

PatrOwl

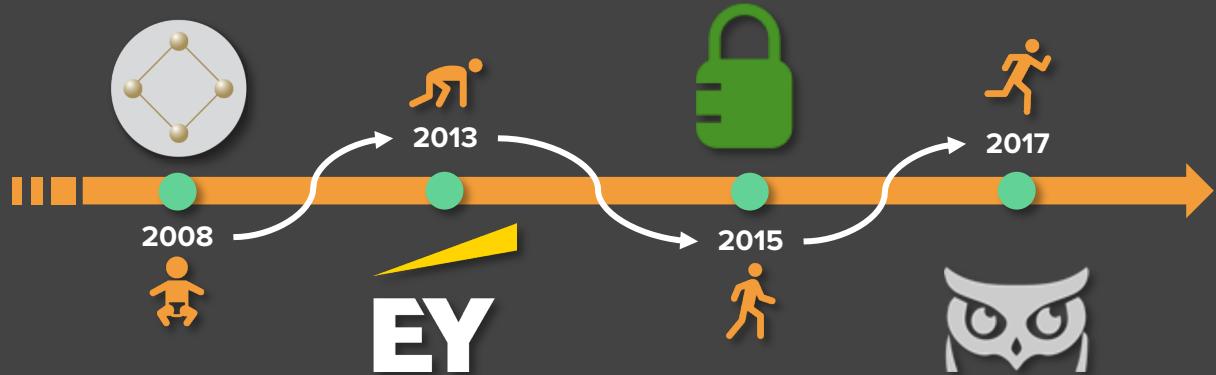
The Red flavour of SOC automation

SecOps orchestration with an open-source SOA(R) platform
#SOAR #SecOps #OpenSource #PreventiveSecurity

Let me introduce myself



Nicolas MATTIOCCO
@MaKyOtOx
35 y/o



- ▶ Security auditor
- ▶ Currently onboarded in the **Red Team** of an internal CERT/CSIRT for a financial institution in France
- ▶ First-timer on an OSS project
- ▶ Proud dad (first-timer too)

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

My own definition of **SecOps** ©



What is PatrOwl ?

Open source, unified, integrated and scalable platform for SecOps automation and orchestration:

- **Continuous** and **full-stack** security overview
- Define threat intelligence & vulnerability assessment scans policies
- Orchestrate scans using tailor-made engines
- Collect & aggregate findings
- Contextualize, track and prioritize findings
- Check fixes and remediation effectiveness

End-Users:

- CERT/CSIRT, SOC, CTI, DFIR, Penetration testers, Risk Manager, Internal Audit, CISO, Fusion Center
- CTO, Dev[Sec]Ops, Network and system engineers, QA Team, Developers
- M&A, Compliance teams
- InsurTech

The screenshots illustrate the PatrOwl Manager's dashboard and specific findings pages:

- Top Left Dashboard:** Shows overall security scores (86 Assets defined, 405 New findings), active scans (0 Active scans), active rules (1 Active rules), and engines (7 Active engines). It includes sections for Asset grades, Most critical assets, Findings by criticity, and Most critical findings.
- Top Right Asset Grade Report:** A grid showing Asset grades (Grade: Low, Medium, High) across categories (A, B, C, D, E, F).
- Middle Left Findings Detail:** A detailed view of a finding for 'XSS Testing site [url]'. It shows Name: XSS Testing site [url], Description: https://xss-game.appspot.com/level1/frame, Tag: + add, Created at: 2018-02-20, and Download report: json -> html -> pdf -> raw.
- Middle Right Findings Stats:** A summary of findings stats with counts for High, Medium, and Low severity findings, along with a global security rating of E.
- Bottom Left Scans Overview:** A timeline showing scan activity from 28 Feb to 22 Mar. It lists three scans performed on 21/21/2018: 16:00 (ARACHNI XSS policy), 16:06 (OWF LEAKS! Search BDF leaks on Github), and 16:09 (OWF LEAKS! Search BDF leaks on Twitter).
- Bottom Right Scan Details:** A detailed view of the first scan (ARACHNI XSS policy) with status (new), progress (green bar), last update (2018-03-21T16:07:36.505), and actions (details, edit, run).



The end. Thank you for the attention !

Questions ?



A new deadly tool ! But we missed some details...

Story horse ?



Facing current and future cyber-security challenges

Trends

Facts & Challenges

Assets exposed



Threats

Vulnerabilities | Attackers |
Security incidents



Business impacts
of security incidents



1. **Poor visibility** on Cyber-exposure risks: Need to monitor a large, diversified, unmanaged and complex scope, even others assets ;
2. **Scarcity** of skilled and efficient **resources** in cyber-security ;
3. **Windows of exposure problem**: Cyber-security mediatisation causes high visibility for vulnerabilities and easiness of attacks ;
4. **Tool capacity-based approach** rather a business threats-based approach. Our great security tools are ineffective without proper strategy, expertise and processes.

Cyber-Exposure and risks are continuously growing and quickly changing



Facing current and future cyber-security challenges

Detecting security incidents

Precursors (may occur)

Indicators (have occurred or is happening)

Events monitoring reveals vulnerabilities and suspicious changes

Asset updates

- Application, system or network updates
- Infrastructure changes: open/closed ports, new subdomain, IP or domain assignment
- **Shadow IT ?**

Infosec KB updates

- CVE, CVSS, CPE updates
- 0-days & misconfigurations
- Exploit releasing
- New detection method: scanner update, new tool released, policy updates, infosec researches
- Publication of IOCs

Ext. resource updates

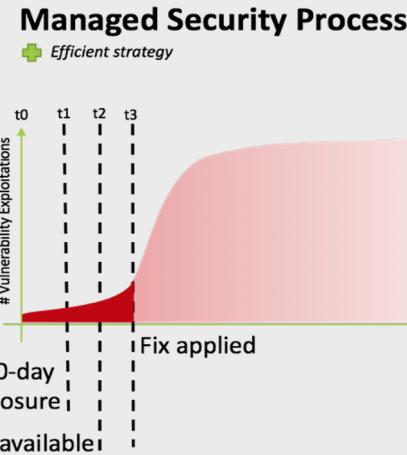
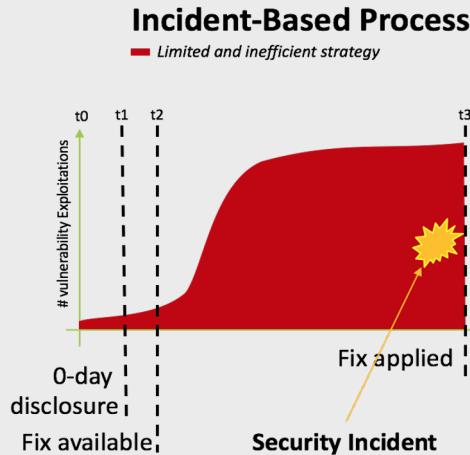
- Data leaks
- Fraud: IP or DNS blacklists, Malware analysis, Typosquatting, ...
- Phishing campaign
- Changes on potential attackers' assets
- Attacks announcements
- Suspicious activities (SIEM)



Facing future cyber-security challenges



The “Window of Exposure” problem



Proactive detection
+ Alert notification
= Early fixing
= Safe earlier

QED

Attackers will attack your assets.
Tackling the window of exposure is now a top priority.

