TLP: WHITE

OSSIR 2021

PatrowlHears

Vulnerability Intelligence Center

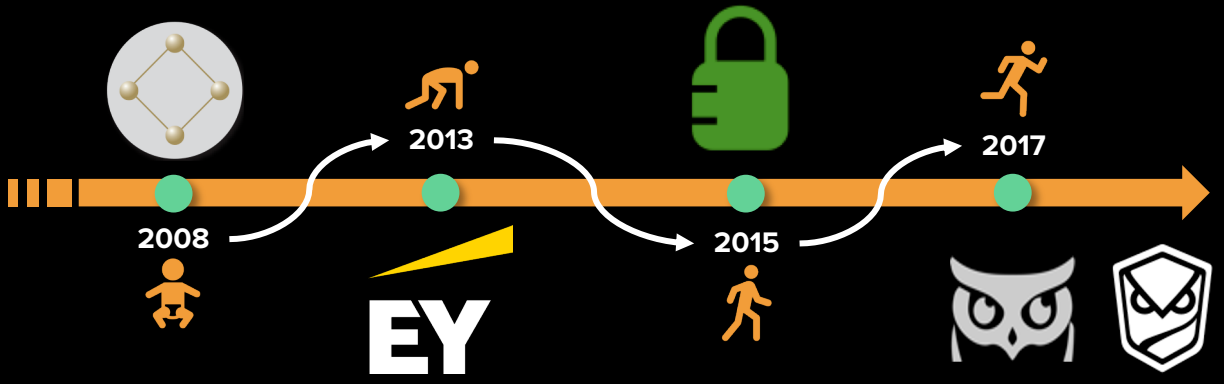
#FOSS #CVE #Exploits #Feeds

2021 – **Patrowl SAS**
"Meme" edition
All rights reserved
Contact getsupport@patrowl.io

PatrOwl
Continuous Threat Management

Let me introduce myself

Nicolas MATTIOCCO
@MaKyOtOx
36 y/o 🇫🇷



- Security auditor moving to Dev[Ops]
- Currently onboarded in an internal CERT/CSIRT for a French financial institution (**Red Team** & Engineering)
- Proud dad

You don't even ~~care~~ need to know more about me...

Qui sommes-nous ?

Tous droits réservés – Diffusion limitée

Nos solutions: automatiser pour gagner en efficicaté

Conseil et Audit

GreenLock Advisory

Défensif

- **C**onseil et **A**rchitecture
- **A**ssistance RSSI
- CSIRT/CERT/SOC

Offensif

- **Tests d'intrusion** et **RedTeam**
- Audits d'**architecture infra**. et **Cloud**
- Revue de **code source**
- Social Engineering

Cyber Surveillance

PatrOwl
Continuous Threat Management

Offres SaaS ***et*** On-Premise

- **C**artographie sécurité continue
- **C**ontrôles sécurité continus
- Réévaluation des risques en temps réel

Notation du Risque cyber

Intégration ***et*** dév. Spécifiques

Support et formation à PatrOwl

Vulnerability Intelligence

PatrOwl Hears
Continuous Vulnerabilities Management and Scoring

Offres SaaS ***et*** On-Premise

- Analyse de l'Actualité en temps réel
- Réévaluation des risques en temps réel
- Notation des vulnérabilités par rapport au contexte et à l'exposition cyber
- Réévaluation des notations en temps réel
- Alertes en temps réel

Qui sommes-nous ?

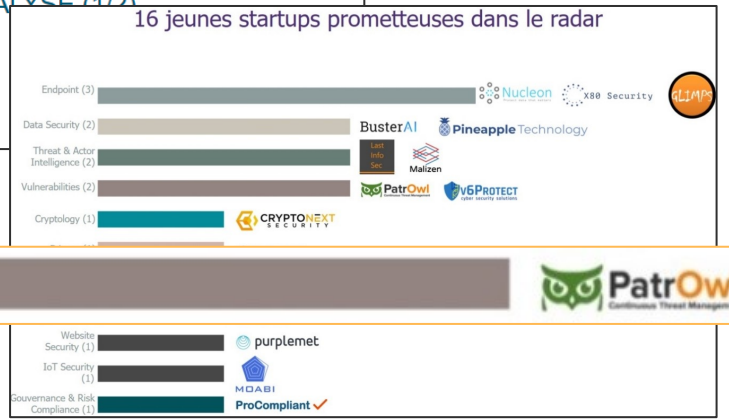
Tous droits réservés – Diffusion limitée

