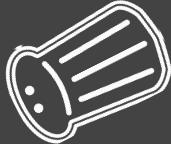


TLP: WHITE  
Pass The Salt 2019



# PatrOwl

SecOps orchestration with an open-source SOAR platform

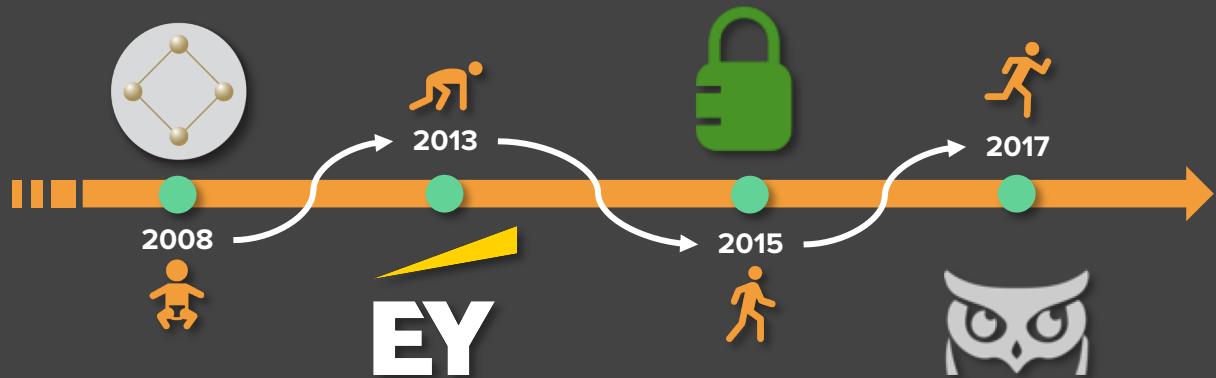
#SOA(R) #SecOps #OpenSource #PreventiveSecurity  
2019.07.03

© 2019 – Nicolas Mattiocco – **GreenLock Advisory**  
All Rights Reserved.  
Contact [getsupport@patrowl.io](mailto:getsupport@patrowl.io) for more

# Let me introduce myself



Nicolas MATTIOCCH  
@MaKyOtOx  
34 y/o



- ▶ Freelancer 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, IssurTech

The image displays three screenshots of the PatrOwl Manager web application, illustrating its features for asset management, finding details, and scan history.

- Top Screenshot: Asset Management Overview**
  - Assets defined:** 86
  - New findings:** 405
  - Active score:** 0
  - Active rules:** 1
  - Action engines:** 7

Key sections include:
  - Asset grades:** Grade (Low, Medium, High) vs Criticity (A-F).
  - Most critical assets:** Grade Value (e.g., 750), Score (e.g., 520), and a list of findings (e.g., Intra-int-bdf-int-local, https://game.appspot.com/level1/frame).
  - Findings by criticity:** A pie chart showing the distribution of findings across High, Medium, Low, and Info levels.
  - Most critical findings:** A table listing findings with their severity, title, and asset.
- Middle Screenshot: Finding Details**
  - Name:** XSS Testing site (url)
  - Description:** https://xss-game.appspot.com/level1/frame
  - Tags:** XSS, Testing, + add
  - Created at:** 2018-02-20
  - Download report:** json -> html -> pdf -> raw

**Findings Stats:** High (red), Medium (orange), Low (yellow).  
# Findings: 3 (3 times, 0:0:0)  
# Findings with CVSS: 7.0 : 2  
# Scans related: 2 performed, 0 defined, 0 currently running  
# Scans from engines: ARACHNI-3
- Bottom Screenshot: Scan History**
  - Scans:** A timeline showing scans performed on [back].
  - Selection:** 3 scan(s) on 21/21/2018 - 16:00 (1h)
  - Scan Details:**
    - [ARACHNI] Check Arachni XSS policy
    - [OWF LEAKS] Search BDF leaks on GitHub
    - [OWF LEAKS] Search BDF leaks on Twitter

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



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

## Security Incident Management

**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 & misc.
- 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)



How to face these bigger, better, badder threats ?

What about  
**Automation and  
Orchestration ?**



How to face these bigger, better, badder threats ?