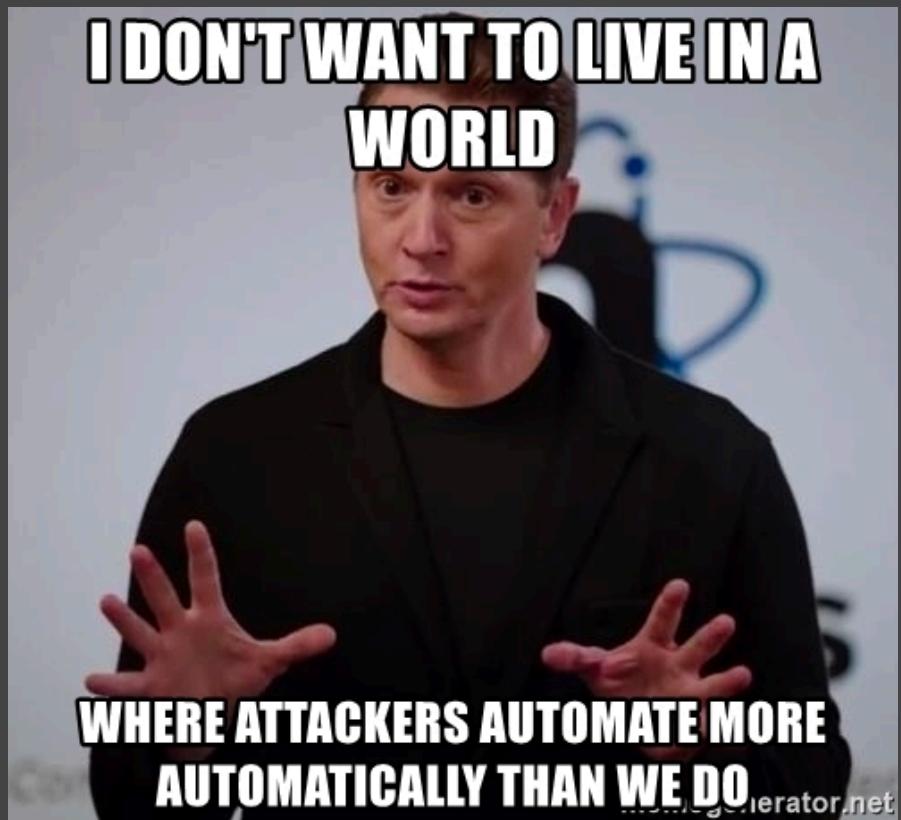


How to face these bigger, better, badder threats ?

What about
**Automation and
Orchestration ?**



■ How to face these bigger, better, badder threats ?



Me too !

Why automating SecOps ?

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

AUTOMATION



PLEASE TAKE MY JOB



Of course, there are several known limits...

It does not cover 100% of risks in itself (do not be so naïve... Black magic does not exist)

Number of alerts ?

False-Positives ?

Functional vulnerabilities ?

Qualification & Contextualisation ?

Total Costs of Ownership ?

Cyber-Defence Strategy ?

... and probably all others generic downsides of automated systems ...



SecOps automation as a new standard ?