Actualité

Startup prometteuse

PatrOwl dans le radar 2020 des startups prometteuses en cyber sécurité

Wavestone / RiskInsight



How to manage **vulnerabilities** ?

Identification through automation

Do more checks

- Cover a larger and diversified scope
- Empower new capacities and improve cyber-security maturity level
- Get a better overview of cyber-exposure (full-stack)

Do it more often

- Continuously checking for vulnerabilities and suspicious changes
- Reduce delays in discovering and fixing a security incident (vulnerability or pwnage)
- Keep updated of your cyber-exposition risks

Do it more efficiently

- Reduce time to low value-adding tasks to focus on more complex security cases
- Reduce and manage costs
- Assess effectiveness of your SecOps activities through measurable KPIs

Do compliance and benchmarks

- Define and expedite controls
- Assess compliance level regarding corporate, regulatory and statutory standards
- Benchmark security level of assets using same control policies

Vulnerability management challenges

More controls + More often

=

More findings

=

More alerts

How to manage **vulnerabilities** **efficiently** ?

A lots of findings...

How about **prioritization** ?

Once upon a time in a CERT/CSIRT

Morning routine

How to **prioritize** findings ?

- **Our morning routine when a new vulnerability is discovered:**

  Sources: Vulnerability Feeds, CTI, Bluez, Redz, 'Private channels' …

  - We need answers about our **exposure** and **compromising** statuses:
    - ~~✓ Is it a named vulnerability, with a logo and and dedicated website? @All: Don't panic!~~
    - ✓ What is the CVSS Base Score ? @SOC: Tell us ! Classical communication only to known product owners if it is upper than 7.0 and continue if it's upper than 9.0.
    - ✓ Are we vulnerable ? @SOC+Redz: Confirm the versions, the running configurations and counter-measures in place on our assets, contact product owners !
    - ✓ Are we exposed from the Internet ? @SOC+CTI: Tell us !
    - ✓ Is the vulnerability identified on critical assets ? @SOC: Tell us !
    - ✓ Are we aware of any functional exploit ? @Redz+CTI: Go find them and test it !
    - ✓ Is there any patch or compensation measure available ? @SOC+CTI: Tell us !
    - ✓ Are there any likelihood catalysts: exploited in the wild? Media hype level ? Exploited by relevant threat actors ? @CTI: Tell us !
    - ✓ Are we already p0wned ? @DFIR: Investigate and reassure us !
    - ✓ Are we able to detect exploitation ? @DFIR: Tell us and/or try to setup alerts !
    - ✓ OK folks, do we have enough data to initiate a CSIRT alert ? @CSIRT manager: yes / no !

How to **prioritize** findings ?

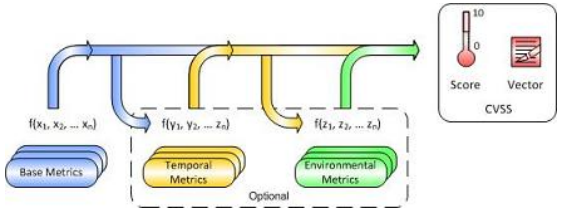
- It is a **teamwork**,
  - Not just within the CERT/CSIRT/SOC team
  - Other IT and Business teams are involved
- Vulnerability metadata are **not static**. They are continuously updating over the time:
  - New patch available !?!
  - New exploit released !
  - New security research blog post available !

Prioritize or die

Is the **CVSS Base Score** sufficiently **enough** to be a primary factor of discrimination in vulnerability management ?

