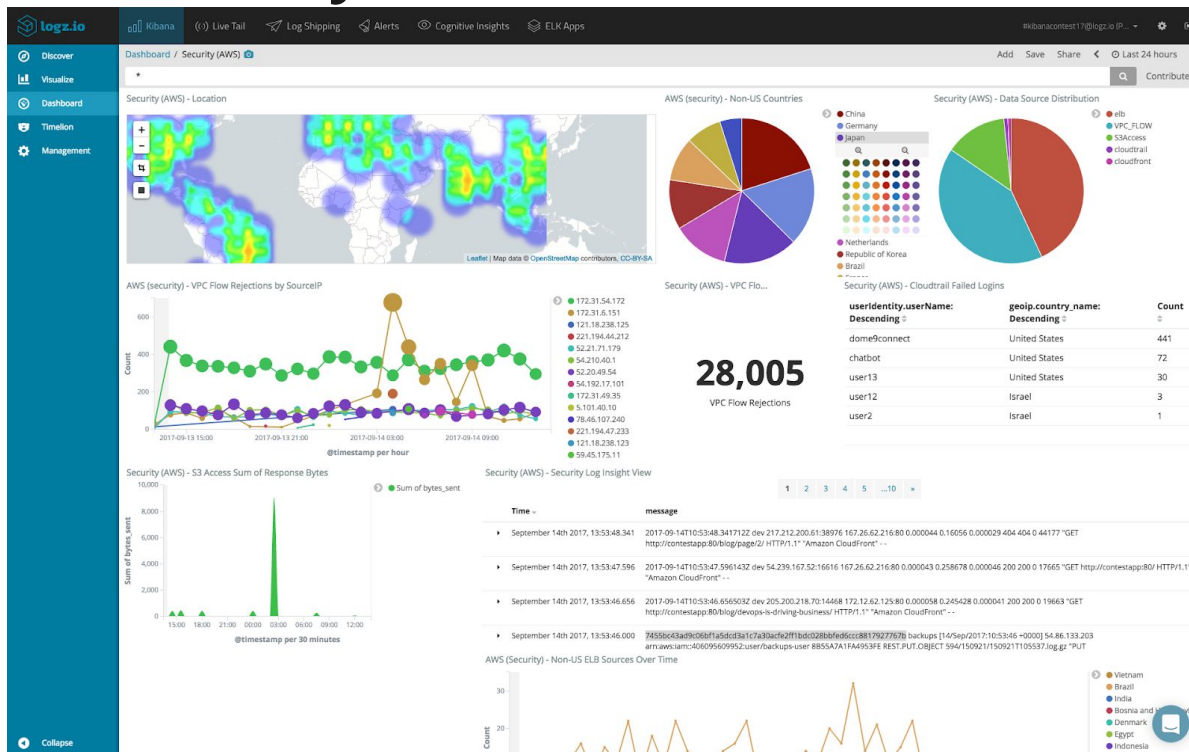
    - name: Reboot Server if Necessary
      command: shutdown -r now "Ansible Updates Triggered"
      become: true
      async: 30
      poll: 0
      when: result.rc is defined and result.rc == 1
```



Monitor: Security Monitoring



Elastic Security

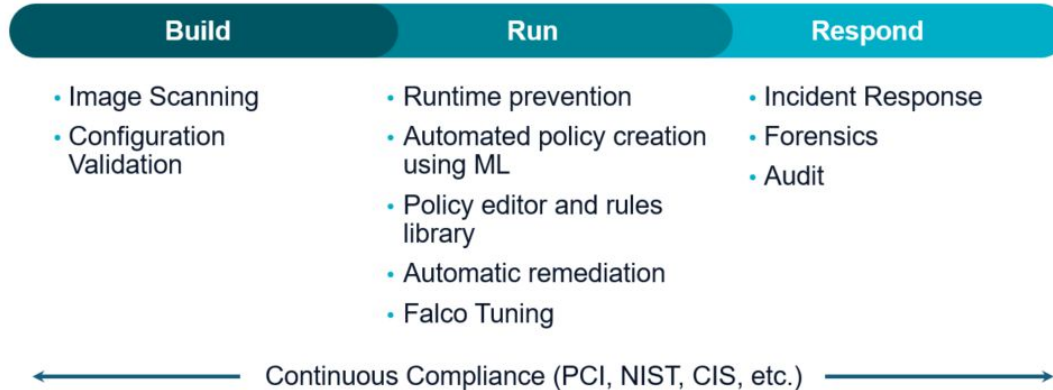


SIEM at the speed of Elasticsearch



Falco

- Runtime detection
- Alerts





OVH Bastion (SSH proxy)

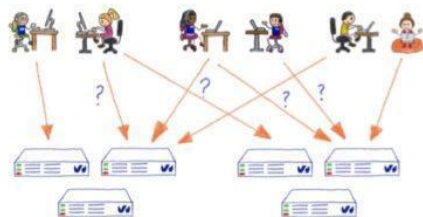
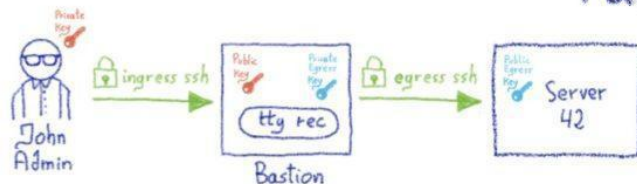
The



OVHcloud

Bastion

Part #1



```
slesimpl@bastion-2.99.99-rc9.2-ovh1:~$ zdevbst --ssh help
```

```
-----*
|THIS IS A PRIVATE COMPUTER SYSTEM, UNAUTHORIZED ACCESS IS STRICTLY PROHIBITED.|
|ALL CONNECTIONS ARE LOGGED. IF YOU ARE NOT AUTHORIZED, DISCONNECT NOW.      |
|-----*
```

```
Enter PIN for 'PIV Card Holder pin (PIV_II)':
```

```
-----the-bastion-2.99.99-rc9.2-ovh1---
=> OSH help
```

```
> MANAGE YOUR ACCOUNT
```

```
- manage your ingress credentials (you->bastion):
```

```
selfListIngressKeys selfAddIngressKey selfDelIngressKey
selfGenerateEgressKey selfListEgressKeys selfGenerateEgressKey
selfListAccesses selfAddPersonalAccess selfDelPersonalAccess
```