BTW, we built **PatrOwl**
for automating and
orchestrating **SecOps**

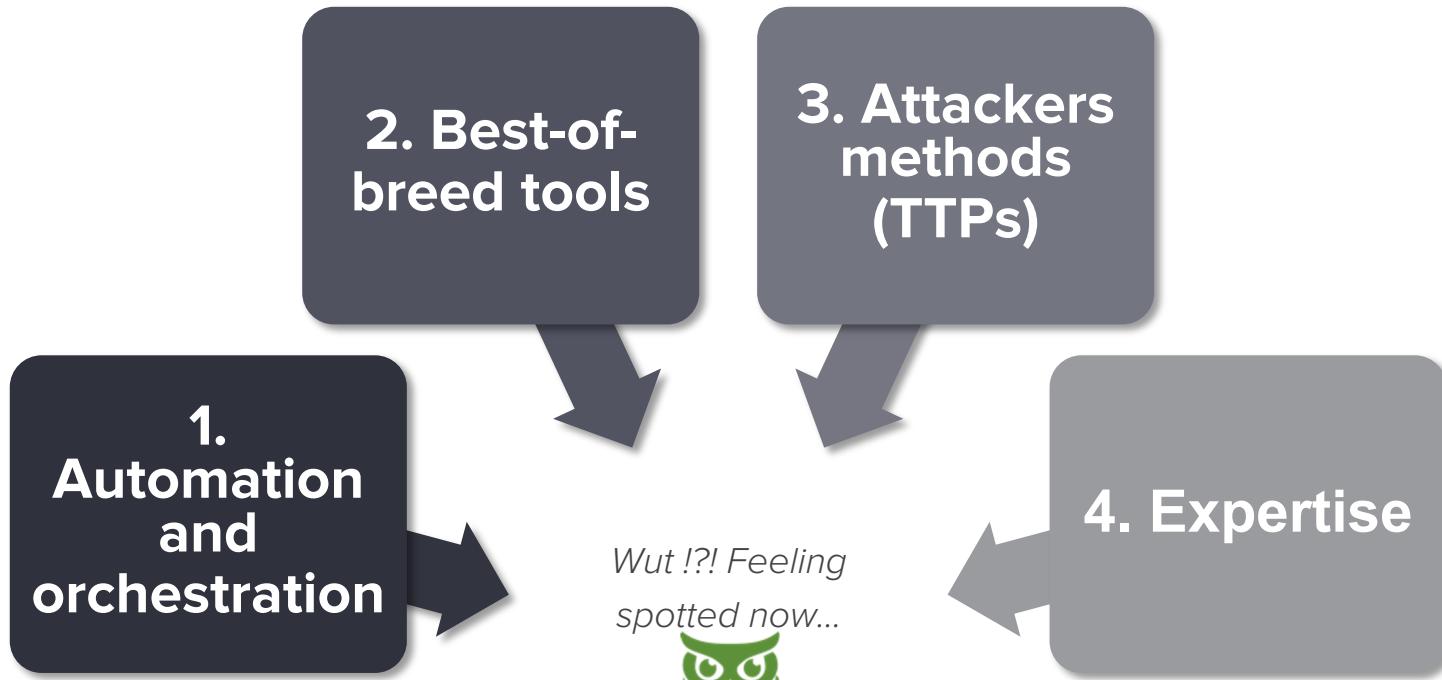




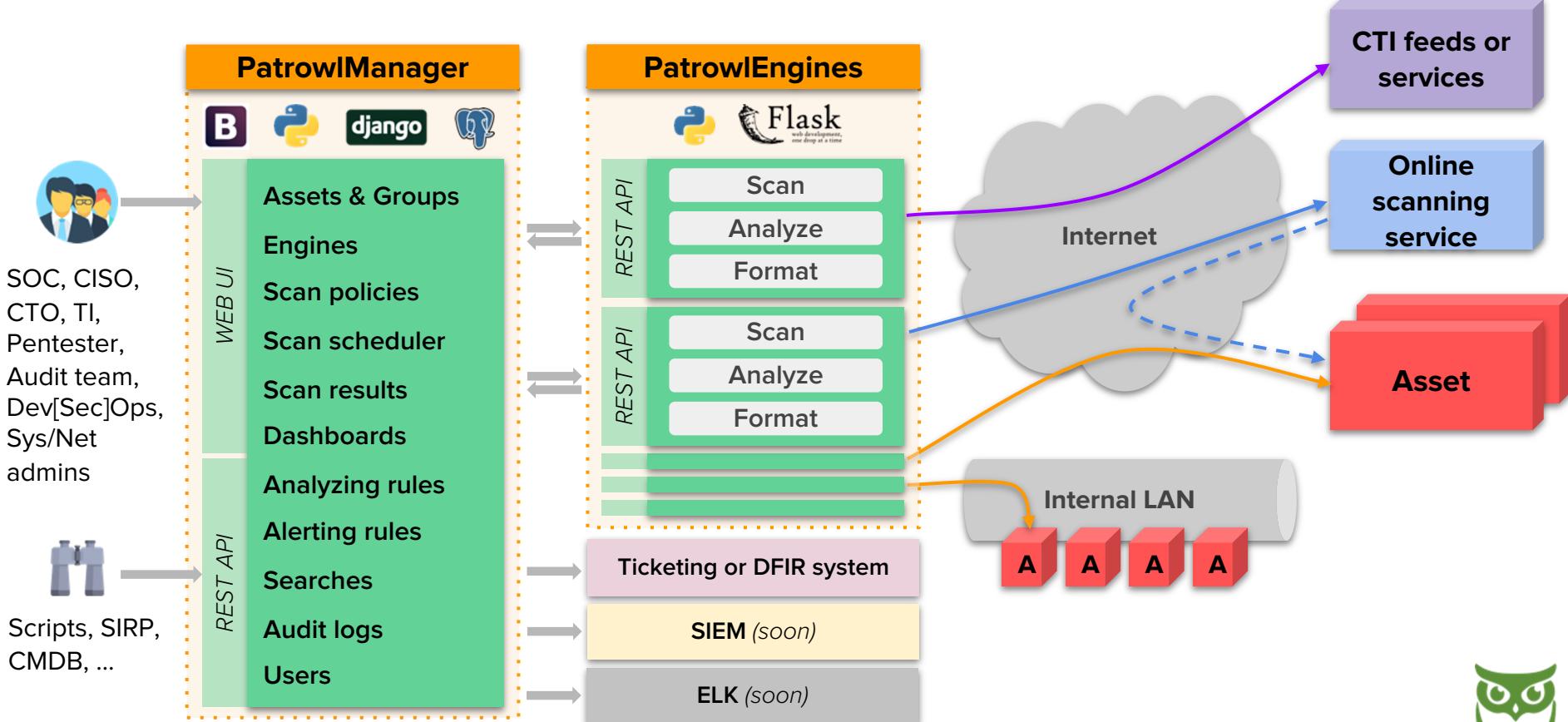
gifbin.com

PatrOwl's incentives

Efficiently moving from a reactive to a more *predictive* security posture with:

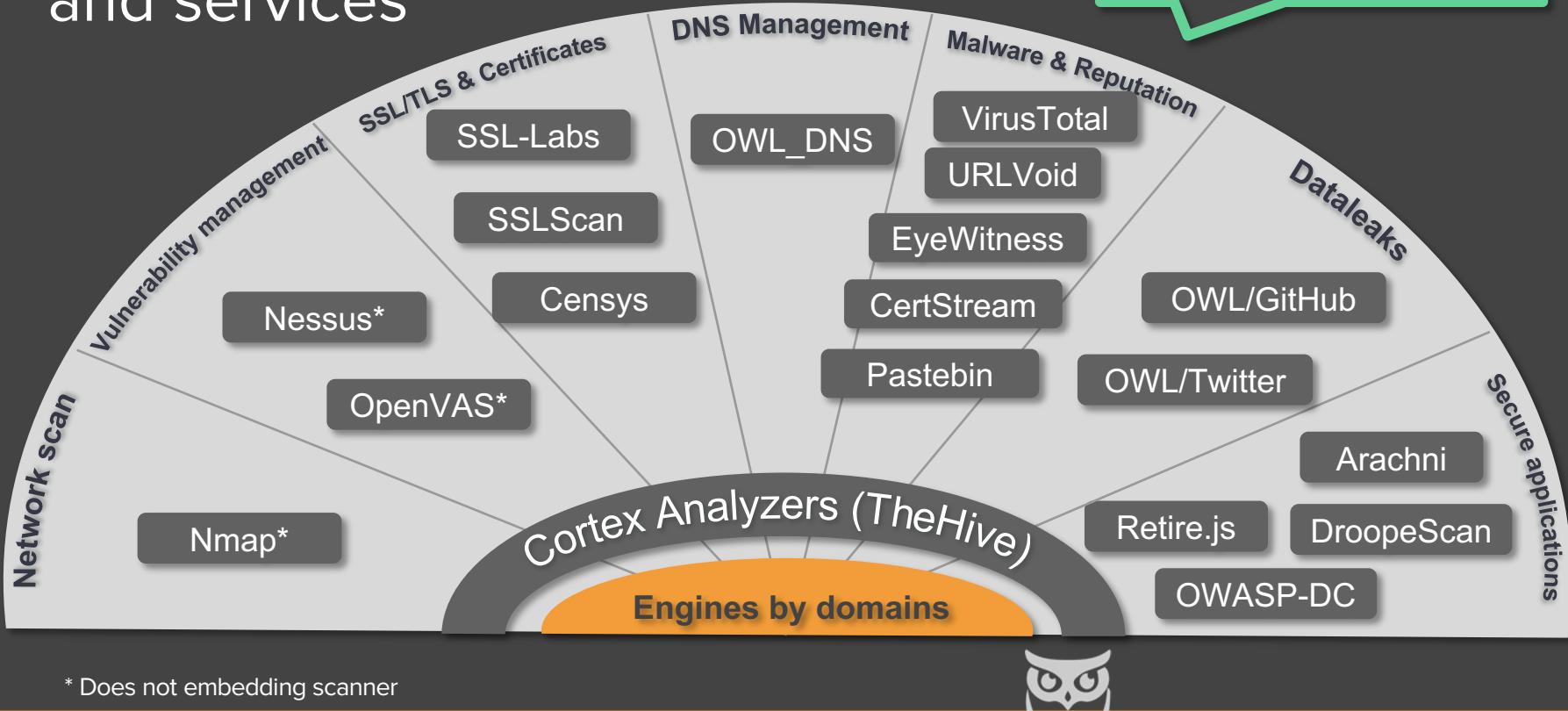


PatrOwl: Technical architecture



PatrowlEngines: Supported tools and services

Turnkey micro-apps:
Docker images +
REST-API



* Does not embedding scanner

■ Next engines in the pipeline (to be confirmed)

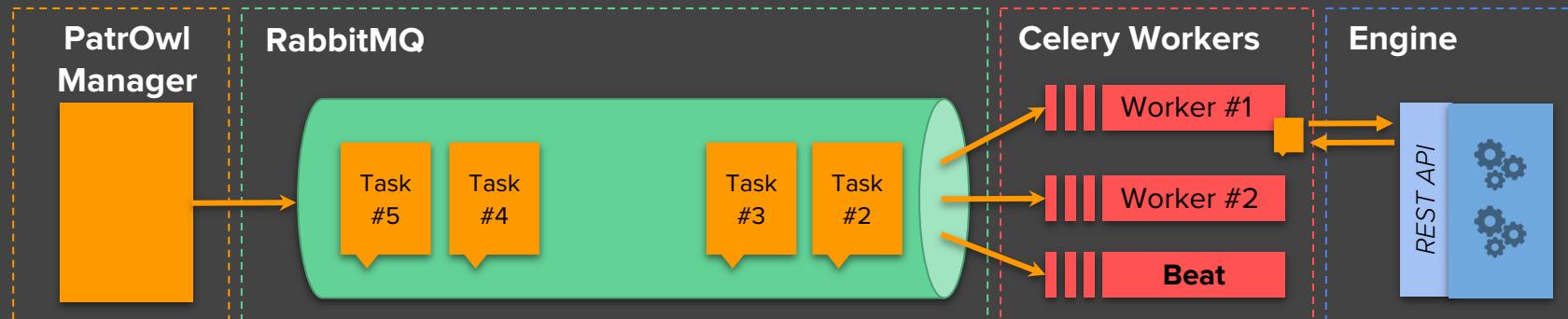
- **Vulnerability management:**
Qualys, Rapid7 IVM/Nexpose
- **Pasties:** AIL-Framework (CIRCL)
- **CTI:** MISP, Shodan, Onyphe
- **WEB:** Acunetix, Burp, WPScan
- **Containers:** AquaSec, CLAIR,
Jfrog Xray, TwistLock
- **Dataleaks:** Git/truffleHog,
gitGraber, Clouseau
- **Cloud:** ScoutSuite, CloudSploit
- ... Any other idea ?



