



Security Operations Orchestration

The next stage of proactive and efficient threat management

June 2018

© 2018 - Nicolas Mattiocco (GreenLock Advisory)
All Rights Reserved.
Contact getsupport@patrowl.io for more

Cyber-Security challenges

Trends

Assets exposed



Threats

Vulnerabilities | Attackers |
Security incidents



Business impacts
of security incidents



Facts & Challenges

1. Cyber-security **mediatisation** causes high visibility of vulnerabilities and easiness of attacks
2. Poor **visibility** on Cyber-exposure risks
3. Security **tools** exists, largely adopted but ineffective without proper strategy, expertise and processes
4. Need to monitor a large, diversified, unmanaged and complex **scope**, even others assets
5. Scarceness of efficient **resources** in cyber-security
6. Tool capacity-based **approach** rather a business threats-based approach

Cyber-Exposure and risks are continuously growing and fastly changing



Cyber-Security challenges

Security Incidents

Precursors (may occur)

Indicators (have occurred or is happening now)

Events monitoring reveals vulnerabilities and suspicious changes

Infosec KB updates

- CVE, CVSS, CPE updates
- Unsecure configuration
- Exploit releasing
- New detection method: scanner update, new tool released, policy updates, infosec researches
- IOC published

Assets updates

- Application or system updates
- Infrastructure changes: open/closed ports, new subdomain detection
- IP or domain assignment

Ext. resource updates

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

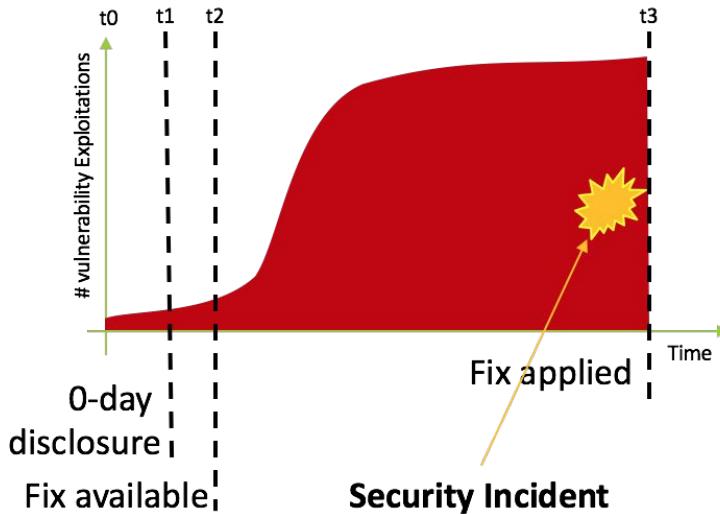


Our vision

Legend:
Risk exposure window = $t_3 - t_0$
Time-to-Patch = $t_3 - t_2$
Red area = threat occurrence

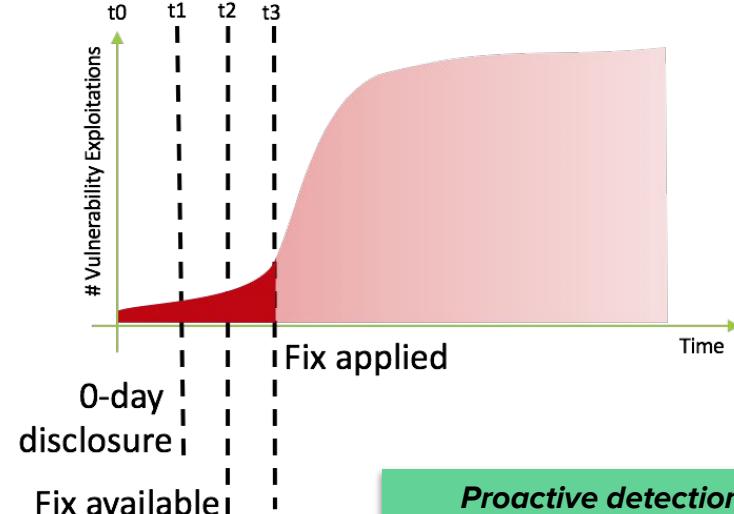
Incident-Based Process

■ Limited and inefficient strategy



Managed Security Process

■ Efficient strategy



Our vision

We need to efficiently moving from a proactive to a predictive security posture

**Thinking and acting
like hackers**

Using their mindset (tools, tactics and procedures), full-stack targeting

**Security automation
and orchestration**

Enable to continuously scan an organisation's environment for any changes that might indicate a potential threat

