

# Open Source Vulnerability Management with Faraday

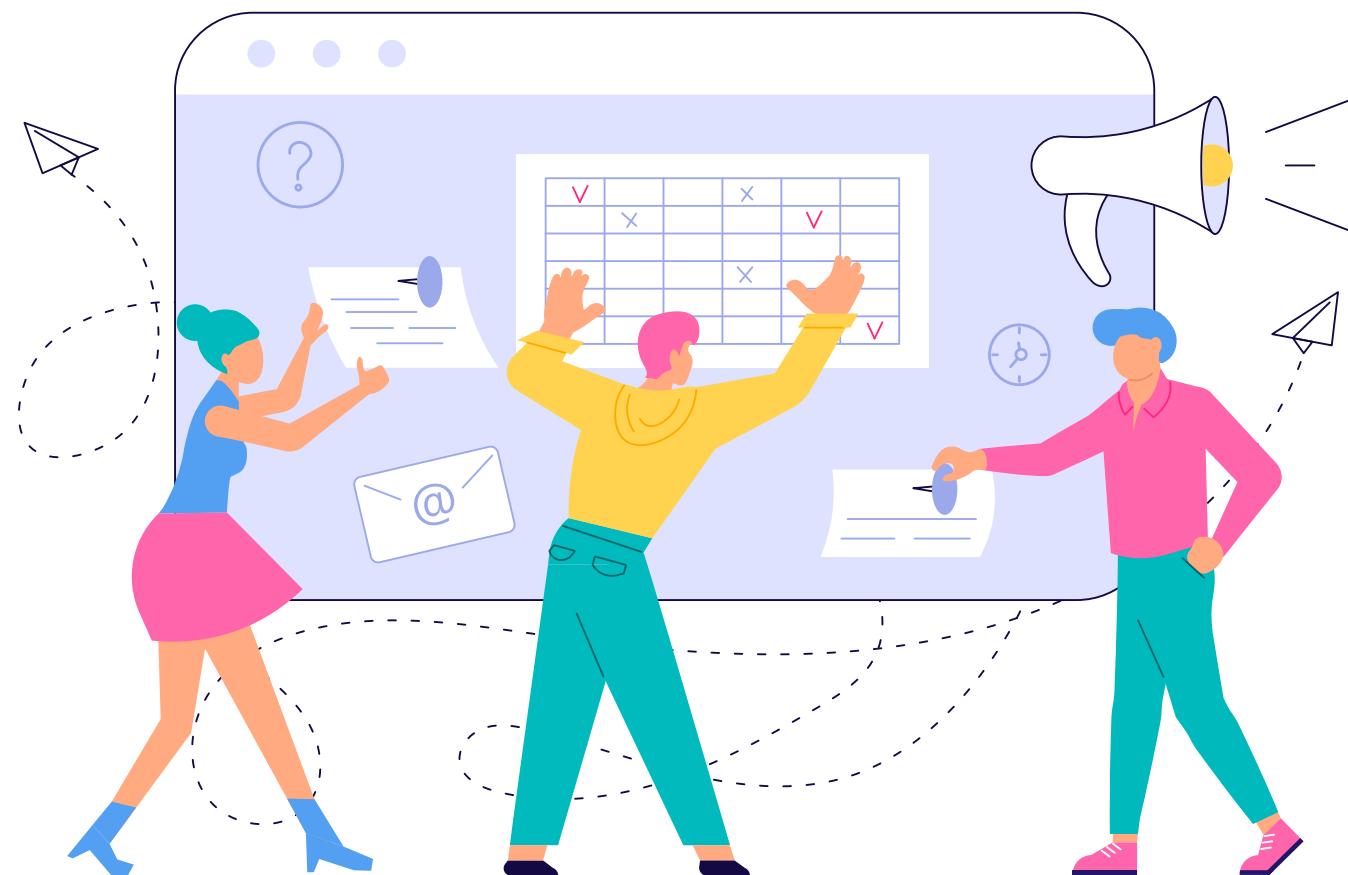


**Federico Kirschbaum**  
CEO & Co-Founder @ Faraday  
Co-Founder @ Ekoparty  
Security Conference

"Federico is currently the CEO of Faraday, a cybersecurity company based in Buenos Aires, Argentina. Through his extensive experience in computer security and telecommunications, he has developed a deep knowledge in the space which he utilizes in his current executive role. Federico is also a Co-founder of one of the biggest security conferences in Latin America, Ekoparty."