Looking for scalability

Asynchronous scans:

- **RabbitMQ** is used as a message broker and **Celery** as the task queue processor. Messages are sent for monitoring engines or managing scans
- **Celery Beat** is the worker in charge of scheduled tasks



Current challenge: how to manage large amount of assets ? Findings ?



PatrOwl is a SOA(R) framework

Basic use cases



Use case #1: Recon steps for external pentests

Objectives

- First steps of every penetration tests: identify vulnerable targets and explore the best ways to exploit them

Basic strategy

1. Search subdomains (SE, brute-force)
2. Resolve IP addresses
3. List open ports
4. Fingerprint listening services
5. Search for vulnerabilities
6. Search for SSL/TLS misconfigurations
7. Sitemap and autonomous scans

Added values

- Free/Open-source tools:
 - Nmap (+scripts), OpenVAS, SSLScan, Sublist3r
 - Tenable.io || Qualys alternative for online monitoring ?
- Continuous tracking of exposed infrastructure assets and suspicious changes:
 - Open/closed ports
 - Service versions
 - Vulnerabilities & available exploits (i.e. Vulners script)
 - Public subdomains tracking
 - Known resolved IPs
 - Allowed SSL/TLS cipher-suites
 - Certificate expiry dates



Use case #2: SAST/DAST in a DevSecOps pipeline

Objectives

- Examining source code and running WEB applications for security defects

Basic strategy

1. On each commit || tag || merge detected on the code repository: clone the project and start a static code analysis of external libraries (SAST)
2. Once the WEB application is deployed on a staging environment, start an autonomous scan (DAST)

Added values

- Free/Open-source tools:
 - OWASP-DC → .Net, Java external libs (at least)
 - Retire.js → JS dependencies
 - Arachni → Web application scanner
- Easy integration of other security tools (REST API + **Patrowl4py** client)
- Early detection of (basic) vulnerabilities
 - But potentially critical !
- Areas of improvement:
 - Docker images checks
 - More integrations are coming: Checkmarx, Acunetix, Burp ...



Use case #3: Phishing preparation scenario

Objectives

- Search for early signs of malicious domains/websites presence

Basic strategy

1. Search for suspicious domains
 - randorizSec.fr, randourisec.fr, ...
2. Monitor them, looking for changes
 - Still parked domains ?
 - Issued certificates ?
 - New exposed services ?

Added values

- Free/Open-source tools:
 - CertStream : Search for potential fraudulent domains/certificates
 - EyeWitness: Take screenshots
 - OWL_DNS & VirusTotal: Gather data on (sub-)domains from CTI feeds
- Continuous discovery and monitoring of suspicious impersonating domains
- Areas of improvement:
 - Typosquatting vectors
 - Image recognition



Use case #4: Code leaks on GitHub

Objectives

- Search for leaked internal source code, API Keys, passwords, scripts, ...

Basic strategy

1. List the text pattern you want to monitor (beware of false-positives !).

Ex:

- Internal server and application names
- Internet domain names
- Cloud API Keys
- Sensitive email addresses

2. Search these patterns on public GitHub repositories

Added values

- Free/Open-source tools:
 - OWL/GitHub: Search text patterns on GitHub
- Continuous monitoring of public GitHub repositories, including history and development branches!
- Areas of improvement:
 - Search secrets on public and internal Git/SVN repositories (^truffleHog, gitGrabber, ...)



Various use cases

Data leaks

Monitor code leaks on GitHub, sharing platforms (Pasties), emails in dump leaks, open AWS buckets, ...

Vulnerability and remediation tracking

Identify vulnerabilities, send a full report to ticketing system (TheHive, JIRA, ...) and rescan to check for remediation

Vulnerability assessment

Orchestrate regular scans on a fixed perimeter, check changes (asset, vulnerability, CVSS, available exploits)

Monitoring attacker or suspicious assets

Ensure readiness of teams by identifying attackers' assets and tracking changes of their IP, domains, WEB applications

Monitoring Internet-facing systems

Scan continuously websites, public IP, domains and subdomains for vulnerabilities, misconfigurations, ...

Phishing / APT scenario preparation

Monitor early signs of targeted attacks: new domain registration, suspicious Tweets, suspicious pasties, VirusTotal submissions, phishing reports, ...

Regulation and Compliance

Evaluate compliance gaps using tailor-made scan templates

Penetration tests

Perform the reconnaissance steps, the full-stack vulnerability assessment and the remediation checks

Securing the CI / CD pipeline

Automation of static code analysis, external resources assessment and web application vulnerability scans



PatrOwl produces findings. A lots of findings...

How to about
prioritization ?



Once upon a time in a CERT/CSIRT

Morning routine



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 a dedicated website?~~ **@All:** We're screwed !
- ✓ 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 a critical asset ? **@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 ? **@CERT manager:** yes / no !



Prioritize findings

► Wrap up

- It is definitely a teamwork, not just within the CERT/CSIRT team
- CVSSv2 Base Score as a primary criteria
- Vulnerability metadata are not static. They are continuously evolving over the time. Ex:
 - New patch available
 - New exploit released



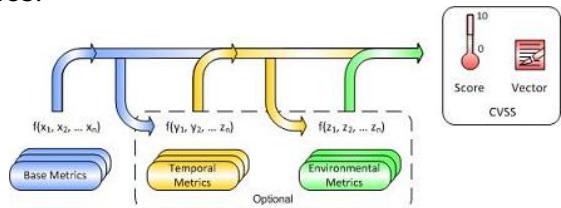
Prioritize or die

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
<ul style="list-style-type: none">▪ THE standard▪ Largely adopted▪ Transparent▪ Understandable from everyone	<ul style="list-style-type: none">▪ Availability (v2 vs. v3 vs. nothing)▪ Accuracy▪ Completeness▪ Updates▪ Trust▪ Equations ?!?

- ▶ 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 ?



