SecOps orchestration with an open-source SOAR platform
Let me introduce myself

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)

Nicolas MATTIOCCO
@MaKyOtOx
34 y/o 🇫🇷

You don’t even care. Need to know more about me…
My own definition of **SecOps** ©

- Penetration Testing
- Security Control assessment
- Vulnerability Management
- Cyber-Threat Intel. & Hunting
- Security Compliance
- Security Incidents & DFIR Operations
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 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

- **Assets exposed**
- **Threats**
  - Vulnerabilities | Attackers | Security incidents
- **Business impacts**
  - of security incidents

Facts & Challenges

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**

**Precursores** (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?

AUTOMATE

ALL THE THINGS!

I DON'T WANT TO LIVE IN A WORLD

WHERE ATTACKERS AUTOMATE MORE AUTOMATICALLY THAN WE DO
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.
Efficiently moving from a reactive to a more **predictive** security posture with:

1. Automation and orchestration
2. Best-of-breed tools
3. Attackers methods (TTPs)
4. Expertise

*Wut !?! Feeling spotted now...*
PatrOwl: Technical architecture

### PatrOwlManager
- Assets & Groups
- Engines
- Scan policies
- Scan scheduler
- Scan results
- Dashboards
- Analyzing rules
- Alerting rules
- Searches
- Audit logs
- Users

### PatrOwlEngines
- REST API
  - Scan
  - Analyze
  - Format

### Integration Points
- CTI feeds or services
- Online scanning service
- Asset
- Internal LAN
- Ticketing or DFIR system
- SIEM

- SOC, CISO, CTO, TI, Pentester, Audit team, Dev[Sec]Ops, Sys/Net admins
- Scripts, SIRP, CMDB, ...
**PatrowlEngines**: Supported tools and services

- Nmap*
- Nessus*
- OWL_DNS
- VirusTotal
- URLVoid
- EyeWitness
- OWL/GitHub
- OWL/Twitter
- SSL-Labs
- SSLScan
- Censys
- CertStream
- Retire.js
- Arachni
- OWASPD-DC

* Does not embedding scanner

**Turnkey** micro-apps: Docker images + REST-API
Next engines in the pipeline (to be confirmed)

- **Vulnerability management:** OpenVas, Qualys, Rapid7 IVM
- **Pasties:** All-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 rescans 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 Entreprise solution (Cloud and on-premise). Stay tuned !**
  - Pro features: LDAP/AD/SAML/OAuth authentication, Asset sync., Cloud security assessment engines, awesome dashboards, …
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) ...
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


Find us everywhere on earth:

Now: Just in front of you
Mail: getsupport@patrowl.io
Web: https://patrowl.io
Twitter: @patrowl_io (Follow us!)
GitHub: @Patrowl (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 vulnerabilities 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
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
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 compare view

Highlighting differences:
- new and missing findings
- same finding type but different details

Link to the findings comparison view
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 performed view

- Scans heatmap over days, weeks and months
- Advanced filters
- Run or delete scans
- Show scan details
- Compare selected scans
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 - Finding compare view

Highlighting differences between findings
PatrOwl Manager - Alerting rules management view

Create, copy, modify or delete alerting rules
Change functional 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:
PatrOwl Manager - Engine policy views

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

Engine policy details:
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) ...
We have questions !?!

We want a demo !?!

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


Find us everywhere on earth:

Mail: getsupport@patrowl.io
Web: https://patrowl.io
Twitter: @patrowl_io (Follow us !)
GitHub: @Patrowl (Star and fork us !)