# 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**

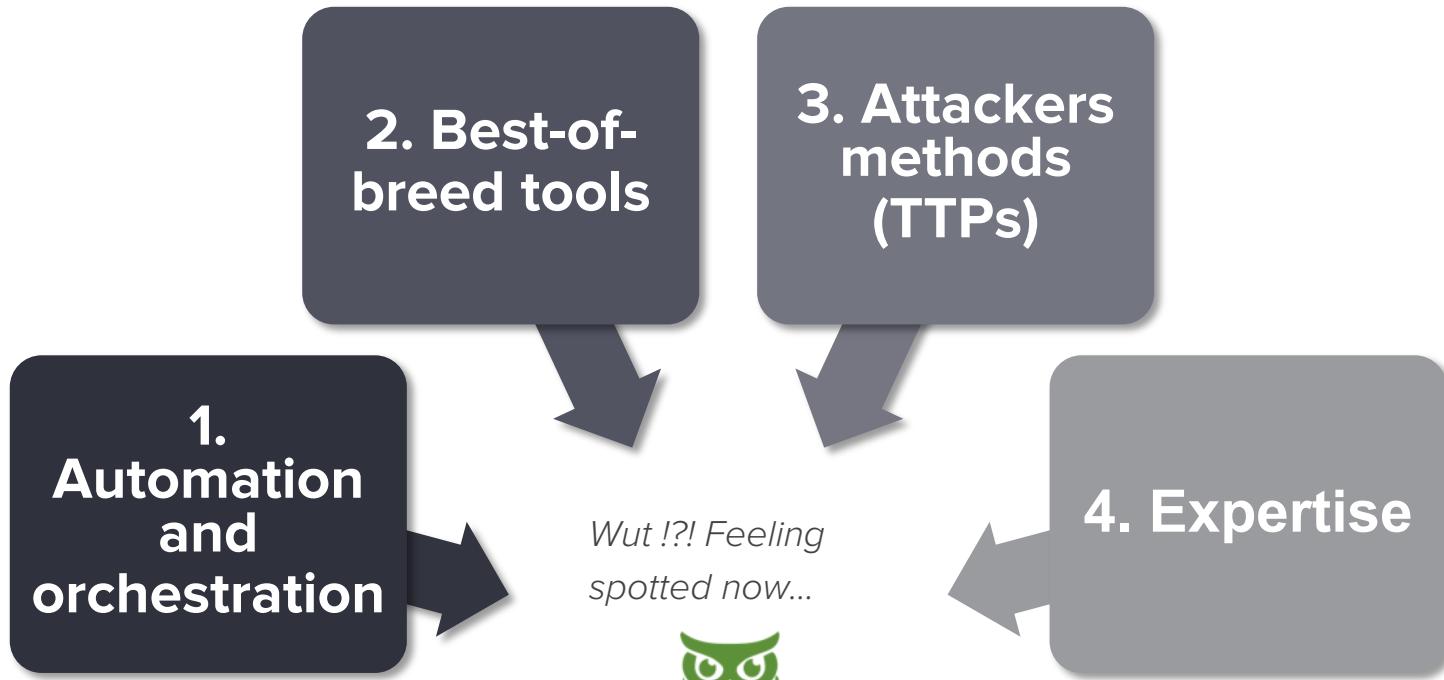




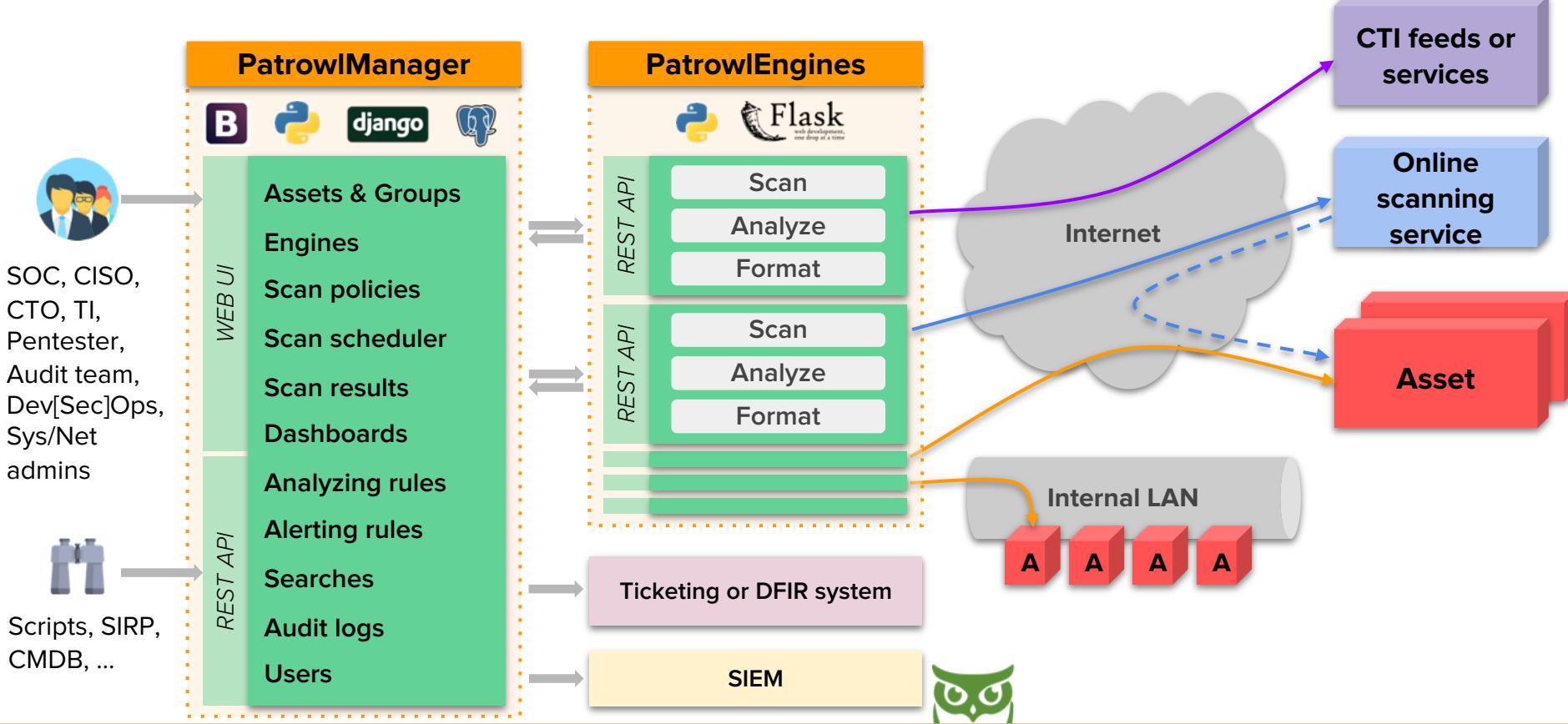
gifbin.com

# PatrOwl's incentives

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

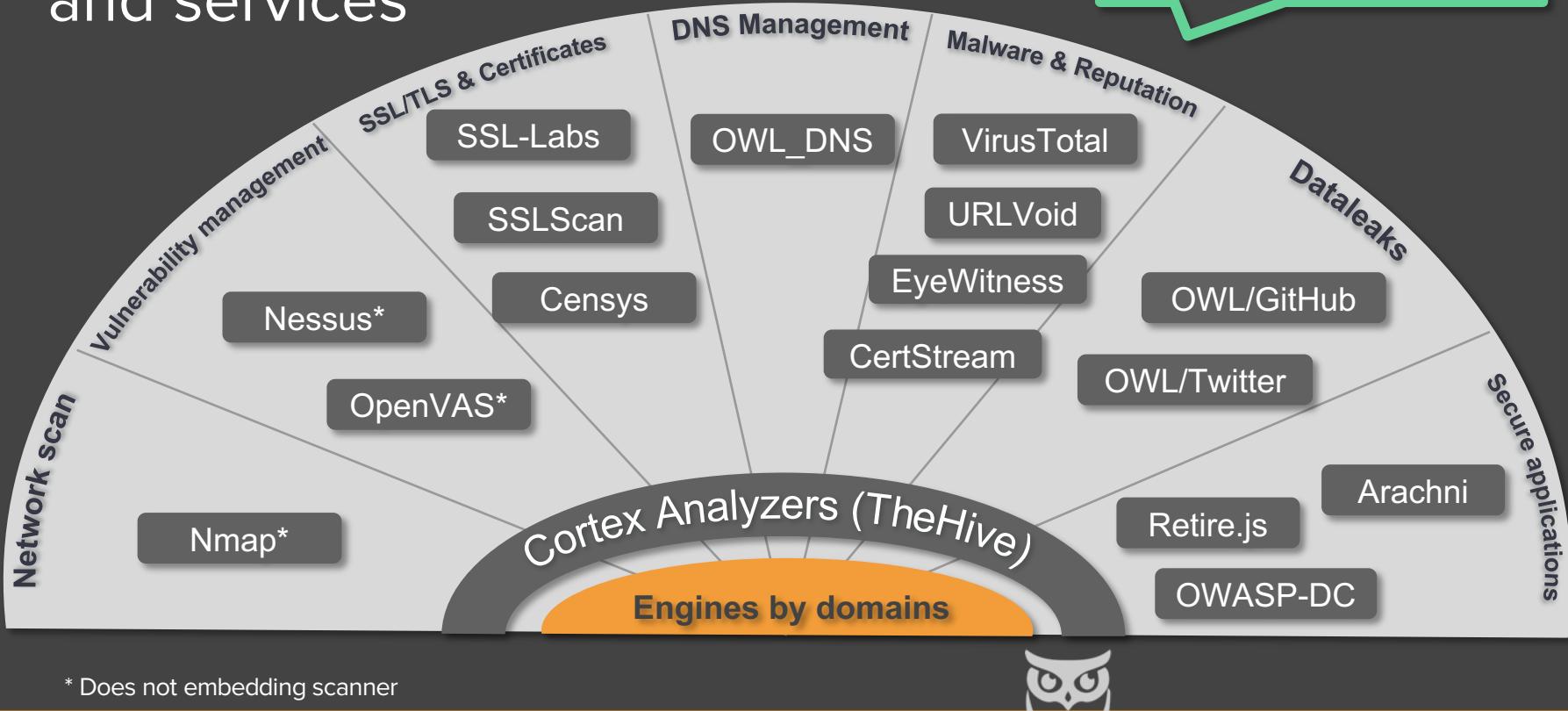


# PatrOwl: Technical architecture



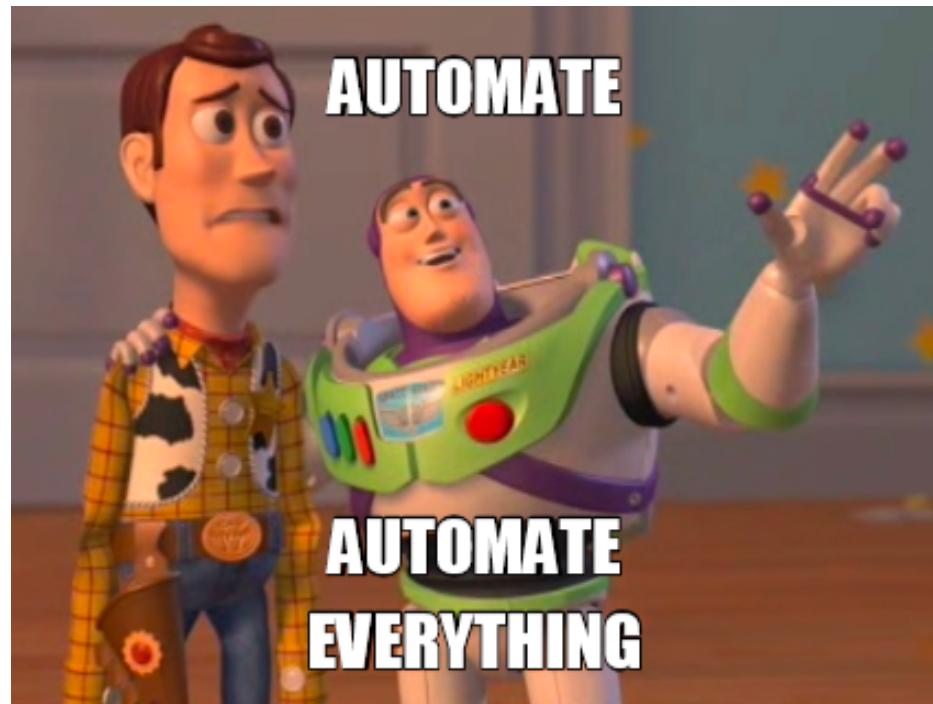
# PatrowlEngines: Supported tools and services

Turnkey micro-apps:  
Docker images +  
REST-API



# ■ Next engines in the pipeline (to be confirmed)

- **Vulnerability management:**  
OpenVas, Qualys, Rapid7 IVM
- **Pasties:** AIL-Framework (CIRCL)
- **CTI:** MISP, Shodan.io, Onyphe.io
- **WEB:** Acunetix, Burp, WPScan,  
DroopScan
- **Containers:** AquaSec, CLAIR, Jfrog  
Xray
- **Dataleaks:** Git/truffleHog
- **Cloud:** Scout2, CloudSploit
- ... Any other idea ?



# 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



# 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)
- Documenting (endlessly too !) + scan templates
- ...
- Building an Enterprise solution (Cloud and on-premise). Stay tuned !
  - Pro features: LDAP/AD/SAML/OAuth authentication, Asset sync., Cloud security assessment engines, awesome dashboards, ...



**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 ?**
- **Funding 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) ?

