PatrOwl

Automation and Orchestration of Security Operations

#SOA(R) #SecOps #OpenSource #PreventiveSecurity
2019.05.10

TLP: WHITE

© 2019 – Nicolas Mattiocco – GreenLock Advisory
All Rights Reserved.
Contact getsupport@patrowl.io for more
Yet another guy ...

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

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

**Indicators** (have occurred or is happening)
- 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

**Events monitoring** reveals vulnerabilities and suspicious changes
- 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?

AUTOMATE

ALL THE THINGS!

I DON'T WANT TO LIVE IN A WORLD

WHERE ATTACKERS AUTOMATE MORE AUTOMATICALLY THAN WE DO
Why automating SecOps?

<table>
<thead>
<tr>
<th>Do more checks</th>
<th>Do it more often</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cover a larger and diversified scope</td>
<td>Continuously checking for vulnerabilities and suspicious changes</td>
</tr>
<tr>
<td>Empower new capacities and improve cyber-security maturity level</td>
<td>Reduce delays in discovering and fixing a security incident (vulnerability or pwnage)</td>
</tr>
<tr>
<td>Get a better overview of cyber-exposure (full-stack)</td>
<td>Keep updated of your cyber-exposition risks</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Do it more efficiently</th>
<th>Do compliance and benchmarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reduce time to low value-adding tasks to focus on more complex security cases</td>
<td>Define and expedite controls</td>
</tr>
<tr>
<td>Reduce and manage costs</td>
<td>Assess compliance level regarding corporate, regulatory and statutory standards</td>
</tr>
<tr>
<td>Assess effectiveness of your SecOps activities through measurable KPIs</td>
<td>Benchmark security level of assets using same control policies</td>
</tr>
</tbody>
</table>
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 ...
BTW, we built PatrOwl for automating and orchestrating SecOps.
PatrOwl’s incentives

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

SOC, CISO, CTO, TI, Pentester, Audit team, Dev[Sec]Ops, Sys/Net admins

Scripts, SIRP, CMDB, ...

CTI feeds or services

Online scanning service

Asset

Internet

Online scanning service

Internal LAN

Ticketing or DFIR system (Ex: TheHive, JIRA, MISP, Slack, ServiceNow, ...)

SIEM (Splunk, QRadar, ...)

WEB UI
PatrowlEngines: Supported tools and services

- NMap
- Nessus*
- NMap
- OWL_DNS
- VirusTotal
- URLVoid
- OWL/GitHub
- OWL/Twitter
- Retire.js
- Arachni
- OWASP-DC

Turnkey micro-apps: Docker images + REST-API

Cortex Analyzers (TheHive)

Engines by domains
Next engines in the pipeline (to be confirmed)

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

**Monitoring attacker or suspicious assets**
Ensure readiness of teams by identifying attackers’ assets and tracking changes of their IP, domains, WEB applications

**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 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
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) …

* FR-EN translation hint: “Oui Nide lou” == “We Need You”
Trust me, it’s a veeeery funny joke in french
Q&A

1. We have lots of questions !?!  
   -- Meet us @Armory!

2. We want a demo !?!  
   -- Meet us @Armory!

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
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
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:

PatrOwl Manager - Engine policy views

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

Engine policy details:
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
  o ID, starting datetime, finding counters by severities, status

Quick run button

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

## Findings Comparison

<table>
<thead>
<tr>
<th>Finding A (ID: 1181)</th>
<th>Finding B (ID: 1177)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Title</strong></td>
<td>Port 'tcp/80' is filtered</td>
</tr>
<tr>
<td><strong>Severity</strong></td>
<td>Info</td>
</tr>
<tr>
<td><strong>Asset</strong></td>
<td>8.8.8.8</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>The scan detected that the port 'tcp/80' was filtered</td>
</tr>
<tr>
<td><strong>Solution</strong></td>
<td>n/a</td>
</tr>
<tr>
<td><strong>Risk info</strong></td>
<td>vuln_publication_date: 2018/01/16 vuln_publication CVEs: 1 vuln_base_score: 0.0</td>
</tr>
<tr>
<td><strong>Vuln info</strong></td>
<td>n/a</td>
</tr>
<tr>
<td><strong>Links</strong></td>
<td>No Links</td>
</tr>
<tr>
<td><strong>Tags</strong></td>
<td>No Tags</td>
</tr>
<tr>
<td><strong>Created at</strong></td>
<td>2018/01/16 12:01:32</td>
</tr>
</tbody>
</table>

**Scans & Policies**

- **Scan title**: List open ports on Google DNS
- **Scan policy**: List open ports (TCP/53,56,80,443,8080)
- **Scan engine**: NMAP - nmap-002
PatrOwl Manager - Alerting rules management view

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Scope</th>
<th>Condition</th>
<th>Trigger</th>
<th>Severity</th>
<th>Target</th>
<th>Status</th>
<th>Last update</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>New findings found (Slack)</td>
<td>finding.status</td>
<td>'new'</td>
<td>auto</td>
<td>Low</td>
<td>slack</td>
<td>Disabled</td>
<td>2018-02-20</td>
<td></td>
</tr>
<tr>
<td>Findings with severity='info' -&gt; email</td>
<td>finding.severity</td>
<td>'info'</td>
<td>auto</td>
<td>Low</td>
<td>email</td>
<td>Disabled</td>
<td>2018-01-23</td>
<td></td>
</tr>
<tr>
<td>Findings with info severity</td>
<td>finding.severity</td>
<td>'info'</td>
<td>ondemand</td>
<td>Low</td>
<td>slack</td>
<td>Enabled</td>
<td>2018-02-01</td>
<td></td>
</tr>
<tr>
<td>Findings with low severity</td>
<td>finding.severity</td>
<td>'low'</td>
<td>auto</td>
<td>Low</td>
<td>slack</td>
<td>Disabled</td>
<td>2018-02-20</td>
<td></td>
</tr>
<tr>
<td>Findings with high severity</td>
<td>finding.severity</td>
<td>'high'</td>
<td>auto</td>
<td>Low</td>
<td>slack</td>
<td>Disabled</td>
<td>2018-01-16</td>
<td></td>
</tr>
<tr>
<td>New findings found</td>
<td>finding.status</td>
<td>'new'</td>
<td>auto</td>
<td>Low</td>
<td>thehive</td>
<td>Disabled</td>
<td>2018-02-11</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Actions</th>
<th>Title</th>
<th>Asset</th>
<th>criticity</th>
<th>On-demand</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>To logfile</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Send email</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>To TheHive</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>To Splunk</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>To Slack</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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


Find us everywhere on earth:

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