# Agenda



- **10:00-10:10 | Kickoff**
  - Introduction
  - Chit Chat
- **10:10-11:10 | Presentation**
  - Speaker
- **11:10-11:15 | Break**
  - Pre Q&A
- **11:15-11:30 | Q&A**
  - Discussion
- **11:30-11:35 | Wrap Up**
  - Contact Speaker

Hosted by

Sako M

DevOps



## Chapter04 Session08



# GOUP

Community driven Open source accelerator!  
<https://goupaz.com>

# Metabob

It's the fast, easy, and visual way of  
debugging code.

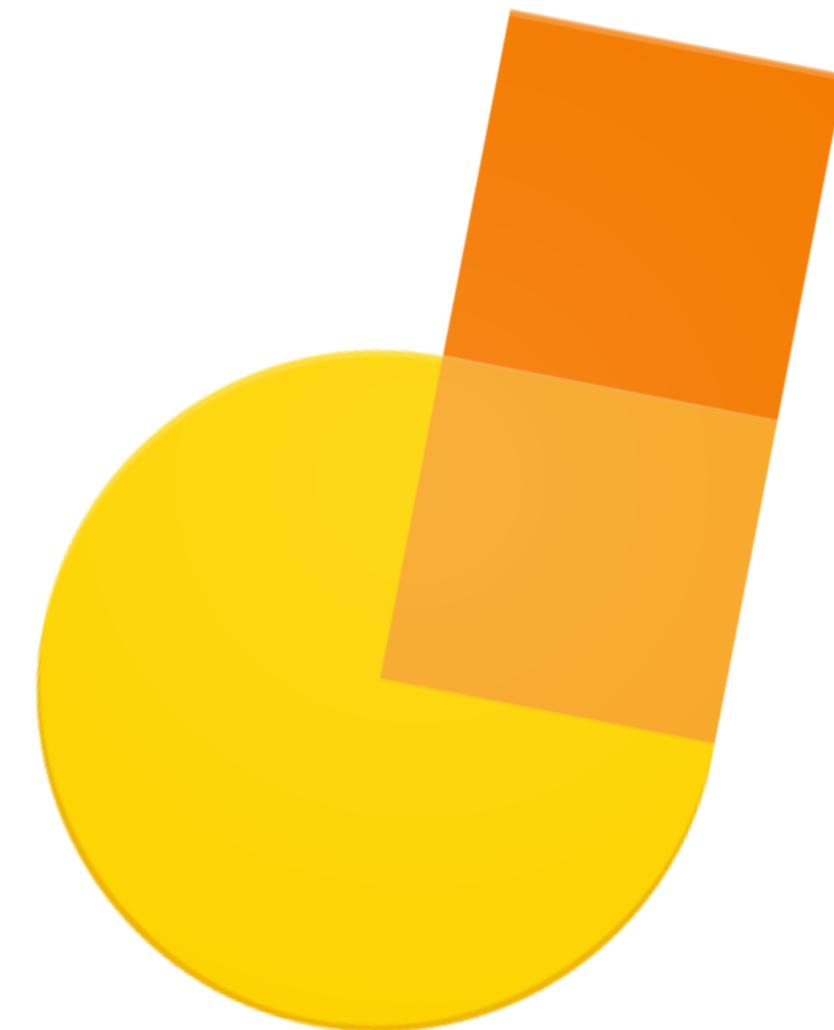
<https://metabob.com>

Are you ready?

Let's Begin!

CHITCHAT

# JAMBOARD



<https://tinyurl.com/hz6f378c>

POLL

How well you are experienced with application security & vulnerability management?