Brief reminder of CVSS scoring

- Score ranging from **0.0** (low) to **10.0** (high/critical)
- Metrics:
  - **Base**: represents the intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments.
  - **Temporal**: represents the characteristics of a vulnerability that change over time but not among user environments.
  - **Environmental**: represents the characteristics of a vulnerability that are relevant and unique to a user's environment.
- Vector string: text representation of a set of CVSS metrics.



- Several versions: CVSSv1 (2005, NIAC/DHS), CVSSv2 (2007, NIST), CVSSv3.0 (2015, FIRST), CVSSv3.1 (2019, FIRST), ***CVSSv4.0 (202x, FIRST)***

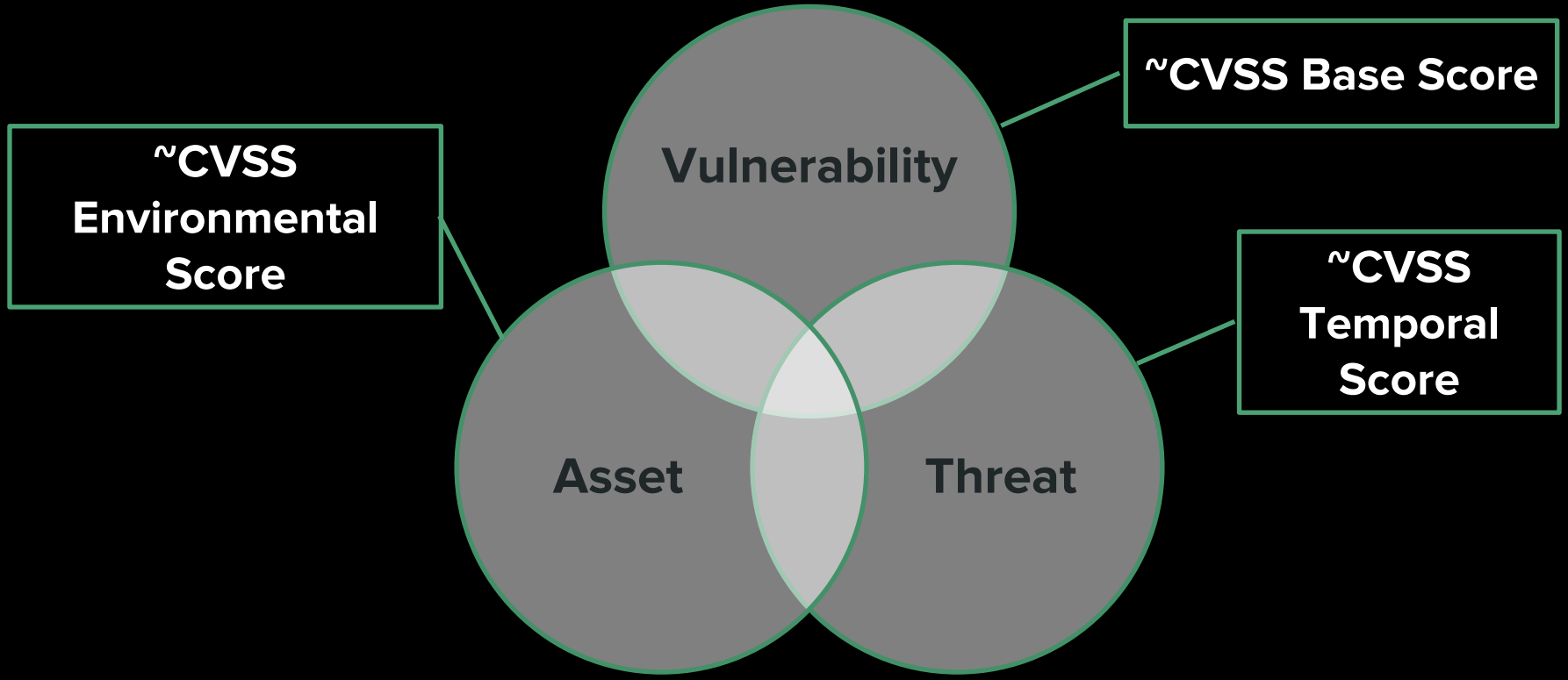
Pros	Cons
▪ THE standard ▪ Largely adopted ▪ Transparent ▪ Understandable from everyone	▪ Availability (v2 vs. v3 vs. nothing) ▪ Accuracy ▪ Completeness ▪ Updates ▪ Trust ▪ Equations ?!? Srly ?

