La sécurité dès la conception du projet

David Aparicio

BreizhCamp
Jeudi 30 Juin 2022, 10h30

by Howard Bouchevereau
The pictures are from Unsplash

@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, 3 ans)

400 000 serveurs

1,6 million de clients

Leader européen

2021 IPO

Café de la Bourse

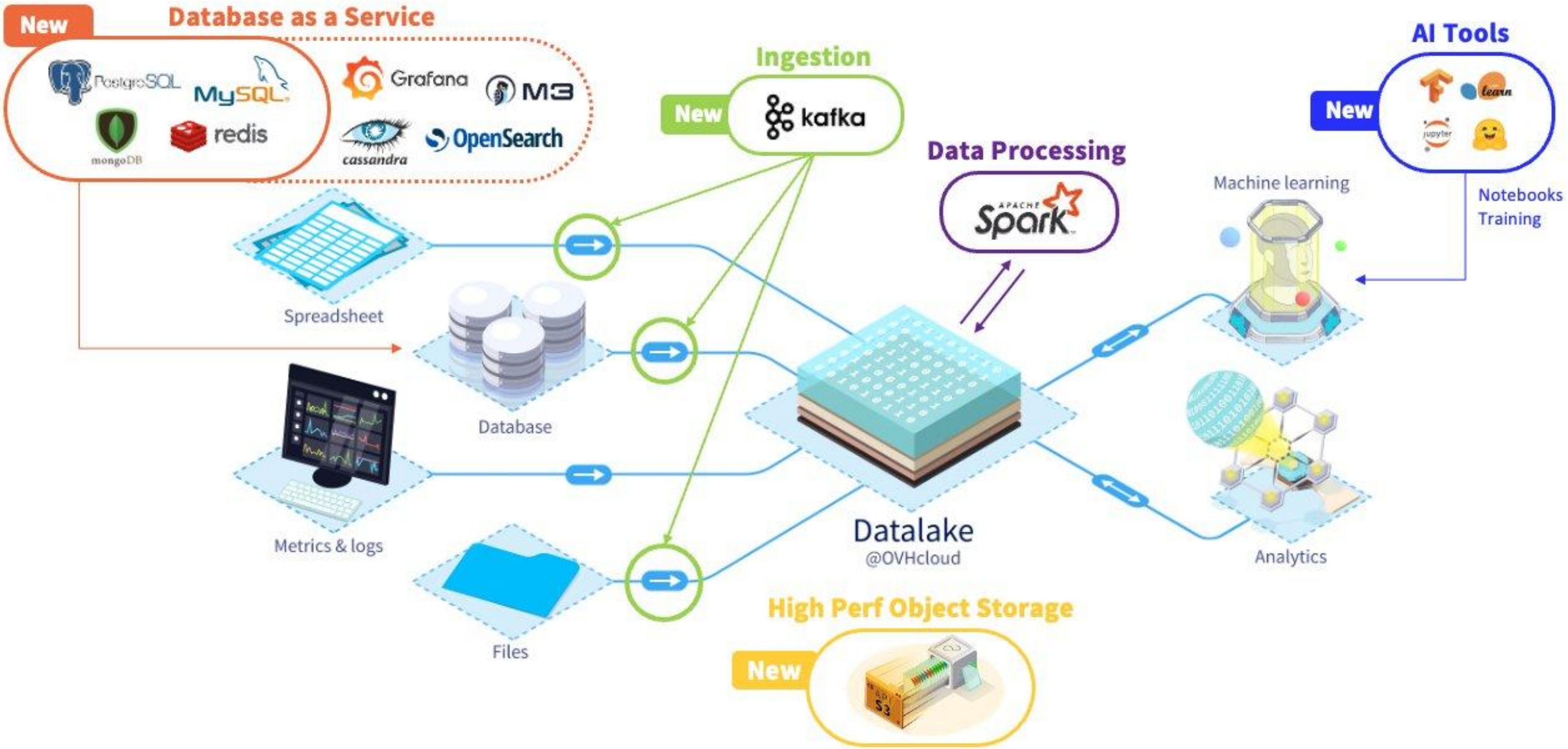
30 Datacenters

gaia-x

SecNumCloud

Depuis Déc 2020

GIS-DATA



New
Database as a Service
PostgreSQL
MySQL
mongoDB
redis
Grafana
M3
cassandra
OpenSearch

Ingestion
New
kafka

Data Processing
Spark

AI Tools
New
learn
jupyter
Notebooks
Training

Machine learning

Spreadsheet
Database
Metrics & logs
Files

Datalake
@OVHcloud

Analytics

High Perf Object Storage
New
S3

careers.ovhcloud.com

Agenda

Introduction

Retour d'expérience

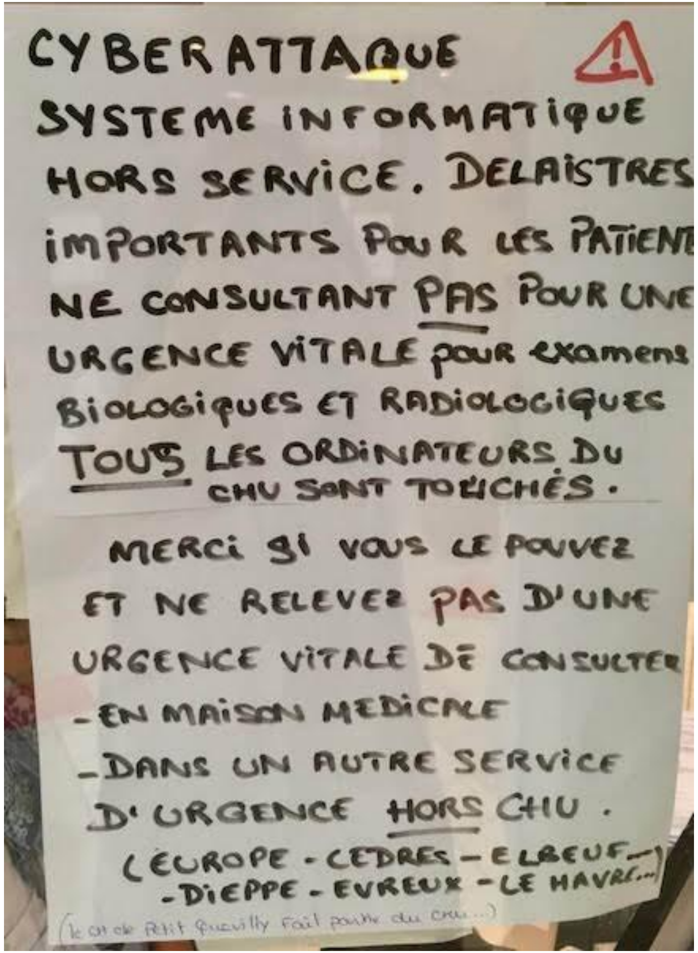
Conseils

Outils

Conclusion

Introduction

Pourquoi ce talk ?



CYBERATTAQUE ⚠

SYSTEME INFORMATIQUE HORS SERVICE. DELAISTRES IMPORTANTS POUR LES PATIENT NE CONSULTANT PAS POUR UNE URGENCE VITALE pour examens BIOLOGIQUES ET RADIOLOGIQUES

TOUS LES ORDINATEURS DU CHU SONT TOUCHÉS.

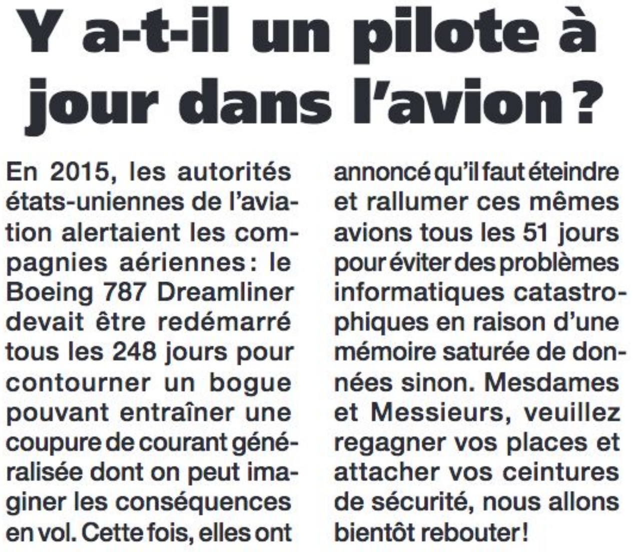
MERCI SI VOUS LE POUVEZ ET NE RELEVEZ PAS D'UNE URGENCE VITALE DE CONSULTER
- EN MAISON MEDICALE
- DANS UN AUTRE SERVICE D'URGENCE HORS CHU.

(EUROPE - CEDRES - ELBEUF...
- DIEPPE - EVREUX - LE HAVRE...)

(le CH de Petit Quevilly fait partie du CHU...)

[Thread @zigazou](#)

Dès la Conception !!



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 !

OOOH... C'EST FASCINANT TOUS CES CADRANS ET CES BOUTONS, COMMANDANT ! ET CES TOUCHES CTRL+ALT+SUPPR, LÀ, ÇA SERT À QUOI ?
HEU, JE... MGBLL... C'EST UN SECRET !

🎯 Octobre 2020,
Le Virus Informatique
n°44 (papier/en ligne)

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**

Quelques chiffres 🇫🇷

🎯 Rapport ANSSI 2019

Selon l'ANSSI

2018: 1 869

2296

Signalements en 2019

2018: 16

9

Incidents majeurs

2018: 14

16

Opérations de cyberdéfense

2019: 370 incidents
2018: 391 Incidents

Quelques chiffres en Outre-Altantique 🇺🇸

Selon l'Institut Ponemon, en 2017

2,4 M$

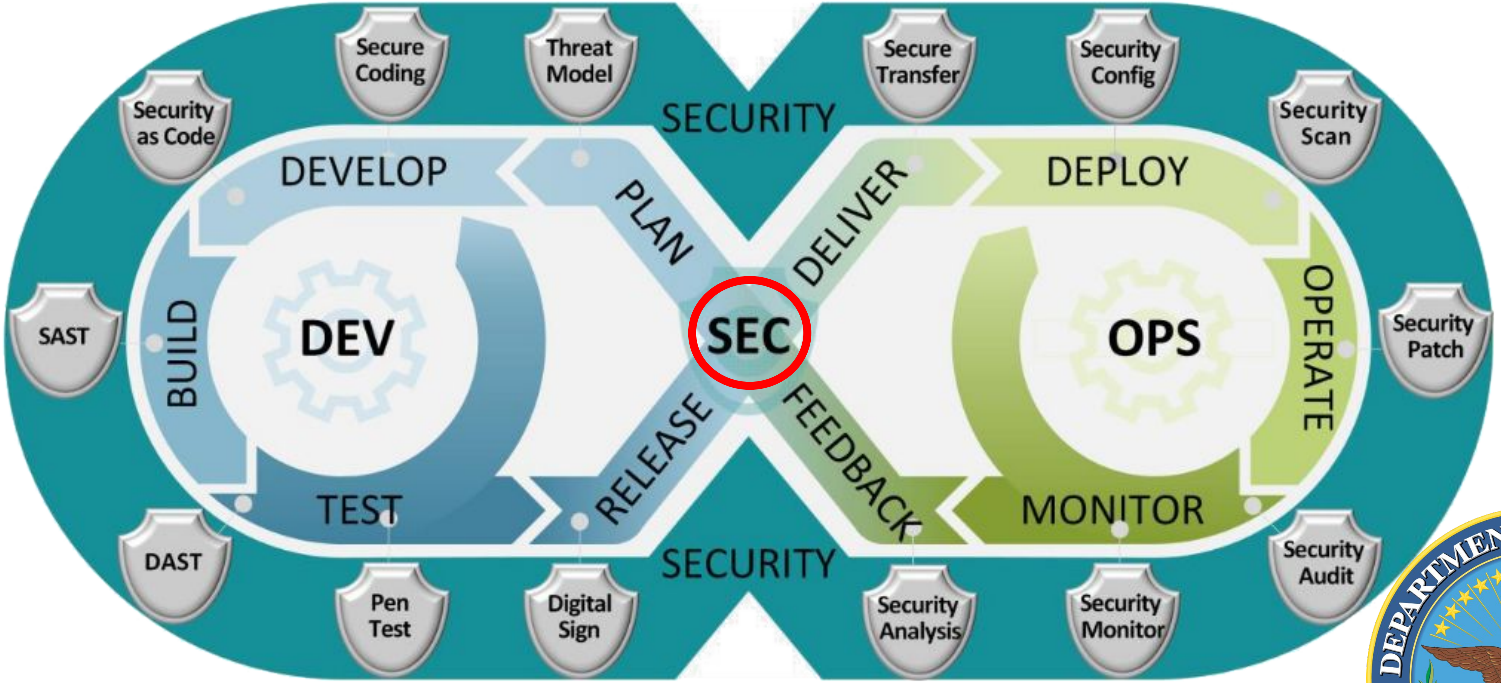
Ce qui coûte en moyenne à une entreprise, pour une attaque de malware

Selon le département américain de la Défense

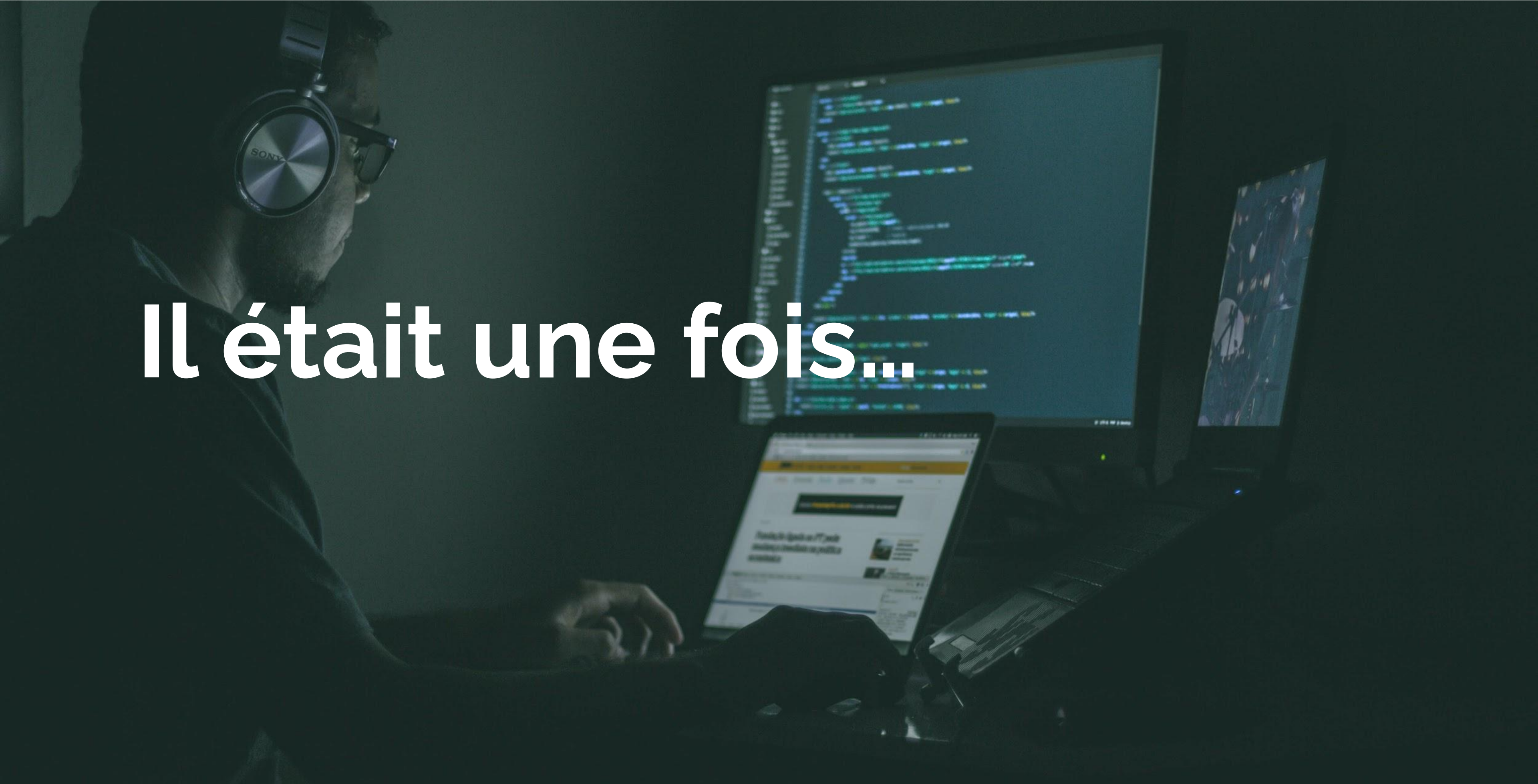
x 17

le nombres d'intrusions dans les infrastructures américaines cruciales en 3 ans

Shift-left Security

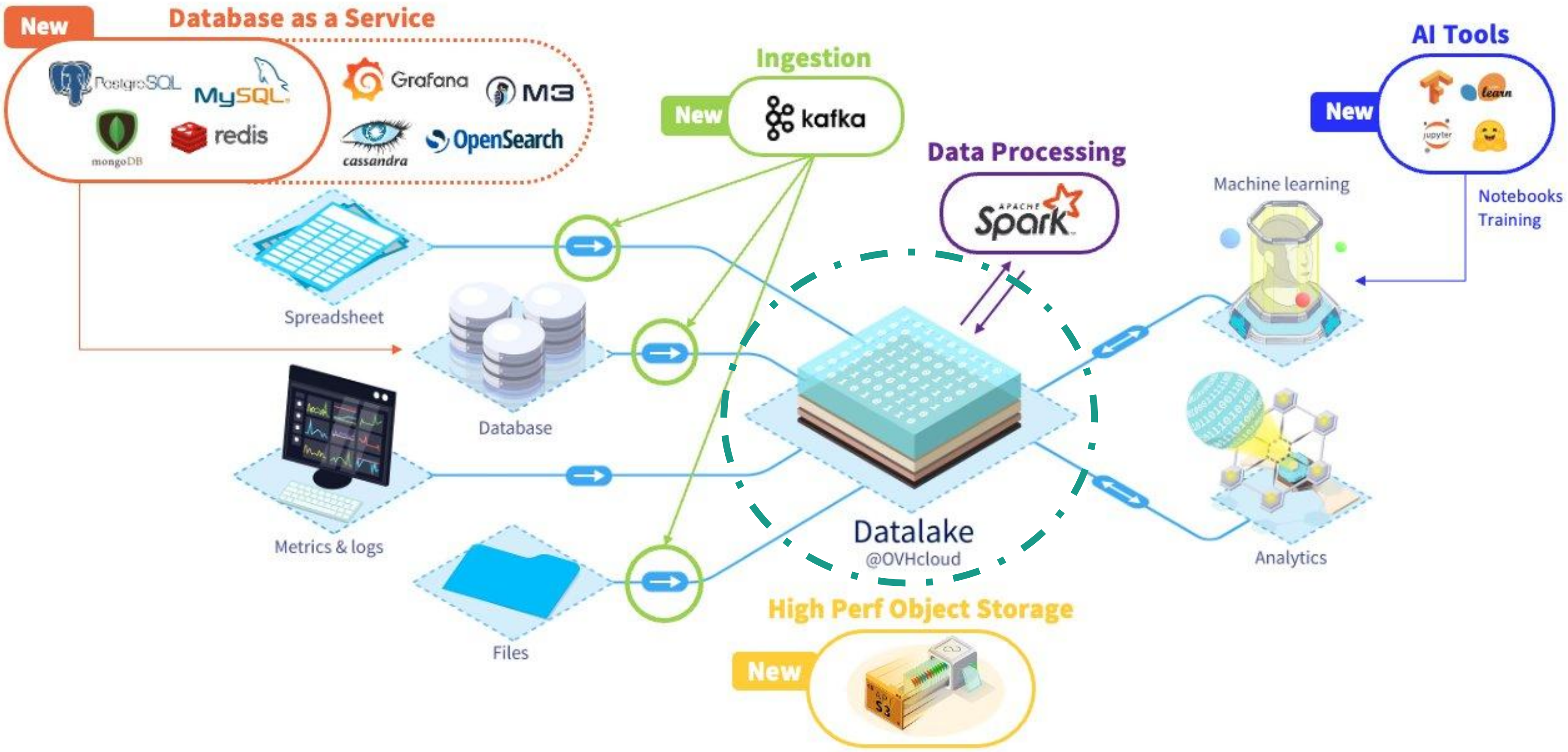


🎯 dodcio.defense.gov



Il était une fois…

Un Datalake


New
Database as a Service
PostgreSQL
MySQL
mongoDB
redis
Grafana
M3
cassandra
OpenSearch
Ingestion
New
kafka
Data Processing
APACHE Spark
AI Tools
New
learn
jupyter
Machine learning
Notebooks
Training
Spreadsheet
Database
Metrics & logs
Files
Datalake
@OVHcloud
Analytics
High Perf Object Storage
New
S3

Un ticket

En tant qu'

utilisateur ou administrateur du Datalake

Je veux

un service toujours disponible, avec de la redondance (SLO/SLA)

Pour cela

Il faut sauvegarder régulièrement la configuration & la base de données de Kerberos
Car c'est un des SPOF (Point de défaillance unique) identifié de l'infrastructure

Un ticket

En tant qu'

utilisateur ou administrateur du Datalake

Je veux

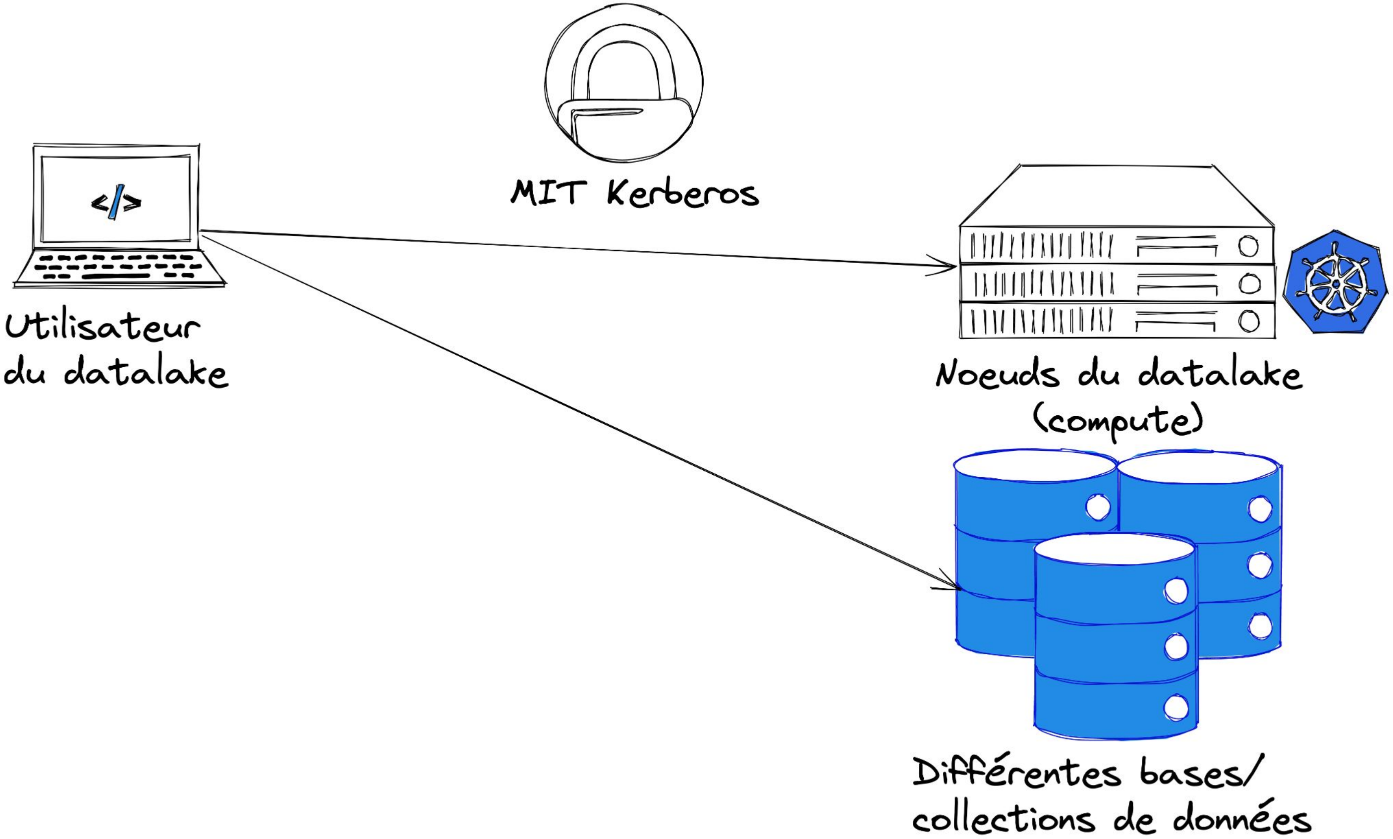
un service toujours disponible, avec de la redondance (SLO/SLA)

Pour cela

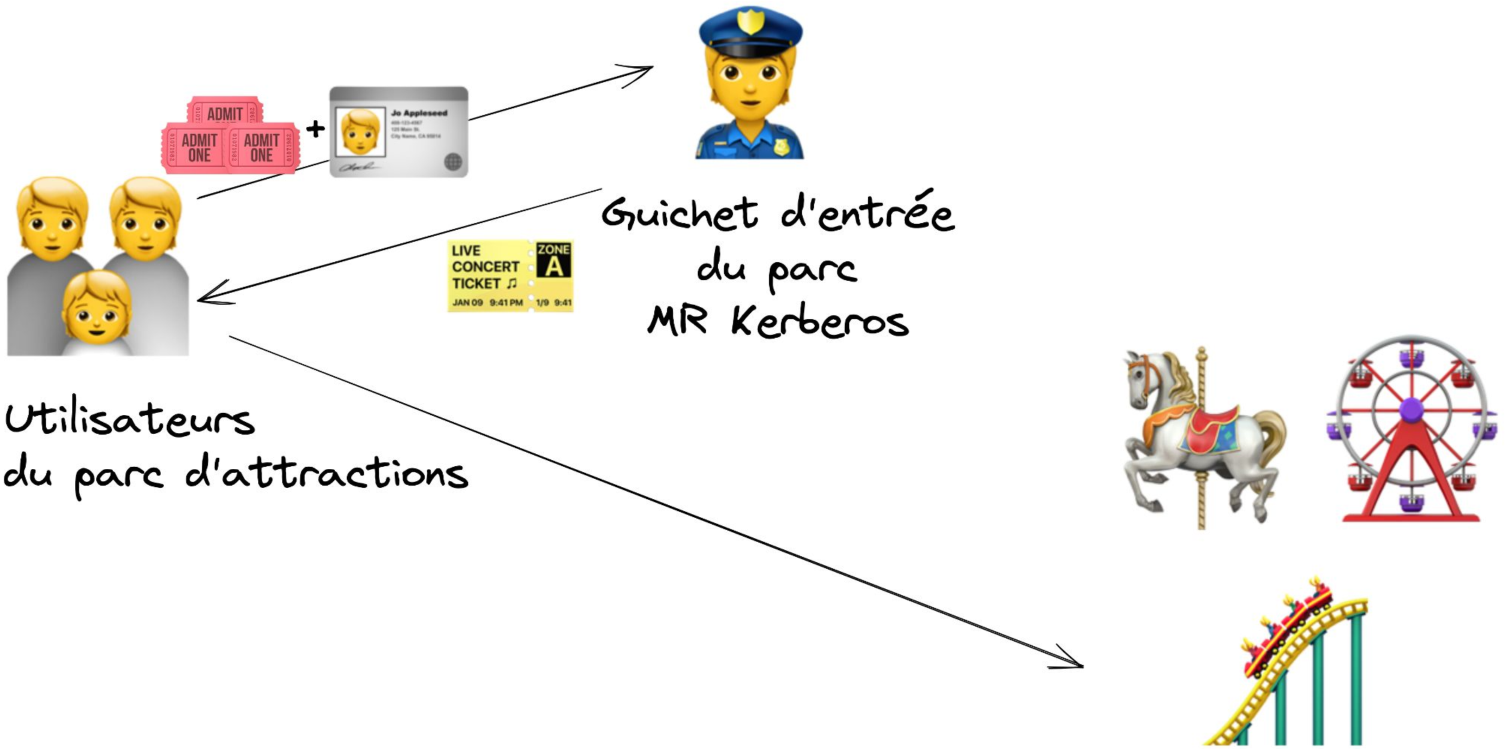
Il faut sauvegarder régulièrement la configuration & la base de données de Kerberos
Car c'est un des SPOF (Point de défaillance unique) identifié de l'infrastructure

En effet, pas de ressources dispo pour rendre Kerberos HA (Haute disponibilité)

Kerberos Kézako?