**Best-of-breed and
custom tools**

Unique cockpit and rationalized use of best-of-breed and custom tools to support the cyber-threat monitoring strategy and remediation workflow

Cyber Exposure assessment objectives:

- Identify the vulnerabilities before attackers
- Identify the risk exposure as seen by 3rd parties
- Identify early warning signs of threat scenarios
- Identify compromising of assets or data leaks ASAP

Monitoring scope:

- Company's known and unknown assets
- External resources (ex: Threat intelligence feeds)
- Attackers' assets



Our vision





Provide a centralized platform to :

- Full-stack security overview (IP to Data)
- Define threat intelligence & vulnerability assessment scans policies
- Orchestrate scans using tailor-made engines
- Collect & aggregate findings
- Contextualize, tracks, prioritize findings
- Check remediation effectiveness

The screenshot displays several panels of the PatrOwl Manager interface:

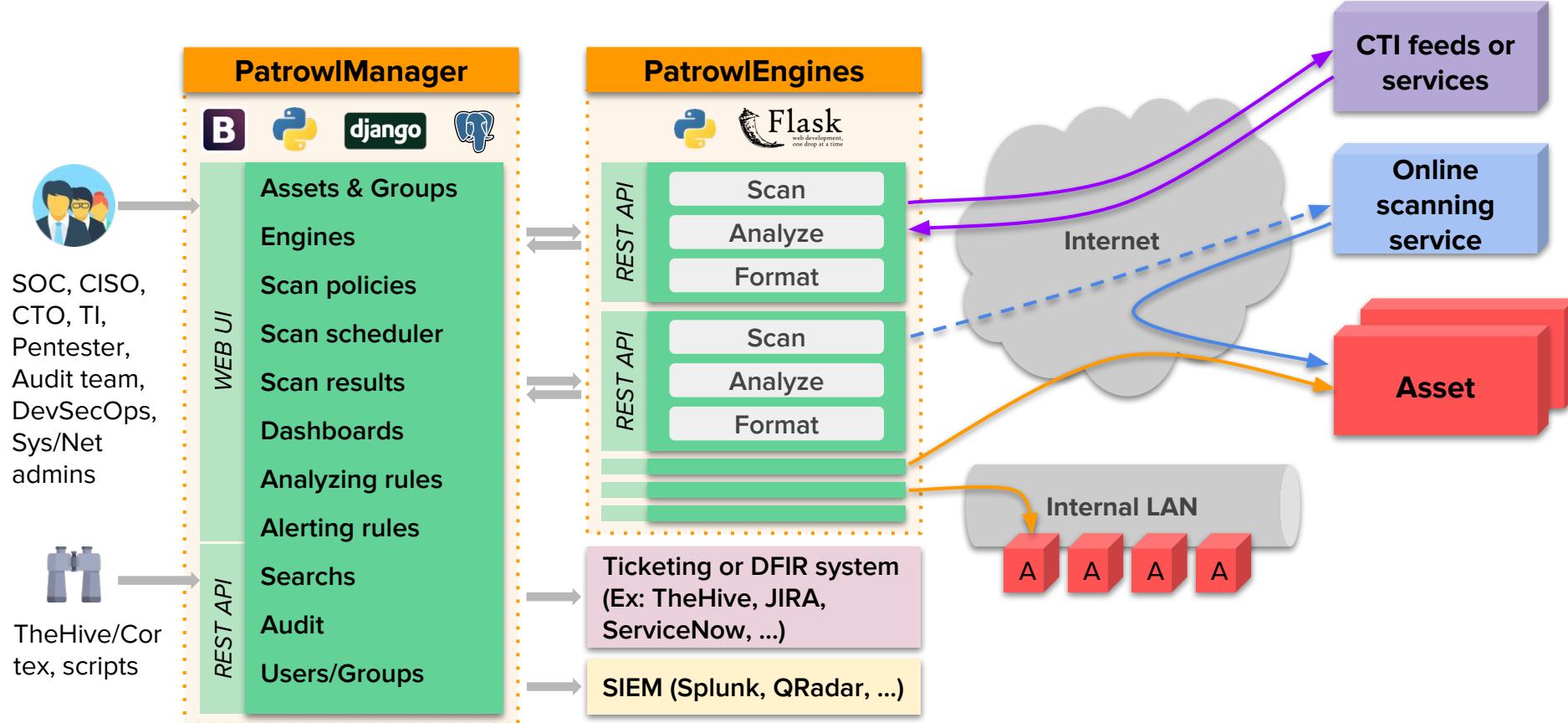
- Top Dashboard:** Shows key metrics: Assets defined (86), New findings (405), Active scans (0), Active rules (1), and Active engines (7). It also includes sections for Asset grades, Most critical assets, Findings by criticities (a pie chart showing High: 710, Medium: 520, Low: 13, Info: 294), and Most critical findings.
- Asset Group Grades:** A grid showing asset group grades across Low, Medium, and High criticity levels.
- Most Critical Asset Groups:** A list of groups with their names, scores, and descriptions.
- Last Scan:** A summary of the last scan including title, status, date, and findings.
- Findings Details:** A detailed view of a specific finding (XSS Testing site URL) with fields for Name, Value, Description, Tags, Criticity, Created at, and Download report.
- Findings Stats:** A summary of findings statistics including High (2), Medium (1), Low (0), and Info (1).
- Global Security Rating:** An overall rating of E with trends for -1d, -1w, and -1m.
- Findings Tab:** A table listing findings categorized by Type (xss, xss_script_context, sitemap), Severity (high, new), Status (new), From (ARACHNI), Last update (various dates), and Actions (details, Run, Stop).
- Scans Tab:** A table listing scans performed with columns for Title, Status, Progress, Last update, and Actions (details, Run, Stop).
- Scans Timeline:** A timeline showing scan activity from 28 Feb to 22 Mar.