Find us everywhere on earth:

**Now:** Just in front of you

**Mail:** [getsupport@patrwl.io](mailto: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 !)

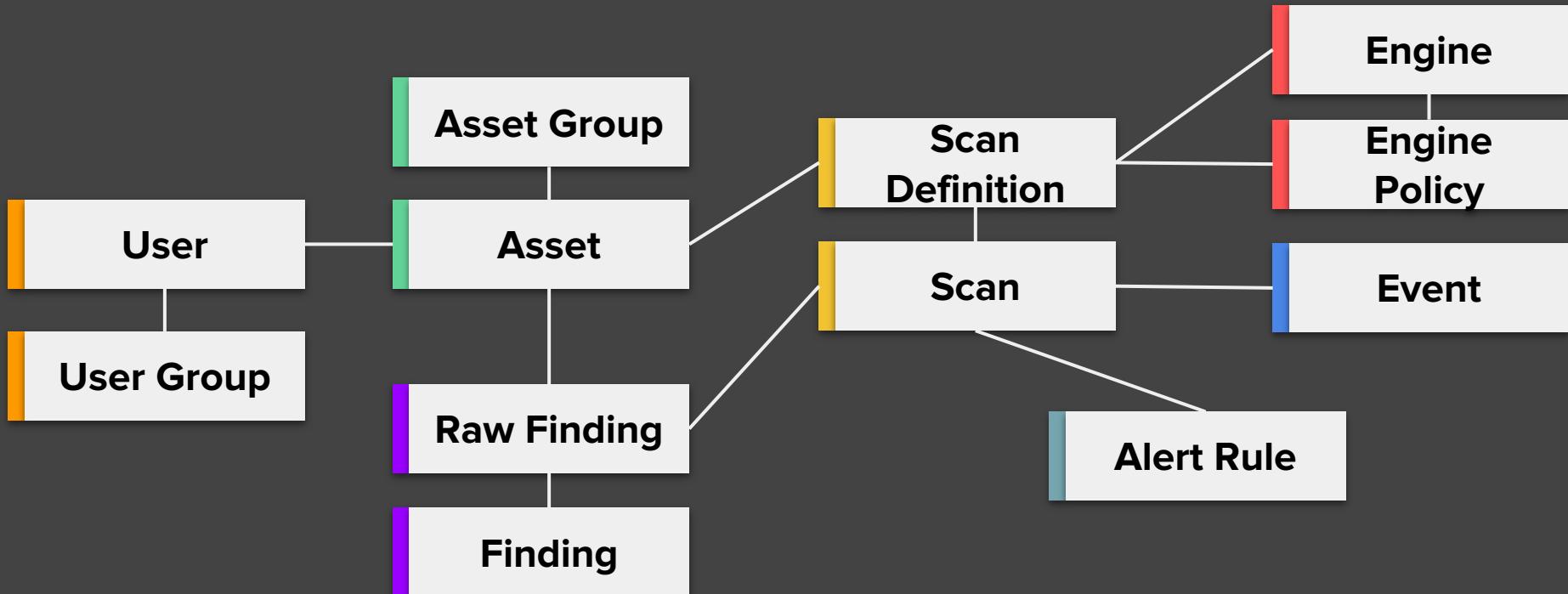
# Before you ask: Why PatrOwl is named “PatrOwl” ?