MIT Kerberos
Utilisateur du datalake
Noeuds du datalake (compute)
Différentes bases/ collections de données

SSO

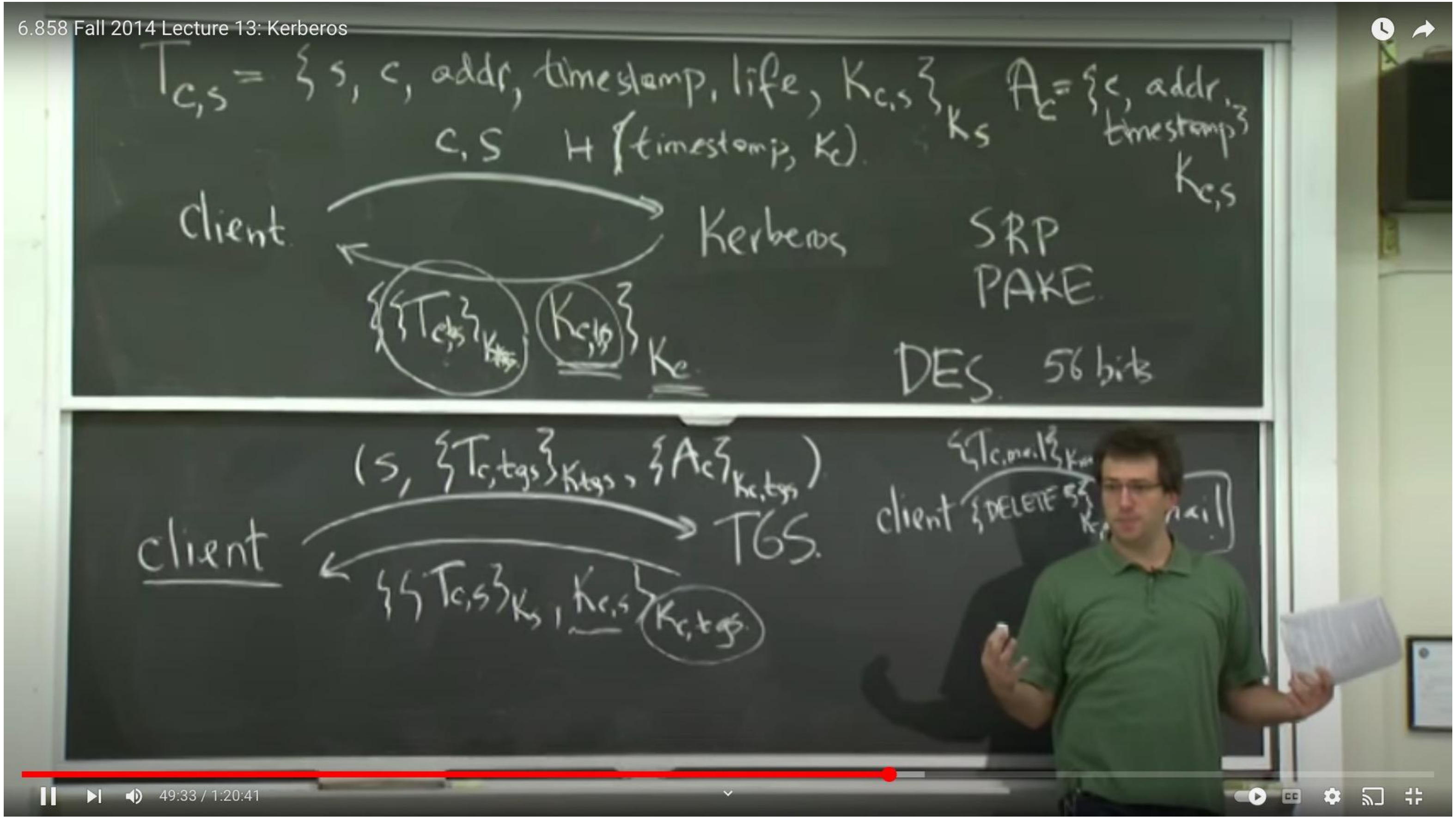


Guichet d'entrée
du parc
MR Kerberos

Utilisateurs
du parc d'attractions

Différents manèges
(autorisés selon
son âge/ses droits)

Pour aller plus loin

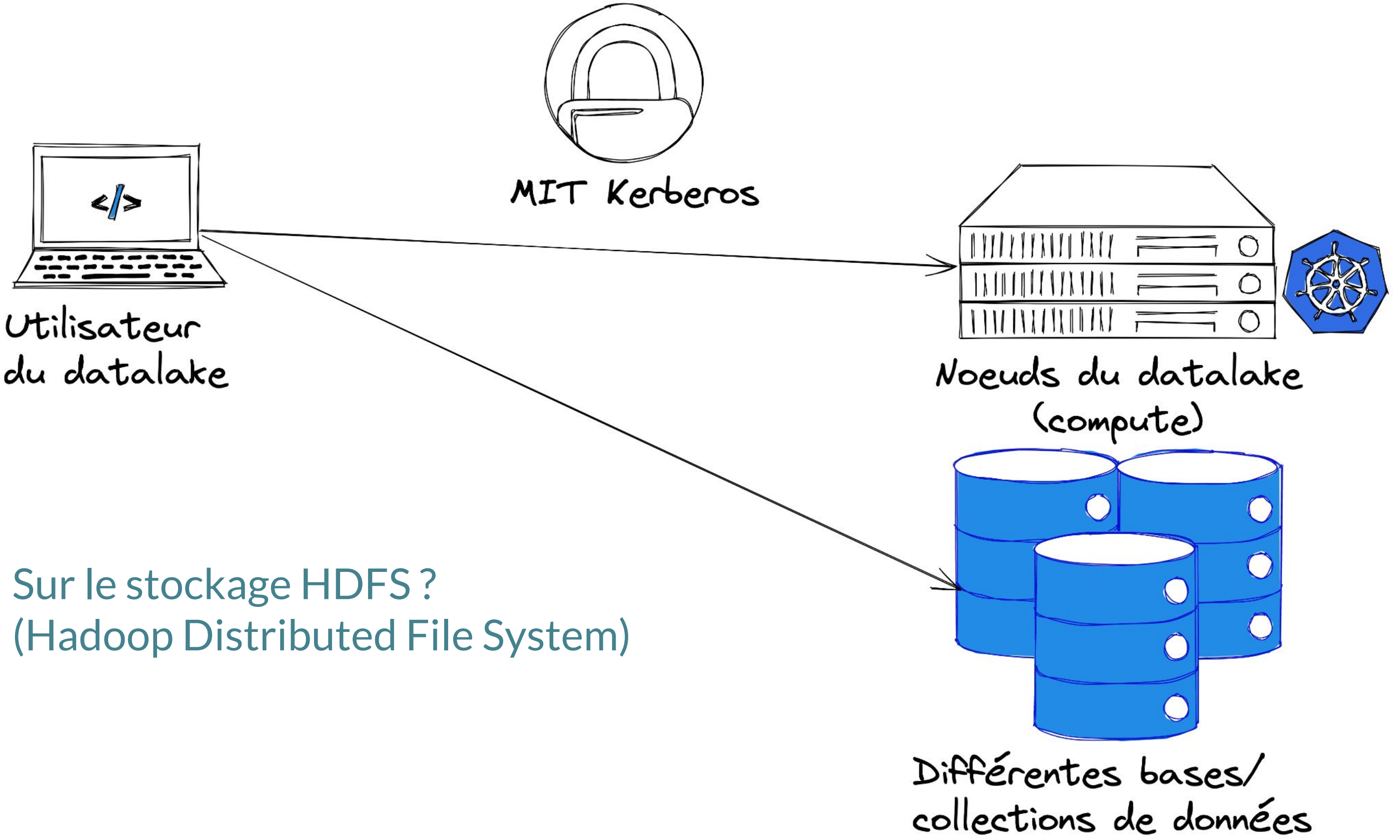


6.858 Fall 2014 Lecture 13: Kerberos

49:33 / 1:20:41

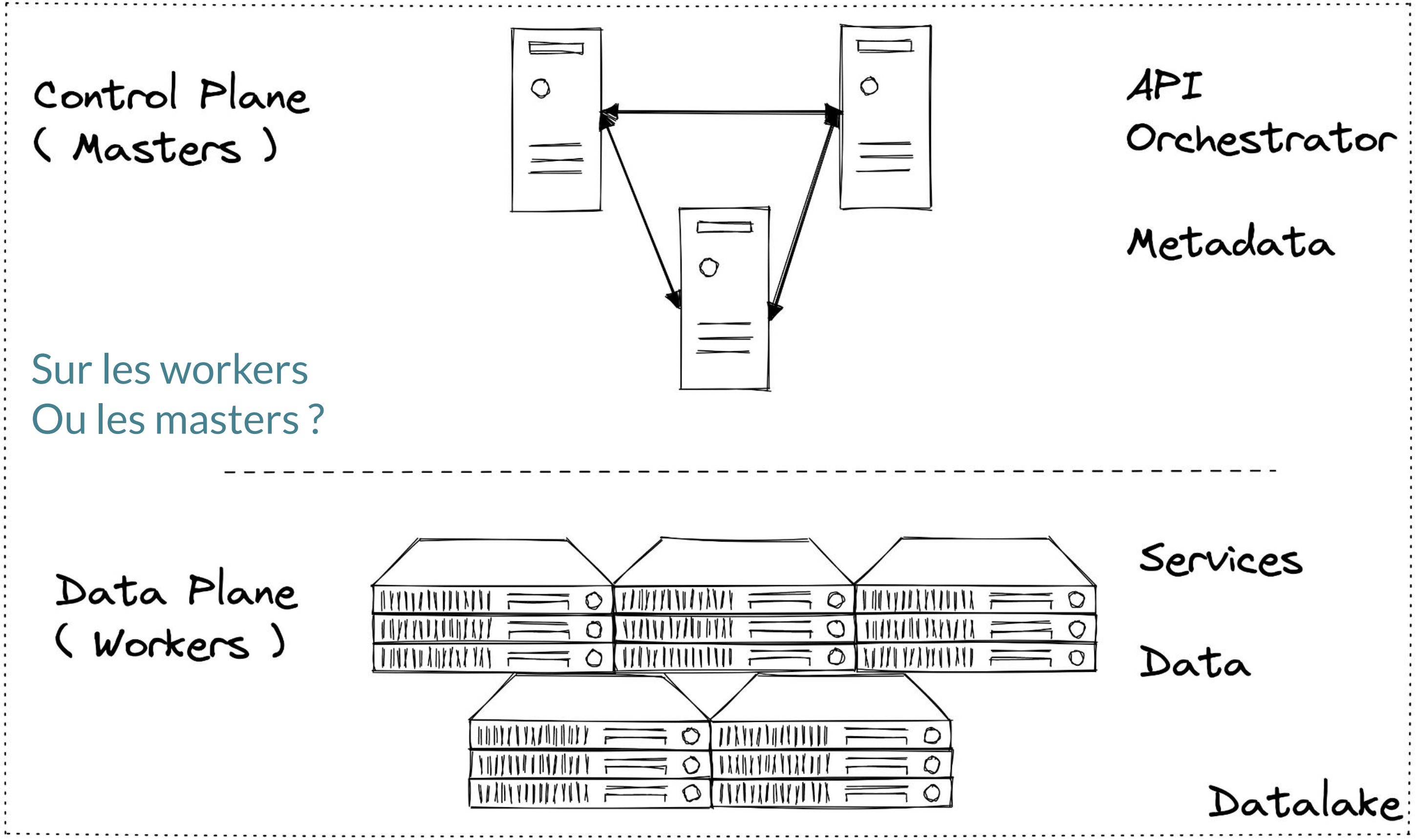
🎯 6.858 Fall 2014 Lecture 13: Kerberos

Où stocker le backup ?


MIT Kerberos
</>
Utilisateur du datalake
Noeuds du datalake (compute)
Différentes bases/ collections de données

Sur le stockage HDFS ?
(Hadoop Distributed File System)

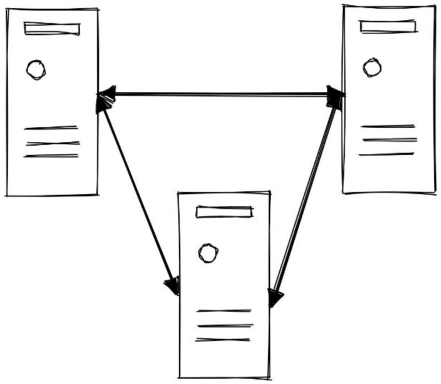
Où stocker le backup ?



Sur les workers
Ou les masters ?

SSOT
(source unique de vérité)

Control Plane
(Masters)

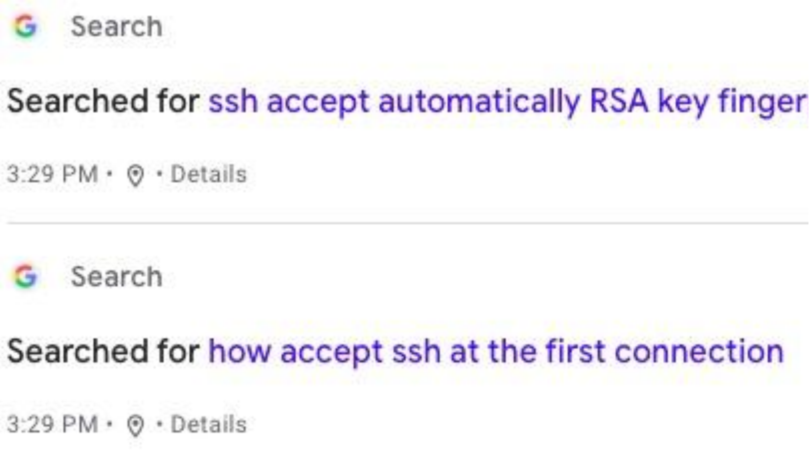


API
Orchestrator

Metadata

Sur les masters, avec le déployeur (Puppet Master)

Google



Search

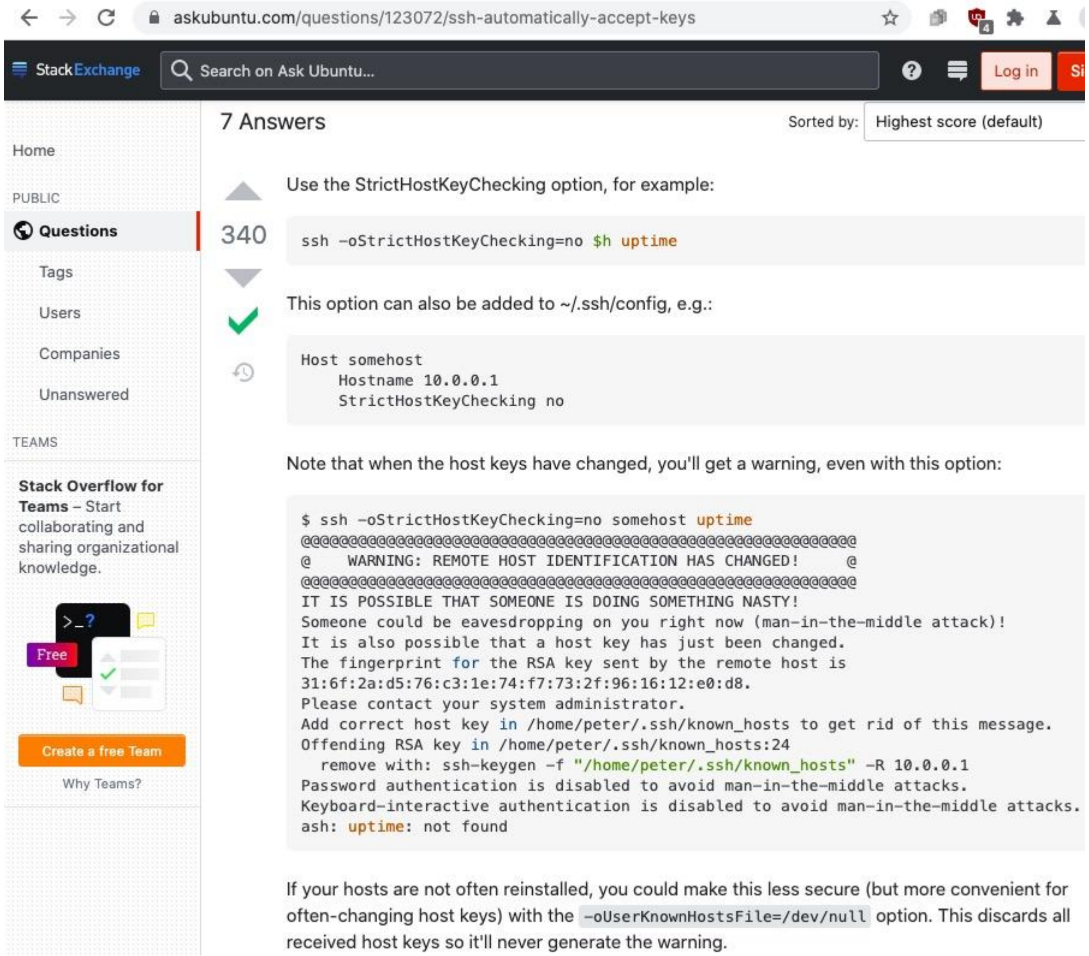
Searched for ssh accept automatically RSA key finger

3:29 PM • • Details

Search

Searched for how accept ssh at the first connection

3:29 PM • • Details



askubuntu.com/questions/123072/ssh-automatically-accept-keys

Stack Overflow for Teams – Start collaborating and sharing organizational knowledge.

7 Answers

Sorted by: Highest score (default)

340

Use the StrictHostKeyChecking option, for example:

```
ssh -oStrictHostKeyChecking=no $h uptime
```

This option can also be added to ~/.ssh/config, e.g.:

```
Host somehost
    Hostname 10.0.0.1
    StrictHostKeyChecking no
```

Note that when the host keys have changed, you'll get a warning, even with this option:

```
$ ssh -oStrictHostKeyChecking=no somehost uptime
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
31:6f:2a:d5:76:c3:1e:74:f7:73:2f:96:16:12:e0:d8.
Please contact your system administrator.
Add correct host key in /home/peter/.ssh/known_hosts to get rid of this message.
Offending RSA key in /home/peter/.ssh/known_hosts:24
  remove with: ssh-keygen -f "/home/peter/.ssh/known_hosts" -R 10.0.0.1
Password authentication is disabled to avoid man-in-the-middle attacks.
Keyboard-interactive authentication is disabled to avoid man-in-the-middle attacks.
ash: uptime: not found
```

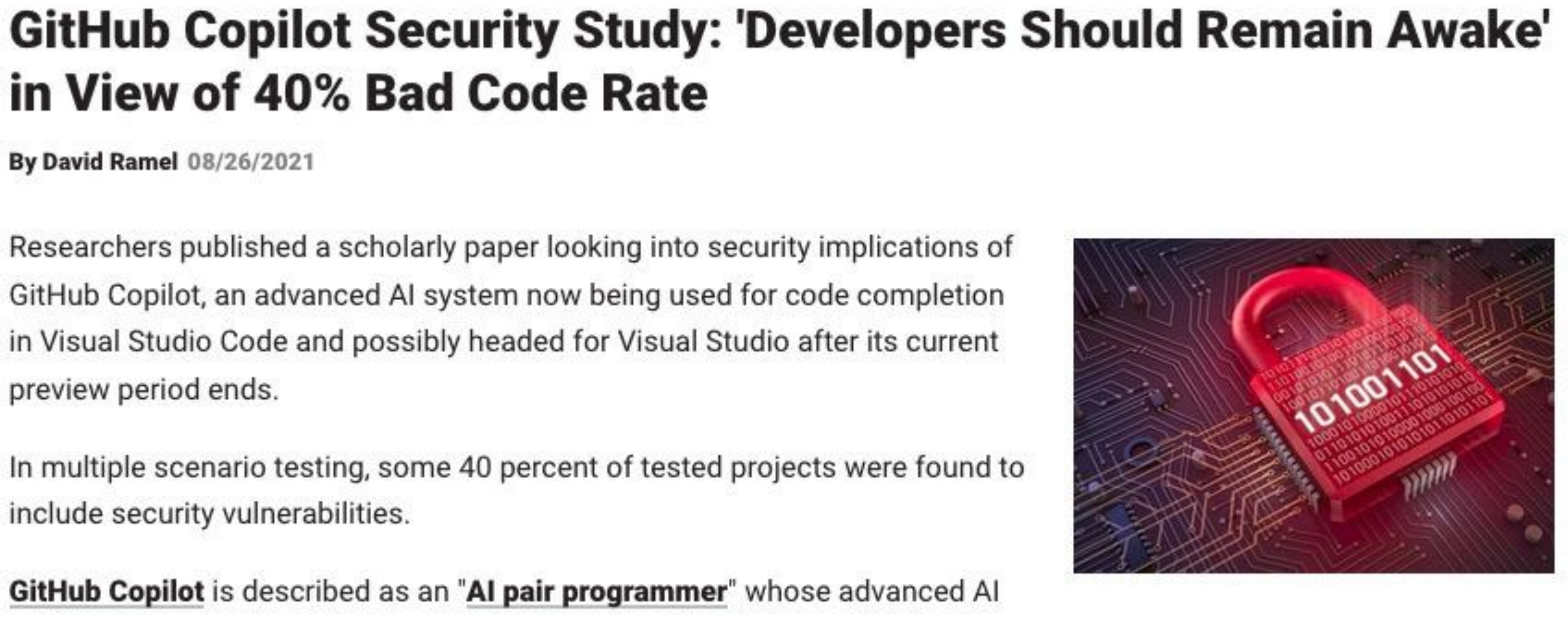
If your hosts are not often reinstalled, you could make this less secure (but more convenient for often-changing host keys) with the `-oUserKnownHostsFile=/dev/null` option. This discards all received host keys so it'll never generate the warning.