Users:

- CERT/SOC, CTO, CISO, Risk Manager, Audit teams, Penetration testers, Webmasters, Network and system engineers, Q&A teams, Business & App owners



Technical overview



Supported Engines (June 2018)

Tool	Description	System infra.	Network infra.	Domains	HTTPS & Certificates	E-Reputation	Data leaks	Malware	Web Applications
<i>NMAP</i>	Network scanner	✗	✗						
<i>Tenable Nessus</i>	Vulnerability assessment (Nessus Scanner only)	✗	✗		✗				
<i>Arachni</i>	Web Vulnerability scanner								✗
<i>Censys</i>	Internet-wide data scanner			✗	✗				
<i>VirusTotal</i>	Online malware and artefact analyzer			✗		✗		✗	
<i>UrlVoid</i>	Website Reputation Checker				✗	✗	✗		✗
<i>Qualys SSL-Labs</i>	TLS/SSL configuration scanner			✗	✗				



Supported Engines (June 2018)

Tool	Description	System infra.	Network infra.	Domains	HTTPS & Certificates	E-Reputation	Data leaks	Malware	Web Applications
<i>OwlDNS</i>	(Sub-)Domain analyzer			✗		✗			
<i>OwlLeaks</i>	Data scrapper on Google, GitHub, Twitter, ...						✗		
<i>OwlCode</i>	Retire.js and OWASP-DC analyzer								✗
<i>Cortex</i>	TheHive companion (30+ analyzers)	✗	✗	✗	✗	✗	✗	✗	✗



PatrOwl Engines ?

- An engine uses local binaries, scripts or remote services
- Data analysis are performed on the results, then findings are formatted in a generic format
- Custom engines can be connected to the back-end:
 - JSON REST API with strictly formatted inputs and outputs and a strict (but simple) workflow
 - A meta-engine is provided
 - Full documentation is in progress
 - Token and Basic authentication features will be soon supported
- ≈1 day needed for writing a simple engine
- All submitted engines by the community is be tested by SurvivOwl' engineers before being officially released



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 of internal systems

Orchestrate regular scans on a fixed perimeter, check changes (asset, vulnerability, criticality)

Attacker assets monitoring

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

Monitoring Internet-faced 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, paste, VirusTotal submissions, phishing reports, ...

Regulation and Compliance

Evaluate compliance gaps using provided scan templates

Penetration tests

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

Continuous Integration / Continuous Delivery

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



Business Model

Products

Open-source release

Github repository

Marketplace

Engines, policies, AI rules, dashboards

Premium release - SaaS services

Shared or dedicated servers

Premium release - On-Premise

Appliance or Docker

Private Threat Intelligence feeds

Risk Scorecards

Marketplace

Advanced AI rules, policies, dashboards

Services

Community services

Documentation
Support
Bug fixes + features

Premium Support

Private ticketing, chats, phone
Documentations + Trainings

R&D

Custom developments,
Threat Intelligence services

Consulting

SOC/CTI Strategy,
product integration or review,
security audits, investigations

Free

Paying (Contact GreenLock Advisory)



Competitors



spiderfoot



Greenbone

Adaptability

Core market



Kenna



CRONUS



PatrOwl



NormShield

Techno-based

Risk-based

PENTESTON
Stay secure

Qualys.