- Only the CVSS Base score is usually provided. Temporal and Environmental scores are on our behalf
- Other fun facts:
  - HeartBleed (CVE-2014-0160) was scored at 5.0
  - Spectre (CVE-2017-5753) was scored at 4.7

Prioritize or die

Again:
Is the **CVSS Base Score** sufficiently **enough** to be a primary factor of discrimination in vulnerability management ?

Vulnerability scoring for prioritization



Criteria for prioritization (1/3)

Vulnerability

- **CVSSv2 Impact & exposure**
  - Low (0.0 – 3.9)
  - Medium (4.0 – 6.9)
  - High (7.0 – 10.0)
- **Patch availability**
  - Official/Temporal fix /No/Unknown
- **Age of vulnerability**
  - Hot (0 – 14 days)
  - Recent (15 – 89 days)
  - Old (> 90 days)
- **Discovery ease**
  - ~impossible, difficult, easy
- **Detection ease**
  - ~impossible, difficult, easy

~ CVSS Base Score metrics

Criteria for prioritization (2/3)

Threat

- **Exploit availability**
  - No known exploit available
  - A private exploit is available
  - A public exploit is available
- **Exploit maturity**
  - Trusting level: Tested, Validated, Shared by a trusted partner
- **Exploit ease**
  - Theoretical, difficult, easy, auto
- **Threat intensity**
  - Exploited in the wild (yes/no) ?
  - In the news (yes/no) ?
- **Threat relevancy**
  - Exploited by monitored threat actors ?

~ CVSS Temporal metrics

Criteria for prioritization (3/3)

Asset

- **Criticality (from Risk analysis)**
  - Low
  - Medium
  - High
- **Vulnerable asset interface exposure**
  - Internet
  - Intranet
  - Restricted network
- **Distribution (number of occurrences)**
  - $0 < x$ assets ≤ 5
  - $6 < x$ assets ≤ 100
  - > 100 assets

~ CVSS Environmental metrics

Criteria for prioritization

Vulnerability

- **CVSS Impact & exposure**
- **Patch availability**
- **Age of vulnerability**
- **Discovery ease**
- **Detection ease**

Threat

- **Exploit availability**
- **Exploit maturity**
- **Exploit ease**
- **Threat intensity**
- **Threat relevancy**

Asset

- **Criticality**
- **Vulnerable asset interface exposure**
- **Distribution**

Suggested actions

- **1/ Now+**: Immediate correction + CSIRT crisis
- **2/ Now**: Immediate correction
- **3/ Next**: Apply fix in the next patching campaign
- **4/ Never**: Apply fix if possible (attention needed / possibly acceptable)

Contextualized metrics over dumb scoring

Metrics	**Vulnerability #1**	**Vulnerability #2**	**Vulnerability #3**
CVSS Base score	10.0 critical	6.2 medium	8.9 high
Remotely exploitable	**Yes**	**Yes**	No
Asset exposure	Internal network	**Internet**	**Internet**
Asset criticality	high	high	unkown
Exploit available ?	No	**Yes**	**Yes**
Patch available ?	**Yes**	**Yes**	No
Relayed in the news ?	No	No	**Yes**

- Question #1 : You have resources for fixing 1 vulnerability only. Which one do you plan to remediate ?
- Question #2 : On average, you have to manage 100 new vulnerabilities every day. **How do you proceed at scale ?**

Exploits and threat news monitoring challenges

Availability ?

Trusted ?

Format ?

Feeds ?

Maturity ?

Age ?

Interest ?