Pas copier-coller depuis StackOverFlow

98% snippets sécu/crypto sont insecures

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

PS: Copilot aussi



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

By David Ramel 08/26/2021

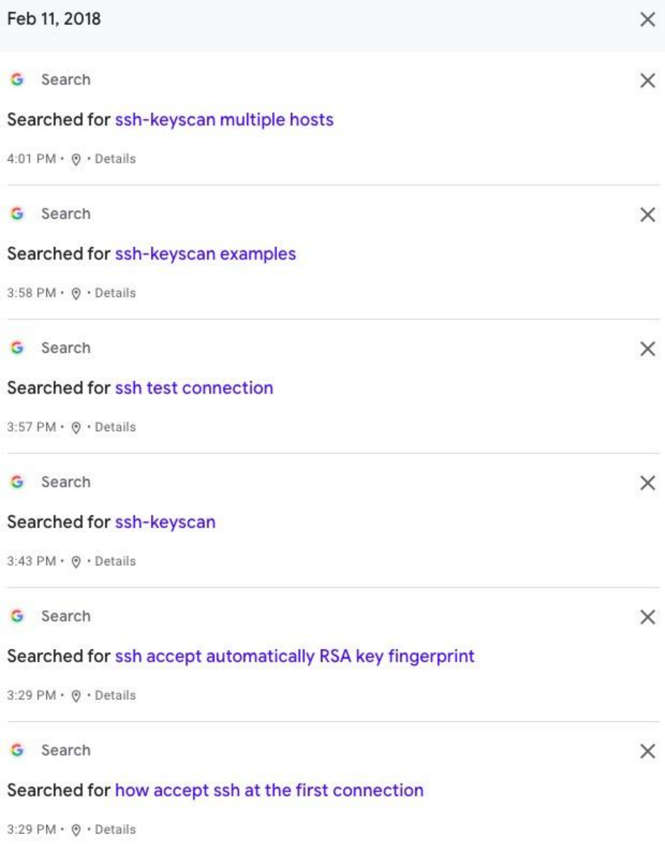
Researchers published a scholarly paper looking into security implications of GitHub Copilot, an advanced AI system now being used for code completion in Visual Studio Code and possibly headed for Visual Studio after its current preview period ends.

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

Prendre du recul



Feb 11, 2018 ✕

Search ✕

Searched for ssh-keyscan multiple hosts

4:01 PM • • Details

Search ✕

Searched for ssh-keyscan examples

3:58 PM • • Details

Search ✕

Searched for ssh test connection

3:57 PM • • Details

Search ✕

Searched for ssh-keyscan

3:43 PM • • Details

Search ✕

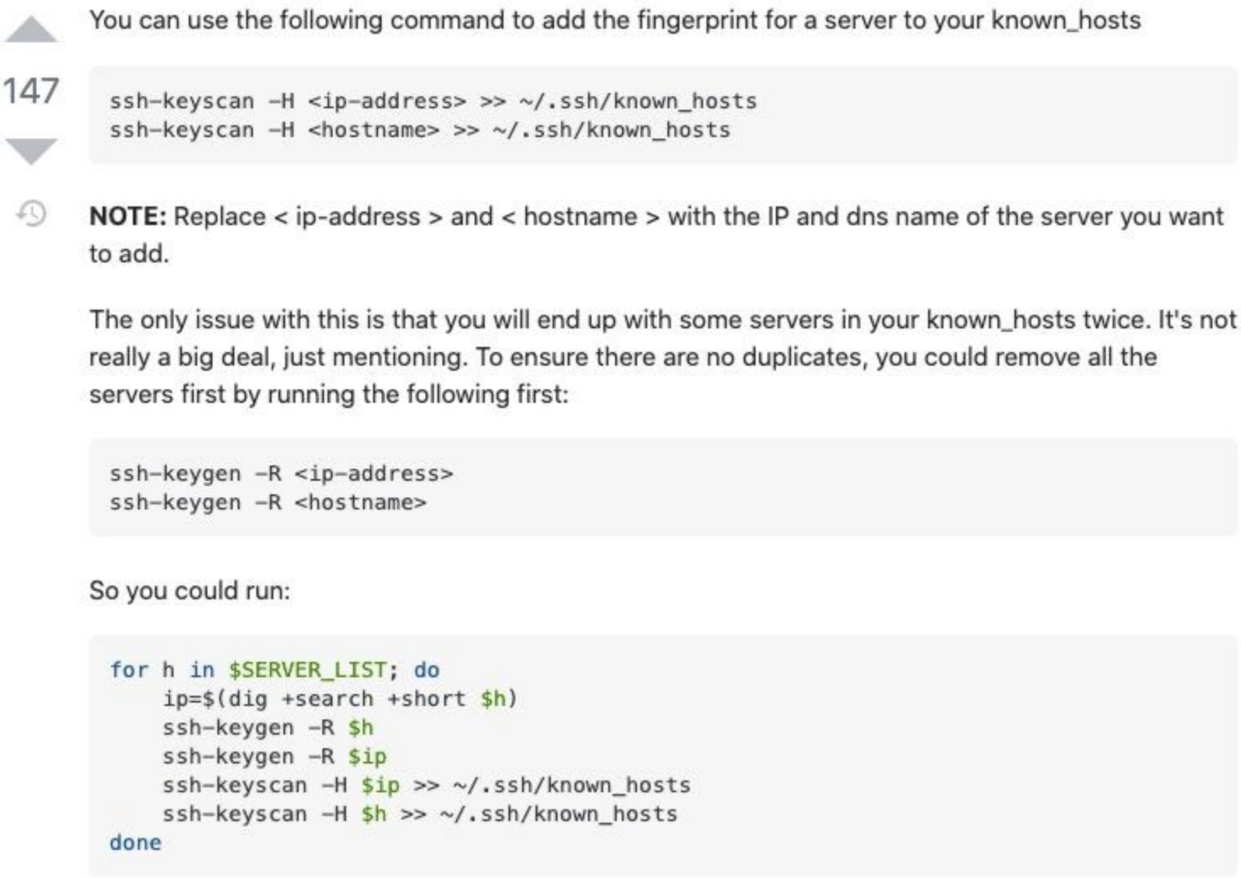
Searched for ssh accept automatically RSA key fingerprint

3:29 PM • • Details

Search ✕

Searched for how accept ssh at the first connection

3:29 PM • • Details



147

You can use the following command to add the fingerprint for a server to your known_hosts

```
ssh-keyscan -H <ip-address> >> ~/.ssh/known_hosts
ssh-keyscan -H <hostname> >> ~/.ssh/known_hosts
```

NOTE: Replace < ip-address > and < hostname > with the IP and dns name of the server you want to add.

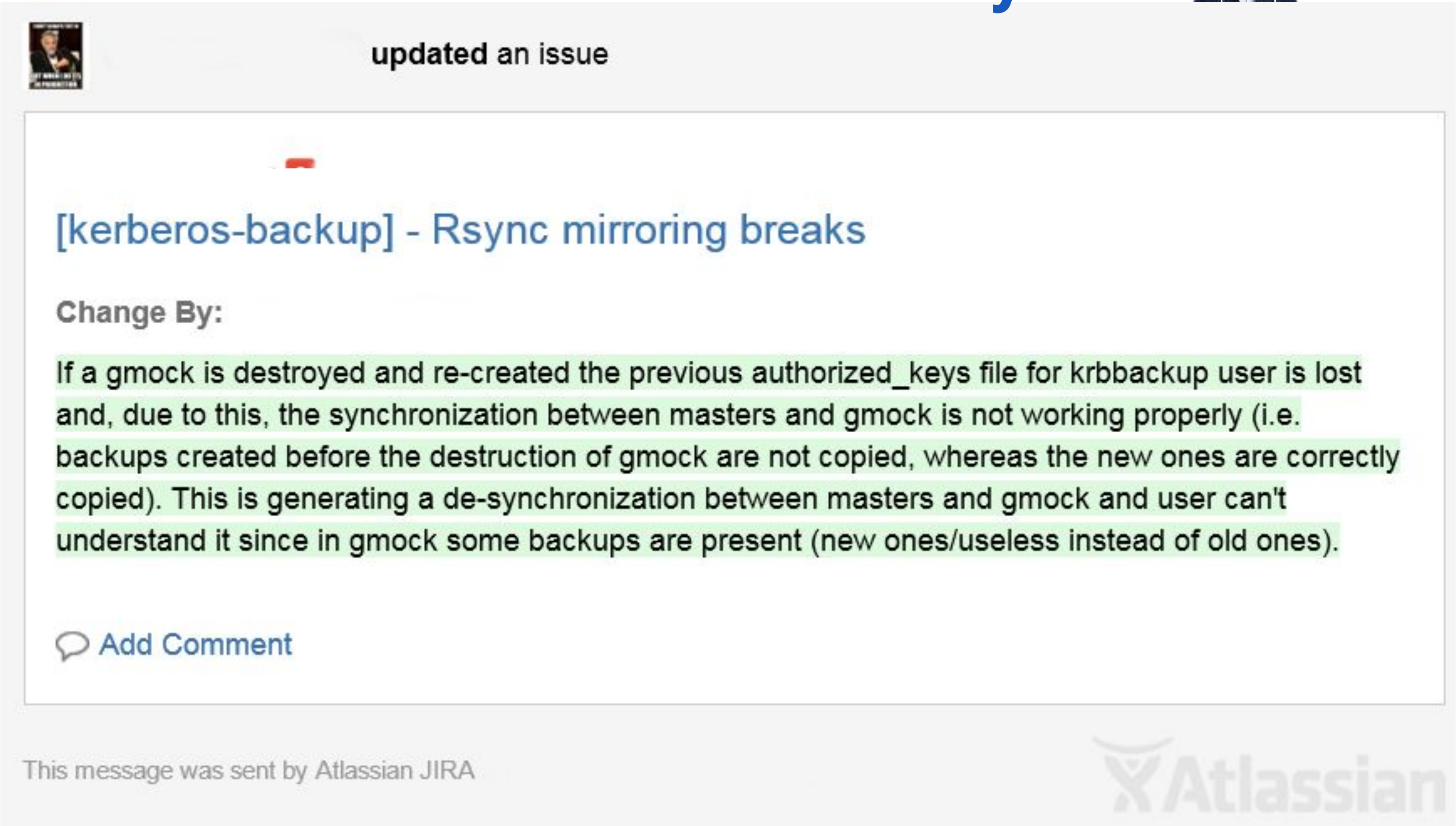
The only issue with this is that you will end up with some servers in your known_hosts twice. It's not really a big deal, just mentioning. To ensure there are no duplicates, you could remove all the servers first by running the following first:

```
ssh-keygen -R <ip-address>
ssh-keygen -R <hostname>
```

So you could run:

```
for h in $SERVER_LIST; do
    ip=$(dig +search +short $h)
    ssh-keygen -R $h
    ssh-keygen -R $ip
    ssh-keyscan -H $ip >> ~/.ssh/known_hosts
    ssh-keyscan -H $h >> ~/.ssh/known_hosts
done
```

Chaos Monkey



updated an issue

[kerberos-backup] - Rsync mirroring breaks

Change By:

If a gmock is destroyed and re-created the previous authorized_keys file for krbbackup user is lost and, due to this, the synchronization between masters and gmock is not working properly (i.e. backups created before the destruction of gmock are not copied, whereas the new ones are correctly copied). This is generating a de-synchronization between masters and gmock and user can't understand it since in gmock some backups are present (new ones/useless instead of old ones).

Add Comment

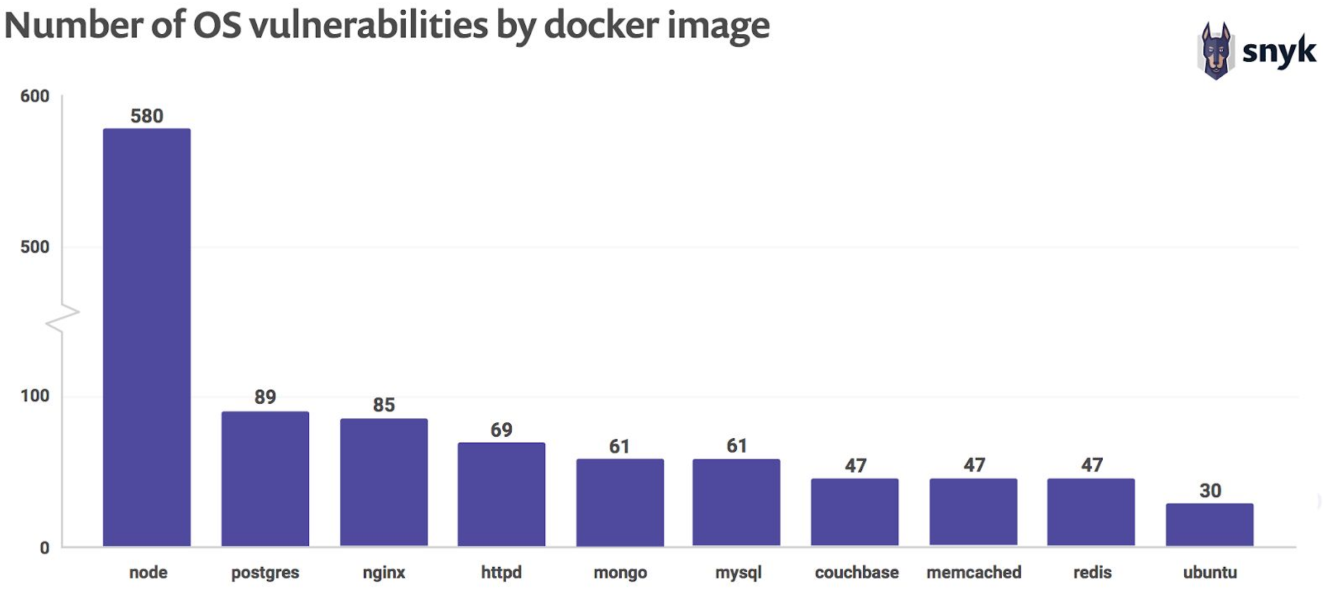
This message was sent by Atlassian JIRA

Problèmes

- Cluster sans Kerberos (MapR ticket)
- Pas de 50/50 (épuisement)
- Temps de livraison (junior)
- Sécurité ? (auto-formation)
- Chiffrement des sauvegardes
- Accompagnement du Management

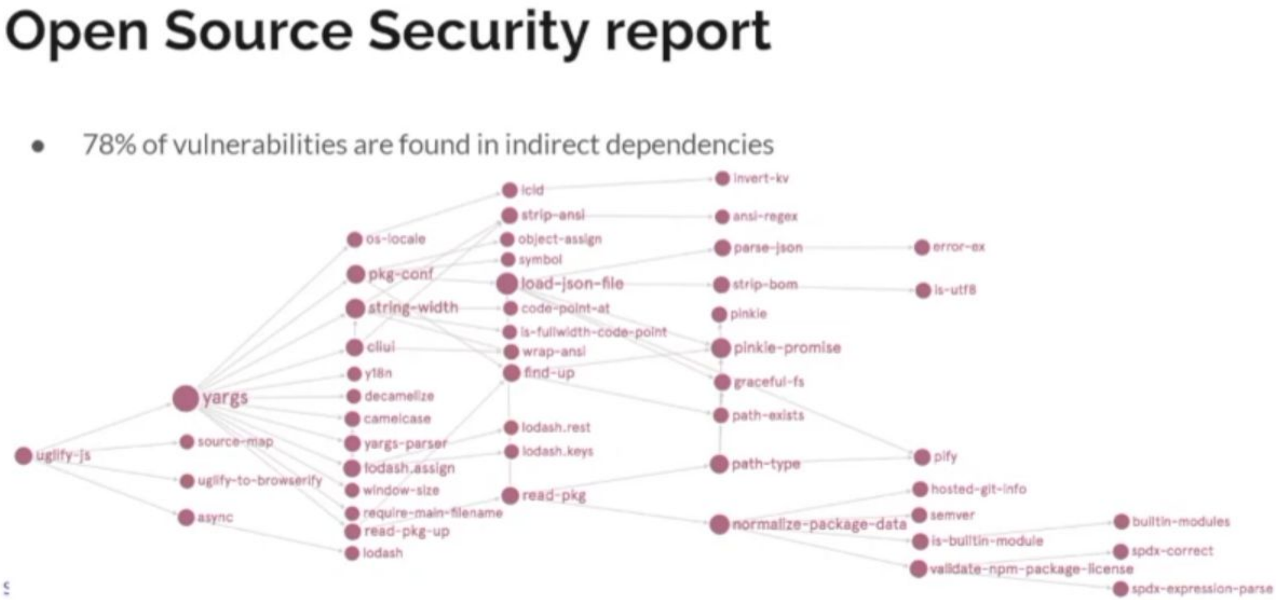
Conseils

Attention avec Docker



🎯 The state of open source security – 2019

Attention avec vos dépendances

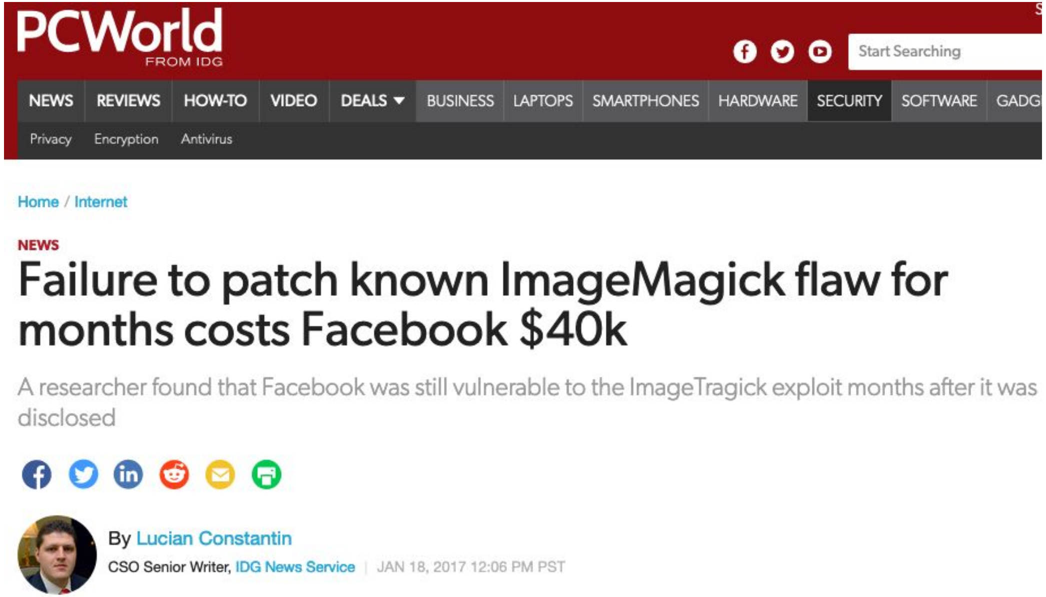


Open Source Security report

- 78% of vulnerabilities are found in indirect dependencies

🎯 [The state of open source security – 2019]

Attention avec vos dépendances


PCWorld
FROM IDG
Start Searching
NEWS REVIEWS HOW-TO VIDEO DEALS BUSINESS LAPTOPS SMARTPHONES HARDWARE SECURITY SOFTWARE GADG
Privacy Encryption Antivirus
Home / Internet

NEWS

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

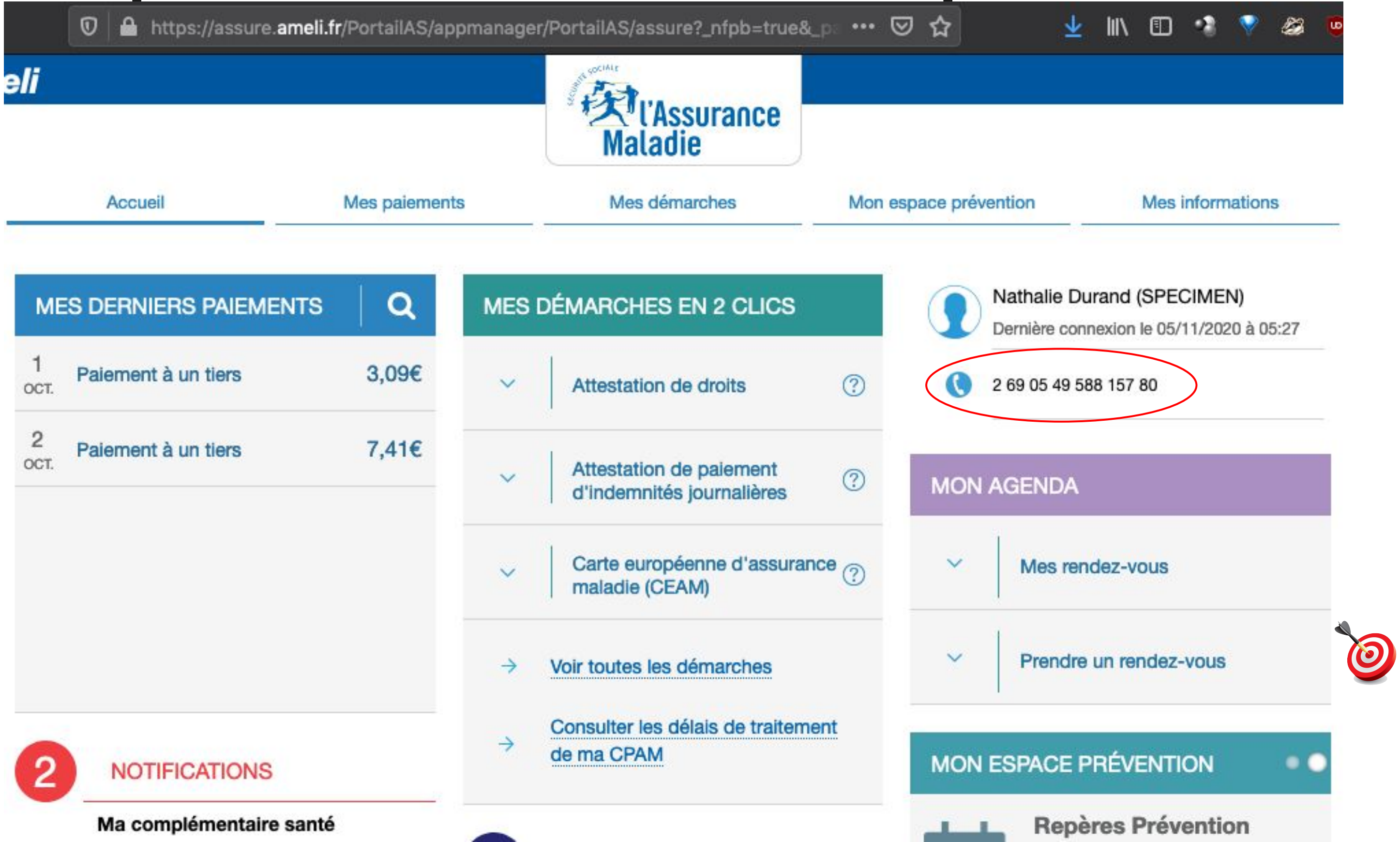
A researcher found that Facebook was still vulnerable to the ImageTragick exploit months after it was disclosed

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)



https://assure.ameli.fr/PortailAS/appmanager/PortailAS/assure?_nfpb=true&_p

eli

l'Assurance Maladie

MES DERNIERS PAIEMENTS

1 OCT.	Paiement à un tiers	3,09€
2 OCT.	Paiement à un tiers	7,41€

2 NOTIFICATIONS

Ma complémentaire santé

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

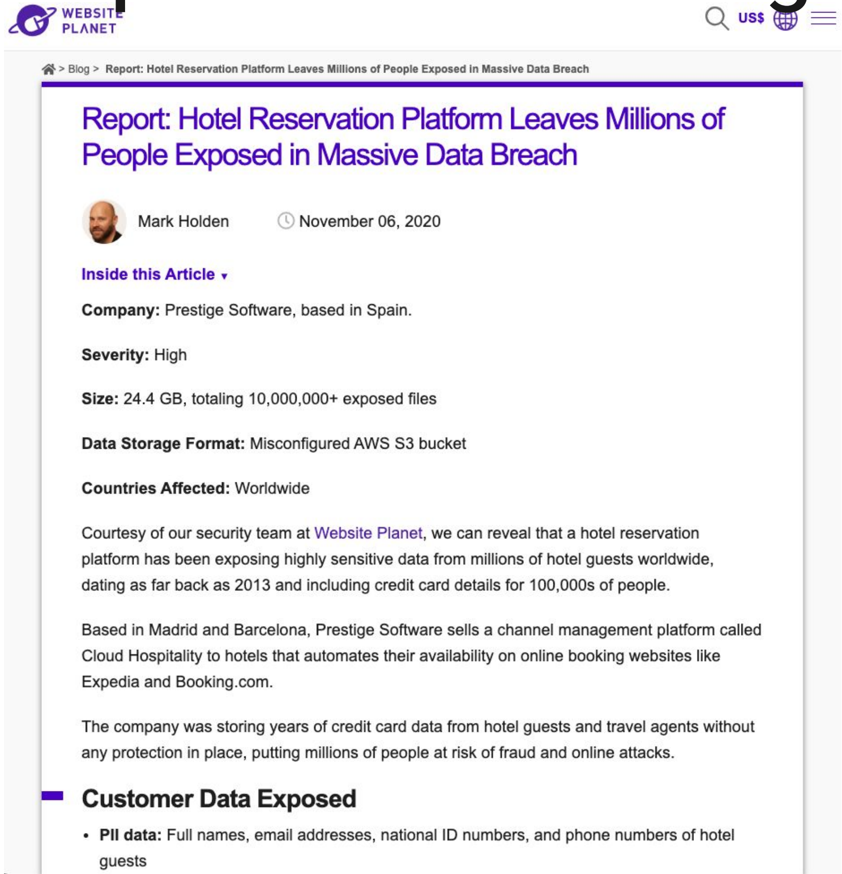
MON ESPACE PRÉVENTION

Repères Prévention

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

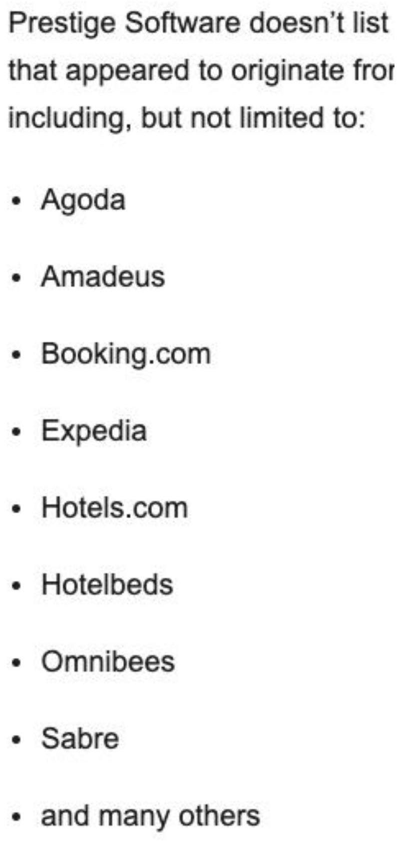
Courtesy of our security team at Website Planet, we can reveal that a hotel reservation platform has been exposing highly sensitive data from millions of hotel guests worldwide, dating as far back as 2013 and including credit card details for 100,000s of people.