```
- manage your egress credentials (bastion->server):
```

```
selfListEgressKeys selfGenerateEgressKey
```

```
- manage your accesses to servers:
```

```
selfListAccesses selfAddPersonalAccess selfDelPersonalAccess
```

```
- manage your own bastion:
```

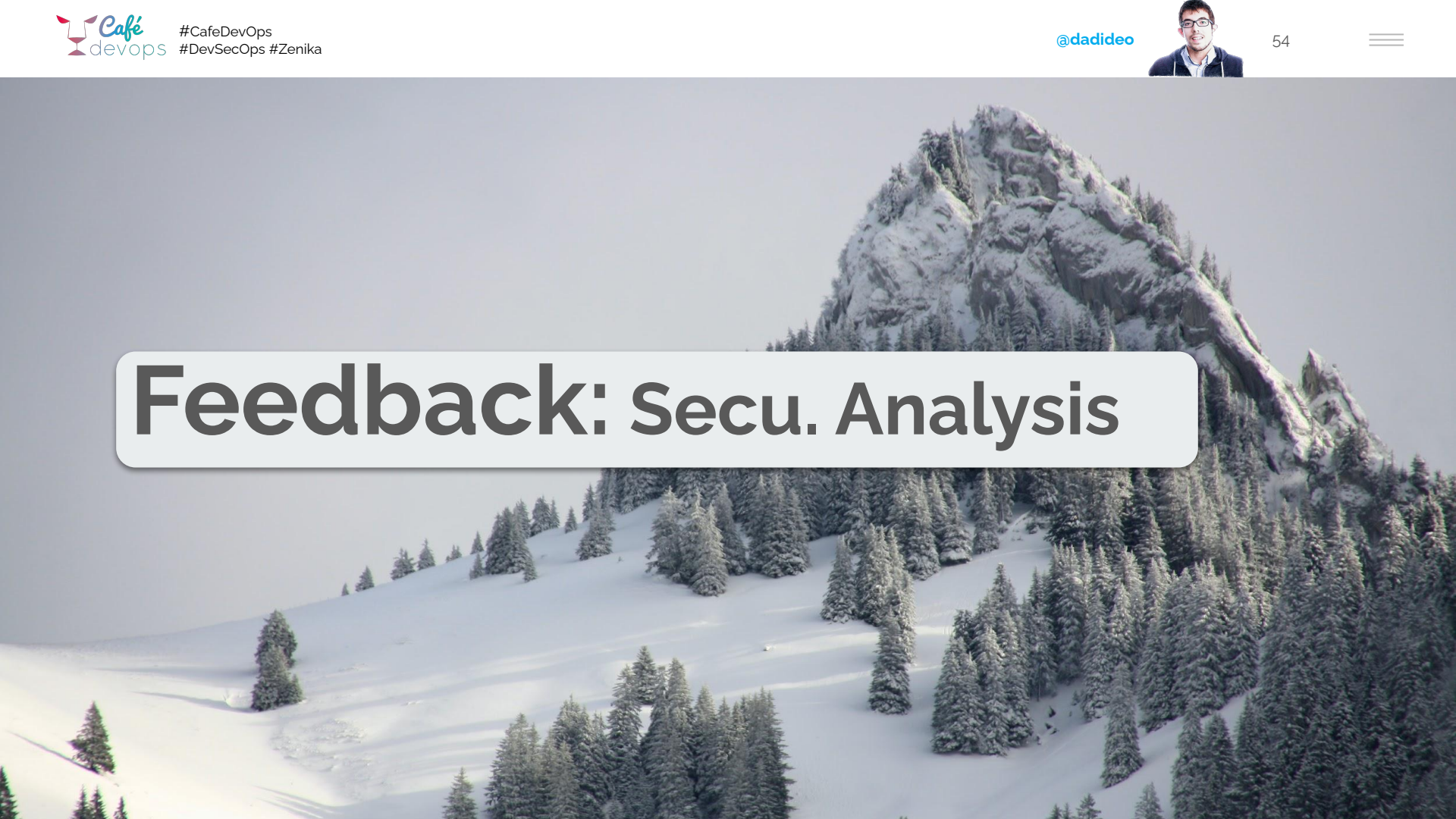
```
selfListBastions
```