Criteria for prioritization

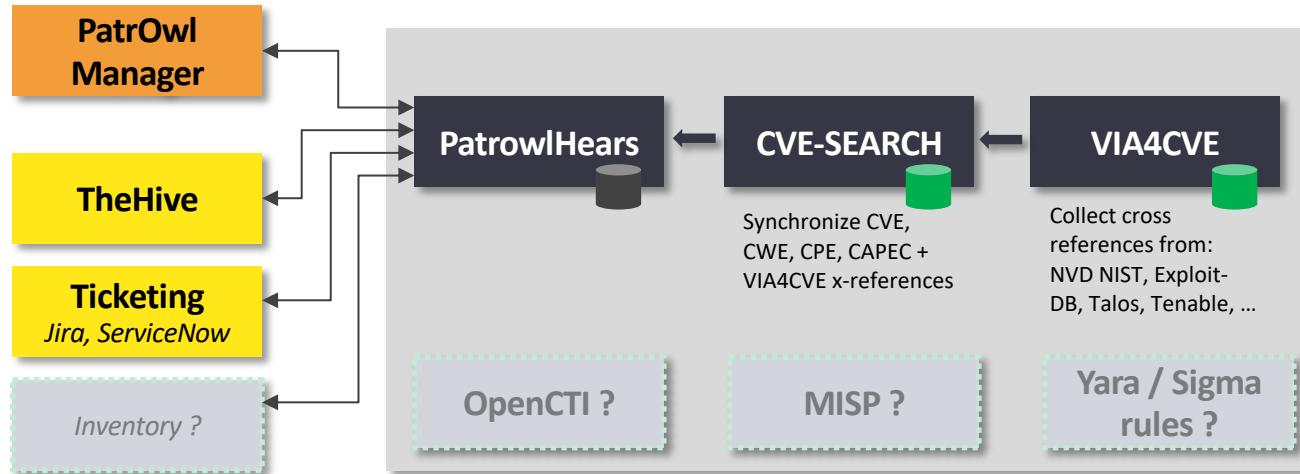
Threat	Vulnerability	Asset
<ul style="list-style-type: none">▶ Exploit availability<ul style="list-style-type: none">▪ No known exploit available▪ A private exploit is available▪ A public exploit is available▶ Exploit maturity<ul style="list-style-type: none">▪ Trusting level: Tested, Validated, Shared by a trusted partner▶ Exploit ease<ul style="list-style-type: none">▪ Theoretical, difficult, easy, auto▶ Threat intensity<ul style="list-style-type: none">▪ Exploited in the wild (yes/no) ?▪ In the news (yes/no) ?▶ Threat relevancy<ul style="list-style-type: none">▪ Exploited by monitored threat actors (yes/no) ?	<ul style="list-style-type: none">▶ CVSSv2 Impact & exposure<ul style="list-style-type: none">▪ Low (0.0 – 3.9)▪ Medium (4.0 – 6.9)▪ High (7.0 – 10.0)▶ Patch availability<ul style="list-style-type: none">▪ Official/Temporal fix /No/Unknown▶ Age of vulnerability<ul style="list-style-type: none">▪ Hot (0 – 14 days)▪ Recent (15 – 89 days)▪ Old (> 90 days)▶ Discovery ease<ul style="list-style-type: none">▪ ~impossible, difficult, easy▶ Detection ease<ul style="list-style-type: none">▪ ~impossible, difficult, easy	<ul style="list-style-type: none">▶ Criticality (ERM-based)<ul style="list-style-type: none">▪ Low▪ Medium▪ High▶ Vulnerable asset interface exposure<ul style="list-style-type: none">▪ Internet▪ Intranet▪ Restricted network▶ Distribution (number of occurrences)<ul style="list-style-type: none">▪ $0 < x \text{ assets} \leq 5$▪ $6 < x \text{ assets} \leq 100$▪ $> 100 \text{ assets}$

4 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)



PatrOwlHears architecture



- Collect and clean data: CVE, CPE, cross-references
- Create / Update vulnerability metadata from:
 - Collected data
 - User inputs
- Compute a vulnerability prioritization rating using:
 - Vulnerability metadata
 - Asset criticality and exposure
- Monitor vulnerabilities and Vendor/Products: track changes:
 - Track changes (CVSS, exploits, ...)
 - Alert: TheHive, Email, Slack, Jira
- Share feeds: public/private



Take-away



Cost-Effective

Rationalize tools integration,
product licenses and skills



Time-To-Value

Ease of use and deployment,
templates for scan policies



Adaptability & Scalability

REST API, Open-Source connectors,
adaptable to organisation's
ecosystems



360° overview

Full-stack assessment of cyber-exposure, in real-time with relevant data



Always updated

Vulnerability KB, detection methods,
threat scenarios



Made with ❤️ by experts

Our team members are A+ security engineers



We currently work on:

- More integration with:
 - Security Incident Response
 - IT Automation and Continuous Configuration
- Patrowl4py: Python API client for PatrowlManager and PatrowlEngines
- Testing various use cases
- Debugging and improving quality (endlessly) and security
- Documenting (endlessly too !) + scan templates
- Supporting MITRE ATT&CK & scenario-based tests
- Building an Enterprise solution (SaaS and on-premise). Stay tuned !
 - *Pro features: LDAP/AD/SAML/OAuth authentication, Cloud security assessment engines, assets auto-discovery and synchronisation, awesome custom dashboards, risk-based controls, Jira/ServiceNow integration, ELK ...*



TheHive



Cortex



It's an open-source project: Contribution is needed !!

Who's up for:

- **Testing it** and giving us lots of **feedbacks** !
- **Contributing:**
 - New engines
 - Debug
 - Features ??
- **Joining the core team ?**
- **Support us ?**



Dev[Sec]Ops,
Security
engineer, Cloud
Architect, UX/UI
Designer, QA
Tester, Wonder-
Woman
(Batman is
tolerated too) ...



Q&A

1

**We have lots of
questions !?!**

2

**We want a
demo !?!**

-- Meet us at the bar !

3

**Enough ! Please
stop talking bro !?!**

-- Thanks for the attention !

Contacts

More details ? Meet us ? Contributing ? Want a demo ? Want an awesome sticker ? Share a beer ? Requesting a Cloud/SaaS demo account (BETA test) ? Join us (**we are hiring**) ?

Find us everywhere on earth:

Now: Just in front of you

Mail: getsupport@patrwl.io

Web: <https://patrwl.io>

Twitter: [@patrwl_io](https://twitter.com/patrwl_io) (Follow us !)

GitHub: [@Patrwl](https://github.com/Patrwl) (Star and fork us !)

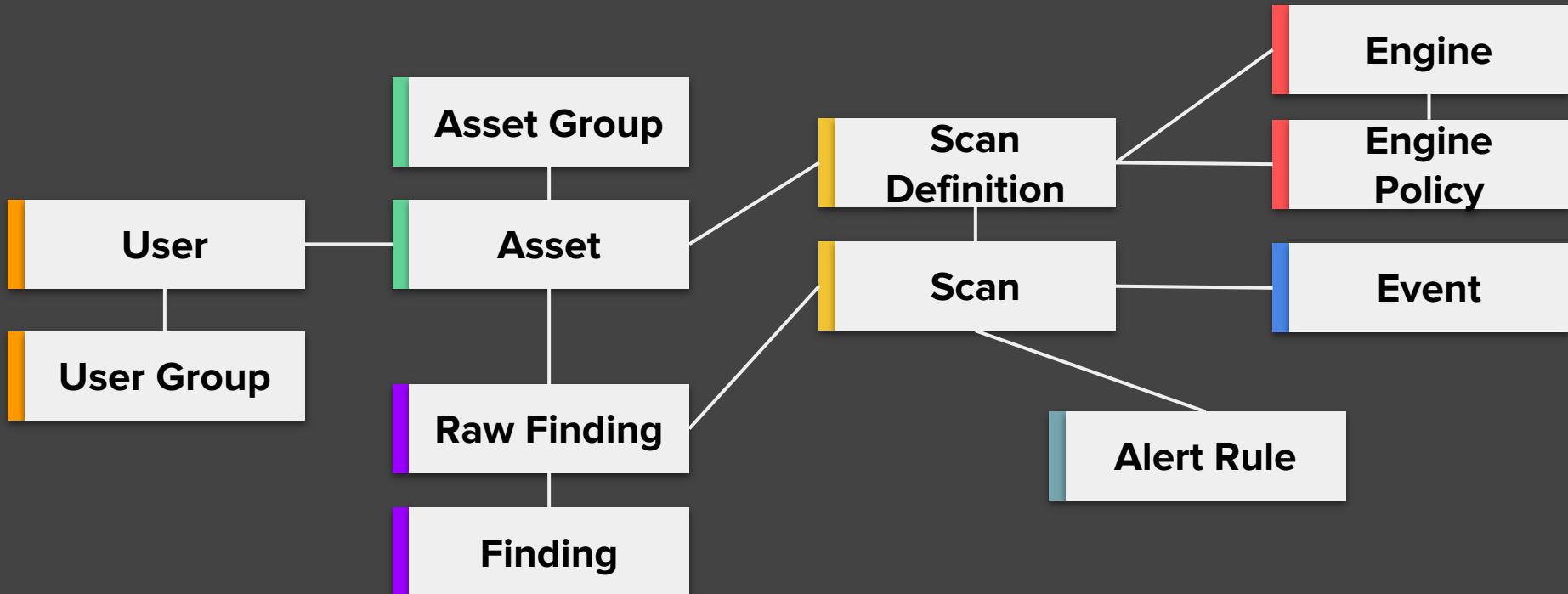
Before you ask: Why PatrOwl is named “PatrOwl” ?