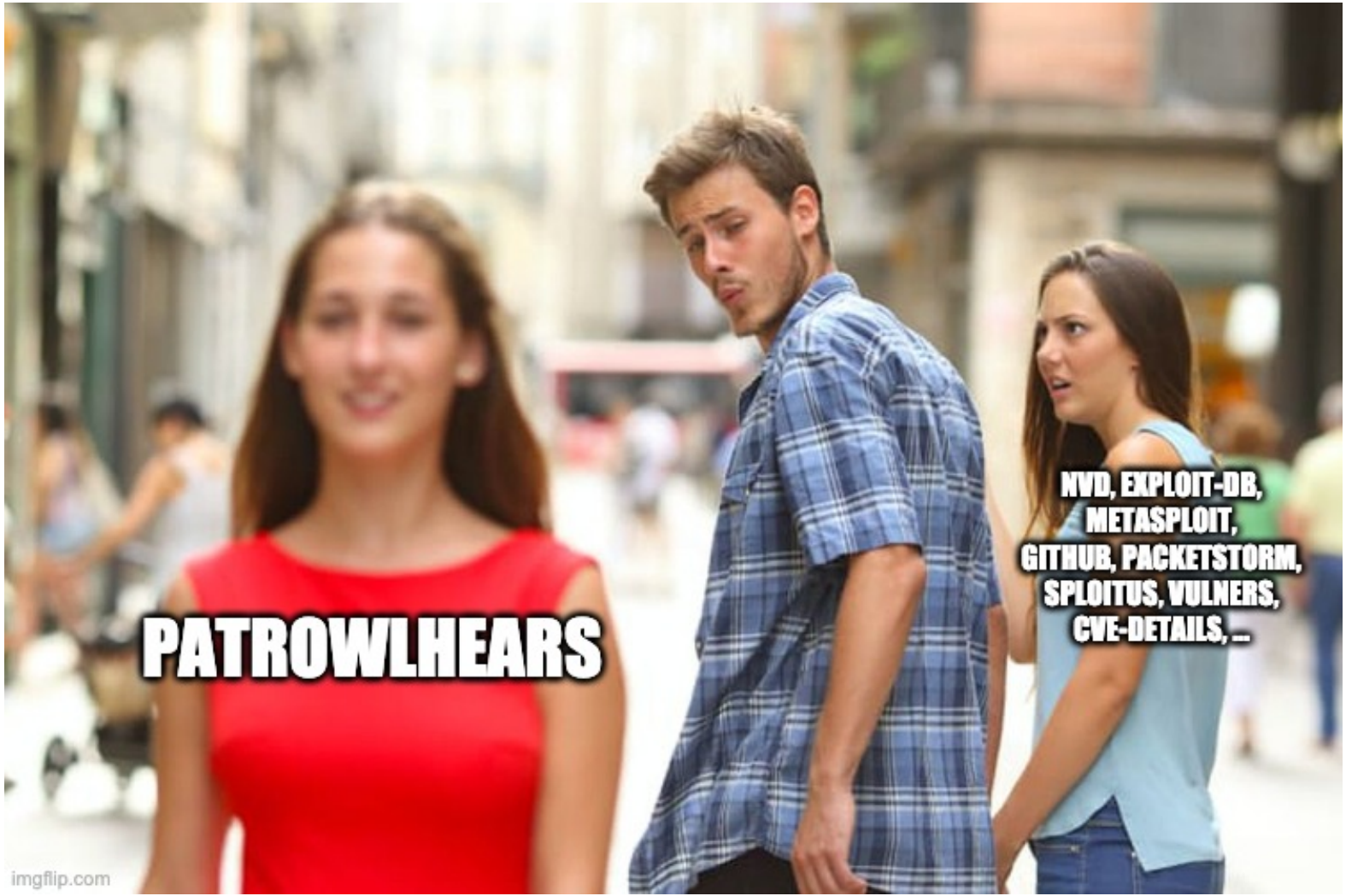
Prioritize or die

So we built **PatrowlHears** to

>> monitor vulnerabilities

>> speed up metrics updates

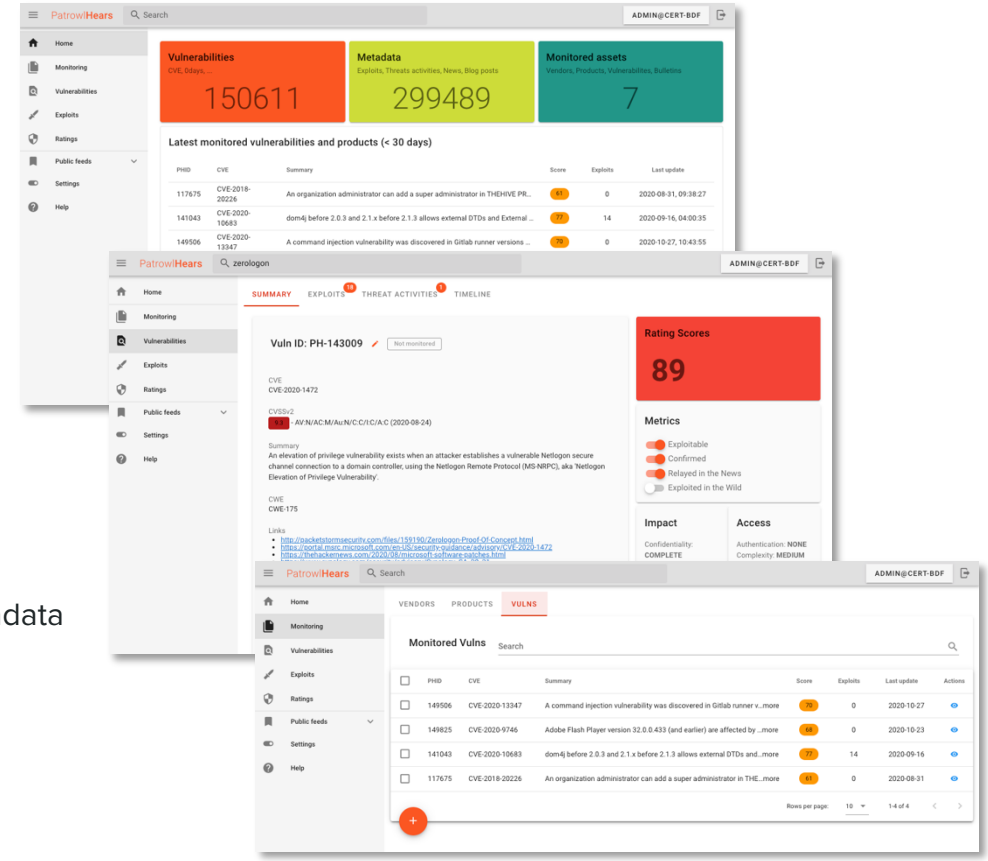
>> share vulnerabilities and metrics


PATROWLHEARS
NVD, EXPLOIT-DB,
METASPLOIT,
GITHUB, PACKETSTORM,
SPLOITUS, VULNERS,
CVE-DETAILS, ...
imgflip.com

Overview

PatrowlHears in a nutshell

- Vulnerability and metadata DB
  - **CVE/CPE/CWE** definitions from NVD
  - “**CVE-less**” vulnerabilities
  - **Exploits**: PoC, script, blog post, whitepaper, slidedeck, mail, tweet, video, notes, ...
  - **Threat news**: Article, Blog post, Tweet
  - Vendor security **advisories** / bulletins
- Monitoring tower
  - Vendor, product, packages, vulnerabilities
  - Track updates
- Collaboration
  - Share monitoring lists, vulnerabilities and metadata
- Vulnerability scoring system
- Alerting
  - Email and Slack notifications
  - Daily/Weekly/Monthly
- Responsive WEB + REST-API