```
- manage your bastions:
```

```
selfListBastions selfAddBastion selfDelBastion
```



[Blog article](#) / [Documentation](#) / [Source Code](#)



Feedback: Secu. Analysis



AlienVault OTX

 OPEN THREAT
EXCHANGE

Hi David,

A user you are subscribed to (AlienVault) has posted a new pulse:



**Introducing The Jupyter
Infostealer/Backdoor**

[VIEW PULSE](#) [SUGGEST EDIT](#) [SCAN ENDPOINTS](#)

To view the pulse, please visit <https://otx.alienvault.com/pulse/5faf00679c90b876019cc653/>

Click "Embed" on the pulse to insert this pulse in your blog.

You can also [tweet](#) it out to your followers.

Get this updated threat intelligence automatically in your infrastructure using [the OTX API](#)



[OTX: Open Threat Exchange \[EN\]](#)



AlienVault OTX

[Browse](#)
[Scan Endpoints](#)
[Create Pulse](#)
[Submit Sample](#)
[API Integration](#)

All Search OTX



Introducing The Jupyter Infostealer/Backdoor

CREATED 2 DAYS AGO by [AlienVault](#) | Public | TLP: White

During what began as a routine incident response process, Morphisec has identified (and prevented) a new .NET infostealer variant called Jupyter. Morphisec discovered this variant as part of assisting a higher education customer in the U.S. with their incident response. Jupyter is an infostealer that primarily targets Chromium, Firefox, and Chrome browser data. However, its attack chain, delivery, and loader demonstrate additional capabilities for full backdoor functionality.

REFERENCE: https://www.morphisec.com/hubfs/eBooks_and_Whitepapers/Jupyter%20Infostealer%20WEB.pdf

TAGS: [Jupyter Loader](#), [Infostealer](#), [Backdoor](#), [Academia](#), [Russian Actors](#), [Docx2Rtf](#), [Magix Photo Manager](#), [Jupyter Client](#), [PoshC2](#)

INDUSTRY: [Education](#)

MALWARE FAMILIES: [PoshC2 - 50378](#), [Jupyter Loader](#), [Jupyter Client](#)

ATT&CK IDS:

T1564 - Hide Artifacts, T1033 - System Owner/User Discovery, T1082 - System Information Discovery, T1140 - Deobfuscate/Decode, T1127 - Trusted Developer Utilities Proxy Execution, T1059.001 - PowerShell, T1055.012 - Process Hollowing, T1036 - Masquerading, T1217 - Browser Bookmark Discovery, T1560.001 - Archive via Utility, T1059.003 - Windows Command Shell, T1547.001 - Registry Run, T1049 - System Network Connections Discovery, T1016 - System Network Configuration Discovery

ENDPOINT SECURITY Scan your endpoints for IOCs from this Pulse!

[Indicators of Compromise \(39\)](#)
[Related Pulses \(8\)](#)
[Comments \(0\)](#)
[History \(0\)](#)



Show 10 entries

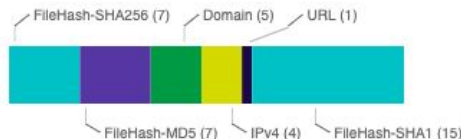
TYPE	INDICATOR	ROLE	TITLE
IPv4	91.241.19.21		

Indicators of Compromise (39)

Related Pulses (8)

Comments (0)

History (0)



TYPES OF INDICATORS



THREAT INFRASTRUCTURE

Show 10 entries

TYPE	INDICATOR	ROLE	TITLE
IPv4	91.241.19.21		
IPv4	45.146.165.219		
IPv4	45.146.165.222		
IPv4	45.135.232.131		
FileHash-SHA1	6ad28e1810eb1be26e835e5224e78e13576887b9		



Introducing The Jupyter Infostealer/Backdoor

OpenCVE



Search...



Sign in

Register

Have an account ?

 Vulnerabilities (CVE)

 Vendors (CPE)

 Categories (CWE)

FILTER



Search

ALL

LOW

MEDIUM

HIGH



130145

total CVE

CVE	Vendors	Products	Updated	CVSS
CVE-2019-2215	1 Google	1 Android	2019-10-16	4.6
A use-after-free in binder.c allows an elevation of privilege from an application to the Linux Kernel. No user interaction is required to exploit this vulnerability, however exploitation does require either the installation of a malicious local...				
CVE-2019-2183	1 Google	1 Android	2019-10-16	2.1
In generateServicesMap of RegisteredServicesCache.java, there is a possible account protection bypass due to a caching optimization. This could lead to local information disclosure with no additional execution privileges needed. User interaction...				
CVE-2019-9533	1 Cobham	1 Explorer 710 Firmware	2019-10-16	10.0
The root password of the Cobham EXPLORER 710 is the same for all versions of firmware up to and including v1.08. This could allow an attacker to reverse-engineer the password from available versions to gain authenticated access to the device.				
CVE-2019-2187	1 Google	1 Android	2019-10-16	2.1
In nfc_ncif_decode_rf_params of nfc_ncif.cc, there is a possible out of bounds read due to an integer underflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for...				
CVE-2019-17420	2 Oisf, Suricata-ids	2 Libhttp, Suricata	2019-10-16	5.0
In OISF LibHTP before 0.5.31, as used in Suricata 4.1.4 and other products, an HTTP protocol parsing error causes the http_header signature to not alert on a response with a single \r\n ending.				
CVE-2019-2184	1 Google	1 Android	2019-10-16	9.3
In PV_DecodePredictedIntraDC of dec_pred_intra_dc.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for...				



Site Web OpenCVE



OpenCVE / Vue d'une CVE



CVE-2019-2215

A use-after-free in binder.c allows an elevation of privilege from an application to the Linux Kernel. No user interaction is required to exploit this vulnerability, however exploitation does require either the installation of a malicious local application or a separate vulnerability in a network facing application. Product: Android Android ID: A-141720095

CVSS v3.0

7.8 HIGH

CVSS v2.0

4.6 MEDIUM

7.8/10

CVSS v3.0 : HIGH

V3 Legend ↗

Vector :

Exploitability : 1.8 / Impact : 5.9

Attack Vector

LOCAL

Attack Complexity

LOW

Privileges Required

LOW

User Interaction

NONE

Confidentiality Impact

HIGH

Integrity Impact

HIGH

Availability Impact

HIGH

Scope

UNCHANGED

References

Link

<http://packetstormsecurity.com/files/154911/Android-Binder-Use-After-Free.html>

<http://packetstormsecurity.com/files/155212/Slackware-Security-Advisory-Slackware-14.2-kernel-Updates.html>

<http://packetstormsecurity.com/files/156495/Android-Binder-Use-After-Free.html>

<http://seclists.org/fulldisclosure/2019/Oct/38>

Resource



CERT-FR (Flux RSS)

[Menaces et incidents](#)

CERT-FR

PUBLICATIONS ▾

SCANS

ARCHIVES ▾