- The owl is able to see in the dark ~~deep web~~ with a large peripheral vision (almost 360°)
- The domain “patrowl.io” name was not already registered



Data Model (simplified)



PatrOwl Manager - Dashboard

Global indicators on assets,
findings, scans, engines and rules
Asset and asset group grades
Most vulnerable assets and asset
groups

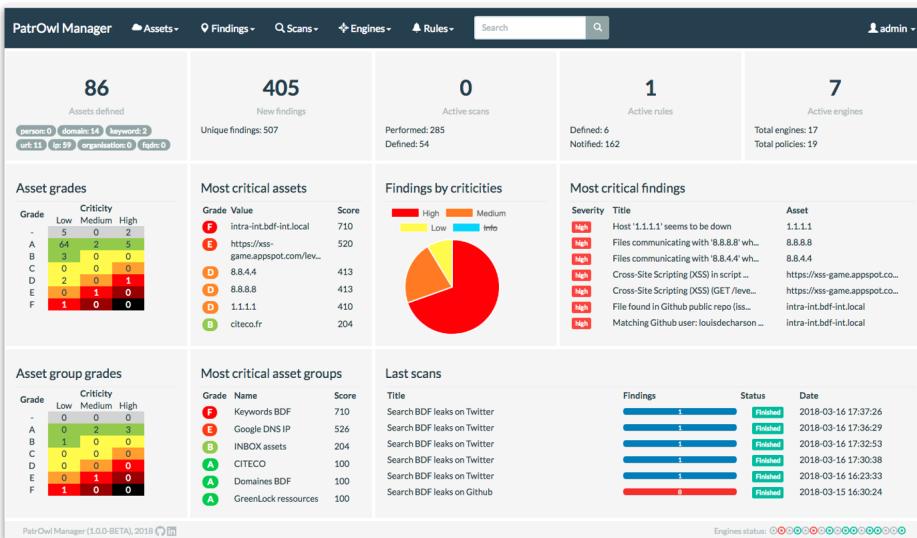
Most critical findings

Findings repartition by severity

Last scans status and results

Top CVSS Score / Findings

Top CVE, CWE, CPE, ...



PatrOwl Manager - Asset detailed view

Current finding counters, risk grade and trends (last week, months, ...)

Findings by threat domains:

- Domain, HTTPS & Certificate, Network infrastructure, System, Web App, Malware, E-Reputation, Data Leaks, Availability

All findings and remediations tips

Related scans and assets

Investigation links

Export HTML, CSV or JSON reports

Custom tags

The screenshot shows the PatrOwl Manager interface for an asset at <https://xss-game.appspot.com/level1/frame>. The asset details include:

- Name: XSS Testing site (url)
- Value: <https://xss-game.appspot.com/level1/frame>
- Description: https://xss-game.appspot.com/level1/frame
- Tags: oracle weblogic [x] + add
- Criticality: medium
- Created at: 2018-02-20
- Download report: json - html - pdf - raw

Findings Stats:

- High: 2
- Medium: 0
- Low: 0

Global Security Rating: E

Findings Table:

Actions	Title	Type	Severity	Status	From	Last update	Actions
<input type="checkbox"/>	Cross-Site Scripting (XSS) (GET /level1/frame [query])	xss	high	new	ARACHNI	2018-02-24	
<input type="checkbox"/>	Cross-Site Scripting (XSS) in script context (GET /level1/frame [query])	xss_script_context	high	new	ARACHNI	2018-02-24	
<input type="checkbox"/>	Sitemap https://xss-game.appspot.com/level1/frame (#URL: 3, HASH: e313ad)	sitemap	info	new	ARACHNI	2018-02-24	



PatrOwl Manager - Scan definition creation view

Search and select assets and asset groups on their value or name

Filter policies by engine type or threat domain

Select engine

- If no engine is selected, an engine is randomly chosen in available engines for each scan

The screenshot shows the 'Add a new scan definition' page in the PatrOwl Manager. At the top, there are tabs for 'Assets', 'Findings', 'Scans', 'Engines', and 'Rules'. A search bar is also at the top right. The main form has fields for 'Title' (with placeholder 'Enter a title...'), 'Description' (placeholder 'Enter a quick description...'), 'Scan Type' (radio buttons for 'On-demand' and 'Periodical' with a frequency dropdown), and 'Start scan' (radio buttons for 'Later', 'Now', and 'Scheduled at' with a date picker). Below these are sections for 'Search asset(s)' (text input 'Google DNS' with a magnifying glass icon) and 'Asset(s) selected' (checkbox checked for 'Google DNS IP (group)'). There are two sets of filter buttons: 'Filter by Engine' (radio buttons for All, NMAP, NESSUS, ARACHNI, VIRUSTOTAL, OWL_DNS, SSLLABS, URLVOID, CORTEX, and OWL_LEAKS) and 'Or, Filter by Category' (radio buttons for All, Network Infrastructure, System Infrastructure, Domain, Web App, HTTPS & Certificates, E-Reputation, Malware, Availability, and Dataleaks). Under 'Select Policy', a radio button is selected for 'Unauth vulnerability scan - NESSUS'. Under 'Select Engine', a dropdown menu shows '---- random (by default) ----'. At the bottom is a large orange 'Create a new scan' button.



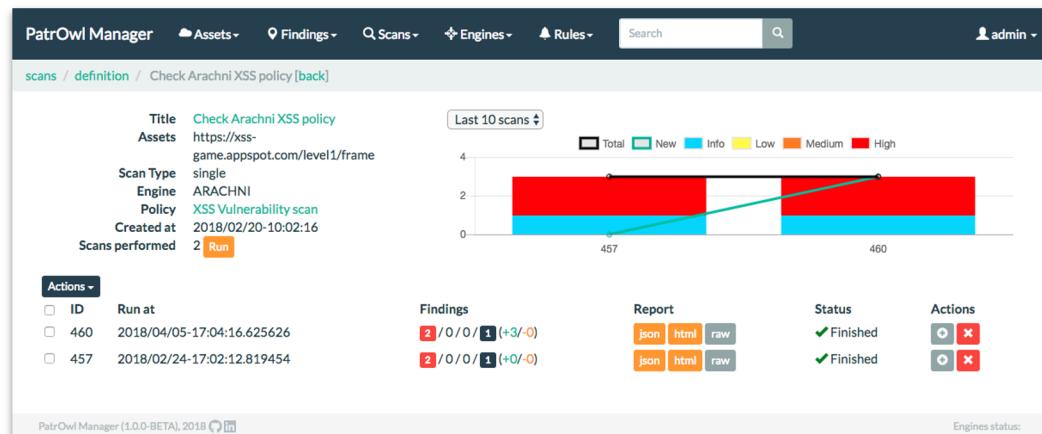
PatrOwl Manager - Scan definition view

Related scan results overview

- o ID, starting datetime, finding counters by severities, status

Quick run button

Quick scan report (HTML or JSON), delete or show details



PatrOwl Manager - Scan compare view

Highlighting differences:

- o new and missing findings
- o same finding type but different details

Link to the findings comparison view

Scans / compare scan results [back]