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

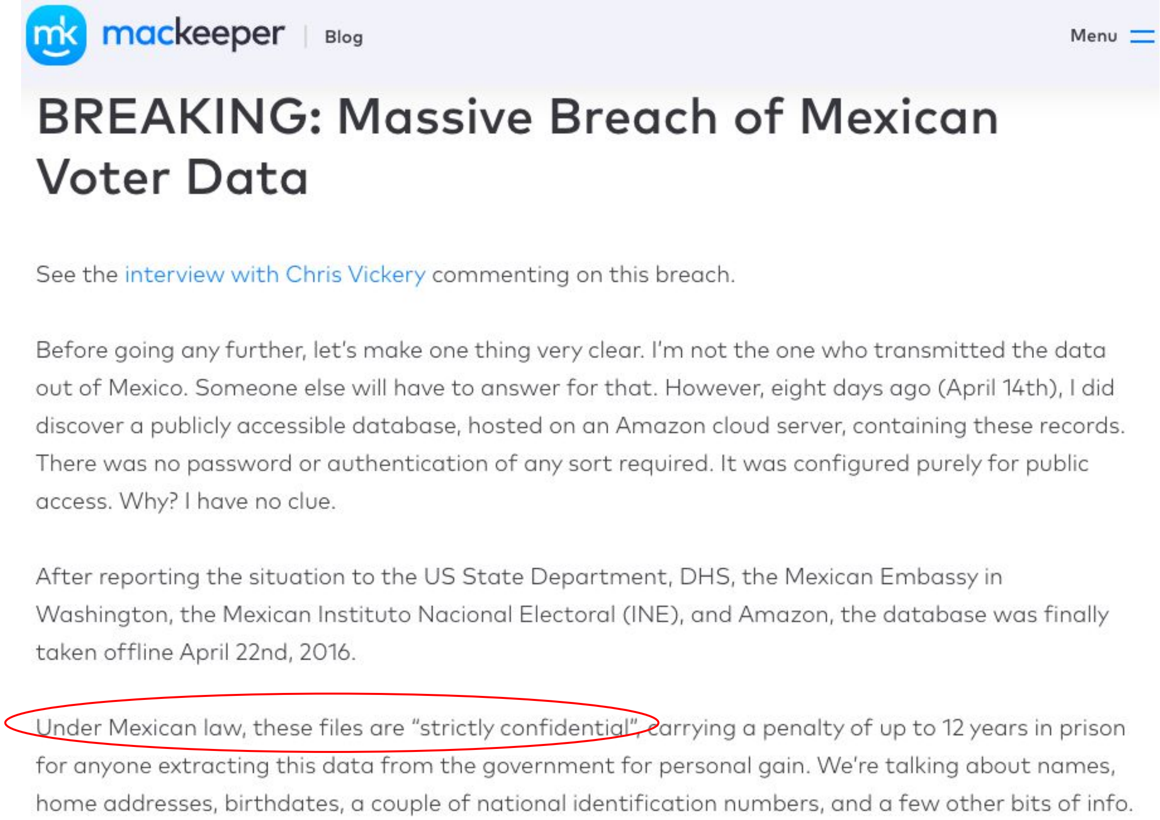


Prestige Software doesn't list that appeared to originate fror including, but not limited to:

- 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



BREAKING: Massive Breach of Mexican Voter Data

See the interview with Chris Vickery commenting on this breach.

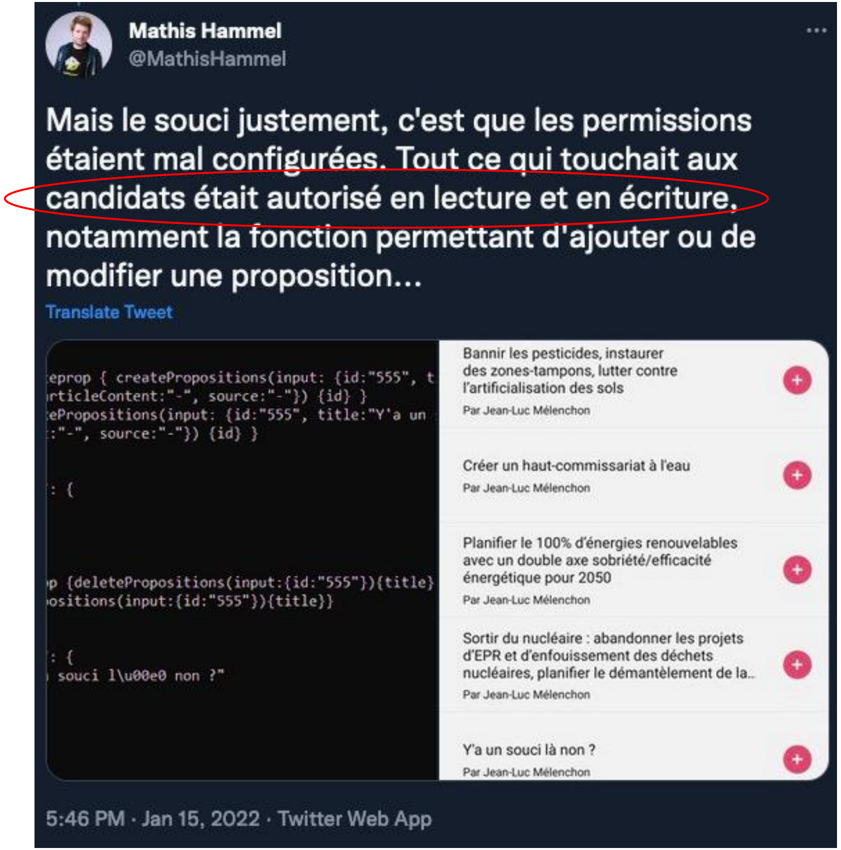
Before going any further, let's make one thing very clear. I'm not the one who transmitted the data out of Mexico. Someone else will have to answer for that. However, eight days ago (April 14th), I did discover a publicly accessible database, hosted on an Amazon cloud server, containing these records. 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...

```
eprop { createPropositions(input: {id:"555", t
rticleContent:"-", source:"-"}) {id} }
ePropositions(input: {id:"555", title:"Y'a un
:"-", 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

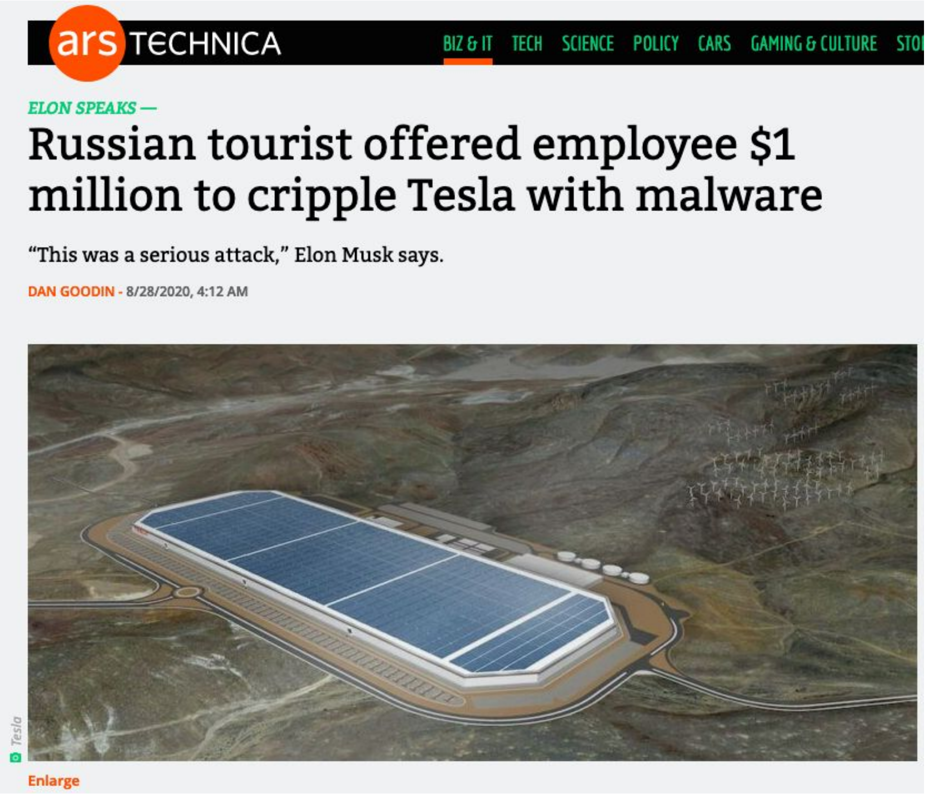
Sortir du nucléaire : abandonner les projets d'EPR et d'enfouissement des déchets nucléaires, planifier le démantèlement de la..
Par Jean-Luc Mélenchon

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



ELON SPEAKS —

Russian tourist offered employee $1 million to cripple Tesla with malware

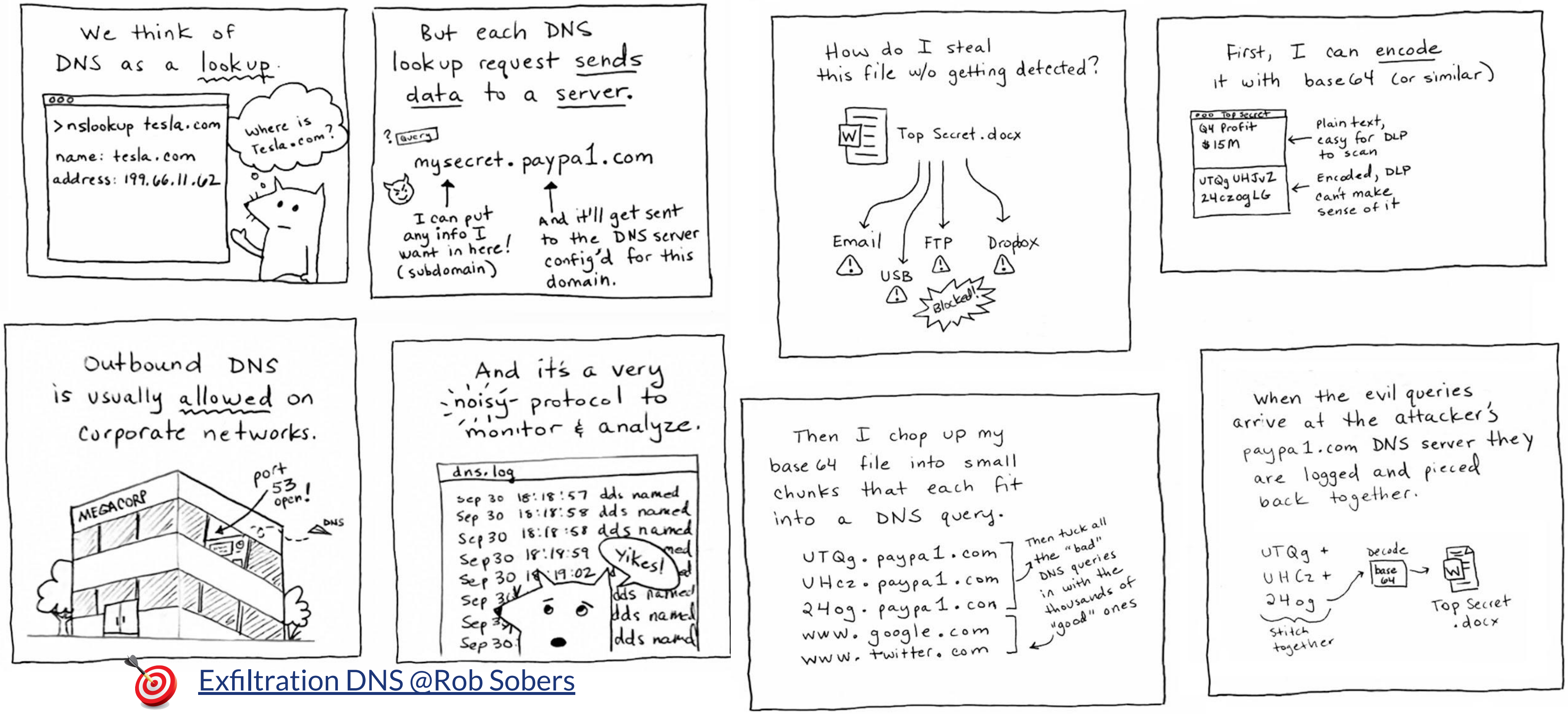
“This was a serious attack,” Elon Musk says.

DAN GOODIN - 8/28/2020, 4:12 AM

🎯 Ars Technica [EN]

Attention au traffic sortant aussi !

Introduction à DNSSEC

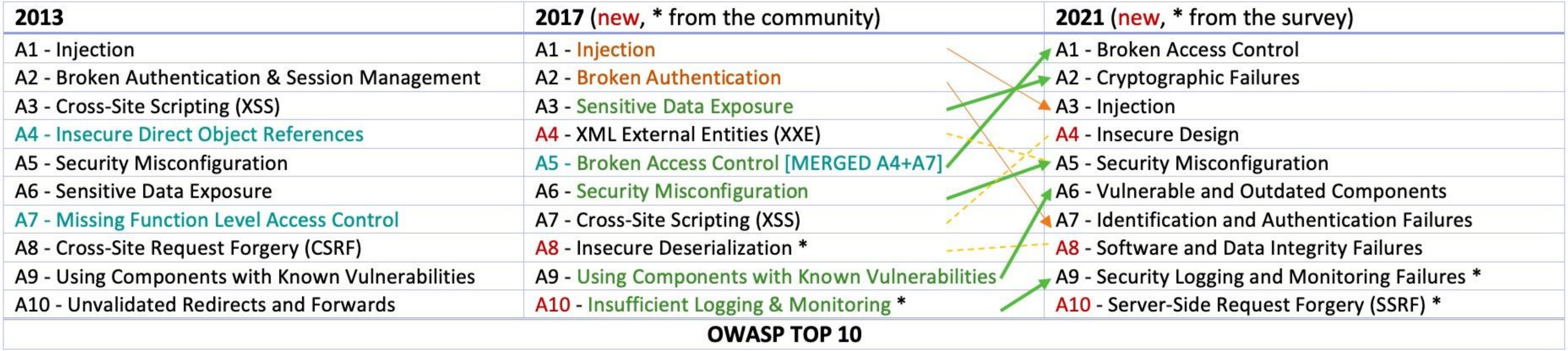

We think of DNS as a lookup.
>nslookup tesla.com
name: tesla.com
address: 199.66.11.62
Where is Tesla.com?
But each DNS lookup request sends data to a server.
? Query
mysecret.paypa1.com
I can put any info I want in here! (subdomain)
And it'll get sent to the DNS server config'd for this domain.
How do I steal this file w/o getting detected?
Top Secret.docx
Email
USB
FTP
Dropbox
Blocked!
First, I can encode it with base64 (or similar)
Top Secret
Q4 Profit $15M
Plain text, easy for DLP to scan
UTQg UHJvZ 24czogLG
Encoded, DLP can't make sense of it
Outbound DNS is usually allowed on corporate networks.
MEGACORP
port 53 open!
DNS
And it's a very noisy protocol to monitor & analyze.
dns.log
Sep 30 18:18:57 dds named
Sep 30 18:18:58 dds named
Sep 30 18:18:58 dds named
Sep 30 18:18:59 med
Sep 30 18:19:02 ed
Yikes!
dds named
dds named
dds named
Then I chop up my base64 file into small chunks that each fit into a DNS query.
UTQg.paypa1.com
UHcz.paypa1.com
24og.paypa1.com
www.google.com
www.twitter.com
Then tuck all the "bad" DNS queries in with the thousands of "good" ones
When the evil queries arrive at the attacker's paypa1.com DNS server they are logged and pieced back together.
UTQg +
UHCz +
24og
Stitch together
Decode
base 64
Top Secret .docx

Exfiltration DNS @Rob Sobers

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 ?



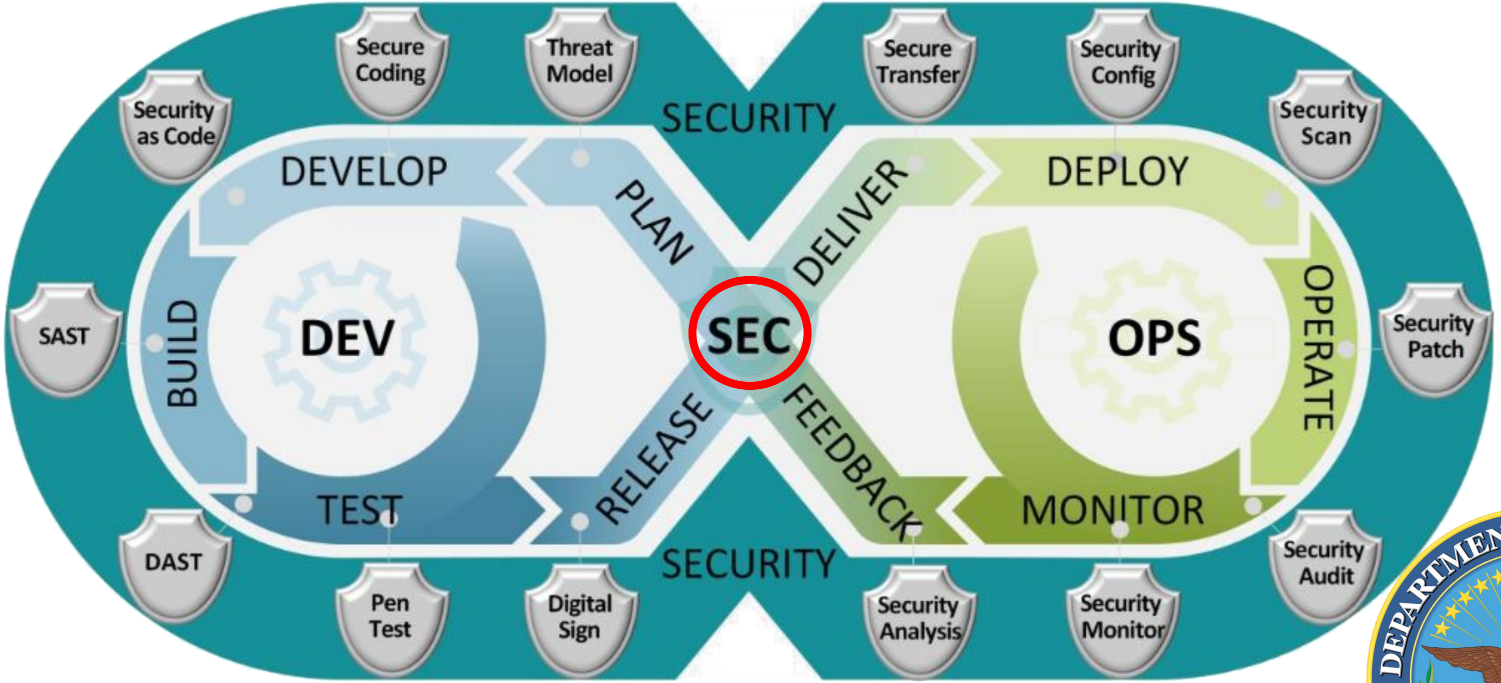
2013	2017 (new, * from the community)	2021 (new, * from the survey)
A1 - Injection	A1 - Injection	A1 - Broken Access Control
A2 - Broken Authentication & Session Management	A2 - Broken Authentication	A2 - Cryptographic Failures
A3 - Cross-Site Scripting (XSS)	A3 - Sensitive Data Exposure	A3 - Injection
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

OWASP Top 10

Outils

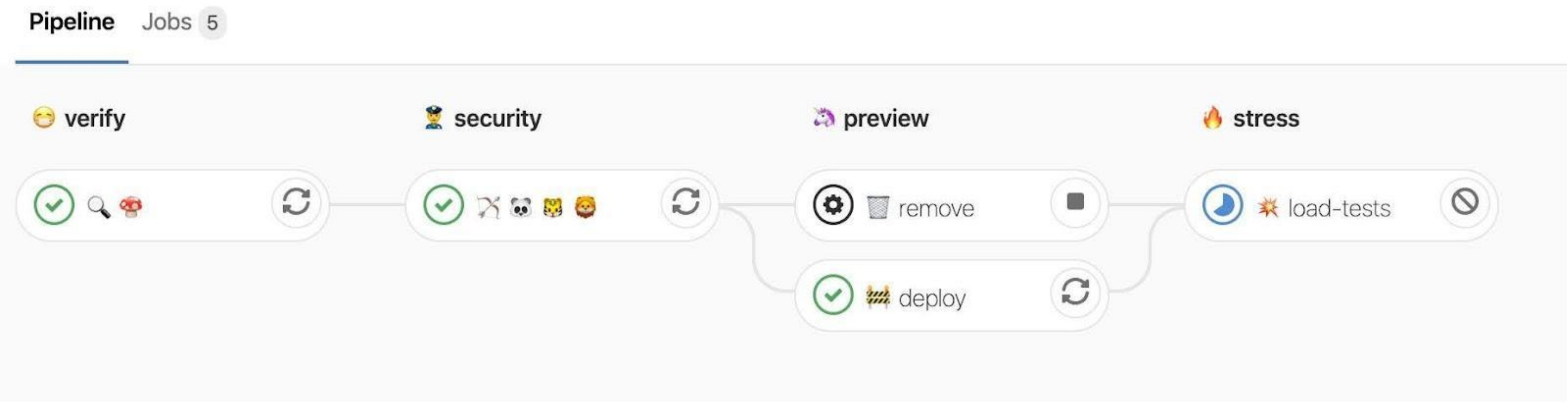
Shift-left Security



dodcio.defense.gov

DevOps

CI/CD



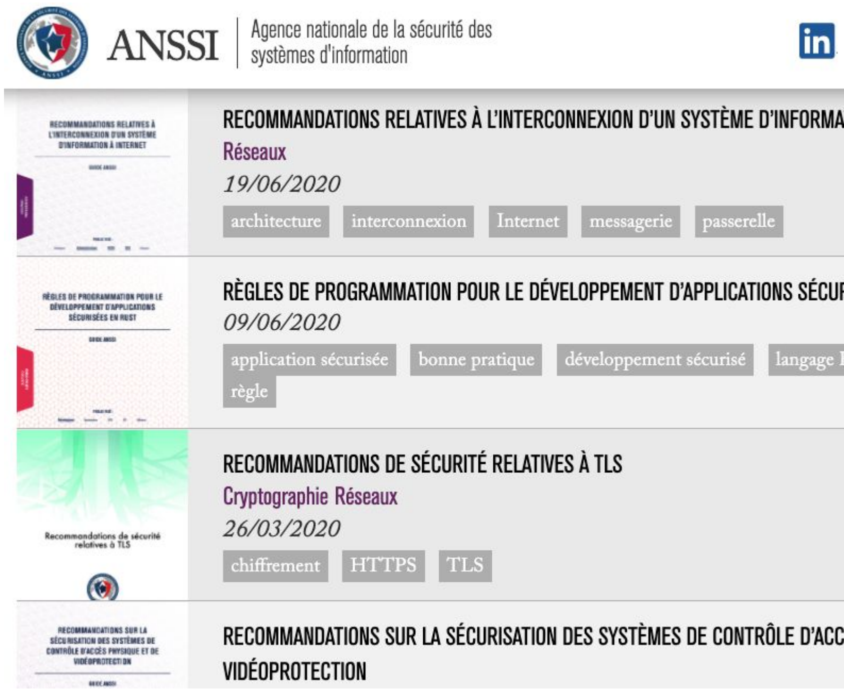
🎯 https://twitter.com/k33g_org/

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
GUIDE ANSSI
RÈGLES DE PROGRAMMATION POUR LE DÉVELOPPEMENT D'APPLICATIONS SÉCURISÉES EN RUST
GUIDE ANSSI
Recommandations de sécurité relatives à TLS
RECOMMANDATIONS SUR LA SÉCURISATION DES SYSTÈMES DE CONTRÔLE D'ACCÈS PHYSIQUE ET DE VIDÉOPROTECTION
GUIDE ANSSI

RECOMMANDATIONS RELATIVES À L'INTERCONNEXION D'UN SYSTÈME D'INFORMA
Réseaux
19/06/2020
architecture | interconnexion | Internet | messagerie | passerelle

RÈGLES DE PROGRAMMATION POUR LE DÉVELOPPEMENT D'APPLICATIONS SÉCUR
09/06/2020
application sécurisée | bonne pratique | développement sécurisé | langage l | règle

RECOMMANDATIONS DE SÉCURITÉ RELATIVES À TLS
Cryptographie Réseaux
26/03/2020
chiffrement | HTTPS | TLS

RECOMMANDATIONS SUR LA SÉCURISATION DES SYSTÈMES DE CONTRÔLE D'ACC
VIDÉOPROTECTION

🎯 [Bonnes pratiques de sécurité numérique (ANSSI)](#)

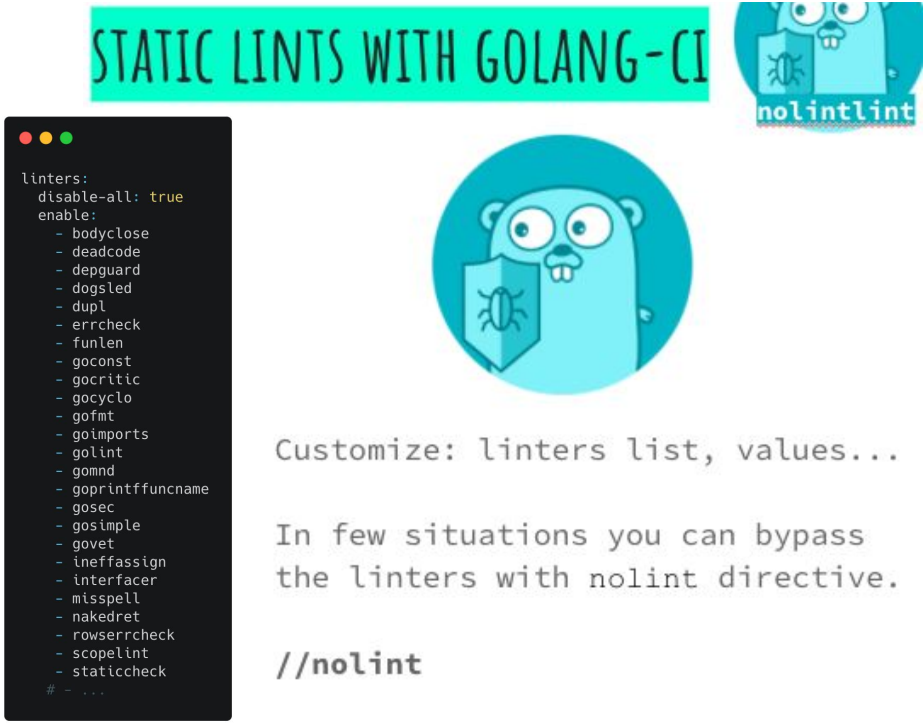
black hat
LE HACK www.lehack.org PARIS
HITB
OFFENSIVECON BY Blue Frost Security

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