RÉSEAU DES CSIRT ▾

RECRUTEMENT

CONTACT

À PROPOS



MENACES ET INCIDENTS

LE MALWARE-AS-A-SERVICE EMOTET

CERTFR-2020-CTI-010 • Publié le 2 novembre 2020

Observé pour la première fois en 2014 en tant que cheval de Troie bancaire, Emotet a évolué vers une structure modulaire à partir de 2015. Depuis 2017, Emotet ...



DEVELOPMENT OF THE ACTIVITY OF THE TA505 CYBERCRIMINAL GROUP

CERTFR-2020-CTI-009 • Publié le 27 août 2020

The intrusion set TA505 has been active since at least 2014 when it initially stole financial information through the use of Dridex and mass distributed ransomwares. It evolved and ...



THE MALWARE DRIDEX: ORIGINS AND USES

CERTFR-2020-CTI-008 • Publié le 17 juillet 2020

Surfacing in June 2014 as a variant of the banking trojan Bugat, Dridex is a malware which has evolved a lot since then in terms of functionalities and uses. This report provides ...



Lifecycle: Decommission



Planification (LTS/Migration/EoL)

techradar pro IT INSIGHTS FOR BUSINESS

US Edition

PAYMENTS INDUSTRY INTELLIGENCE
Payments
Cards & Mobile



News

Security

Web hosting

VPN

Website builder

Resources

News

PUBLICATIONS

RESEARCH

CONSULTING

CONFERENCES / ADVERTISE / WEBINARS

Home > News > Computing

ATM security still running Windows XP

By Anthony Spadafora November 15, 2018

New study reveals ATM security is mostly for show

New research from Positive Technologies has revealed that ATM machines are vulnerable to a number of basic attack techniques that could allow hackers to steal thousands in cash.

The company's researchers studied over two dozen different models of ATMs and discovered that almost all of them are vulnerable to network or local access attacks that would allow hackers to obtain money from them illegally.

Positive Technologies' study had its researchers try to penetrate 26 machines from various manufacturers and service providers.

The researchers found that 15 of the ATMs were running Windows XP, 22 were vulnerable to a "network spoofing" attack, 18 were vulnerable to 'black box' attacks, 20 could be forced to exit kiosk mode via USB or PS/2 and 24 had no data encryption in place on their hard drives.

HOME > DAILY NEWS > ATM MIGRATION TO WINDOWS 10 – THE TIME IS NEAR!

ATM migration to Windows 10 – the time is near!

BY ALEX ROLFE

DECEMBER 11, 2019

DAILY NEWS

SHARE:



2,903 VIEWS

The banking sector will face a big ATM migration challenge in 2020. Microsoft made the official announcement: Windows 7 (operating system for many ATMs) extended support will end on January 14, 2020. Consequently, all banks have to update their entire ATM network by installing a new operating system caring about data security.

There are about 3.2 million ATMs in the world. They are used daily by billions of people, but only a few know that most ATMs work on the Windows operating system.

A lot of ATMs around the globe are still running Windows XP embedded, long after Microsoft ceased support with security and stability patches. Support for Windows XP was discontinued in 2014, which means that since then the Microsoft Company has not rolled out any security updates for this Windows version.

In June 2018, The Central Bank of India issued a statement saying that all ATMs in the country should be updated from Windows XP to the newer platform by December 2019. It is estimated that about 50% of ATMs use Windows XP operating system.



ATM migration to Windows 10 – the time is near!



Synthèse



DevSecOps Toolbox

- Secure Coding
 - [Linters](#), [gosec](#), [npm-audit](#), [git-secrets](#)/[GitGuardian](#), [42Crunch](#)
- Security as Code
 - [Cilium](#) (Network), [gVisor](#)/[Kata](#) (Sandbox), [Istio](#)/[maesh](#) (SSL)
- SAST / DAST / IAST
 - [SonarQube](#), [Gitlab SAST](#)/[GitHub](#), [Clair](#)/[Anchore](#)/[Dagda](#) (CVE)
- Pentest
 - [Parrot](#)/[Kali OS](#), [YesWeHack](#)/[Yogosha](#), [Hetty](#)/[Burp Suite](#)/[SuperTruder](#)/[ffuf](#), [OWASP ZAP](#)
- Digital signature / Secure Transfer
 - [Notary](#), [JFrog Artifactory](#)
- Security Configuration, Security Scan
 - [Argo+Vault](#), [OpenSCAP](#)
- Security Patching, Security Audit
 - [Puppet](#), [Chef](#), [Ansible Playbook](#)/[AWX](#) ou [RedHat Tower](#)
- Security Monitoring
 - [Elastic Security](#), [Falco](#), [OVH Bastion](#)
- Security Analysis
 - [OpenCVE](#), [AlienVault OTX](#)

And more... (not exhaustive) 🤖



Open Source Security Scanning -- focus on cloud native

Vulnerability Scans

Trivy

Clair

Syft

IaC Misconfiguration Scans

Trivy

tfsec

terrascan

KICS

checkov

Secret Scanning

tfsec (terraform)

Trivy (K8s)

squealer

gitleaks

gitleaks

git-all-secrets

many-more non cloud native

Compliance Scans

kube-bench CIS

kube-beacon CIS

Starboard NSA

Kubescape NSA

SBOM

Trivy

Syft

In-Cluster Scans

Trivy

Kubescape

kube-hunter

chain-bench



Demo





DDoS

The screenshot shows a web browser window with the address bar displaying `https://x.com/liran_tal/status/1863600765492695148`. The browser's top bar includes various system icons and the date/time: Mon 2 Dec 16:13. The tweet is from Liran Tal (@liran_tal) and contains the following text:

Post

Liran Tal @liran_tal

⚠️ Beware of DoS attacks in Node.js! Learn how to protect your applications with rate limiting, timeouts, and asynchronous operations

[#nodejs](#) [#security](#) [#webdev](#)

4:07 PM · Dec 2, 2024 · 1 View

Interactions: Reply, Retweet (1), Like (1), Bookmark, Share

Post your reply [Reply](#)

Discover more
Sourced from across X

Relevant people

Liran Tal @liran_tal [Following](#)

Node.js Secure Coding:
[nodejs-security.com](#) ⭐
Awarded @GitHub Star 🏆
Awarded @OpenJS Pathfinder award for Security 🟢 DevRel
[@snyksec](#)

What's happening

News · Trending
ALERTE INFO
6,661 posts



[Twitter @Liran Tal](#)

DDoS



[GitHub Namecheck](#)



github-advanced-security bot found potential problems on Oct 23, 2022

[View reviewed changes](#)

cmd/server/main.go