1



Not experienced

2



Somewhat experienced

3



Semi-experienced

4



Experienced

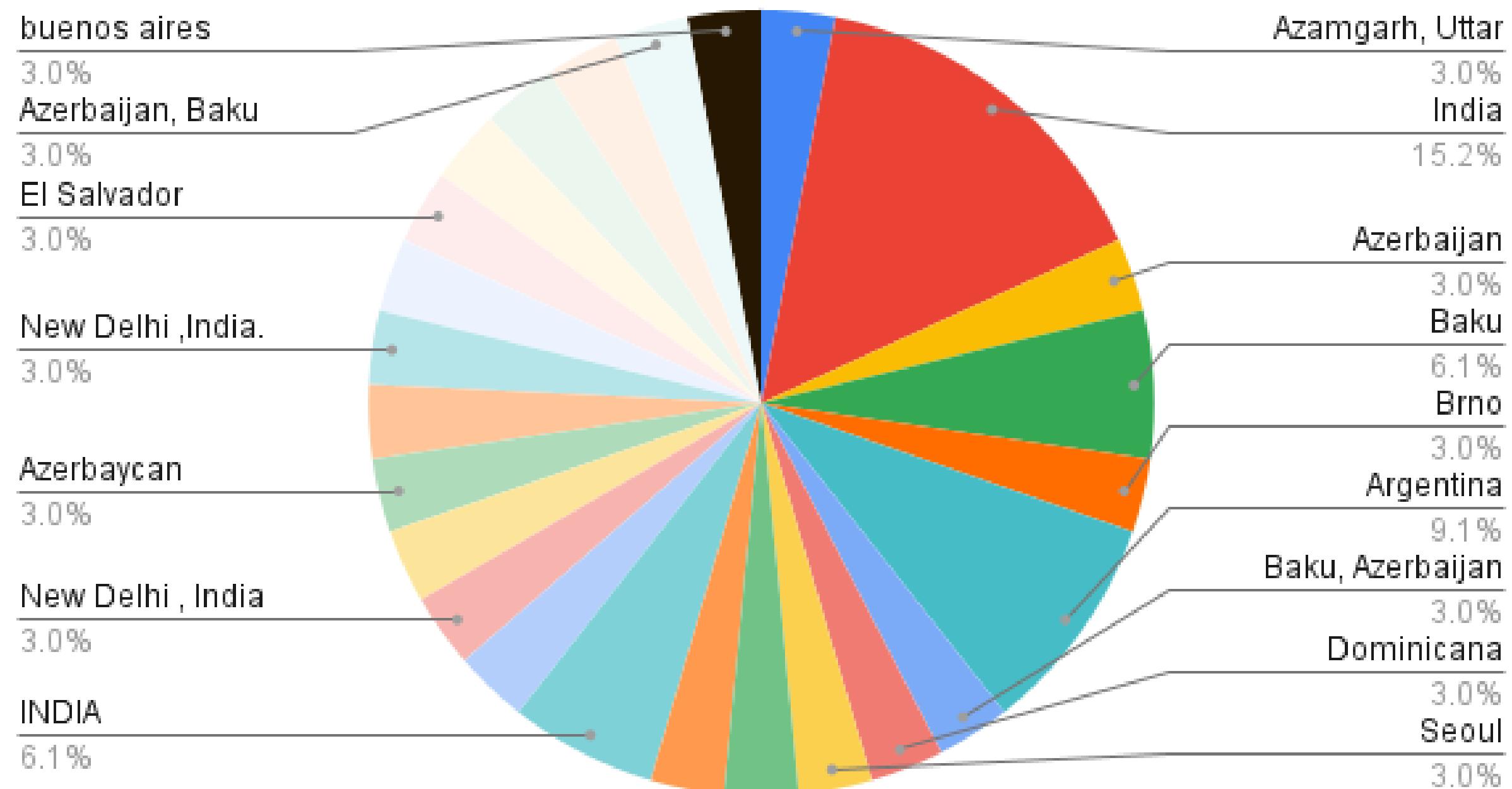
5



Very experienced

# Audience

GOUP Chapter04 Session08 - Diversity rocks!