```
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
   # - ...
```

Customize: linters list, values...

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

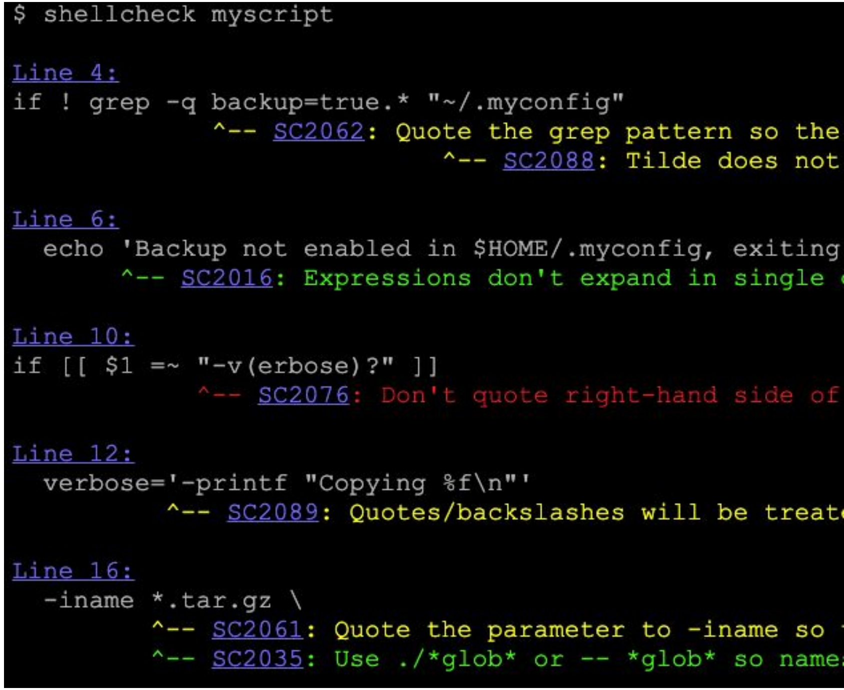
```
//nolint
```

🎯 ["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 languages

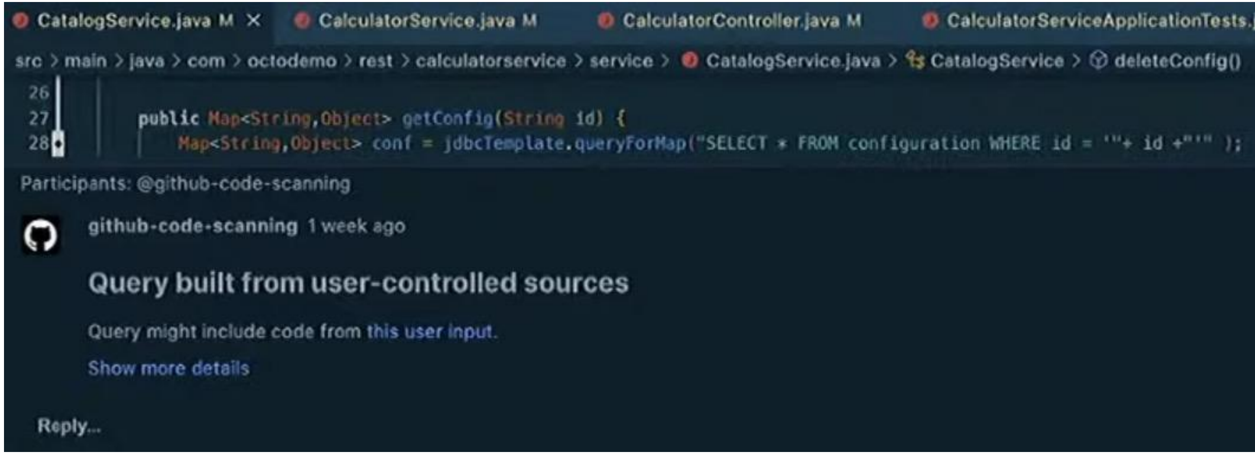


```
$ shellcheck myscript

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(erbose)?" ]]
            ^-- 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](#)

Github
Code Scanning

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


CatalogService.java M ×
CalculatorService.java M
CalculatorController.java M
CalculatorServiceApplicationTests.j
src > main > java > com > octodemo > rest > calculatorservice > service > CatalogService.java > CatalogService > deleteConfig()

```
    public Map<String,Object> getConfig(String id) {
        Map<String,Object> conf = jdbcTemplate.queryForMap("SELECT * FROM configuration WHERE id = '"+ id +"'" );
```

Participants: @github-code-scanning

github-code-scanning 1 week ago

Query built from user-controlled sources

Query might include code from this user input.

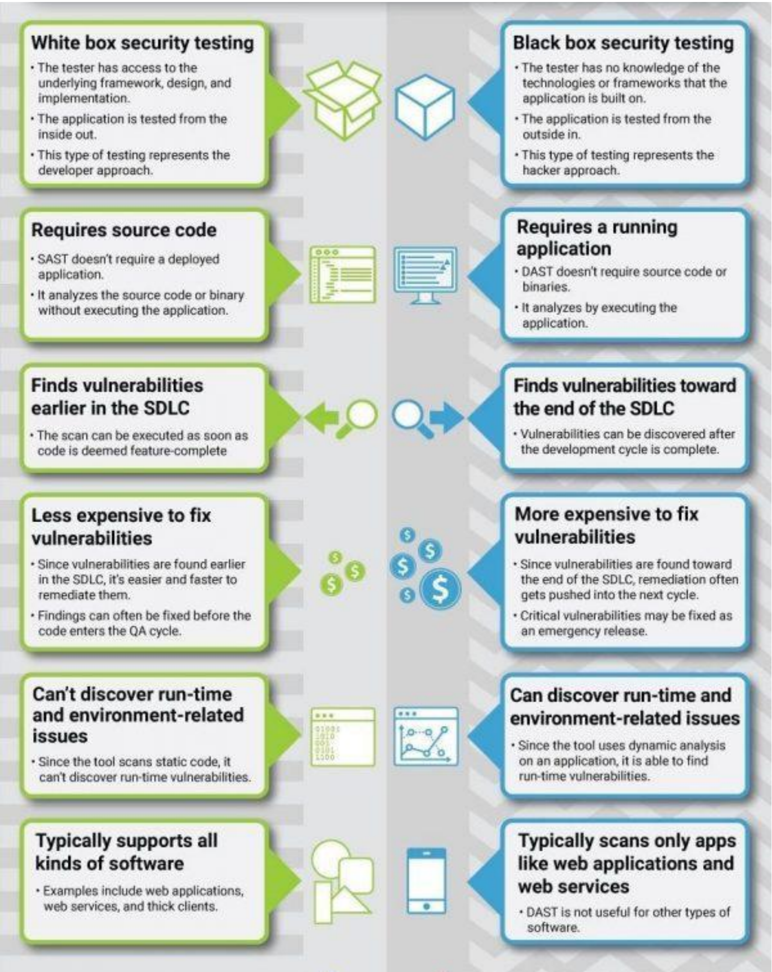
Show more details

Reply...

🎯 [Github Code Scanning](#) / [Démo TelecomValley](#)

Build: SAST / DAST / IAST

SAST
DAST
IAST
App Security Test



White box security testing
- The tester has access to the underlying framework, design, and implementation.
- The application is tested from the inside out.
- This type of testing represents the developer approach.

Black box security testing
- The tester has no knowledge of the technologies or frameworks that the application is built on.
- The application is tested from the outside in.
- This type of testing represents the hacker approach.

Requires source code
- SAST doesn't require a deployed application.
- It analyzes the source code or binary without executing the application.

Requires a running application
- DAST doesn't require source code or binaries.
- It analyzes by executing the application.

Finds vulnerabilities earlier in the SDLC
- The scan can be executed as soon as code is deemed feature-complete

Finds vulnerabilities toward the end of the SDLC
- Vulnerabilities can be discovered after the development cycle is complete.

Less expensive to fix vulnerabilities
- Since vulnerabilities are found earlier in the SDLC, it's easier and faster to remediate them.
- Findings can often be fixed before the code enters the QA cycle.

More expensive to fix vulnerabilities
- Since vulnerabilities are found toward the end of the SDLC, remediation often gets pushed into the next cycle.
- Critical vulnerabilities may be fixed as an emergency release.

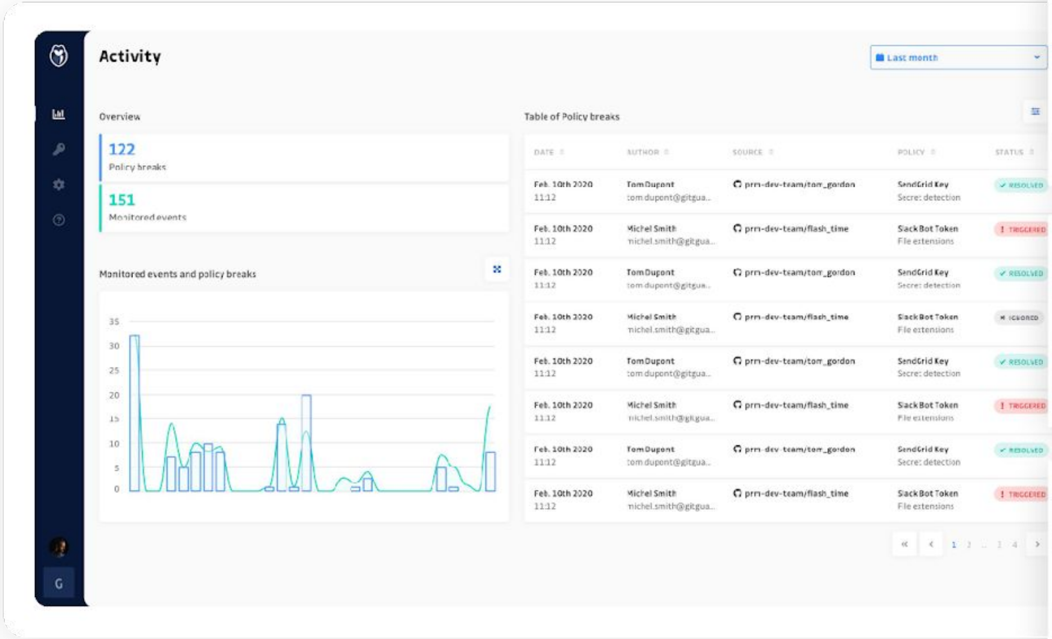
Can't discover run-time and environment-related issues
- Since the tool scans static code, it can't discover run-time vulnerabilities.

Can discover run-time and environment-related issues
- Since the tool uses dynamic analysis on an application, it is able to find run-time vulnerabilities.

Typically supports all kinds of software
- Examples include web applications, web services, and thick clients.

Typically scans only apps like web applications and web services
- DAST is not useful for other types of software.

AWS git-secrets / GitGuardian



Activity

Overview

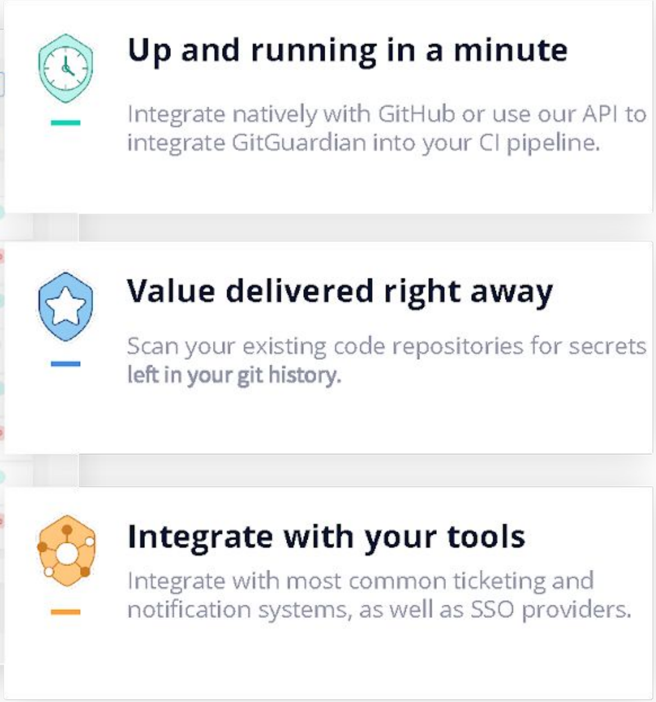
122
Policy breaks

151
Monitored events

Monitored events and policy breaks

Table of Policy breaks

DATE	AUTHOR	SOURCE	POLICY	STATUS
Feb. 10th 2020 11:12	TomDupont tom.dupont@gitgua...	prm-dev-team/tom_gordon	SendGrid Key Secret detection	✓ RESOLVED
Feb. 10th 2020 11:12	Michel Smith michel.smith@gitgua...	prm-dev-team/flash_time	Slack Bot Token File extensions	! TRIGGERED
Feb. 10th 2020 11:12	TomDupont tom.dupont@gitgua...	prm-dev-team/tom_gordon	SendGrid Key Secret detection	✓ RESOLVED
Feb. 10th 2020 11:12	Michel Smith michel.smith@gitgua...	prm-dev-team/flash_time	Slack Bot Token File extensions	✕ IGNORED
Feb. 10th 2020 11:12	TomDupont tom.dupont@gitgua...	prm-dev-team/tom_gordon	SendGrid Key Secret detection	✓ RESOLVED
Feb. 10th 2020 11:12	Michel Smith michel.smith@gitgua...	prm-dev-team/flash_time	Slack Bot Token File extensions	! TRIGGERED
Feb. 10th 2020 11:12	TomDupont tom.dupont@gitgua...	prm-dev-team/tom_gordon	SendGrid Key Secret detection	✓ RESOLVED
Feb. 10th 2020 11:12	Michel Smith michel.smith@gitgua...	prm-dev-team/flash_time	Slack Bot Token File extensions	! TRIGGERED



Up and running in a minute

Integrate natively with GitHub or use our API to integrate GitGuardian into your CI pipeline.

Value delivered right away

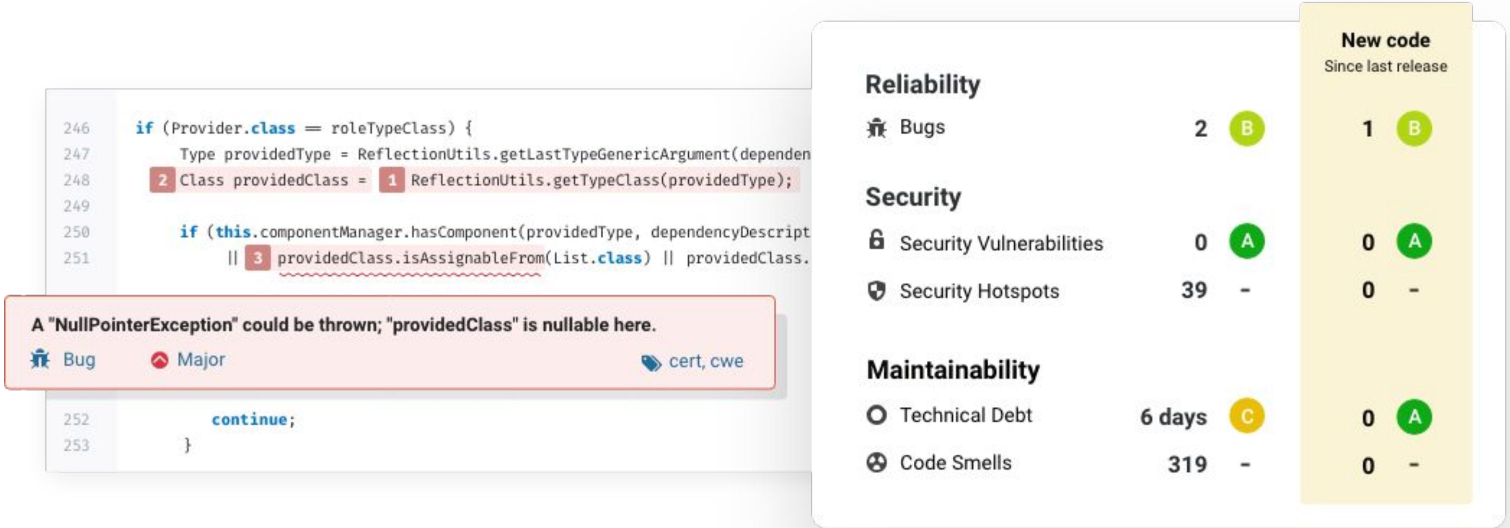
Scan your existing code repositories for secrets left in your git history.

Integrate with your tools

Integrate with most common ticketing and notification systems, as well as SSO providers.

🎯 git-secrets (OpenSource) / Automated Secrets Detection for Application Security

Sonar



```
if (Provider.class == roleTypeClass) {
    Type providedType = ReflectionUtils.getLastTypeGenericArgument(dependen
  2 Class providedClass = 1 ReflectionUtils.getTypeClass(providedType);

    if (this.componentManager.hasComponent(providedType, dependencyDescript
        || 3 providedClass.isAssignableFrom(List.class) || providedClass.
```

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

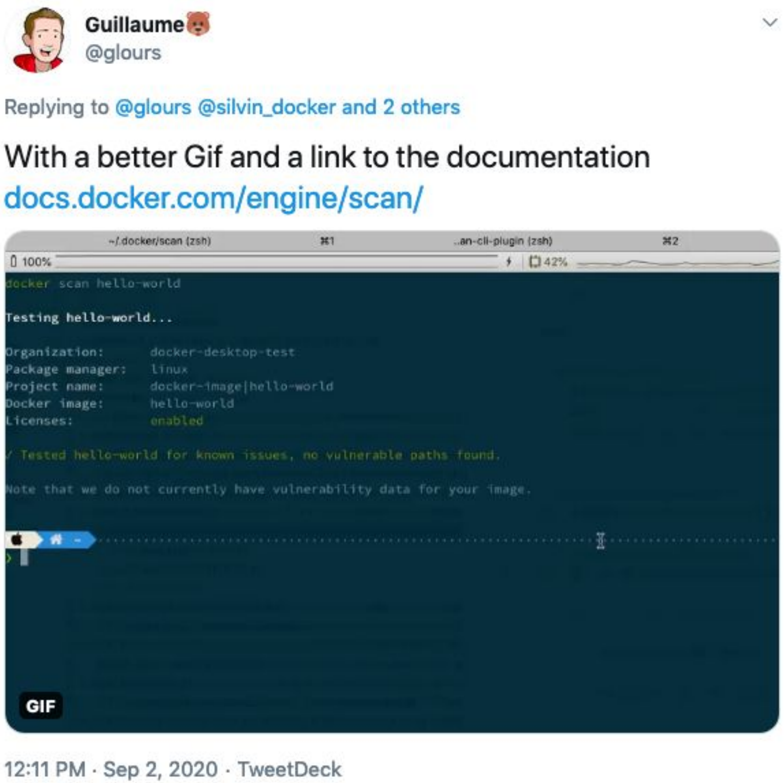
Bug   Major   cert, cwe

```
            continue;
    }
```

			New code Since last release	
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	-

🎯 Sonar Dashboard

Docker CLI



Guillaume🐻
@glours

Replying to @glours @silvin_docker and 2 others

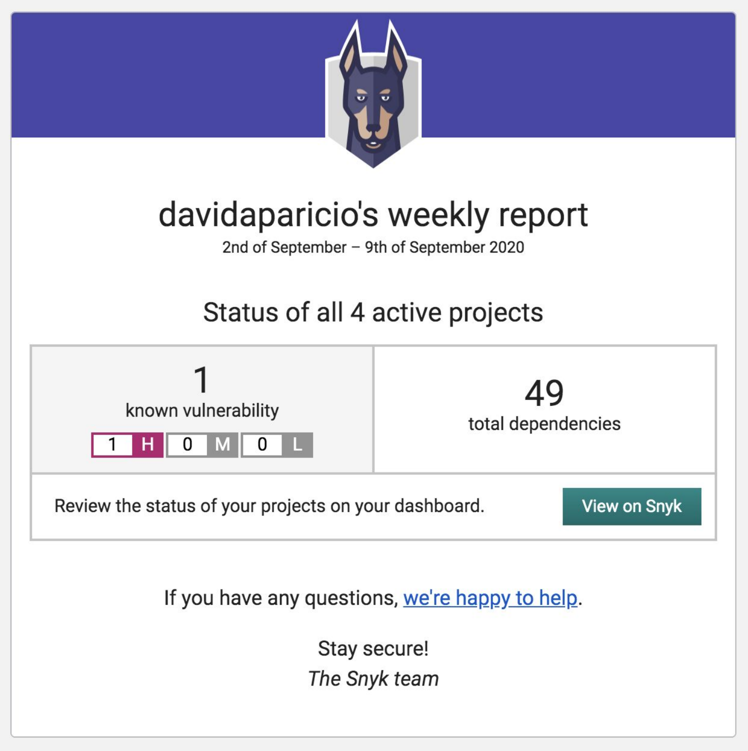
With a better Gif and a link to the documentation docs.docker.com/engine/scan/

```
docker scan 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/)

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

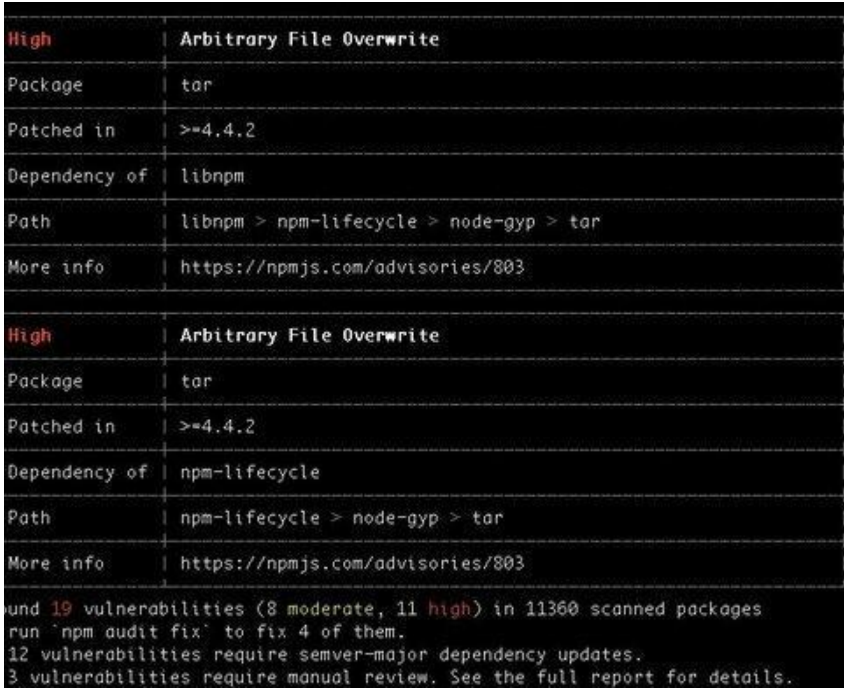
If you have any questions, we're happy to help.

Stay secure!
The Snyk team

🎯 Email report

npm-audit
Javascript

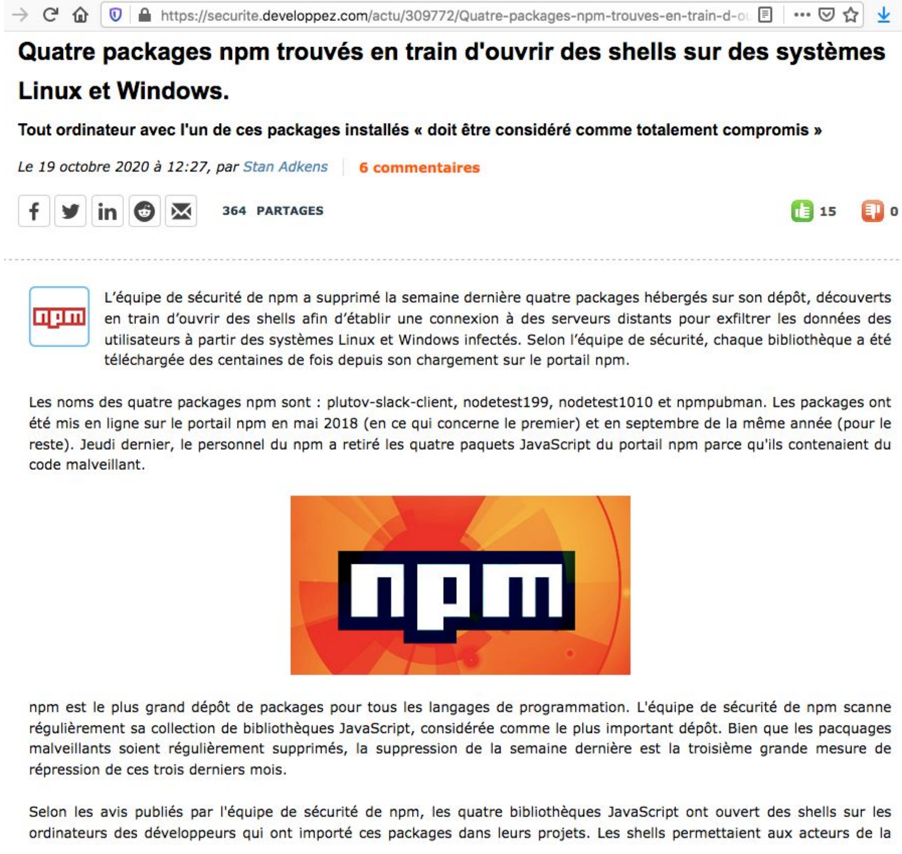
Auditer les vulnérabilités connues des librairies et des dépendances associées



```
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
und 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]

19/10/20


https://securite.developpez.com/actu/309772/Quatre-packages-npm-trouves-en-train-d-o

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.