```
61 - }
62 -
63 - if err := srv.ListenAndServe(); err != nil {
52 + if err := http.ListenAndServe(":8080", nil); err != nil {
```

✗ Check failure

🔄 Code scanning / gosec

Use of net/http serve function that has no support for setting timeouts

Use of net/http serve function that has no support for setting timeouts

[Show more details](#)



Reply...



sonarcloud bot commented on Dec 31, 2022

...

Kudos, SonarCloud Quality Gate passed!

Passed

🔍 [0 Bugs](#)

🔒 [0 Vulnerabilities](#)

🛡️ [0 Security Hotspots](#)

🐛 [0 Code Smells](#)

📊 No Coverage information

🔄 [0.0% Duplication](#)



David Aparicio > gokvs > Pull Requests > 81 – 🔥 rem: Go Meetup 3 December 2024 (Batch, Lyon) 🔄 ✅

Summary Issues Security Hotspots Measures Code

PR Summary

4 New Lines • 🔗 meetup_3Dec24 → 🔗 main



Quality Gate ?

Passed

Last analysis 44 minutes ago • 🧑‍🔧 [dc7b9770](#)

New Issues

0

No conditions set

Accepted Issues

0

Valid issues that were not fixed



Coverage

There is not enough lines to compute coverage

Duplications

0.0%

Required $\leq 3.0\%$
on 4 New Lines

0.0% Estimated after merge



Security Hotspots

0

No conditions set



```
[main.go:12] - G304: Potential file inclusion via variable
(Confidence: HIGH, Severity: MEDIUM)
    11: func readFile(filename string) {
> 12:   data, err := ioutil.ReadFile(filename)
    13:   if err != nil {
```



```
package main

import (
    "fmt"
    "io/ioutil"
)

func main() {
    userInput := "/etc/passwd" // Entrée contrôlée par l'attaquant
    content, err := ioutil.ReadFile(userInput)
    if err != nil {
        panic(err)
    }
    fmt.Println(string(content))
}
```



```
package main

import (
    "fmt"
    "io/ioutil"
    "path/filepath"
    "strings"
)

func main() {
    userInput := "/etc/passwd" // Entrée contrôlée par l'attaquant
    safeBasePath := "/safe/path"

    cleanPath := filepath.Clean(userInput)
    if !strings.HasPrefix(cleanPath, safeBasePath) {
        panic("Chemin non autorisé")
    }

    content, err := ioutil.ReadFile(cleanPath)
    if err != nil {
        panic(err)
    }
    fmt.Println(string(content))
}
```




AI-inside

Auto fixing vulnerabilities

gosec can suggest fixes based on AI recommendation. It will call an AI API to receive a suggestion for a security finding.

You can enable this feature by providing the following command line arguments:

- `ai-api-provider` : the name of the AI API provider, currently only `gemini` is supported.
- `ai-api-key` or set the environment variable `G0SEC_AI_API_KEY` : the key to access the AI API, For gemini, you can create an API key following [these instructions](#).
- `ai-endpoint` : the endpoint of the AI provider, this is optional argument.