SecurityCenter SCTM
tenable.ioTM

Specialized

Competitors

	SaaS	On-Premise	Open-Source
 PatrOwl	✓	✓	✓
 spiderfoot	✓	✓	✓
 Kenna	✓	✓	✓
 NormShield	✓	✓	✓
 Greenbone Sustainable Resilience	✓	✓	✓
 Qualys	✓	✓	✓
 SecurityCenter SC™	✓	✓	✓
 tenable.io	✓	✓	✓

Competitive advantages



Cost-Effective

Rationalize tools integration, product licenses and skills



Time-To-Value

Ease of use and deployment, default policies and engines policies



Adaptability & Scalability

REST API, Open-Source connectors, adaptable to organisation maturity level



360° overview

Full cyber-Exposure assessment in real-time with relevant data



Always updated

Vulnerability KB, detection methods, threat scenario

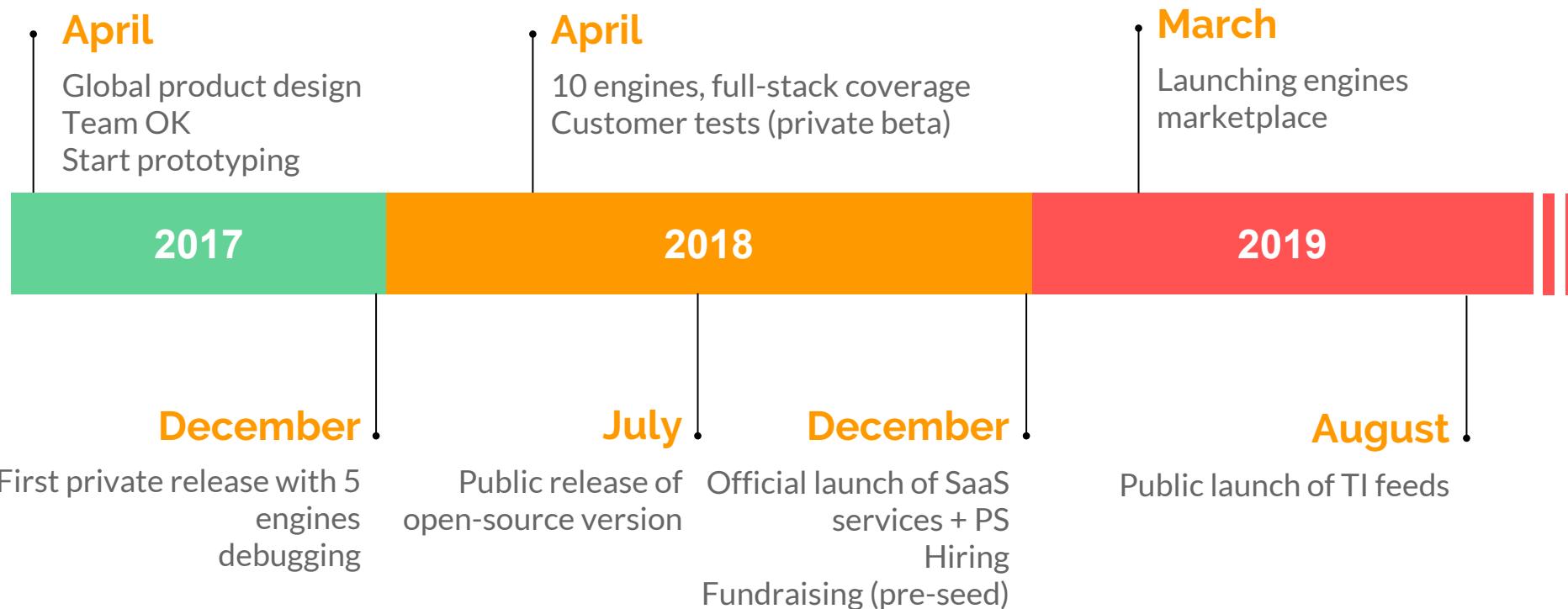


Made by experts

Our team members are A+ security engineers



(Very) Big milestones



Contacts

More details ? Requesting a demo ? Meet us ?

Find us everywhere (no excuses !)