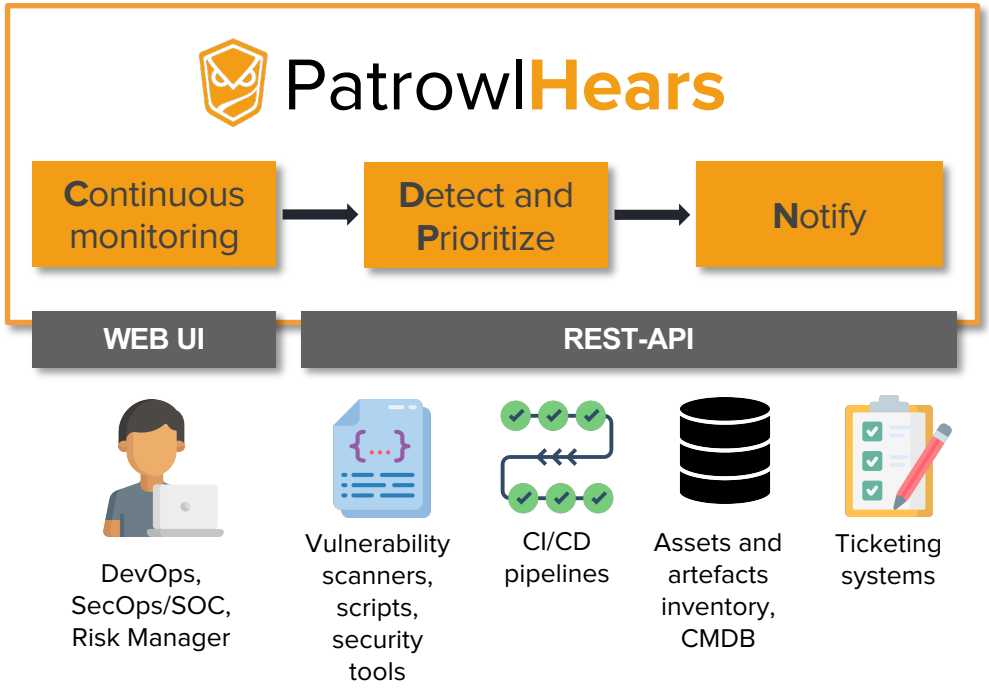
PatrowlHears global architecture

Vulnerabilities
NVD: CVE, CWE, CPE, CAPEC
Unreferenced (pip, npmjs, nuGet, WP, rubyGems, ...)

Exploits metadata
Exploit-DB, Talos, PacketStorm, Nessus DB, HackerOne, SeeBug, TheHackerNews, ...

Vendor security advisories

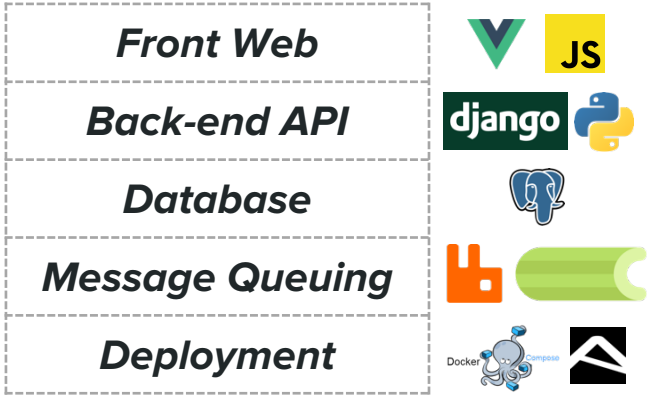
OSINT & PatrowlCERT feeds
Personal and research blogs, Github repositories, Tweets, videos, 'dark-net' forums, ...