```
gosec -ai-api-provider="gemini" -ai-api-key="your_key" ./...
```





Autre

outil

Govulncheck v1.0.0 is released!

Julie Qiu, for the Go security team
13 July 2023

We are excited to announce that govulncheck v1.0.0 has been released, along with v1.0.0 of the API for integrating scanning into other tools!

Go's support for vulnerability management was [first announced](#) last September. We have made several changes since then, culminating in today's release.

This post describes Go's updated vulnerability tooling, and how to get started using it. We also recently published a [security best practices guide](#) to help you prioritize security in your Go projects.

Govulncheck

[Govulncheck](#) is a command-line tool that helps Go users find known vulnerabilities in their project dependencies. The tool can analyze both codebases and binaries, and it reduces noise by prioritizing vulnerabilities in functions that your code is actually calling.

You can install the latest version of govulncheck using [go install](#):

```
go install golang.org/x/vuln/cmd/govulncheck@latest
```

Then, run govulncheck inside your module:

```
govulncheck ./...
```

See the [govulncheck tutorial](#) for additional information on how to get started with using the tool.

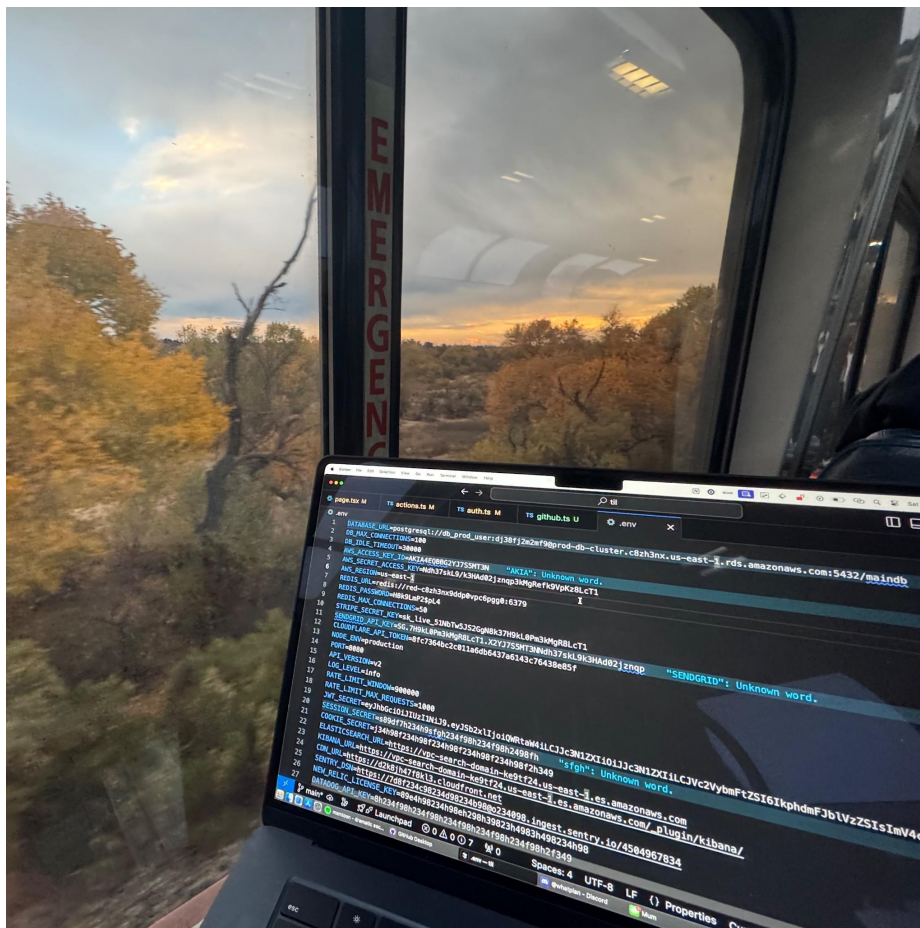
As of this release, there is now a stable API available, which is described at golang.org/x/vuln/scan. This API provides the same functionality as the govulncheck command, enabling developers to integrate security scanners and other tools with govulncheck. As an example, see the [osv-scanner integration with govulncheck](#).

Database

Govulncheck is powered by the Go vulnerability database, <https://vuln.go.dev>, which provides a comprehensive source of information about known vulnerabilities in public Go modules. You can browse the entries in the database at pkg.go.dev/vuln.



Scan Every- where



Twitter
@RhysSullivan

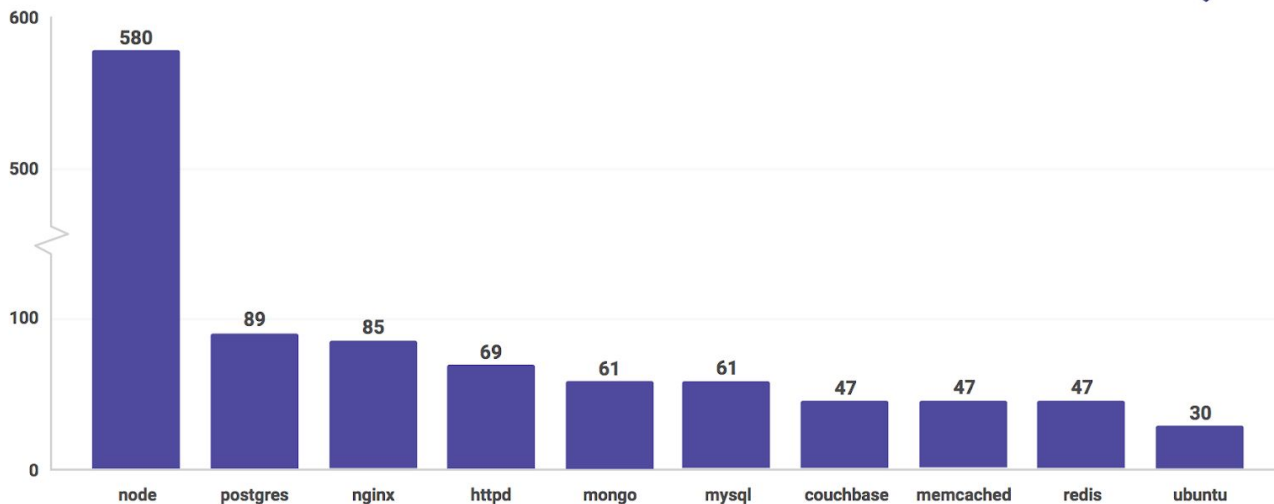


Conseils



Attention avec Docker

Number of OS vulnerabilities by docker image



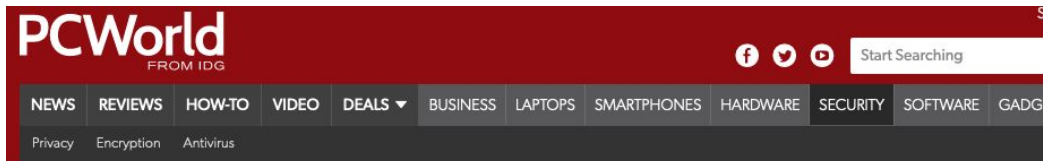
Open Source Security report

- 78% of vulnerabilities are found in indirect dependencies





Attention avec vos dépendances



[Home](#) / [Internet](#)

NEWS

Failure to patch known ImageMagick flaw for months costs Facebook \$40k

A researcher found that Facebook was still vulnerable to the ImageTragick exploit months after it was disclosed



By [Lucian Constantin](#)

CSO Senior Writer, [IDG News Service](#) | JAN 18, 2017 12:06 PM PST



[PCWorld](#) - [Remote Code Execution Exploit \(Write-up\)](#)



Ne pas afficher des données personnelles (PII)

The screenshot shows the Ameli.fr website interface. At the top, there's a navigation bar with the Ameli logo and a search bar. Below the navigation bar, there's a section for 'MES DERNIERS PAIEMENTS' (My last payments) and 'MES DÉMARCHES EN 2 CLICS' (My démarches in 2 clicks). The 'MES DÉMARCHES EN 2 CLICS' section lists several options: 'Attestation de droits', 'Attestation de paiement d'indemnités journalières', and 'Carte européenne d'assurance maladie (CEAM)'. A red circle highlights the phone number '2 69 05 49 588 157 80' in the user profile section. The user profile section also shows the name 'Nathalie Durand (SPECIMEN)' and the last connection date '05/11/2020 à 05:27'. At the bottom, there's a 'NOTIFICATIONS' section with a red circle around the number '2'.

eli

l'Assurance Maladie

Accueil Mes paiements Mes démarches Mon espace prévention Mes informations

MES DERNIERS PAIEMENTS

1 OCT. Paiement à un tiers 3,09€

2 OCT. Paiement à un tiers 7,41€

MES DÉMARCHES EN 2 CLICS

Attestation de droits

Attestation de paiement d'indemnités journalières

Carte européenne d'assurance maladie (CEAM)

Voir toutes les démarches

Consulter les délais de traitement de ma CPAM

Nathalie Durand (SPECIMEN)

Dernière connexion le 05/11/2020 à 05:27

2 69 05 49 588 157 80

MON AGENDA

Mes rendez-vous

Prendre un rendez-vous

MON ESPACE PRÉVENTION

Repères Prévention

2 NOTIFICATIONS

Ma complémentaire santé

Site d'Ameli.fr
(numéro modifié
pour illustrer)



CNIL - Donnée
personnelle,
Personally
identifiable
information (PII)



Ne pas utiliser les configurations par défaut



🏠 > Blog > Report: Hotel Reservation Platform Leaves Millions of People Exposed in Massive Data Breach

Report: Hotel Reservation Platform Leaves Millions of People Exposed in Massive Data Breach



Mark Holden

🕒 November 06, 2020

Inside this Article ▾

Company: Prestige Software, based in Spain.

Severity: High

Size: 24.4 GB, totaling 10,000,000+ exposed files

Data Storage Format: Misconfigured AWS S3 bucket

Countries Affected: Worldwide

Courtesy of our security team at [Website Planet](#), we can reveal that a hotel reservation platform has been exposing highly sensitive data from millions of hotel guests worldwide, dating as far back as 2013 and including credit card details for 100,000s of people.

Based in Madrid and Barcelona, Prestige Software sells a channel management platform called Cloud Hospitality to hotels that automates their availability on online booking websites like Expedia and Booking.com.

The company was storing years of credit card data from hotel guests and travel agents without any protection in place, putting millions of people at risk of fraud and online attacks.

Customer Data Exposed

- **PII data:** Full names, email addresses, national ID numbers, and phone numbers of hotel guests

Prestige Software doesn't list that appeared to originate from including, but not limited to:

- Agoda
- Amadeus
- Booking.com
- Expedia
- Hotels.com
- Hotelbeds
- Omnibees
- Sabre
- and many others



[Hotel Reservation Platform Leaves Millions of People Exposed in Massive Data Breach](#)



Ne pas utiliser les configurations par défaut

The screenshot shows a blog post from MacKeeper. The header includes the MacKeeper logo, the word 'Blog', and a 'Menu' link. The main title is 'BREAKING: Massive Breach of Mexican Voter Data'. Below the title, there is a link to an 'interview with Chris Vickery' and a paragraph of text. The text discusses a breach of Mexican voter data, mentioning that the data was publicly accessible on an Amazon cloud server and that it was configured purely for public access. It also mentions that the database was finally taken offline on April 22nd, 2016. At the bottom, a sentence is circled in red, stating that under Mexican law, these files are 'strictly confidential'.

mk mackeeper | Blog Menu

BREAKING: Massive Breach of Mexican Voter Data

See the [interview with Chris Vickery](#) commenting on this breach.

Before going any further, let's make one thing very clear. I'm not the one who transmitted the data out of Mexico. Someone else will have to answer for that. However, eight days ago (April 14th), I did discover a publicly accessible database, hosted on an Amazon cloud server, containing these records. There was no password or authentication of any sort required. It was configured purely for public access. Why? I have no clue.

After reporting the situation to the US State Department, DHS, the Mexican Embassy in Washington, the Mexican Instituto Nacional Electoral (INE), and Amazon, the database was finally taken offline April 22nd, 2016.

Under Mexican law, these files are "strictly confidential", carrying a penalty of up to 12 years in prison for anyone extracting this data from the government for personal gain. We're talking about names, home addresses, birthdates, a couple of national identification numbers, and a few other bits of info.



Massive Breach of
Mexican Voter Data



Ne pas utiliser les permissions par défaut

Mathis Hammel
@MathisHammel

Mais le souci justement, c'est que les permissions étaient mal configurées. Tout ce qui touchait aux candidats était autorisé en lecture et en écriture, notamment la fonction permettant d'ajouter ou de modifier une proposition...

[Translate Tweet](#)

```
eprop { createPropositions(input: {id:"555", title:"-", source:"-"}) {id} }
rticleContent:"- ", source:"-")) {id} }
ePropositions(input: {id:"555", title:"Y'a un souci là non ?", source:"-"}) {id} }