- Email: getsupport@patrowl.io
- Website: <https://www.patrowl.io>
- Twitter: [@patrowl_io](https://twitter.com/@patrowl_io)
- GitHub: [@Patrowl](https://github.com/@Patrowl)

Logos



#76A144

#616161

#FF9900

PatrOwl overview

PatrOwl Manager (Backend)

- Unified platform for managing assets, threats, scans, findings and engines
- Orchestrate scans started on engines

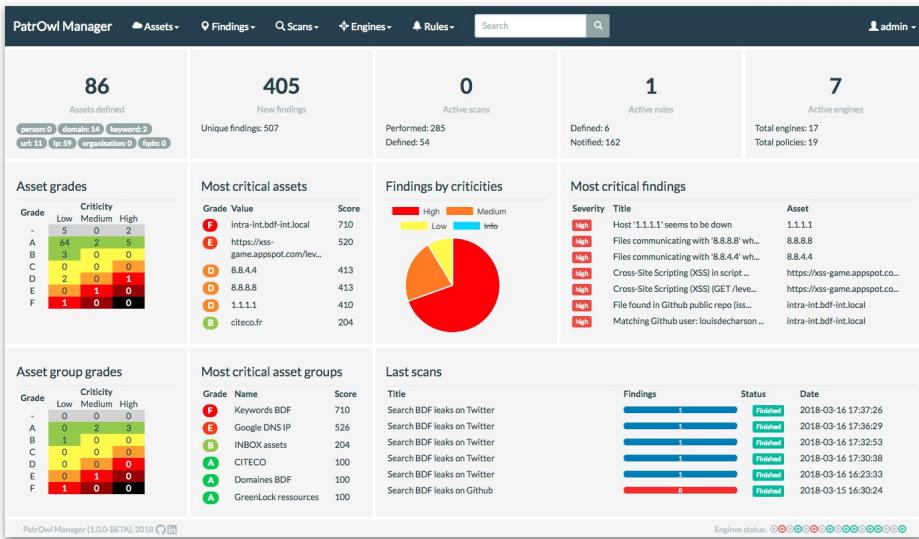
PatrOwl Engines

- REST API
- Perform the scans using locally installed or remote online tools



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 criticity
- Last scans status and results
- Top CVSS Score / Findings
- Top CVE, CWE, CPE, ...



PatrOwl Manager - Asset detailed view

- Current finding counters and 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
- Report to HTML or JSON
 - @todo: PDF

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:** oracle weblogic X + add
- Tags:** oracle weblogic
- Criticality:** medium
- Created at:** 2018-02-20
- Download report:** json · html · pdf · raw

Findings Stats

High	Medium	Low
2	0	0

Findings: 3 (3 new, 0 ack'd.)
Findings with CVSS > 7.0: 2
Scans related: 2 performed, 1 defined, 0 currently running
Scans from engines: ARACHNI: 3

Global Security Rating: E

Trends: -1d, -1w, -1m

Findings (Table):

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

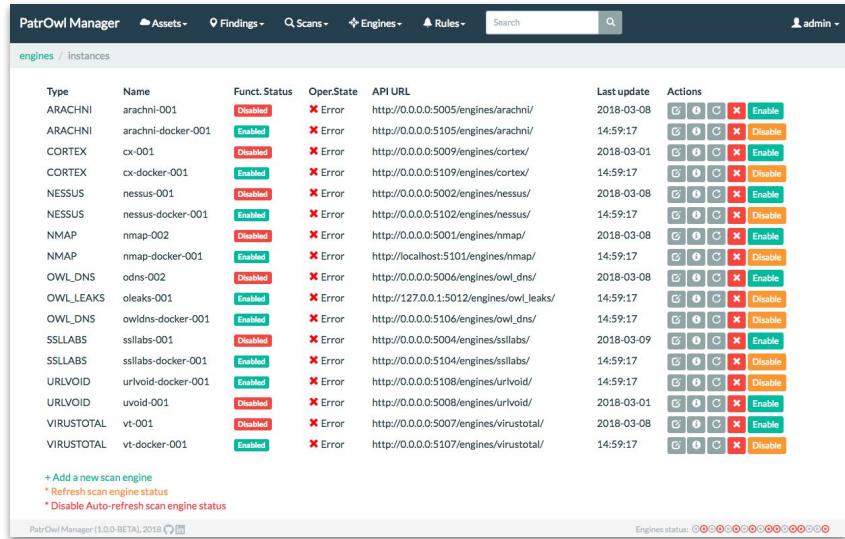
PatrOwl Manager (1.0-BETA), 2018

Engines status:



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



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	<input type="checkbox"/> <input type="button"/> <input type="radio"/> <input type="button"/> <input type="checkbox"/> <input type="button"/> <input type="checkbox"/>
ARACHNI	arachni-docker-001	Enabled	✗ Error	http://0.0.0.0:5105/engines/arachni/	2018-03-01 14:59:17	<input type="checkbox"/> <input type="button"/> <input type="radio"/> <input type="button"/> <input type="checkbox"/> <input type="button"/> <input type="checkbox"/>
CORTEX	cx-001	Disabled	✗ Error	http://0.0.0.0:5009/engines/cortex/	2018-03-01 14:59:17	<input type="checkbox"/> <input type="button"/> <input type="radio"/> <input type="button"/> <input type="checkbox"/> <input type="button"/> <input type="checkbox"/>
CORTEX	cx-docker-001	Enabled	✗ Error	http://0.0.0.0:5109/engines/cortex/	2018-03-08 14:59:17	<input type="checkbox"/> <input type="button"/> <input type="radio"/> <input type="button"/> <input type="checkbox"/> <input type="button"/> <input type="checkbox"/>
NESSUS	nessus-001	Disabled	✗ Error	http://0.0.0.0:5002/engines/nessus/	2018-03-08 14:59:17	<input type="checkbox"/> <input type="button"/> <input type="radio"/> <input type="button"/> <input type="checkbox"/> <input type="button"/> <input type="checkbox"/>
NESSUS	nessus-docker-001	Enabled	✗ Error	http://0.0.0.0:5102/engines/nessus/	2018-03-08 14:59:17	<input type="checkbox"/> <input type="button"/> <input type="radio"/> <input type="button"/> <input type="checkbox"/> <input type="button"/> <input type="checkbox"/>
NMAP	nmap-002	Disabled	✗ Error	http://0.0.0.0:5001/engines/nmap/	2018-03-08 14:59:17	<input type="checkbox"/> <input type="button"/> <input type="radio"/> <input type="button"/> <input type="checkbox"/> <input type="button"/> <input type="checkbox"/>
NMAP	nmap-docker-001	Enabled	✗ Error	http://localhost:5101/engines/nmap/	2018-03-08 14:59:17	<input type="checkbox"/> <input type="button"/> <input type="radio"/> <input type="button"/> <input type="checkbox"/> <input type="button"/> <input type="checkbox"/>
OWL_DNS	odns-002	Disabled	✗ Error	http://0.0.0.0:5006/engines/owl_dns/	2018-03-08 14:59:17	<input type="checkbox"/> <input type="button"/> <input type="radio"/> <input type="button"/> <input type="checkbox"/> <input type="button"/> <input type="checkbox"/>
OWL_LEAKS	oleaks-001	Enabled	✗ Error	http://127.0.0.1:5012/engines/owl_leaks/	2018-03-08 14:59:17	<input type="checkbox"/> <input type="button"/> <input type="radio"/> <input type="button"/> <input type="checkbox"/> <input type="button"/> <input type="checkbox"/>
OWL_DNS	owldns-docker-001	Enabled	✗ Error	http://0.0.0.0:5106/engines/owl_dns/	2018-03-08 14:59:17	<input type="checkbox"/> <input type="button"/> <input type="radio"/> <input type="button"/> <input type="checkbox"/> <input type="button"/> <input type="checkbox"/>
SSL LABS	ssllabs-001	Disabled	✗ Error	http://0.0.0.0:5004/engines/ssllabs/	2018-03-09 14:59:17	<input type="checkbox"/> <input type="button"/> <input type="radio"/> <input type="button"/> <input type="checkbox"/> <input type="button"/> <input type="checkbox"/>
SSL LABS	ssllabs-docker-001	Enabled	✗ Error	http://0.0.0.0:5104/engines/ssllabs/	2018-03-08 14:59:17	<input type="checkbox"/> <input type="button"/> <input type="radio"/> <input type="button"/> <input type="checkbox"/> <input type="button"/> <input type="checkbox"/>
URLVOID	urvoid-docker-001	Enabled	✗ Error	http://0.0.0.0:5108/engines/urvoid/	2018-03-01 14:59:17	<input type="checkbox"/> <input type="button"/> <input type="radio"/> <input type="button"/> <input type="checkbox"/> <input type="button"/> <input type="checkbox"/>
URLVOID	urvoid-001	Disabled	✗ Error	http://0.0.0.0:5008/engines/urvoid/	2018-03-01 14:59:17	<input type="checkbox"/> <input type="button"/> <input type="radio"/> <input type="button"/> <input type="checkbox"/> <input type="button"/> <input type="checkbox"/>
VIRUSTOTAL	vt-001	Disabled	✗ Error	http://0.0.0.0:5007/engines/virustotal/	2018-03-08 14:59:17	<input type="checkbox"/> <input type="button"/> <input type="radio"/> <input type="button"/> <input type="checkbox"/> <input type="button"/> <input type="checkbox"/>
VIRUSTOTAL	vt-docker-001	Enabled	✗ Error	http://0.0.0.0:5107/engines/virustotal/	2018-03-08 14:59:17	<input type="checkbox"/> <input type="button"/> <input type="radio"/> <input type="button"/> <input type="checkbox"/> <input type="button"/> <input type="checkbox"/>