- 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

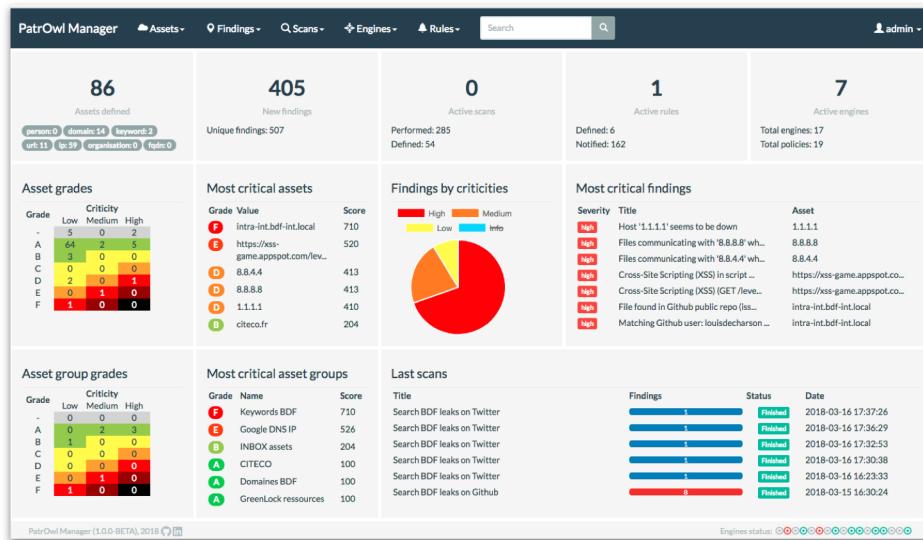
Most critical findings

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	Type	Severity	Status	From	Last update	Actions	
<input type="checkbox"/> Title	xss	high	new	ARACHNI	2018-02-24		
<input type="checkbox"/> Cross-Site Scripting (XSS) (GET /level1/frame [query])	xss_script_context	high	new	ARACHNI	2018-02-24		
<input type="checkbox"/> Cross-Site Scripting (XSS) in script context (GET /level1/frame [query])							
<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 PatrOwl Manager. At the top, there's a navigation bar with links for Assets, Findings, Scans, Engines, Rules, and a search bar. Below the title 'Add a new scan definition', there are fields for 'Title' (with placeholder 'Enter a title...'), 'Description' (placeholder 'Enter a quick description...'), and 'Scan Type' (with 'On-demand' selected). There are also buttons for 'Periodical' and frequency selection ('freq.' and 'Days'). Under 'Start scan', there are buttons for 'Later', 'Now', 'Scheduled at', and a date picker. A 'Search asset(s)' field contains 'Google DNS'. Below it, under 'Asset(s) selected:', there's a checked checkbox for 'Google DNS IP (group)'. A 'Filter by Engine:' section lists engines: All, NMAP, NESSUS, ARACHNI, VIRUSTOTAL, OWL\_DNS, SSLLABS, URLVOID, CORTEX, and OWL\_LEAKS. Another section, 'Or, Filter by Category:', lists categories: 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 right is a large orange 'Create a new scan' button.



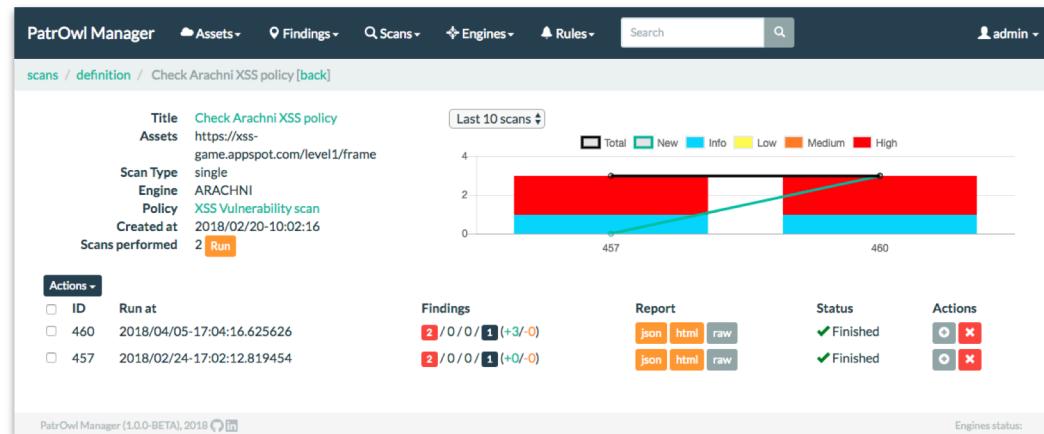
# PatrOwl Manager - Scan definition view