Products

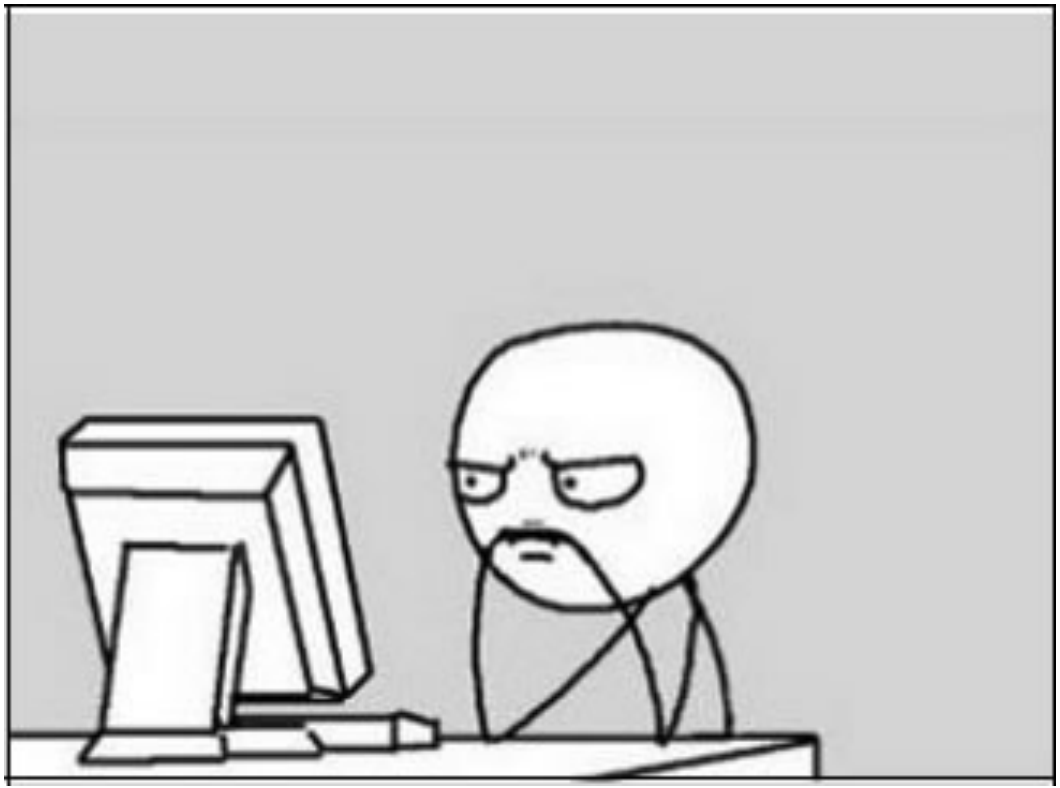
- **PatrowlHears**
  - Back-end, frontend, generic configuration and deployment materials
  - (Poor) Install documentation and OpenAPI definitions
- **PatrowlHearsData**
  - CVE/CPE/CWE/CAPEC + VIA (from CIRCL)
  - Update and loading scripts
  - All metadata stored as JSON files
- **PatrowlHearsFeeds**
  - Search latest exploits and threats metadata on various feeds: PacketStorm, Tenable Nessus DB, Metasploit, Exploit-DB, Seebug, HackerOne, GHSA, GoogleProjectZero, ZDI ...
  - Search package vulnerabilities
  - **Maintain our private exploits references**
  - **Private repo for now.**
- **PatrowlHears4Py**
  - Python client API and CLI for PatrowlHears

Dev Stack



>>>> Test and Star
https://github.com/Patrowl/PatrowlHears

Users



Usual suspects

- CISO/SOC
- DevOps
- Dev

➔ All IT teams

Transparency Act: Known limitations

- CVE publication delay (Microsoft bulletins, …) due to NVD delay
  - ➔Todo: Sync data from major vendor security feeds, including: Microsoft, RedHat, Ubuntu, Vmware, Citrix, Oracle, Acrobat, Mozilla, Chrome, Android, Apple, Cisco, Drupal, F5 and HP
- No SSO
  - ➔Todo: Support LDAP / ADFS authentication for enterprise deployment
- Only CVE and packages known vulnerabilities
  - ➔Todo: Support CNNVD vulnerabilities and ‘unreferenced’ vulnerabilities

Final thoughts

Wrap-up

- Rationalize vulnerability management efforts
- Open-source product
- REST-API ready

Next steps

- Animate the community
- Collect users feedbacks
- Remove known limitations
- Mitre ATT&CK mapping
- Integrate with other tools
  - PatrowlManager (of course)
  - Inventory / CMDB
- Offer a **SaaS Edition** (soon)


SHOWTIME

Votre contact

Nicolas MATTIOCCO

nicolas@patrowl.io

+33 (0) 6.20.70.47.78

PatrOwl

Continuous Threat Management