: {

p { deletePropositions(input:{id:"555"}){title}
ositions(input:{id:"555"}){title}}

: {
souci l\u00e0 non ?"
```

Bannir les pesticides, instaurer des zones-tampons, lutter contre l'artificialisation des sols
Par Jean-Luc Mélenchon

Créer un haut-commissariat à l'eau
Par Jean-Luc Mélenchon

Planifier le 100% d'énergies renouvelables avec un double axe sobriété/efficacité énergétique pour 2050
Par Jean-Luc Mélenchon

Sortir du nucléaire : abandonner les projets d'EPR et d'enfouissement des déchets nucléaires, planifier le démantèlement de la...
Par Jean-Luc Mélenchon

Y'a un souci là non ?
Par Jean-Luc Mélenchon

5:46 PM · Jan 15, 2022 · Twitter Web App



[Thread @MathisHammel](#)



Attention au risque humain

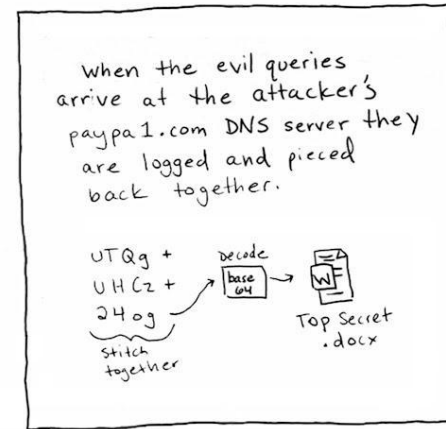
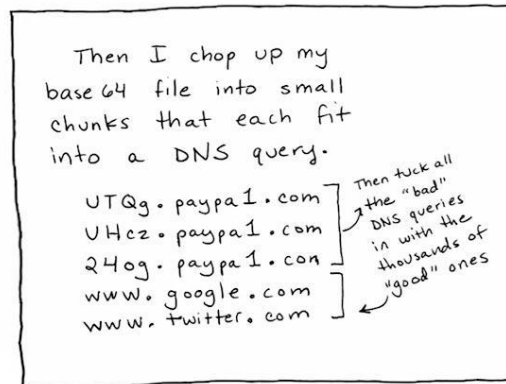
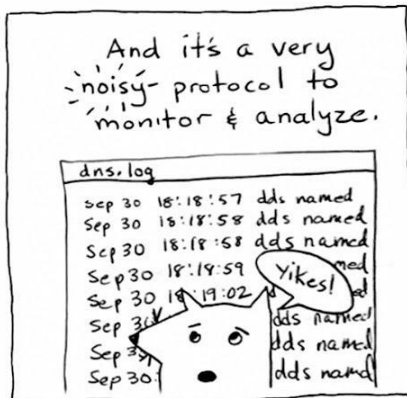
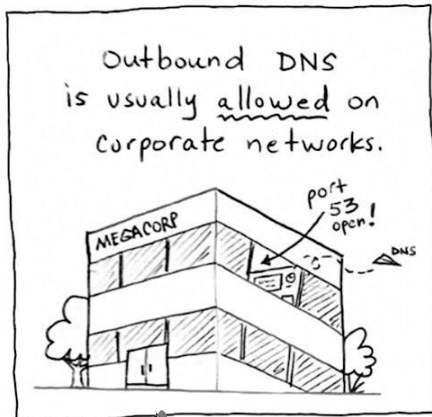
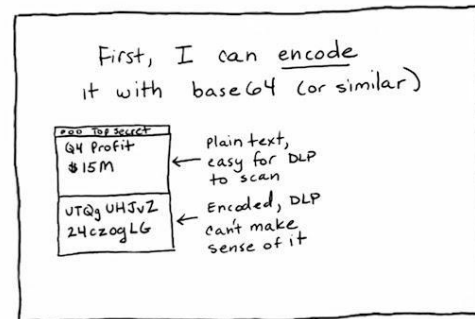
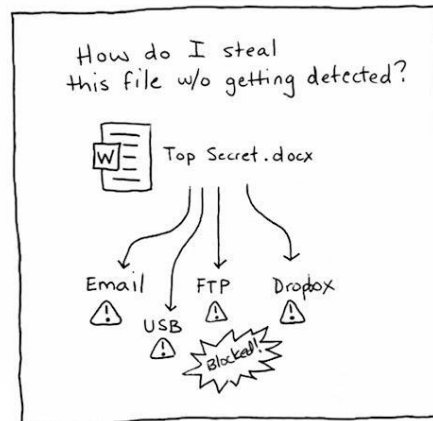
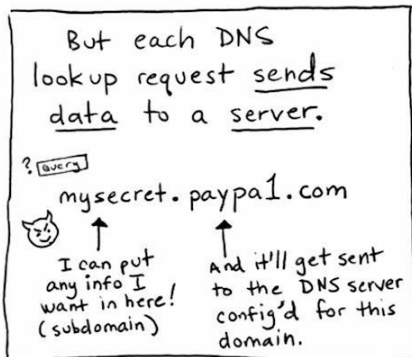
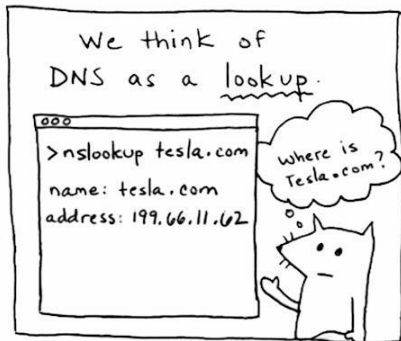




Attention au traffic sortant aussi !



Introduction à DNSSEC





Quelques bonnes pratiques

- Diminuer surface d'attaque (scratch, distroless, ubi-minimal)
- Principe de moindre privilège (!root, 1 user = 1 appli)
- Défense en profondeur (bastion, traceability, siem)
- Détection de connexion, proposer/activer MFA
- Pas de configuration/permissions par défaut (K8s, [MongoDB](#))
- Pas de secrets dans les Docker images ou les repositories Git (Vault, .gitignore)
- Pas de données sensibles dans les GUI (cf slide suivante)
- Ne pas afficher de stacktrace (pas debug | Fail securely)
- Ni de version/nom de framework
- Vérifier les entrées/sorties des clients/noeuds (injection/XSS, protocoles)
- Faire des backups régulièrement et déconnectées du réseau
- Mettre à jour infra/docker images (CI/CD|[GitOps](#))
- PaaS (BUILD/RUN)  OVHcloud/CleverCloud



Pourquoi ?

2013	2017 (new, * from the community)	2021 (new, * from the survey)
A1 - Injection	A1 - Injection	A1 - Broken Access Control
A2 - Broken Authentication & Session Management	A2 - Broken Authentication	A2 - Cryptographic Failures
A3 - Cross-Site Scripting (XSS)	A3 - Sensitive Data Exposure	A3 - Injection
A4 - Insecure Direct Object References	A4 - XML External Entities (XXE)	A4 - Insecure Design
A5 - Security Misconfiguration	A5 - Broken Access Control [MERGED A4+A7]	A5 - Security Misconfiguration
A6 - Sensitive Data Exposure	A6 - Security Misconfiguration	A6 - Vulnerable and Outdated Components
A7 - Missing Function Level Access Control	A7 - Cross-Site Scripting (XSS)	A7 - Identification and Authentication Failures
A8 - Cross-Site Request Forgery (CSRF)	A8 - Insecure Deserialization *	A8 - Software and Data Integrity Failures
A9 - Using Components with Known Vulnerabilities	A9 - Using Components with Known Vulnerabilities	A9 - Security Logging and Monitoring Failures *
A10 - Unvalidated Redirects and Forwards	A10 - Insufficient Logging & Monitoring *	A10 - Server-Side Request Forgery (SSRF) *
OWASP TOP 10		



Conclusion



TL;DR - The state of open source security 2019 report, at a glance



Open source adoption

- ▶ Growth in indexed packages, 2017 to 2018
 - ⚡ Maven Central - 102%
 - ⚡ PyPI - 40%
 - ⚡ npm - 37%
 - ⚡ NuGet - 26%
 - ⚡ RubyGems - 5.6%
- ▶ npm reported 304 billion downloads for 2018
- ▶ 78% of vulnerabilities are found in indirect dependencies



Known vulnerabilities

- ▶ 88% growth in application vulnerabilities over two years
- ▶ In 2018, vulnerabilities for npm grew by 47%. Maven Central and PHP Packagist disclosures grew by 27% and 56% respectively
- ▶ In 2018, we tracked over 4 times more vulnerabilities found in RHEL, Debian and Ubuntu as compared to 2017



Known vulnerabilities in docker images

- ▶ Each of the top ten most popular default docker images contains at least 30 vulnerable system libraries
- ▶ 44% of scanned docker images can fix known vulnerabilities by updating their base image tag



Vulnerability identification

- ▶ 37% of open source developers don't implement any sort of security testing during CI and 54% of developers don't do any docker image security testings