## 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]

Title	Cortex demo CX / Abuse_Finder_2_0 +MaxMind_GeoIP_3_0	Findings by severity:	Title	Cortex demo CX / Abuse_Finder_2_0 +MaxMind_GeoIP_3_0	Findings by severity:
Started at	2018/01/23-22:01:41		Started at	2018/01/23-22:01:03	
Finished at	2018/01/23-22:01:00		Finished at	2018/01/23-22:01:25	
Status	Finished		Status	Finished	
Engine	CORTEX / cx-001		Engine	CORTEX / cx-001	
Asset	Title	Severity	Asset	Title	Severity
<input type="checkbox"/> 8.8.4.4	<a href="#">Abuse_Finder: Address=abuse@level3.com</a>		<input type="checkbox"/> 8.8.4.4	<a href="#">Abuse_Finder: Address=network-abuse@google.com</a>	
<input type="checkbox"/> 8.8.4.4	<a href="#">Abuse_Finder: Address=network-abuse@google.com</a>		<input checked="" type="checkbox"/> 8.8.4.4	<a href="#">Abuse_Finder_2_0 full results (HASH: 722ea)</a>	
<input type="checkbox"/> 8.8.4.4	<a href="#">Artefacts from 'Abuse_Finder_2_0' analyzer (HASH: 985ccb)</a>		<input type="checkbox"/> 8.8.4.4	<a href="#">Artefacts from 'MaxMind_GeoIP_3_0' analyzer (HASH: 65cead)</a>	
<input type="checkbox"/> 8.8.4.4	<a href="#">Artefacts from 'MaxMind_GeoIP_3_0' analyzer (HASH: 65cead)</a>		<input type="checkbox"/> 8.8.4.4	<a href="#">MaxMind: Location="United States/North America"</a>	
<input type="checkbox"/> 8.8.4.4	<a href="#">MaxMind: Location="United States/North America"</a>		<input type="checkbox"/> 8.8.8.8	<a href="#">Abuse_Finder: Address=network-abuse@google.com</a>	
<input checked="" type="checkbox"/> 8.8.8.8	<a href="#">Abuse_Finder: Address=abuse@level3.com</a>		<input checked="" type="checkbox"/> 8.8.8.8	<a href="#">Abuse_Finder_2_0 full results (HASH: f1a2fd)</a>	
<input type="checkbox"/> 8.8.8.8	<a href="#">Abuse_Finder: Address=network-abuse@google.com</a>		<input type="checkbox"/> 8.8.8.8	<a href="#">Artefacts from 'Abuse_Finder_2_0' analyzer (HASH: e29f1a)</a>	
<input type="checkbox"/> 8.8.8.8	<a href="#">Abuse_Finder_2_0 full results (HASH: 793b66)</a>		<input type="checkbox"/> 8.8.8.8	<a href="#">Artefacts from 'MaxMind_GeoIP_3_0' analyzer (HASH: a1c144)</a>	
<input type="checkbox"/> 8.8.8.8	<a href="#">Artefacts from 'Abuse_Finder_2_0' analyzer (HASH: d334ac)</a>		<input type="checkbox"/> 8.8.8.8	<a href="#">MaxMind: Location="United States/North America"</a>	
<input type="checkbox"/> 8.8.8.8	<a href="#">Artefacts from 'MaxMind_GeoIP_3_0' analyzer (HASH: a1c144)</a>		<input type="checkbox"/> 8.8.8.8	<a href="#">MaxMind_GeoIP_3_0 full results (HASH: c05095)</a>	
// 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

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

The screenshot shows the PatrOwl Manager interface for a scan titled "Check Arachni XSS policy". The main dashboard displays findings, assets, and events. On the left, there are tabs for Assets (1), Asset groups (0), Findings (3), and Events (0). The Findings section lists three items:

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]

On the right, the "Scan details" panel provides specific information about the scan:

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:	2018/02/24-17:02:59
Eapsed:	0:00:43.152597
Reports:	[json] [HTML] [raw]

The "Findings summary" section shows metrics:

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

The "Repartition per severity" section is represented by a donut chart with four segments: High (red), Medium (orange), Low (yellow), and Info (blue).

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

Engines status: [Green 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    Assets ▾    Findings ▾    Scans ▾    Engines ▾    Rules ▾    Search    admin ▾

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
<input type="checkbox"/> Title	✓	9	2018-03-27	<a href="#">details</a> <a href="#">Run</a> <a href="#">X</a>
<input type="checkbox"/> [NMAP] List open ports on Google DNS	✓	1	2018-03-21	<a href="#">details</a> <a href="#">Run</a> <a href="#">X</a>
<input type="checkbox"/> [OWL_LEAKS] Search BDF leaks on Twitter	✓	1	2018-03-16	<a href="#">details</a> <a href="#">Run</a> <a href="#">X</a>
<input type="checkbox"/> [OWL_LEAKS] Search BDF leaks on Twitter	✓	1	2018-03-16	<a href="#">details</a> <a href="#">Run</a> <a href="#">X</a>
<input type="checkbox"/> [OWL_LEAKS] Search BDF leaks on Twitter	✓	1	2018-03-16	<a href="#">details</a> <a href="#">Run</a> <a href="#">X</a>
<input type="checkbox"/> [OWL_LEAKS] Search BDF leaks on Twitter	✓	1	2018-03-16	<a href="#">details</a> <a href="#">Run</a> <a href="#">X</a>
<input type="checkbox"/> [OWL_LEAKS] Search BDF leaks on Github	✓	1	2018-03-16	<a href="#">details</a> <a href="#">Run</a> <a href="#">X</a>
<input type="checkbox"/> [OWL_LEAKS] Search BDF leaks on Github	✓	8	2018-03-16	<a href="#">details</a> <a href="#">Run</a> <a href="#">X</a>
<input type="checkbox"/> [OWL_LEAKS] Search BDF leaks on Github	✓		2018-03-15	<a href="#">details</a> <a href="#">Run</a> <a href="#">X</a>
<input type="checkbox"/> [OWL_LEAKS] Search BDF leaks on Github	✓		2018-03-15	<a href="#">details</a> <a href="#">Run</a> <a href="#">X</a>
<input type="checkbox"/> [OWL_LEAKS] Search BDF leaks on Github	✓	5	2018-03-21	<a href="#">details</a> <a href="#">Run</a> <a href="#">X</a>