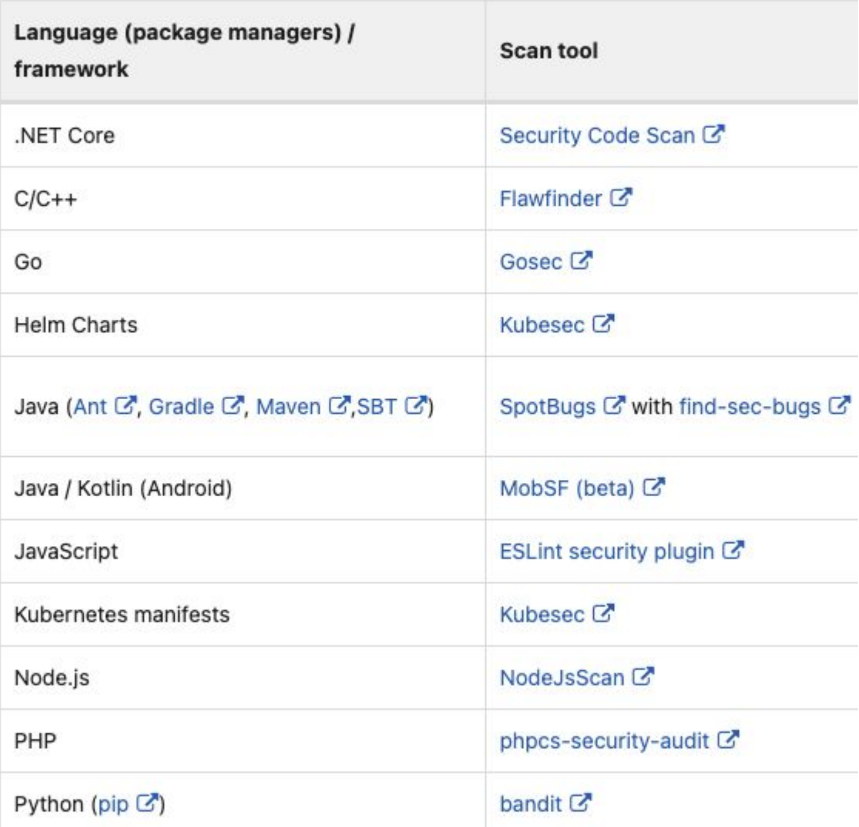
Les noms des quatre packages npm sont : plutov-slack-client, nodetest199, nodetest1010 et npmpubman. Les packages ont été mis en ligne sur le portail npm en mai 2018 (en ce qui concerne le premier) et en septembre de la même année (pour le reste). Jeudi dernier, le personnel du npm a retiré les quatre 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 pacquages malveillants soient régulièrement supprimés, la suppression de la semaine dernière est la troisième grande mesure de répression de ces trois derniers mois.

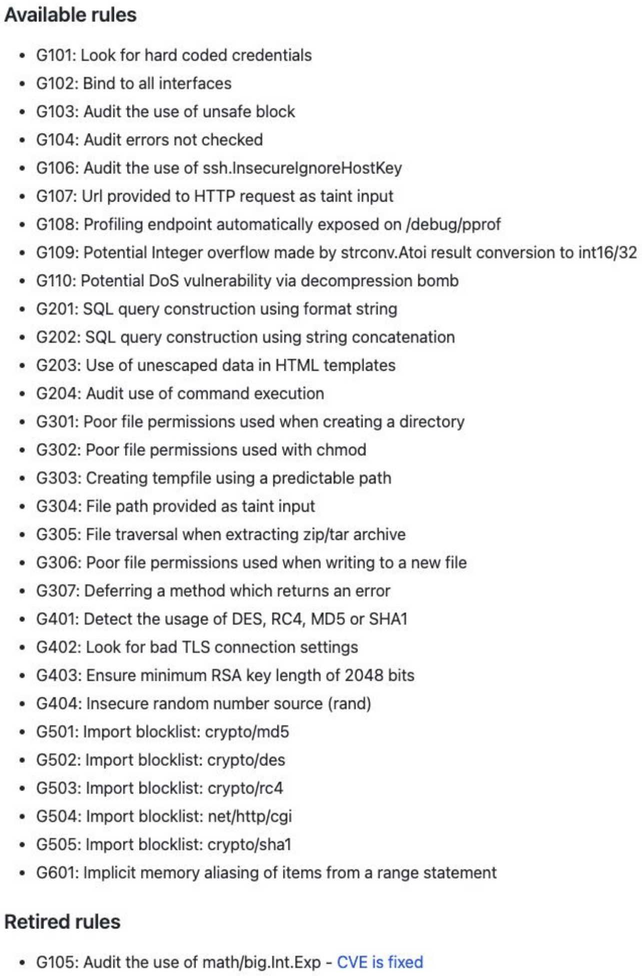
Selon les avis publiés par l'équipe de sécurité de npm, les quatre bibliothèques JavaScript ont ouvert des shells sur les ordinateurs des développeurs qui ont importé ces packages dans leurs projets. Les shells permettaient aux acteurs de la

🎯 4 packages npm ouvrent des shells [Linux/Windows]

DAST (Gitlab)



Language (package managers) / framework	Scan tool
.NET Core	Security Code Scan
C/C++	Flawfinder
Go	Gosec
Helm Charts	Kubesec
Java (Ant, Gradle, Maven,SBT)	SpotBugs with find-sec-bugs
Java / Kotlin (Android)	MobSF (beta)
JavaScript	ESLint security plugin
Kubernetes manifests	Kubesec
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 blocklist: crypto/md5
- G502: Import blocklist: crypto/des
- G503: Import blocklist: crypto/rc4
- G504: Import blocklist: net/http/cgi
- G505: Import blocklist: 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

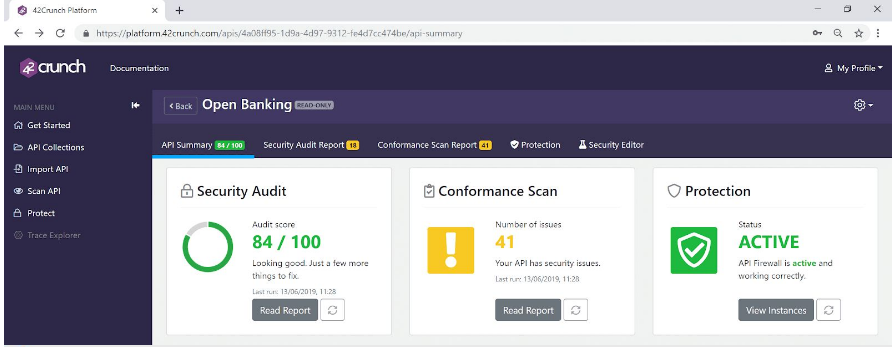
42Crunch
Scanner d'API

Assurer la sécurité des API au rythme du Business
et ne JAMAIS laisser des API non sécurisées atteindre la PROD

Vérifie la consistance de votre API par rapport au contrat d'interface

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



Security Audit

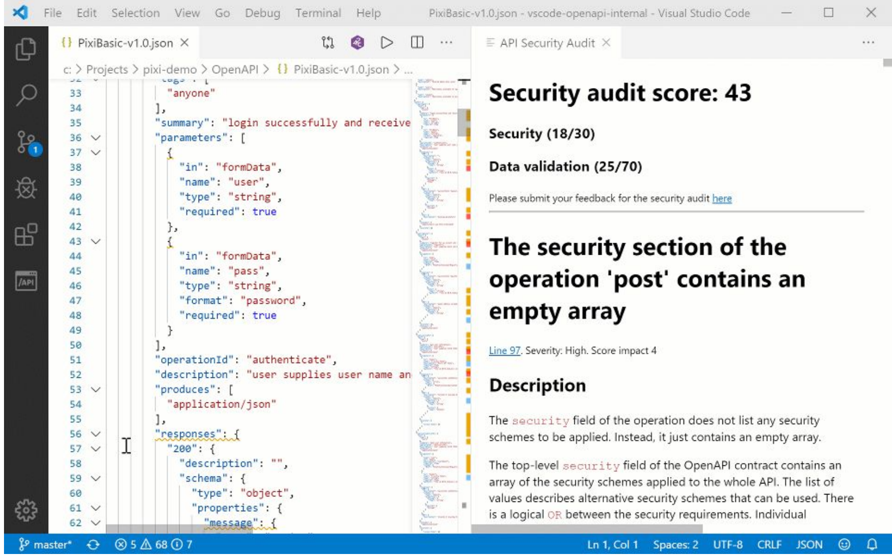
Audit score
84 / 100
Looking good. Just a few more things to fix.
Last run: 13/06/2019, 11:28

Conformance Scan

Number of issues
41
Your API has security issues.
Last run: 13/06/2019, 11:28

Protection

Status
ACTIVE
API Firewall is active and working correctly.


File
Edit
Selection
View
Go
Debug
Terminal
Help
PixiBasic-v1.0.json - vscode-openapi-internal - Visual Studio Code
PixiBasic-v1.0.json
API Security Audit
c: > Projects > pixi-demo > OpenAPI > PixiBasic-v1.0.json > ...
master*
⊗ 5 ⚠ 68 ⓘ 7
Ln 1, Col 1
Spaces: 2
UTF-8
CRLF
JSON

```
          "anyone"
        ],
        "summary": "login successfully and receive
        "parameters": [
          {
            "in": "formData",
            "name": "user",
            "type": "string",
            "required": true
          },
          {
            "in": "formData",
            "name": "pass",
            "type": "string",
            "format": "password",
            "required": true
          }
        ],
        "operationId": "authenticate",
        "description": "user supplies user name an
        "produces": [
          "application/json"
        ],
        "responses": {
          "200": {
            "description": "",
            "schema": {
              "type": "object",
              "properties": {
                "message": {
```

Security audit score: 43

Security (18/30)

Data validation (25/70)

Please submit your feedback for the security audit here

The security section of the operation 'post' contains an empty array

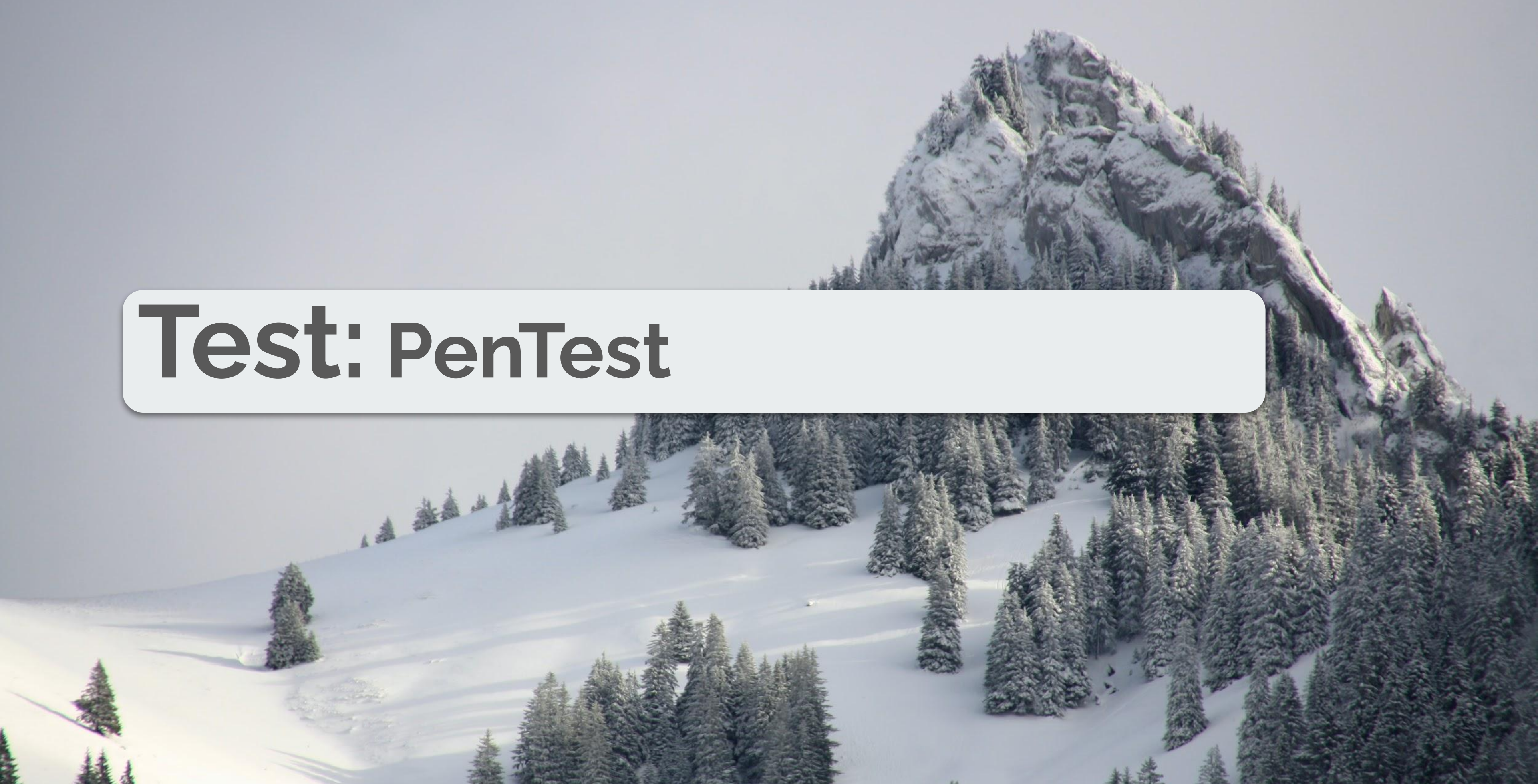
Line 97. Severity: High. Score impact 4

Description

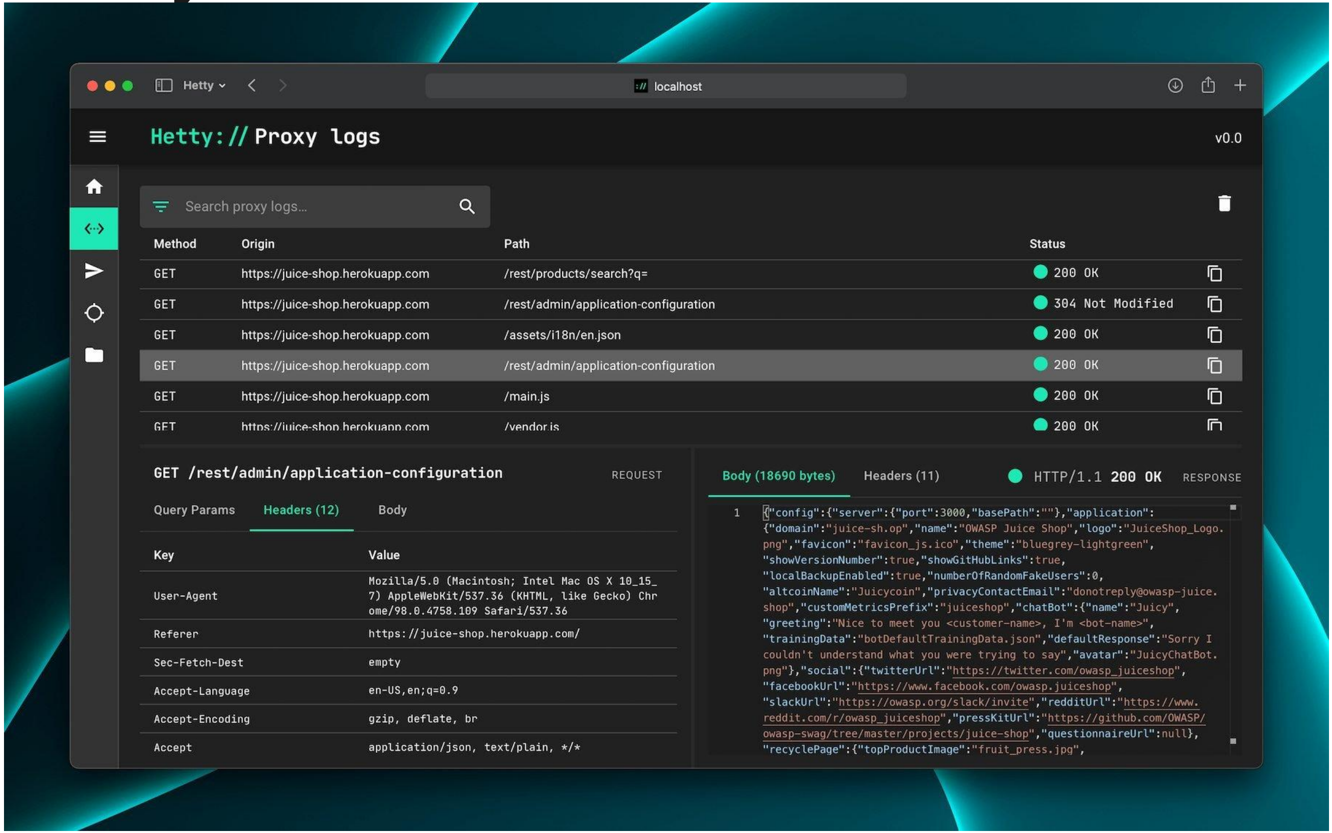
The `security` field of the operation does not list any security schemes to be applied. Instead, it just contains an empty array.

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



Hetty:// Proxy logs

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/i18n/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

Query Params | Headers (12) | Body

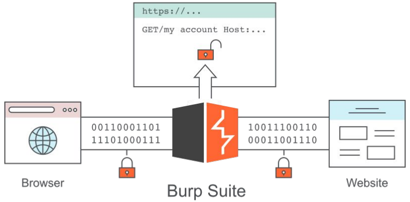
Key	Value
User-Agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.109 Safari/537.36
Referer	https://juice-shop.herokuapp.com/
Sec-Fetch-Dest	empty
Accept-Language	en-US,en;q=0.9
Accept-Encoding	gzip, deflate, br
Accept	application/json, text/plain, */*