Asset	Title	Severity
<input checked="" type="checkbox"/>	8.8.4.4 Abuse Finder: Address=abuse@level3.com	Info
<input type="checkbox"/>	8.8.4.4 Abuse Finder: Address=network-abuse@google.com	Info
<input checked="" type="checkbox"/>	8.8.4.4 Abuse Finder 2.0 full results (HASH: 722ea)	Info
<input checked="" type="checkbox"/>	8.8.4.4 Artefacts from 'Abuse Finder 2.0' analyzer (HASH: 985ccb)	Info
<input type="checkbox"/>	8.8.4.4 Artefacts from 'MaxMind GeoIP 3.0' analyzer (HASH: 65cead)	Info
<input type="checkbox"/>	8.8.4.4 MaxMind: Location="United States/North America"	Info
<input type="checkbox"/>	8.8.4.4 MaxMind_GeoIP_3.0 full results (HASH: f09b3b)	Info
<input checked="" type="checkbox"/>	8.8.8.8 Abuse Finder: Address=abuse@level3.com	Info
<input type="checkbox"/>	8.8.8.8 Abuse Finder: Address=network-abuse@google.com	Info
<input checked="" type="checkbox"/>	8.8.8.8 Abuse Finder 2.0 full results (HASH: 793b66)	Info
<input checked="" type="checkbox"/>	8.8.8.8 Artefacts from 'Abuse Finder 2.0' analyzer (HASH: d334ac)	Info
<input type="checkbox"/>	8.8.8.8 Artefacts from 'MaxMind GeoIP 3.0' analyzer (HASH: a1c144)	Info
<input type="checkbox"/>	8.8.8.8 MaxMind: Location="United States/North America"	Info
<input type="checkbox"/>	8.8.8.8 MaxMind_GeoIP_3.0 full results (HASH: c05095)	Info

// Compare selected findings (2 scans max.)

PatrOwl Manager (1.0.0-BETA), 2018   

Engines status: 



PatrOwl Manager - Scan results view

Scans info: title, assets, status, policy, start/end dates

Findings list + show details link

Quick scan report (HTML or JSON)

Findings summary on metrics

Asset and asset group overview

List of related events

PatrOwl Manager - Scan results view

scans / Check Arachni XSS policy [back]

Assets 1 Asset groups 0 Findings 3 Events 0

Asset	Finding Title	Status	Severity	Actions
https://xss-game.appspot.co...	Cross-Site Scripting (XSS) (GET /level1/frame [query])	new	high	[Edit]
https://xss-game.appspot.co...	Cross-Site Scripting (XSS) in script context (GET /level1/frame [query])	new	high	[Edit]
https://xss-game.appspot.co...	Sitemap https://xss-game.appspot.com/level1/frame (#URL: 3, HASH: e313ad)	new	info	[Edit]

Scan details (ID=460)

Title: Check Arachni XSS policy
Assets: https://xss-game.appspot.co...
Engine: arachni-001 (ARACHNI)
Status: Finished
Policy: XSS Vulnerability scan
Started at: 2018/02/24-17:02:55
Finished at: 2018/02/24-17:02:39
Elapsed: 0:00:43.152597
Reports: json html raw

Findings summary

(A) CVSS > 7: 2
(B) > 30 days: 3
(A) + (B): 2

Repartition per severity:

- High (red)
- Medium (orange)
- Low (yellow)
- Info (blue)

PatrOwl Manager (1.0.0-BETA), 2018 [GitHub] [LinkedIn]

Engines status: [Engines status icons]



PatrOwl Manager - Scan performed view

Scans heatmap over days, weeks and months

Advanced filters

Run or delete scans

Show scan details

Compare selected scans

PatrOwl Manager - Scan performed view

scans / scans performed [back]

C < 1m < 1w < Today > > 1w > 1m Filters

16 Jan 17 Jan 18 Jan 19 Jan 20 Jan 21 Jan 22 Jan 23 Jan 24 Jan 25 Jan 26 Jan 27 Jan 28 Jan 29 Jan 30 Jan 31 Jan 1 Feb 2 Feb 3 Feb 4 Feb 5 Feb 6 Feb

Selection: all findings

Status	Progress	Last update	Actions
✓	9	2018-03-27	details ⌂ Run ✘
✓	1	2018-03-21	details ⌂ Run ✘
✓	1	2018-03-16	details ⌂ Run ✘
✓	1	2018-03-16	details ⌂ Run ✘
✓	1	2018-03-16	details ⌂ Run ✘
✓	1	2018-03-16	details ⌂ Run ✘
✓	1	2018-03-16	details ⌂ Run ✘
✓	8	2018-03-16	details ⌂ Run ✘
✓		2018-03-15	details ⌂ Run ✘
✓		2018-03-15	details ⌂ Run ✘
✓	5	2018-03-21	details ⌂ Run ✘

- Delete selected scans (no confirm)
// Compare selected scans (2 scans max.)

Page 1 of 29. [next](#)

PatrOwl Manager (1.0.0-BETA), 2018 [?](#) [\[info\]](#)

Engines status: ● ● ● ● ● ● ● ●



PatrOwl Manager - Finding view

Finding info

Description, solution, links and hash

Quick actions:

- Generate alerts
- Change metadata: severity, status, tags, CVSS
- Export to file (JSON or STIX2 format)

Show tracking info

- Changes history
- Matching scans

PatrOwl Manager / Assets / Findings / Scans / Engines / Rules / Search / admin

[findings](#) / [details](#) / https://xss-game.appspot.com/level1/frame: Cross-Site Scripting (XSS) (GET /level1/frame [query])

[Summary](#) [Tracking](#)

high Cross-Site Scripting (XSS) (GET /level1/frame [query])

Description

Client-side scripts are used extensively by modern web applications. They perform from simple functions (such as the formatting of text) up to full manipulation of client-side data and Operating System interaction.

Cross Site Scripting (XSS) allows clients to inject scripts into a request and have the server return the script to the client in the response. This occurs because the application is taking untrusted data (in this example, from the client) and reusing it without performing any validation or sanitisation.

If the injected script is returned immediately this is known as reflected XSS. If the injected script is stored by the server and returned to any client visiting the affected page, then this is known as persistent XSS (also stored XSS).

Arachni has discovered that it is possible to insert script content directly into HTML element content.

\n\nRequest: GET /level1/frame?
query=Enter%20query%20here...%3Cxx_b11c3b4a8909dd561d2f10baf852c23%2F%3E&button=Search HTTP/1.1
Host: xss-game.appspot.com
Accept-Encoding: gzip, deflate
User-Agent: Arachni/2.0dev-FullScan
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.6
Accept-Language: en-US,en;q=0.8,he;q=0.6
X-Arachni-Scan-Seed: b11c3b4a8909dd561d2f10baf852c23
\n\nResponse: HTTP/1.1 200 OK

Actions

[Generate alerts](#) [Update Infos](#) [Export](#)

Finding Infos

ID:	5161
Severity:	high
Status:	new
Asset:	https://xss-game.appspot.com/level1/
From engine:	arachni-001 (ARACHNI)
From scan:	Check Arachni XSS policy
From policy:	XSS Vulnerability scan
Type:	xss
Tags:	xss, regex, injection, script
Found at:	2018/02/24-17:02:38

Risk Infos

Publication date: 2018/02/24
CVSS Score: 7.5

References

CWE: 79



PatrOwl Manager - Finding compare view

Highlighting differences
between findings

PatrOwl Manager Assets Findings Scans Engines Rules Search admin

findings / compare [back]

Finding A (ID: 1181)		Finding B (ID: 1179)	
Title	Port 'tcp/80' is filtered	Port 'tcp/56' is filtered	
Severity	info	info	
Asset	8.8.8.8	8.8.8.8	
Description	The scan detected that the port 'tcp/80' was filtered	The scan detected that the port 'tcp/56' was filtered	
Solution	n/a	n/a	
Risk info	vuln_publication_date: 2018/01/16 cvss_base_score: 0.0	vuln_publication_date: 2018/01/16 cvss_base_score: 0.0	
Vuln info	n/a.	n/a.	
Links	No links.	No links.	
Tags	No Tags.	No Tags.	
Created at	2018/01/16-12:01:32	2018/01/16-12:01:30	
Scan title	List open ports on Google DNS ↗	List open ports on Google DNS ↗	
Scan policy	List open ports (TCP/53,56,80,443,8080) ↗	List open ports (TCP/53,56,80,443,8080) ↗	
Scan engine	NMAP - nmap-002	NMAP - nmap-002	