# Code of Conduct

- 1 Learn, benefit, contribute
- 2 No marketing, selling, competing
- 3 Equality despite roles & bg

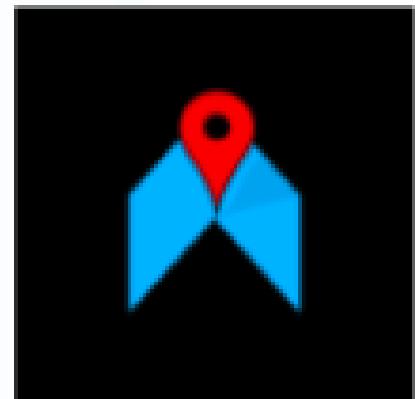


# Photo Shoot Time

Please turn on your camera :D

# Presentation

# Open Source Vulnerability Management



GOUP

<https://github.com/goupaz>

Federico Kirschbaum

[fedek@faradaysec.com](mailto:fedek@faradaysec.com)

 @fede\_k

# About Us

---

We believe that understanding your security posture is the main key to making smarter security investments.

We develop technologies to detect, track and mitigate risks faster and easier. Building a platform that allows you to automate repetitive vulnerabilities detection procedures, summarize results, accomplish custom workflows and visualize risks faster and easier.

- +15 years of experience providing innovative solutions and cutting-edge security consulting services.
- Our specialists are presenters at the best security research conferences such as **Defcon**, **BlackHat**, **Shakacon**, **H2HC**, **Troppers**, **Code Blue**, **AV Tokyo**, **SECCON** and **HITB**
- Exclusive Investigation Center. Several results from our research were published in the last years.
- Constant contribution to the global security community. Faraday's founders are the organizers of **Ekoparty**, the biggest technical security information conference in Latin America with +3000 attendees.



# Vulnerability Management

Vulnerability  
/vʌln(ə)rə'bɪlɪti/

The quality or state of being exposed to the possibility of being attacked or harmed, either physically or emotionally.

## Vulnerability Management (cont.)

In **computer security**, a vulnerability is a **weakness which can be exploited** by a **threat actor**, such as an attacker, to perform unauthorized actions within a computer system. To exploit a vulnerability, an attacker must have at least one applicable tool or technique that can connect to a system weakness. In this frame, vulnerability is also known as the **attack surface**.

# Vulnerability Management (cont.)

Vulnerability management is the "*cyclical practice of identifying, classifying, prioritizing, remediating, and mitigating*" software vulnerabilities.

## **VM is not a Vulnerability Assessment:**

Vulnerability management is the process surrounding vulnerability scanning, also considering other aspects such as risk acceptance.

## **VA is not a Penetration Testing:**

Vulnerability assessment is just part of the first phase of a penetration testing methodology, normally part of the information gathering phase.

# Vulnerability Management

## Detection Schedule:

Any vulnerability not detected after a schedule scan takes place, will only be detected at the next scheduled scan.

For example, the following policies:

- Annual Penetration Testing
- Quarterly Vulnerability Assessment
- Monthly Scanning
- Continuous Scanning