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

Page 1 of 29. [next](#)

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

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 engine

## Change functional state

View engine info, including current scans performed

# Refresh engines states

## Enable/Disable the auto-refresh

PatrOwl Manager		Assets	Findings	Scans	Engines	Rules	Search	admin -
engines / Instances								
Type	Name	Funct.	Status	Oper.	State	API URL	Last update	Actions
ARACHNI	arachni-001		Disabled		✗ Error	http://0.0.0.5005/engines/arachni/	2018-03-08	<span>○</span> <span>●</span> <span>○</span> <span>✗</span> <span>Enable</span>
ARACHNI	arachni-docker-001		Enabled		✗ Error	http://0.0.0.5105/engines/arachni/	14:59:17	<span>○</span> <span>●</span> <span>○</span> <span>✗</span> <span>Disable</span>
CORTEX	cx-001		Disabled		✗ Error	http://0.0.0.5009/engines/cortex/	2018-03-01	<span>○</span> <span>●</span> <span>○</span> <span>✗</span> <span>Enable</span>
CORTEX	cx-docker-001		Enabled		✗ Error	http://0.0.0.5109/engines/cortex/	14:59:17	<span>○</span> <span>●</span> <span>○</span> <span>✗</span> <span>Disable</span>
NESSUS	nessus-001		Disabled		✗ Error	http://0.0.0.5002/engines/nessus/	2018-03-08	<span>○</span> <span>●</span> <span>○</span> <span>✗</span> <span>Enable</span>
NESSUS	nessus-docker-001		Enabled		✗ Error	http://0.0.0.5102/engines/nessus/	14:59:17	<span>○</span> <span>●</span> <span>○</span> <span>✗</span> <span>Disable</span>
NMAP	nmap-002		Disabled		✗ Error	http://0.0.0.5001/engines/nmap/	2018-03-08	<span>○</span> <span>●</span> <span>○</span> <span>✗</span> <span>Enable</span>
NMAP	nmap-docker-001		Enabled		✗ Error	http://localhost:5101/engines/nmap/	14:59:17	<span>○</span> <span>●</span> <span>○</span> <span>✗</span> <span>Disable</span>
OWL_DNS	odns-002		Disabled		✗ Error	http://0.0.0.5006/engines/owl_dns/	2018-03-08	<span>○</span> <span>●</span> <span>○</span> <span>✗</span> <span>Enable</span>
OWL_LEAKS	oleaks-001		Enabled		✗ Error	http://127.0.1:5012/engines/owl_leaks/	14:59:17	<span>○</span> <span>●</span> <span>○</span> <span>✗</span> <span>Disable</span>
OWL_DNS	owldns-docker-001		Enabled		✗ Error	http://0.0.0.5106/engines/owl_dns/	14:59:17	<span>○</span> <span>●</span> <span>○</span> <span>✗</span> <span>Disable</span>
SSLABSLABS	sslabs-001		Disabled		✗ Error	http://0.0.0.5004/engines/sslabs/	2018-03-09	<span>○</span> <span>●</span> <span>○</span> <span>✗</span> <span>Enable</span>
SSLABSLABS	sslabs-docker-001		Enabled		✗ Error	http://0.0.0.5104/engines/sslabs/	14:59:17	<span>○</span> <span>●</span> <span>○</span> <span>✗</span> <span>Disable</span>
URLVOID	urlvoid-docker-001		Enabled		✗ Error	http://0.0.0.5108/engines/urlvoid/	14:59:17	<span>○</span> <span>●</span> <span>○</span> <span>✗</span> <span>Disable</span>
URLVOID	uvoid-001		Disabled		✗ Error	http://0.0.0.5008/engines/urlvoid/	2018-03-01	<span>○</span> <span>●</span> <span>○</span> <span>✗</span> <span>Enable</span>
VIRUSTOTAL	vt-001		Disabled		✗ Error	http://0.0.0.5007/engines/virustotal/	2018-03-08	<span>○</span> <span>●</span> <span>○</span> <span>✗</span> <span>Enable</span>
VIRUSTOTAL	vt-docker-001		Enabled		✗ Error	http://0.0.0.5107/engines/virustotal/	14:59:17	<span>○</span> <span>●</span> <span>○</span> <span>✗</span> <span>Disable</span>

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@patrwl.io](mailto: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 !)