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

PatrOwl Manager | 1.0.0-BETA, 2018

Engines status: 



PatrOwl Manager - Engine policy views

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

The screenshot shows the PatrOwl Manager interface with the 'engines / policies' page selected. The top navigation bar includes links for Assets, Findings, Scans, Engines, Rules, and a search bar. A user 'admin' is logged in. The main content area displays a table of engine 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	

At the bottom, there are buttons for '+ Add a new policy', '* Export selected policies', '* Export all policies', and '# Import policies'. The footer indicates 'PatrOwl Manager (1.0.0-BETA), 2018' and shows an 'Engines status' bar.

- Engine policy details:

The screenshot shows the 'Edit an engine policy' form. The top navigation bar includes links for Assets, Findings, Scans, Engines, Rules, and a search bar. The main content area has the following fields:

- Engine:** ARACHNI
- Name:** XSS Vulnerability scan
- Description:** XSS Vulnerability scan
- Options:** JSON configuration:

```
{"jsons":true, "link_templates":[]}
```

 with a note: "Enter valid JSON"
- File:** Choisir un fichier Aucun fichier choisi
- Scopes:** A list of checkboxes for different scopes:
 - Network Infrastructure
 - System Infrastructure
 - Domain
 - Web App
 - HTTPS & Certificates
 - E-Reputation
 - Malware
 - Availability
 - Dataleaks

A large orange 'Update policy' button is at the bottom right.

PatrOwl Manager - Scan definition creation view

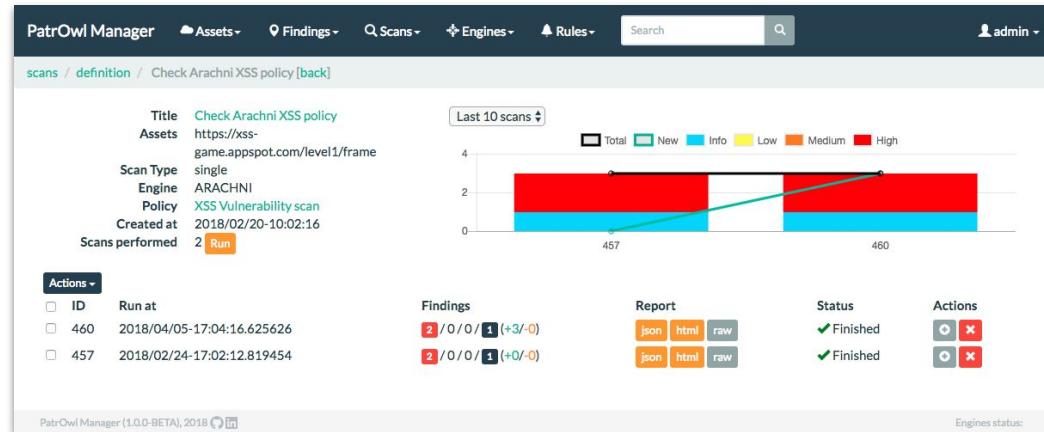
- Search and select asset and asset group on theirs values or names
- Filter policies by engine type or threat domain
- Select engine
 - If no engine is selected, an engine is randomly chosen in available engines for each scan

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 header, the page title is 'scans / add new scan'. 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 frequency dropdowns), and 'Start scan' (radio buttons for 'Later', 'Now', and 'Scheduled at' with a date picker). There's a 'Search asset(s)' input field with a placeholder 'Google DNS' and a search icon. A section for 'Asset(s) selected:' shows a checked checkbox for 'Google DNS IP (group)'. Below that, 'Filter by Engine:' lists engines like All, NMAP, NESSUS, ARACHNI, VIRUSTOTAL, OWL_DNS, SSLABBS, URLVOID, CORTEX, and OWL_LEAKS. Another section for 'Or, Filter by Category:' lists categories like 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'. In the 'Select Engine:' dropdown, it says '---- 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
 - ID, starting datetime, finding counters by severities, status
- Quick run button
- Quick scan report (HTML or JSON), delete or show details



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

scans / Check Arachni XSS policy [back]

Assets	Asset groups	Findings	Events
1	0	3	0

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

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:

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



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

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

- 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 - Scan compare view

- Highlighting differences:
 - new and missing findings
 - same finding type but different details
- Link to the findings comparison view