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

```
{"config":{"server":{"port":3000,"basePath":""},"application":
{"domain":"juice-sh.op","name":"OWASP Juice Shop","logo":"JuiceShop_Logo.
png","favicon":"favicon_js.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-swag/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

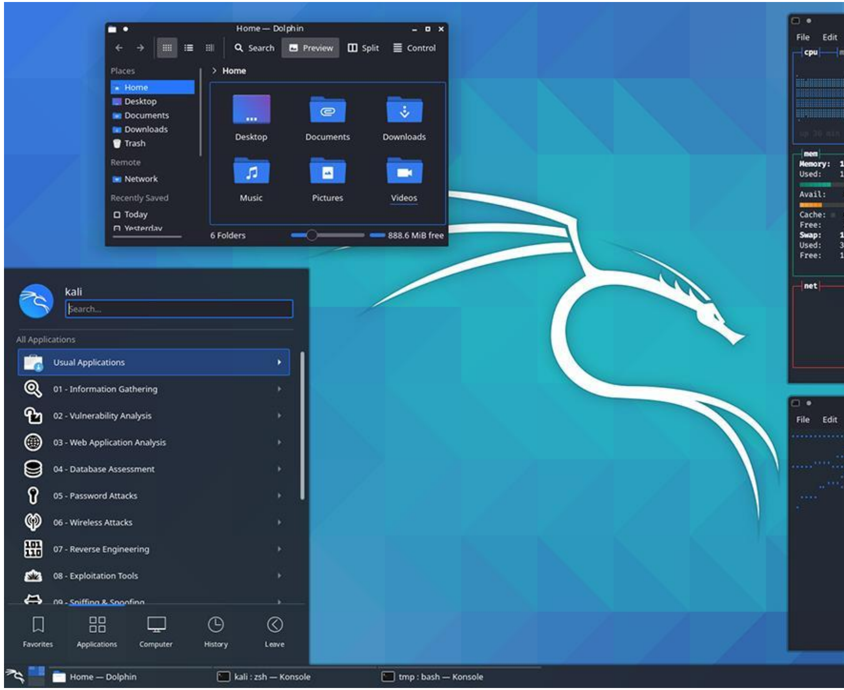


Kali Linux / Parrot OS

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

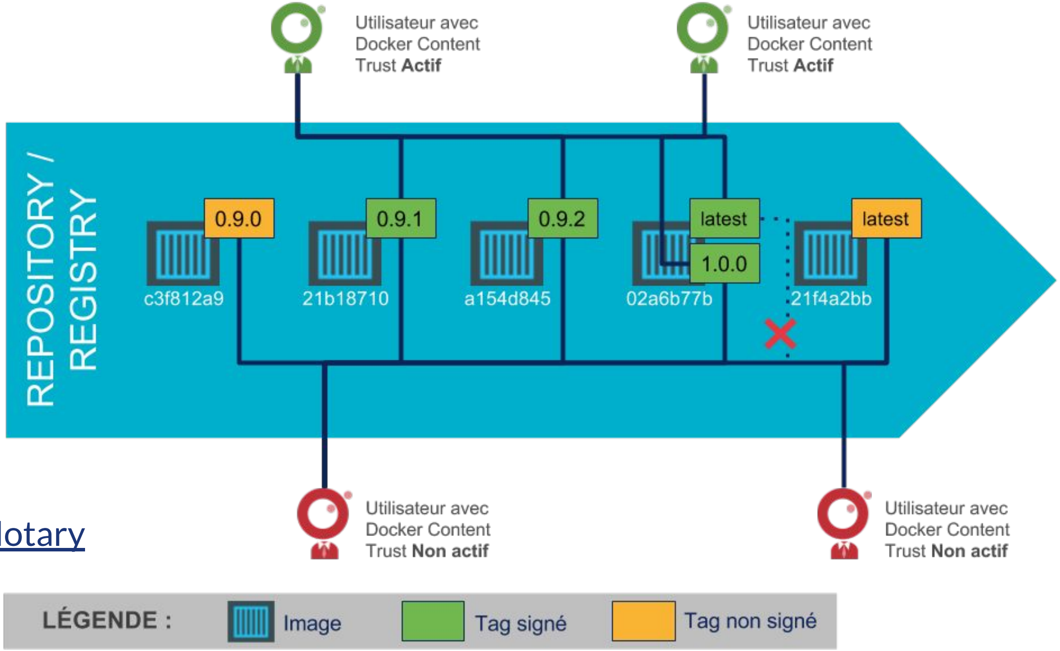
🎯 YesWeHack / Yogosha

Release: Digital Signature

Docker Notary

Ready for PROD

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


Utilisateur avec Docker Content Trust Actif
Utilisateur avec Docker Content Trust Actif
REPOSITORY / REGISTRY
0.9.0
c3f812a9
0.9.1
21b18710
0.9.2
a154d845
latest
1.0.0
02a6b77b
latest
21f4a2bb
Utilisateur avec Docker Content Trust Non actif
Utilisateur avec Docker Content Trust Non actif
LÉGENDE :
Image
Tag signé
Tag non signé

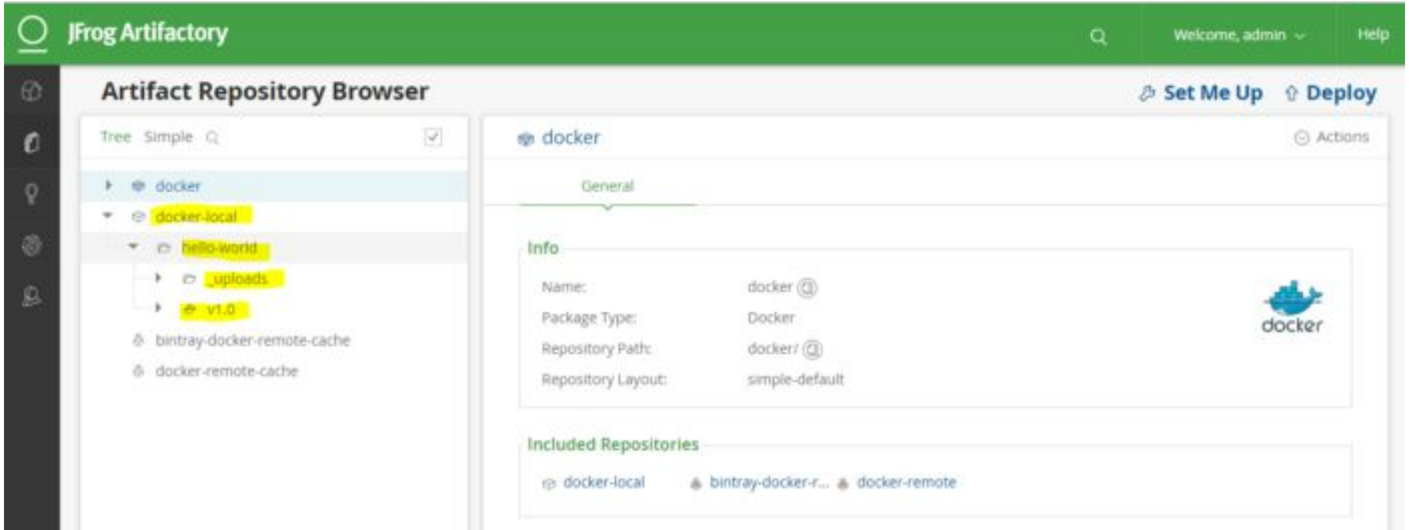
🎯 Documentation Docker Notary [EN]
La signature d’images Docker sur une Registry avec Notary

Deliver: Secure Transfer

JFrog Artifactory

Repository

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



Info

Name:	docker
Package Type:	Docker
Repository Path:	docker/
Repository Layout:	simple-default

Included Repositories

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

Deploy: Security Conf/Scan

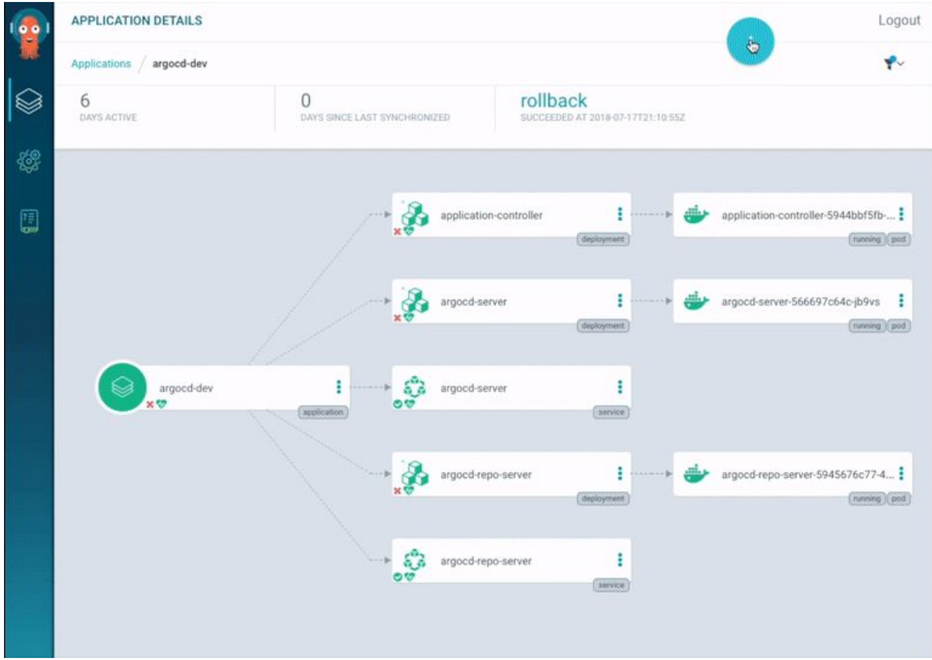
Argo CI + Vault

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

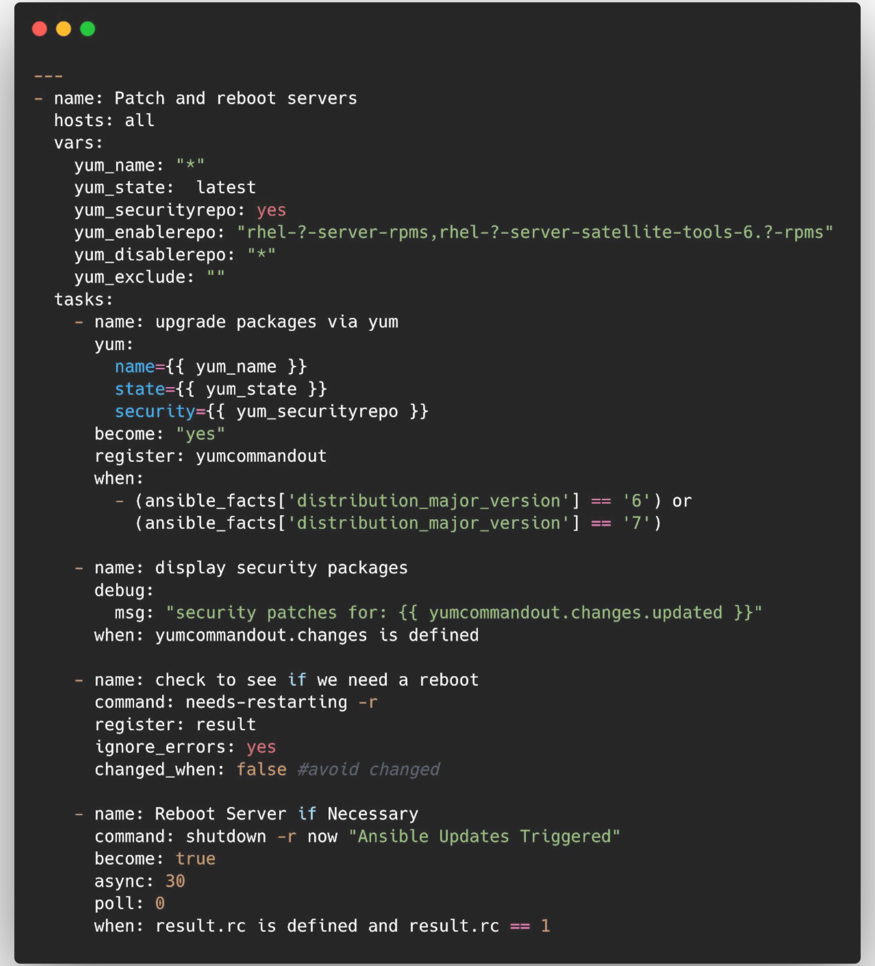
Ansible / Chef / Puppet

Patch & Reboot

Maintenir un système à jour en installant les patchs de sécurité

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

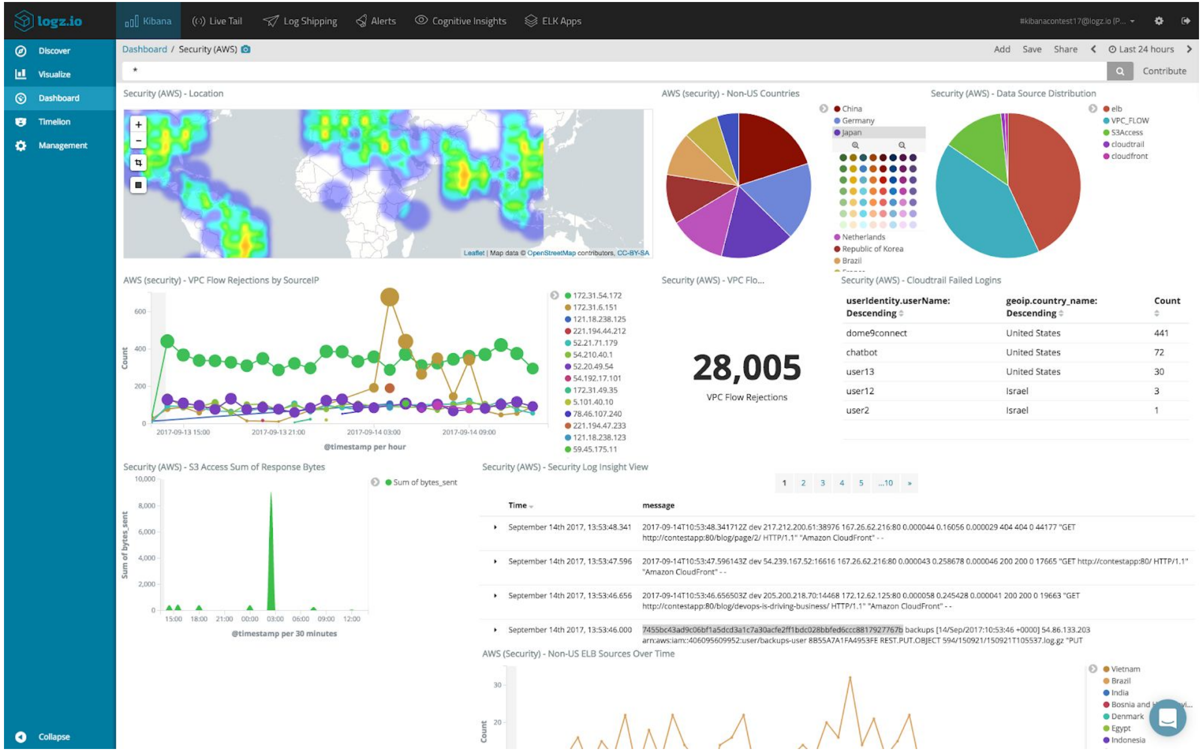
🎯 Playbook: apply patches & perform a reboot if required



```yaml
---
- 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



Security (AWS) - Cloudtrail Failed Logins

userIdentity.userName: Descending	geoip.country_name: Descending	Count
dome9connect	United States	441
chatbot	United States	72
user13	United States	30
user12	Israel	3
user2	Israel	1

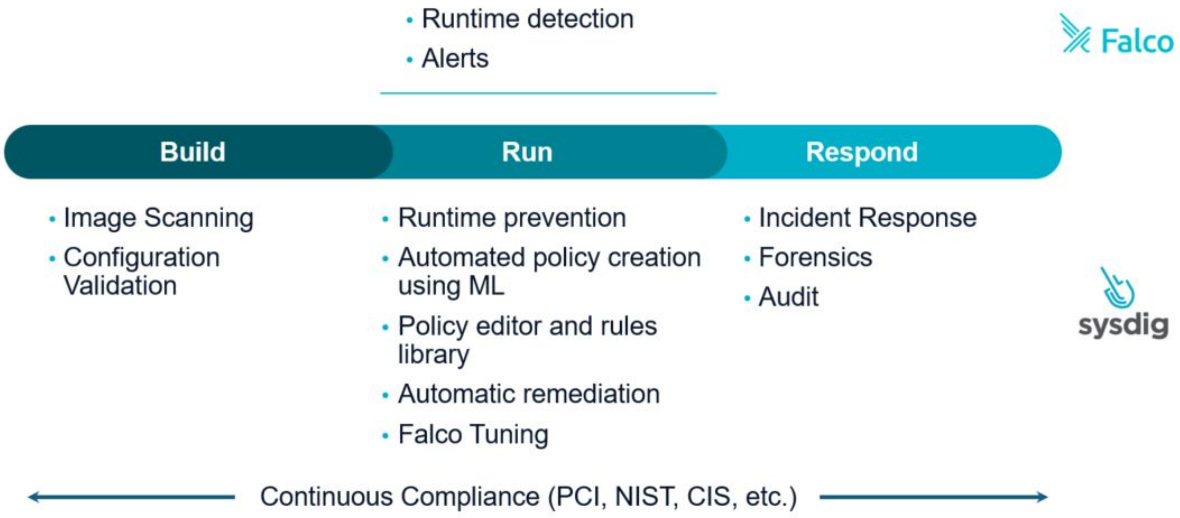
Security (AWS) - Security Log Insight View

1 2 3 4 5 ...10 »

```
Time                                   message
September 14th 2017, 13:53:48.341      2017-09-14T10:53:48.341712Z dev 217.212.200.61:38976 167.26.62.216:80 0.000044 0.16056 0.000029 404 404 0 44177 "GET
                                       http://contestapp:80/blog/page/2/ HTTP/1.1" "Amazon CloudFront" - -
September 14th 2017, 13:53:47.596      2017-09-14T10:53:47.596143Z dev 54.239.167.52:16616 167.26.62.216:80 0.000043 0.258678 0.000046 200 200 0 17665 "GET http://contestapp:80/ HTTP/1.1"
                                       "Amazon CloudFront" - -
September 14th 2017, 13:53:46.656      2017-09-14T10:53:46.656503Z dev 205.200.218.70:14468 172.12.62.125:80 0.000058 0.245428 0.000041 200 200 0 19663 "GET
                                       http://contestapp:80/blog/devops-is-driving-business/ HTTP/1.1" "Amazon CloudFront" - -
September 14th 2017, 13:53:46.000      7455bc43ad9c06bf1a5dcd3a1c7a30acfe2ff1bdc028bbfed6ccc8817927767b backups [14/Sep/2017:10:53:46 +0000] 54.86.133.203
                                       arn:aws:iam::406095609952:user/backups-user 8B55A7A1FA4953FE REST.PUT.OBJECT 594/150921/150921T105537.log.gz "PUT
```

🎯 [SIEM at the speed of Elasticsearch]

Falco



- Runtime detection
- Alerts

Falco

Build	Run	Respond
• Image Scanning • Configuration Validation	• Runtime prevention • Automated policy creation using ML • Policy editor and rules library • Automatic remediation • Falco Tuning	• Incident Response • Forensics • Audit

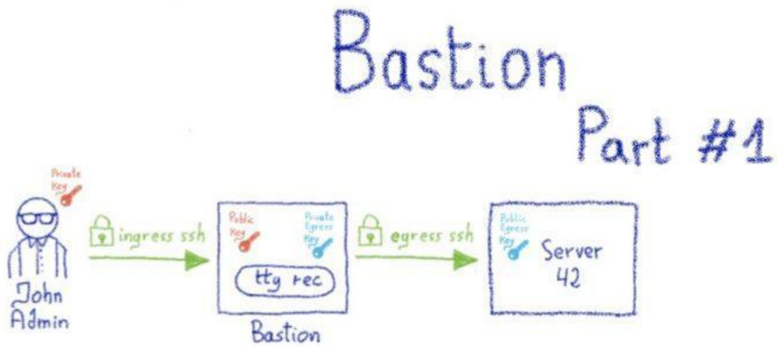
sysdig

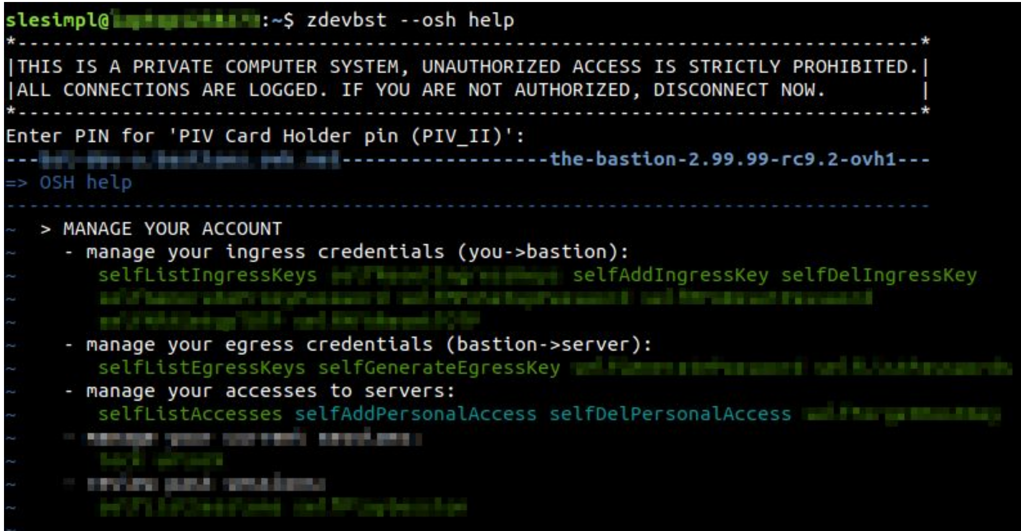
← Continuous Compliance (PCI, NIST, CIS, etc.) →

🎯 [Kris Nova, Fixing the Kubernetes clusterfuck @FOSDEM]

OVH Bastion (SSH proxy)

The
OVHcloud
?
?
?
?



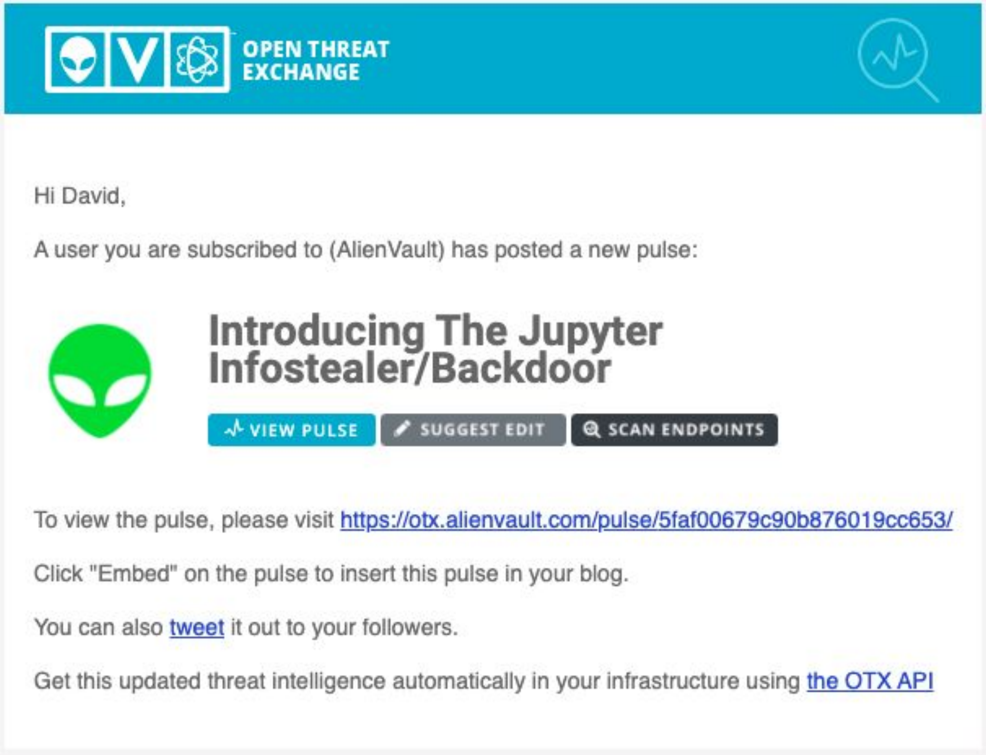


```
slesimpl@[redacted]:~$ zdevbst --osh help
*------------------------------------------------------------------------------*
|THIS IS A PRIVATE COMPUTER SYSTEM, UNAUTHORIZED ACCESS IS STRICTLY PROHIBITED.|
|ALL CONNECTIONS ARE LOGGED. IF YOU ARE NOT AUTHORIZED, DISCONNECT NOW.        |
*------------------------------------------------------------------------------*
Enter PIN for 'PIV Card Holder pin (PIV_II)':
---[redacted]------------------the-bastion-2.99.99-rc9.2-ovh1---
=> OSH help
--------------------------------------------------------------------------------
~  > MANAGE YOUR ACCOUNT
~    - manage your ingress credentials (you->bastion):
~       selfListIngressKeys [redacted] selfAddIngressKey selfDelIngressKey
~       [redacted]
~       [redacted]
~    - manage your egress credentials (bastion->server):
~       selfListEgressKeys selfGenerateEgressKey [redacted]
~    - manage your accesses to servers:
~       selfListAccesses selfAddPersonalAccess selfDelPersonalAccess [redacted]
~    [redacted]
~       [redacted]
~    [redacted]
~       [redacted]
```

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

Feedback: Secu. Analysis

AlienVault OTX



Hi David,

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

Introducing The Jupyter Infostealer/Backdoor

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

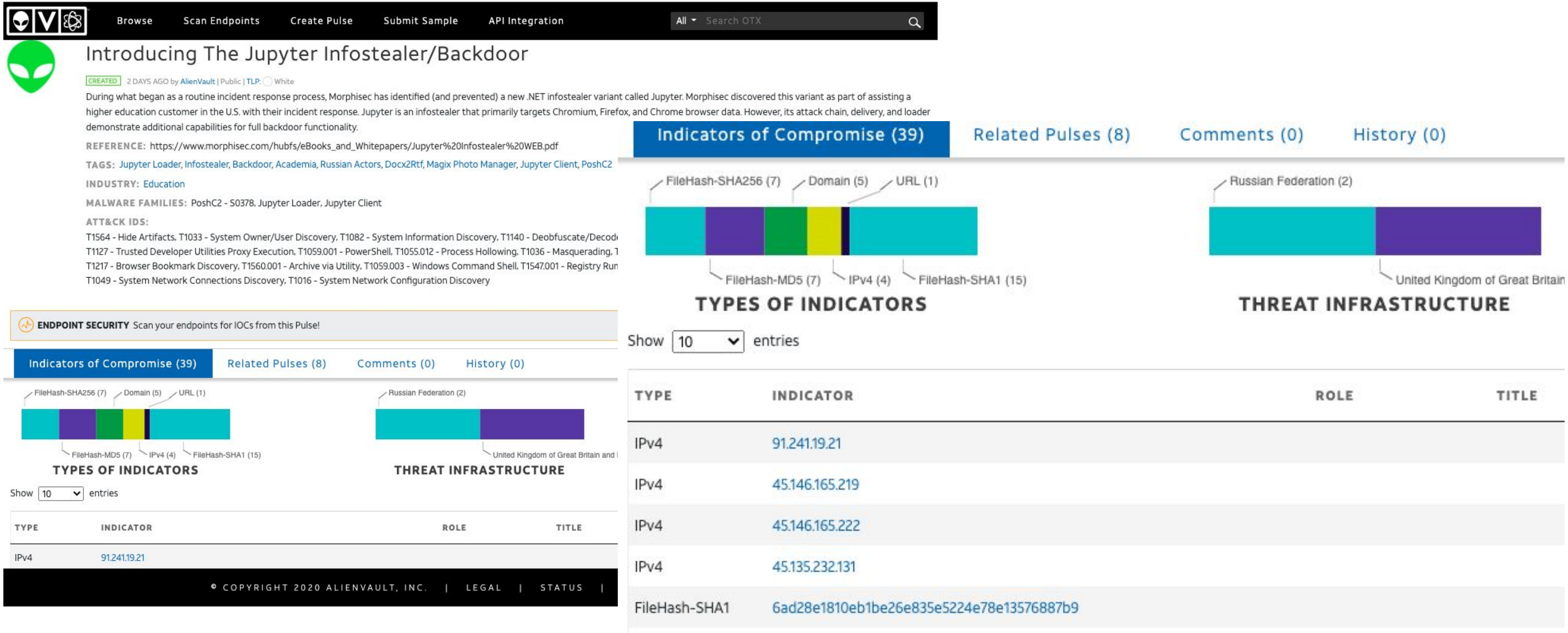
Click "Embed" on the pulse to insert this pulse in your blog.