- ▶ The median time from when a vulnerability was added to an open source package until it was fixed was over 2 years



Who's responsible for open source security?

- ▶ 81% of users feel developers are responsible for open source security
- ▶ 68% of users feel that developers should own the security responsibility of their docker container images
- ▶ Only three in ten open source maintainers consider themselves to have high security knowledge



Snyk stats

- ▶ In the second half of 2018 alone, Snyk opened more than 70,000 Pull Requests for its users to remediate vulnerabilities in their projects
- ▶ CVE/NVD and public vulnerability databases miss many vulnerabilities, only accounting for 60% of the vulnerabilities Snyk tracks
- ▶ In 2018 alone, 500 vulnerabilities were disclosed by Snyk's proprietary dedicated research team



A decorative horizontal bar composed of three segments: a yellow segment on the left, a purple segment in the middle, and an orange segment on the right.

Analogie

« Nul n'est censé ignorer la loi »



A short horizontal bar composed of three segments: yellow, purple, and orange.

Ma devise

« Nul développeur n'est censé ignorer la sécurité »





Pour aller plus loin

- [ANSSI](#) ([Sécurité Agile](#), Applications sécurisés en [Rust](#), Déploiement de conteneurs [Docker](#))
- [10 leçons sur les 10 plus grosses fuites de données](#), de Adrien Pessu (JSC 2020)
- [La Cryptographie en 55' chrono](#) de m4dz (SnowCamp2020)
- [Sécurité du Cloud](#), de Eric Briand (RemoteClazz 2020)
- [La nuit tous les hackers sont gris](#) (Fiction écrite par Vincent Hazard, 2019)





TV5 Monde Analyse d'Incident / Incident Analysis

35

Traumatisme

- Ce genre d'incident de sécurité a plusieurs conséquences
 - Conditions de travail très dures : horaires importants, vacances annulées, pression croissante...
 - Traumatisme lié à l'attaque qui perdure et qui est difficile à percevoir lorsque l'ANSSI intervient
 - La crainte que l'attaquant revienne est permanente

Retour technique de
l'incident de TV5Monde

ANSSI



38:39 / 1:16:25





Pour aller plus loin



[La Sécurité dès la conception \(Secure by design\)](#), Programmez! (Hors-série 8 Septembre/Octobre 2022)



Rappelez-vous: Les hackers n'en ont rien à "faire"

- ☐ À propos du scope de votre projet
- ☐ Il est géré par une tierce partie / sous-traitant
- ☐ C'est un système ancien (Legacy)
- ☐ TPCM / " Touche pas ! C'est magique "
- ☐ C'est "trop critique pour être réparé"
- ☐ A propos de vos périodes de maintenance
- ☐ A propos de votre budget
- ☐ Vous l'avez toujours fait de cette façon
- ☐ À propos de votre date de mise en service
- ☐ Il s'agit seulement d'un pilote/PoC
- ☐ À propos des accords de non-divulgation
- ☐ Ce n'était pas une exigence dans le contrat
- ☐ C'est un système interne
- ☐ Il est vraiment difficile de modifier / changer
- ☐ Vous n'êtes pas sûr de savoir comment y remédier
- ☐ Il doit être remplacé
- ☐ C'est géré dans le Cloud
- ☐ À propos de votre inscription au registre des risques
- ☐ L'éditeur ne prend pas en charge cette configuration
- ☐ C'est une solution provisoire
- ☐ Il est conforme à [insérer la norme ici]
- ☐ Il est crypté sur disque
- ☐ Le rapport coût-bénéfice ne scale pas
- ☐ "Personne d'autre ne pouvait le comprendre"
- ☐ Vous ne pouvez pas expliquer le risque au "Business"
- ☐ Vous avez d'autres priorités
- ☐ Sur votre foi dans la compétence de vos utilisateurs internes
- ☐ Vous n'avez pas de justification commerciale
- ☐ Vous ne pouvez pas montrer le retour sur investissement
- ☐ Vous avez sous-traité ce risque
- ☐ C'était à la mode [insérer la technologie hype ici].
- ☐ De vos certifications



A horizontal bar with three segments of equal length, colored yellow, purple, and orange from left to right.

Merci beaucoup aux organisateurs & à Zenika pour nous accueillir ce soir





Merci pour votre attention !



N'oubliez pas de me donner votre avis sur cette session: <https://tinyurl.com/meetgo24>



Lien des slides dans les commentaires 



Faites-vous confiance aux QR Codes ?