PatrOwl Manager (1.0.0-BETA), 2018

Engines status:



PatrOwl Manager - Alerting rules management view

Create, copy, modify or delete alerting rules
Change functional status

PatrOwl Manager Assets ▾ Findings ▾ Scans ▾ Engines ▾ Rules ▾ Search admin ▾

Rules / List

Name	Scope	Condition	Trigger	Severity	Target	Status	Last update	Actions
New findings found (Slack)	finding.status	is 'new'	auto	Low	slack	Disabled	2018-02-20	
Findings with severity='info' -> email	finding.severity	is 'info'	auto	Low	email	Disabled	2018-01-23	
Findings with info severity	finding.severity	is 'info'	ondemand	Low	slack	Enabled	2018-02-01	
Findings with low severity	finding.severity	is 'low'	auto	Low	slack	Disabled	2018-02-20	
Findings with high severity	finding.severity	is 'high'	auto	Low	slack	Disabled	2018-01-16	
New findings found	finding.status	is 'new'	auto	Low	thehive	Disabled	2018-02-11	

+ Title.. Asset is On-demand Low ✓ PatrOwl event
criticity low

To logfile
Send email
To TheHive
To Splunk
To Slack

Enable Add



PatrOwl Manager - Engine management view

Create, modify or delete engines

Change functional state

View engine info, including current scans performed

Refresh engines states

Enable/Disable the auto-refresh

The screenshot shows a table of engines managed by PatrOwl. The columns include Type, Name, Funct. Status, Oper.State, API URL, Last update, and Actions. The 'Actions' column contains icons for Edit, Delete, and Refresh. The 'Oper.State' column uses red 'x' icons for disabled engines and green checkmarks for enabled ones. The 'Funct. Status' column also uses red 'x' icons for errors and green checkmarks for successes.

Type	Name	Funct. Status	Oper.State	API URL	Last update	Actions
ARACHNI	arachni-001	Disabled	✗ Error	http://0.0.0.0:5005/engines/arachni/	2018-03-08 14:59:17	
ARACHNI	arachni-docker-001	Enabled	✗ Error	http://0.0.0.0:5105/engines/arachni/	2018-03-01 14:59:17	
CORTEX	cx-001	Disabled	✗ Error	http://0.0.0.0:5009/engines/cortex/	2018-03-01 14:59:17	
CORTEX	cx-docker-001	Enabled	✗ Error	http://0.0.0.0:5109/engines/cortex/	2018-03-01 14:59:17	
NESSUS	nessus-001	Disabled	✗ Error	http://0.0.0.0:5002/engines/nessus/	2018-03-08 14:59:17	
NESSUS	nessus-docker-001	Enabled	✗ Error	http://0.0.0.0:5102/engines/nessus/	2018-03-08 14:59:17	
NMAP	nmap-002	Disabled	✗ Error	http://0.0.0.0:5001/engines/nmap/	2018-03-08 14:59:17	
NMAP	nmap-docker-001	Enabled	✗ Error	http://localhost:5101/engines/nmap/	2018-03-08 14:59:17	
OWL_DNS	odns-002	Disabled	✗ Error	http://0.0.0.0:5006/engines/owl_dns/	2018-03-08 14:59:17	
OWL_LEAKS	oleaks-001	Enabled	✗ Error	http://127.0.0.1:5012/engines/owl_leaks/	2018-03-08 14:59:17	
OWL_DNS	owldns-docker-001	Enabled	✗ Error	http://0.0.0.0:5106/engines/owl_dns/	2018-03-08 14:59:17	
SSL LABS	ssllabs-001	Disabled	✗ Error	http://0.0.0.0:5004/engines/ssllabs/	2018-03-09 14:59:17	
SSL LABS	ssllabs-docker-001	Enabled	✗ Error	http://0.0.0.0:5104/engines/ssllabs/	2018-03-09 14:59:17	
URLVOID	urvoid-docker-001	Enabled	✗ Error	http://0.0.0.0:5108/engines/urvoid/	2018-03-01 14:59:17	
URLVOID	urvoid-001	Disabled	✗ Error	http://0.0.0.0:5008/engines/urlvoid/	2018-03-01 14:59:17	
VIRUSTOTAL	vt-001	Disabled	✗ Error	http://0.0.0.0:5007/engines/virustotal/	2018-03-08 14:59:17	
VIRUSTOTAL	vt-docker-001	Enabled	✗ Error	http://0.0.0.0:5107/engines/virustotal/	2018-03-08 14:59:17	

+ Add a new scan engine
* Refresh scan engine status
* Disable Auto-refresh scan engine status

PatrOwl Manager | 1.0.0-BETA, 2018

Engines status:

Engines states are regularly updated and always shown in the footer:

Engines status:



PatrOwl Manager - Engine policy views

Create, copy, modify or delete
engine policies
Quick policy info retrieving

PatrOwl Manager Assets - Findings - Scans - Engines - Rules - Search admin

engines / policies

Engine Name	Name (i: policy file included)	Last update	Actions
ARACHNI	XSS Vulnerability scan	2017-10-19	
CORTEX	CX / Abuse_Finder_2_0 +MaxMind_GeoIP_3_0	2018-01-22	
NMAP	List all open TCP ports	2018-01-07	
OWL_DNS	Get Whois	2018-02-19	
OWL_LEAKS	Search leaks in Github from 2017-01-01	2018-03-13	
OWL_LEAKS	Search leaks on Twitter	2018-03-16	
URLVOID	Check e-reputation of Web Site	2017-10-19	
VIRUSTOTAL	VT / Check Domain	2017-10-10	
VIRUSTOTAL	VT / Check IP	2017-10-10	
VIRUSTOTAL	VT / Check URL	2017-10-10	

+ Add a new policy * Export selected policies or * Export all policies # Import policies

PatrOwl Manager (1.0.0-BETA), 2018 Engines status:

Engine policy details:

PatrOwl Manager Assets - Findings - Scans - Engines - Rules - Search

Edit an engine policy

Engine ARACHNI

Name XSS Vulnerability scan

Description XSS Vulnerability scan

Options `{"jsons":true, "link_templates":[]}`
Enter valid JSON

File Choisir un fichier Aucun fichier choisi

Scopes

- Network Infrastructure
- System Infrastructure
- Domain
- Web App
- HTTPS & Certificates
- E-Reputation
- Malware
- Availability
- Dataleaks

Update policy



Contribution needed !!

Who's up for:

- **Test it** and give us
feedbacks !
- **Contribute !**
 - New engines
 - Debug
 - Features ??

- **Joining the core team ?**
 - Dev[Sec]Ops, Security engineer, Cloud Architect, UX/UI Designer, QA Tester, Wonder-Woman (Batman is tolerated too) ...



Q&A

**We have
questions !?!**

**We want a
demo !?!**

**Stop talking bro !
We want
a break now !?!**

Contacts

More details ? Meet us ? Contributing ? Want a demo ? Want an awesome sticker ? Share a beer ? Requesting an online demo account (BETA test) ?

Find us everywhere on earth:

Mail: getsupport@patrowl.io

Web: <https://patrowl.io>

Twitter: [@patrwl_io](https://twitter.com/@patrwl_io) (Follow us !)

GitHub: [@Patrowl](https://github.com/@Patrowl) (Star and fork us !)