# Vulnerability Management

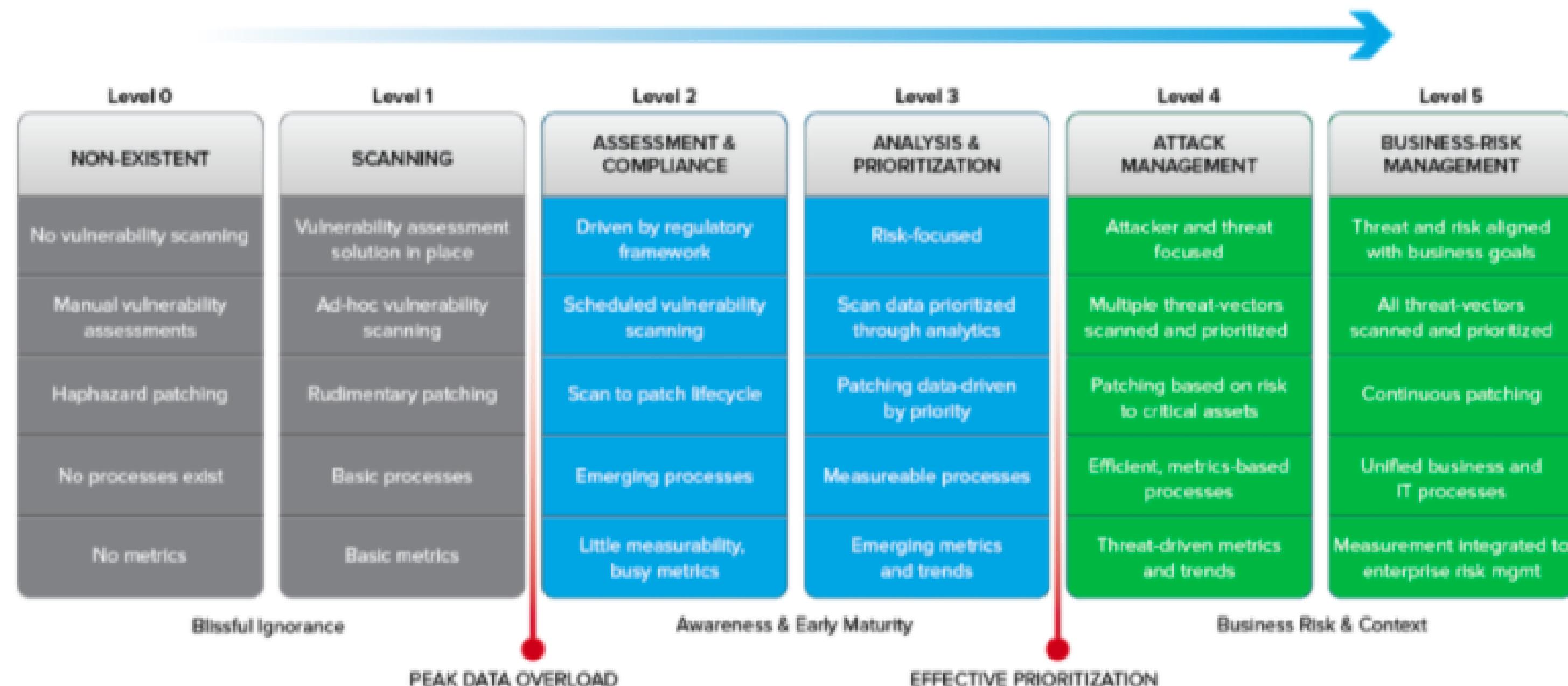
Having a process in place greatly reduces the risks an organization is facing.

## Security is dynamic

Information security has changed drastically in a short amount of time, but defense strategies are not keeping pace with its dynamic nature.

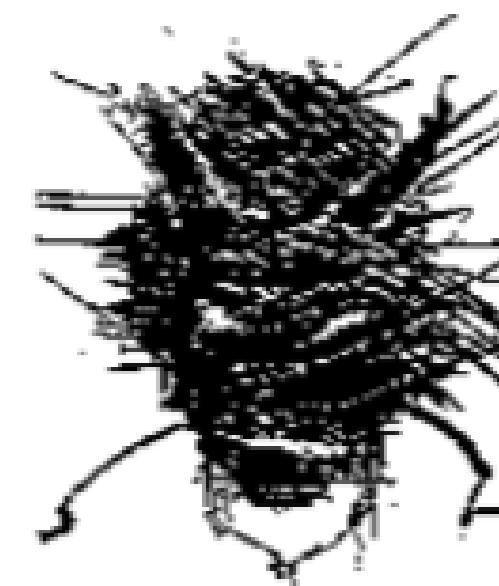
# Vulnerability Management

## VULNERABILITY MANAGEMENT MATURITY MODEL



# Improving the Security of Your Site by Breaking Into it

1993



F



MIND BLOWN

Is security still in the 90s?  
What has changed?

# Vulnerability Management

- Vulnerabilities are the gateways through which threats are manifested.
- Vulnerability scans **without** remediation have **little value**.
- A little scanning and lot of remediation is better than a lot of scanning and little remediation.
- Vulnerabilities in need of fixing must be prioritized based on which ones pose the most immediate risk to the organization.
- Security practitioners need a process that will allow them to stay on the trail of vulnerabilities so the fixes can be more frequent and effective.