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

scans / compare scan results [back]

Title Cortex demo
Policy CX/
Abuse_Finder_2_0
+MaxMind_GeoIP_3_0
Started at 2018/01/23-22:01:41
Finished at 2018/01/23-22:01:00
Status Finished
Engine CORTEX/cx-001

Findings by severity:

Title Cortex demo
Policy CX/
Abuse_Finder_2_0
+MaxMind_GeoIP_3_0
Started at 2018/01/23-22:01:03
Finished at 2018/01/23-22:01:25
Status Finished
Engine CORTEX/cx-001

Findings by severity:

Asset	Title	Severity
8.8.4.4	Abuse_Finder: Address=abuse@level3.com	Info
8.8.4.4	Abuse_Finder: Address=network-abuse@google.com	Info
8.8.4.4	Abuse_Finder_2_0 full results (HASH: 722ea)	Info
8.8.4.4	Artefacts from 'Abuse_Finder_2_0' analyzer (HASH: 985ccb)	Info
8.8.4.4	Artefacts from 'MaxMind_GeoIP_3_0' analyzer (HASH: 65cea6)	Info
8.8.4.4	MaxMind: Location="United States/North America"	Info
8.8.4.4	MaxMind_GeoIP_3_0 full results (HASH: f09b3b)	Info
8.8.8.8	Abuse_Finder: Address=abuse@level3.com	Info
8.8.8.8	Abuse_Finder: Address=network-abuse@google.com	Info
8.8.8.8	Abuse_Finder_2_0 full results (HASH: 793b66)	Info
8.8.8.8	Artefacts from 'Abuse_Finder_2_0' analyzer (HASH: d334ac)	Info
8.8.8.8	Artefacts from 'MaxMind_GeoIP_3_0' analyzer (HASH: a1c144)	Info
8.8.8.8	MaxMind: Location="United States/North America"	Info
8.8.8.8	MaxMind_GeoIP_3_0 full results (HASH: c05095)	Info

// Compare selected findings (2 scans max.)

PatrOwl Manager (1.0-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 - 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])

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?\nquery=Enter%20query%20here...%3Cxxs_b11c3b4a8909dd561d2f10fbaf852c23%2F%3E&button=Search HTTP/1.1\nHost: xss-game.appspot.com\nAccept-Encoding: gzip, deflate\nUser-Agent: Arachni/2.0dev-FullScan\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.6\nAccept-Language: en-US,en;q=0.8,he;q=0.6\nX-Arachni-Scan-Seed: b11c3b4a8909dd561d2f10fbaf852c23\n\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/frame
From engine:	arachni-001 (ARACHNI)
From scan:	Check Arachni XSS policy
From policy:	XSS Vulnerability scan
Type:	xss
Tags:	xss, upgrade, 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 finding differences

Screenshot of the PatrOwl Manager interface showing a comparison between two findings, A (ID: 1181) and B (ID: 1179). The findings are listed in a table with columns for Title, Severity, Asset, Description, Solution, Risk info, Vuln info, Links, Tags, and Created at.

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

PatrOwl Manager (1.0.0-BETA), 2018

Engines status:



PatrOwl Engines

Features

- REST API application written in Flask (Python 2.7)
- Multi-{scans, threads, assets}
- Support local or online scanners:
 - Nmap, Nessus, Cortex, Censys, Arachni, SSL-Labs, URLVoid and VirusTotal
 - owl_leaks: Keyword searches in Github and Twitter
 - owl_dns: DNS info, Subdomain listing, typosquatted domains
- Scan results (findings) are parsed, analyzed and formated
- @todo: support Basic & Token authentications
- @todo: full documentation □ 🙌 🎉 🎉



- Meta-engine available
- Testing scripts available
- Dockerized

Metrics

- ~1 day to write a simple engine
- ~750 LoC per engine



PatrOwl Engines

Key functions

- **info()**: returns engine metadata like version, name, description
- **status()**: returns engine status
- **reloadconfig()**: reload the config file
- **start()**: checks parameters and start the scan
- **stop(<scan_id>)**: stop the scan
- **status(<scan_id>)**: returns the current scan status
 - FINISHED → PatrOwl will call getfindings()
 - ERROR → PatrOwl will stop the scan and raise an error
 - SCANNING → PatrOwl will retry later
- **getfindings(<scan_id>)**: return the findings and a summary
- **getreport(<scan_id>)**: return the raw report file(s)
- **clean(<scan_id>)**: delete all scan-related objects

REST API (JSON)