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



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 - S0378, Jupyter Loader, Jupyter Client

ATT&CK IDS:
T1564 - Hide Artifacts, T1033 - System Owner/User Discovery, T1082 - System Information Discovery, T1140 - Deobfuscate/Decod
T1127 - Trusted Developer Utilities Proxy Execution, T1059.001 - PowerShell, T1055.012 - Process Hollowing, T1036 - Masquerading, T
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		

© COPYRIGHT 2020 ALIENVAULT, INC. | LEGAL | STATUS |

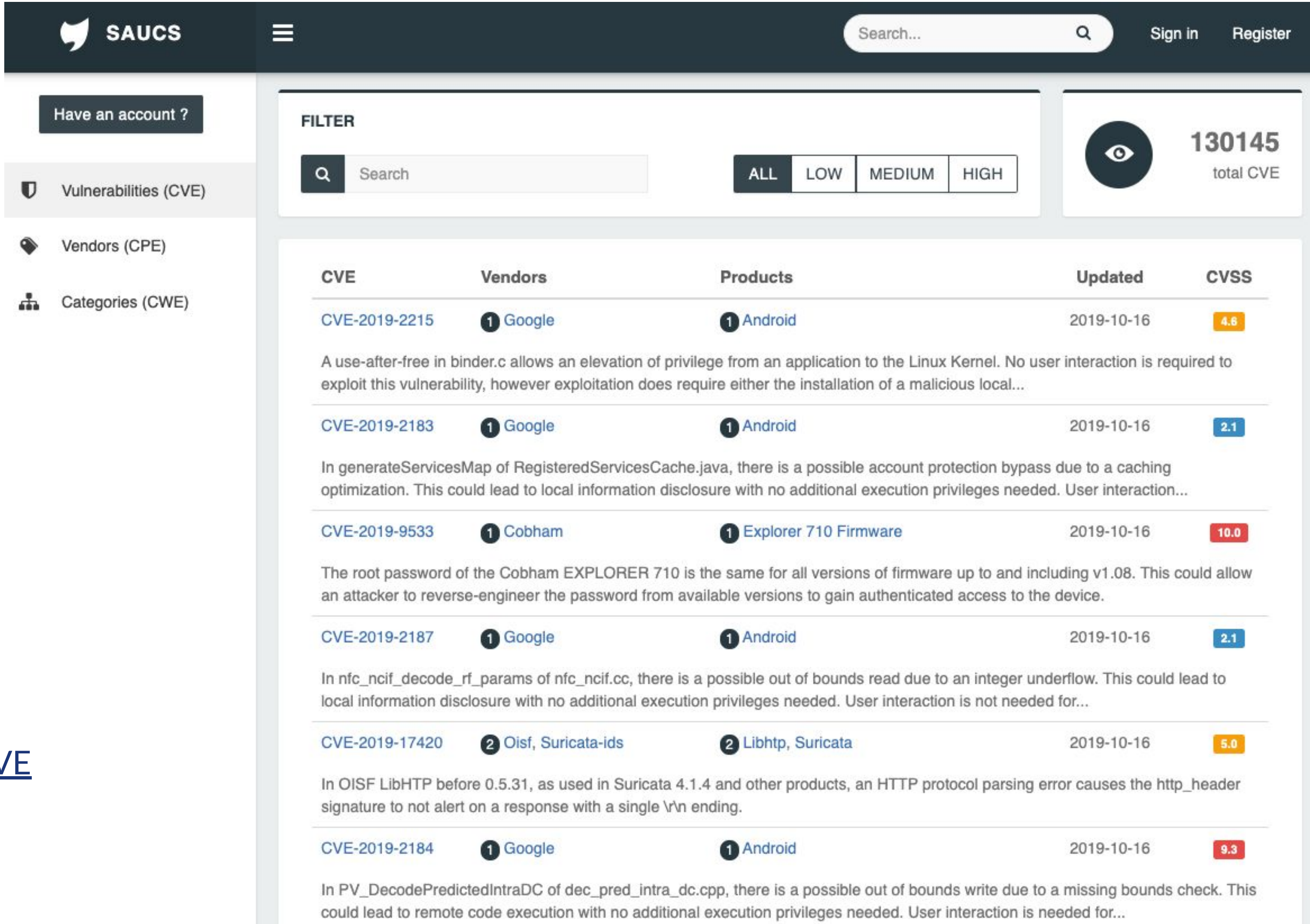
Indicators of Compromise (39) | Related Pulses (8) | Comments (0) | History (0)

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

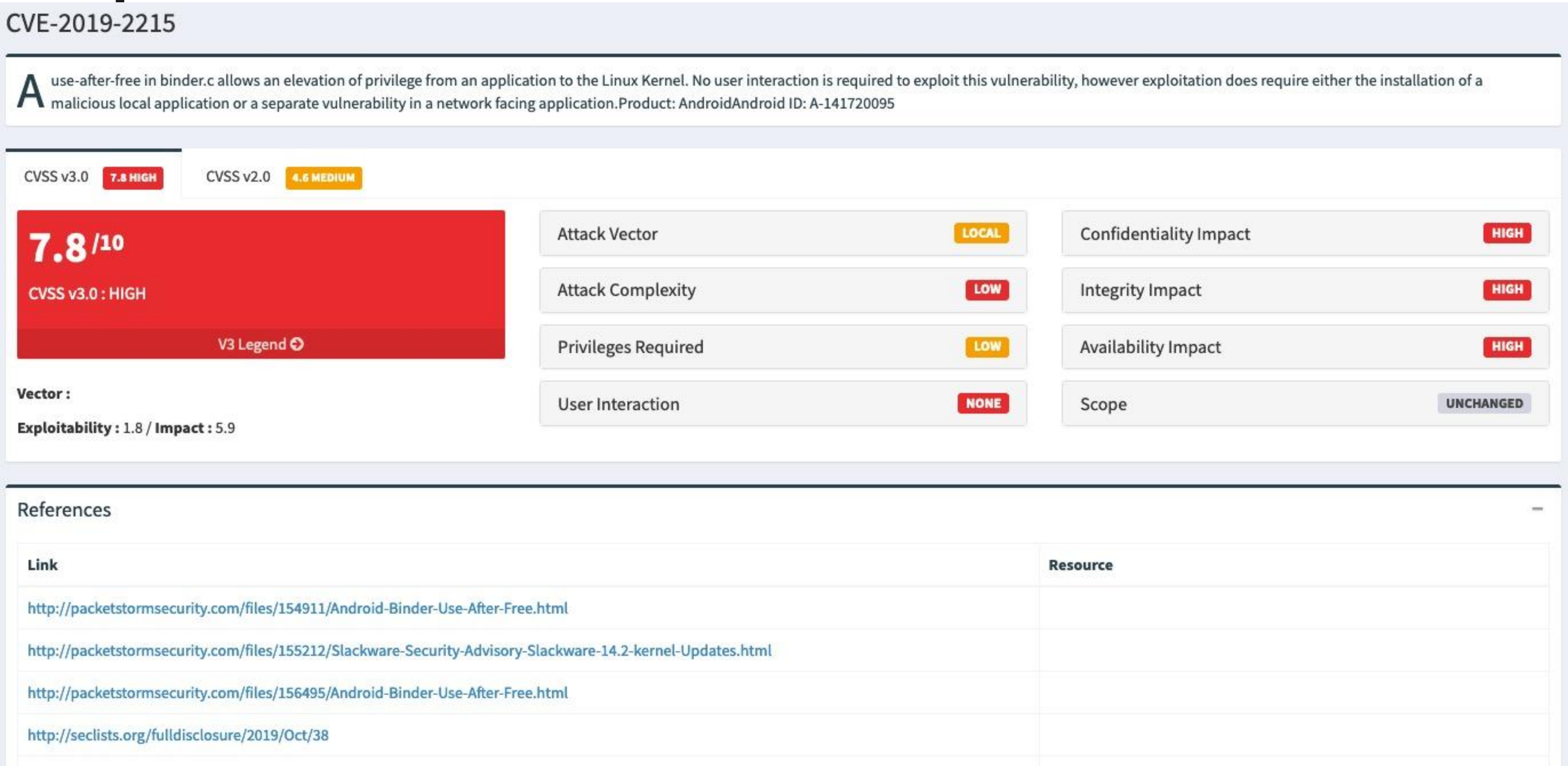


CVE	Vendors	Products	Updated	CVSS
CVE-2019-2215	1 Google	1 Android	2019-10-16	4.6
A use-after-free in binder.c allows an elevation of privilege from an application to the Linux Kernel. No user interaction is required to exploit this vulnerability, however exploitation does require either the installation 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 Libhtp, 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



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: AndroidAndroid 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

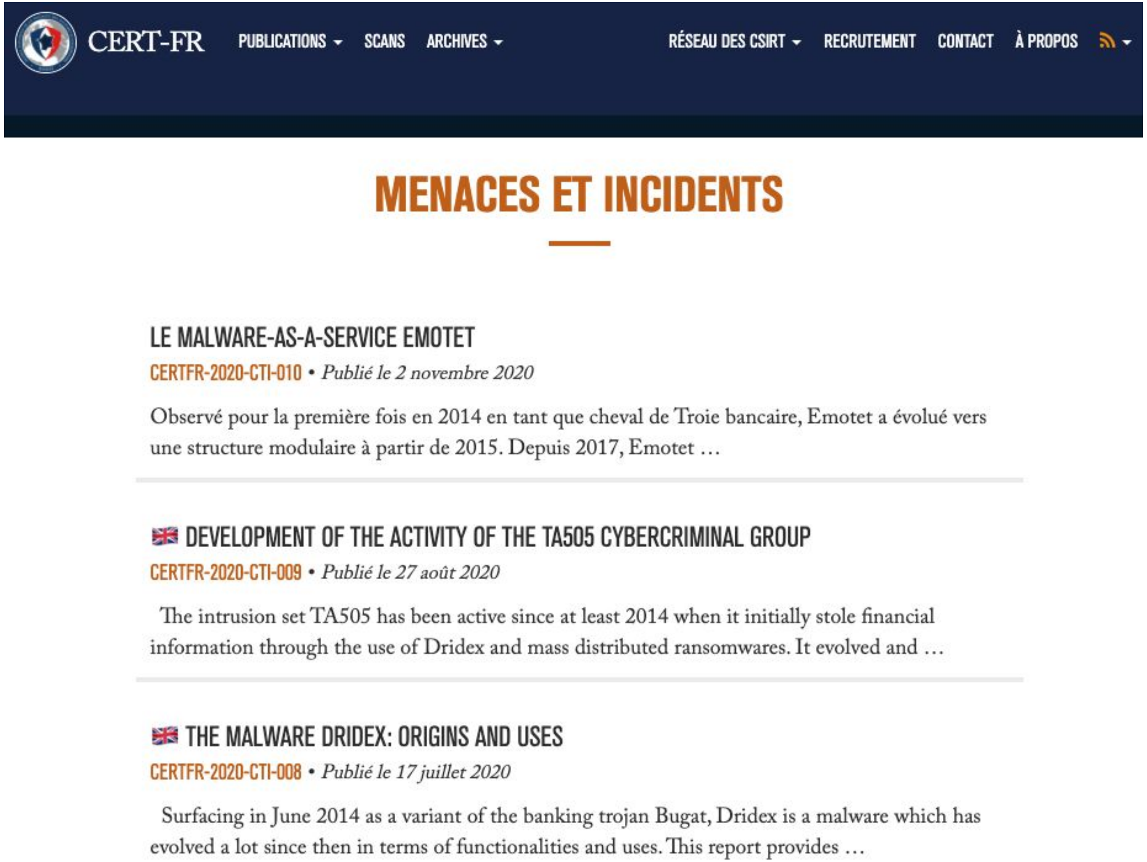
Attack Vector	LOCAL	Confidentiality Impact	HIGH
Attack Complexity	LOW	Integrity Impact	HIGH
Privileges Required	LOW	Availability Impact	HIGH
User Interaction	NONE	Scope	UNCHANGED

References

Link	Resource
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	

CERT-FR (Flux RSS)

🎯 [Menaces et incidents](#)



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 …

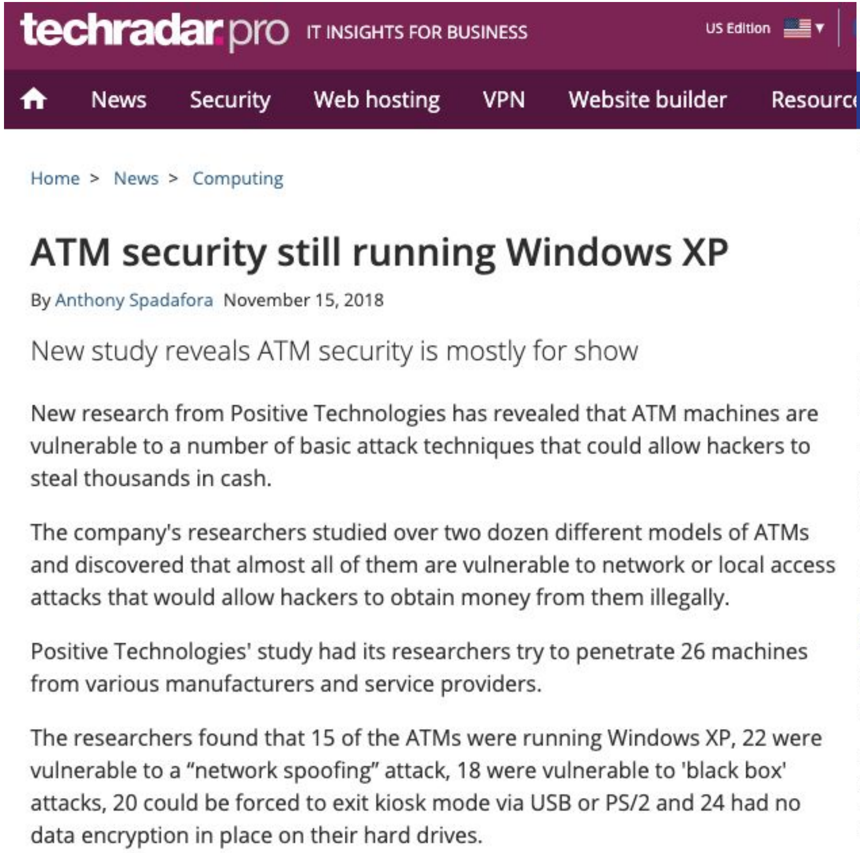
🇬🇧 THE MALWARE DRIDEX: ORIGINS AND USES

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)



Home > News > Computing

ATM security still running Windows XP

By Anthony Spadafora November 15, 2018

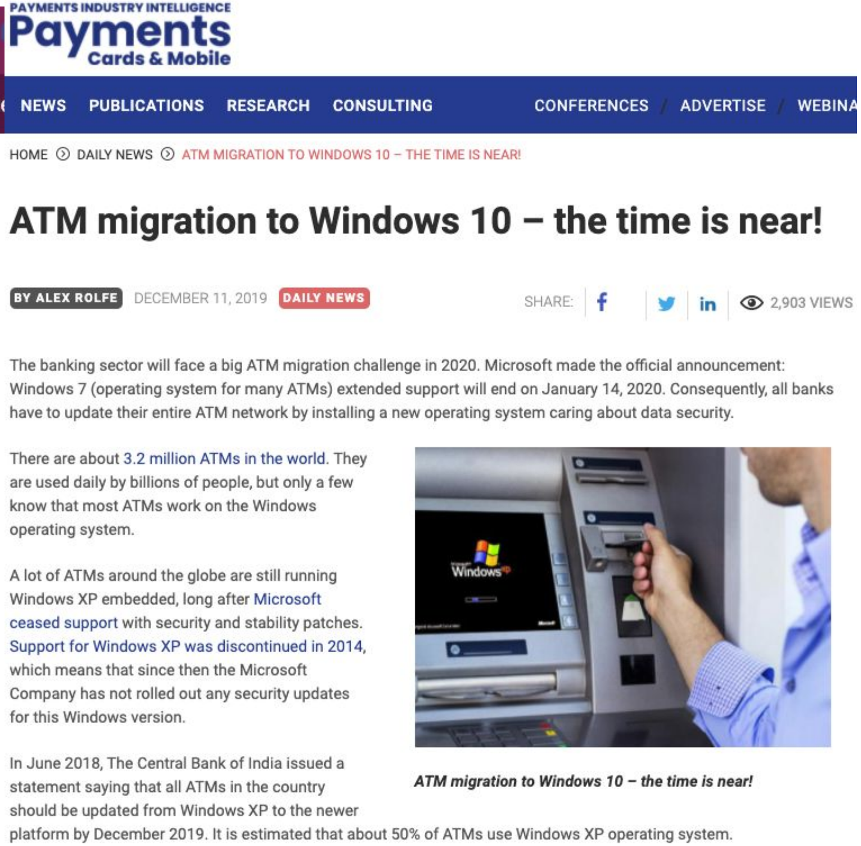
New study reveals ATM security is mostly for show

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.

ATM migration to Windows 10 – the time is near!

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.

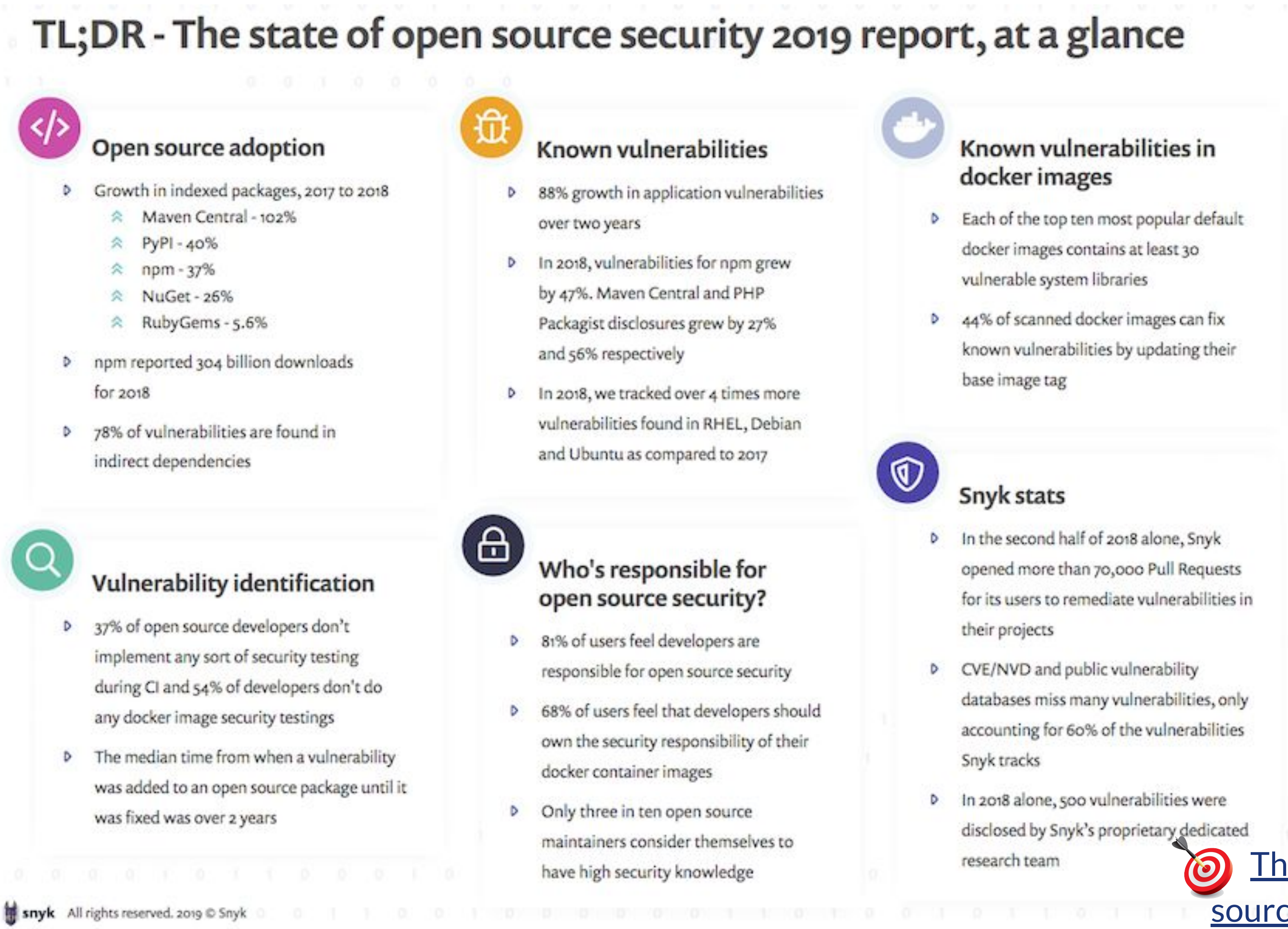
Synthèse

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) 🤓

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

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

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

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

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

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

snyk All rights reserved. 2019 © Snyk

🎯 The state of open source security – 2019

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

@dadideo + Kiwicon 2009 / Hackers don't give a shit

Analogie

« Nul n’est censé ignorer la loi »

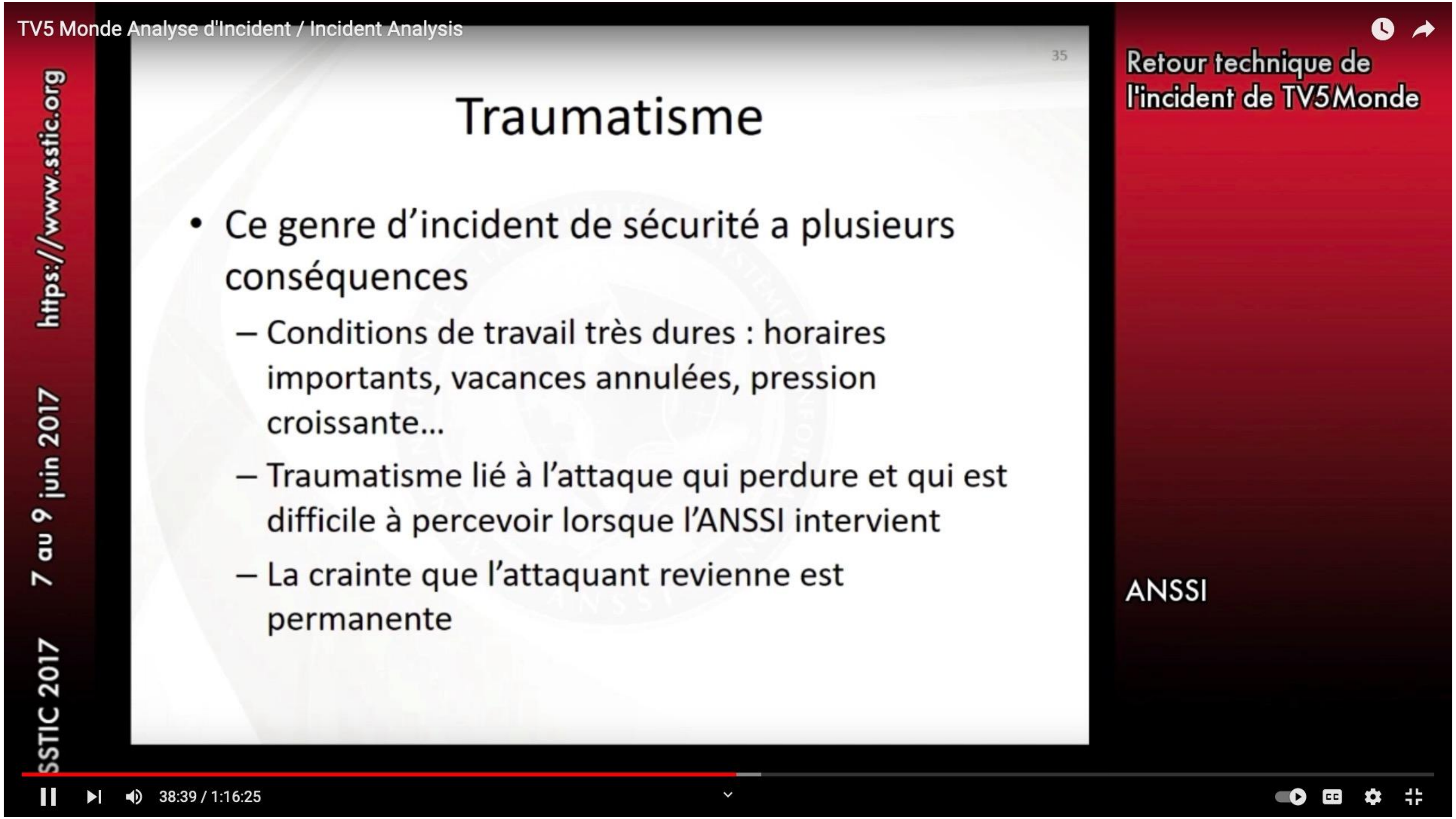
Ma devise

« 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)

Pour aller plus loin



TV5 Monde Analyse d'Incident / Incident Analysis
https://www.sstic.org
SSTIC 2017 7 au 9 juin 2017
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

🎯 TV5 Monde Analyse d'Incident, ANSSI (SSTIC 2017)

Merci pour votre attention !

🧑‍🏫🔊 N'oubliez pas de me donner votre avis sur cette session:

📃 https://s.42l.fr/breizh2022sec

👍 Lien des slides dans les commentaires