# Vulnerability Management

## Common pitfalls in Security Operations

- Friction with engineering/ops teams
- Security Tooling Information lives in silos.
- Information duplicated in numerous platforms.
- Reporting takes too much time.
- Coverage
- No Metrics
- Lack of Asset tracking



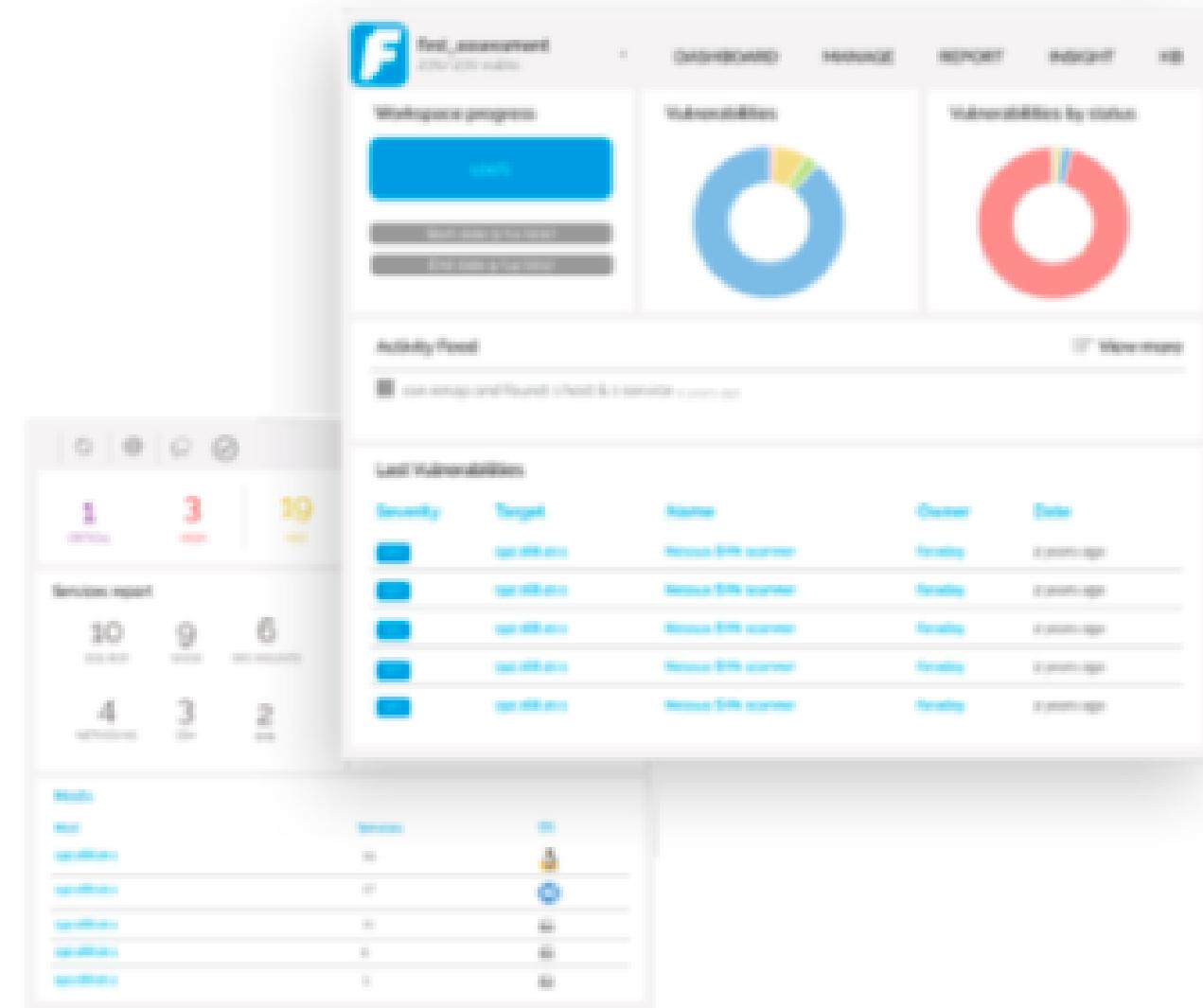


To the rescue?

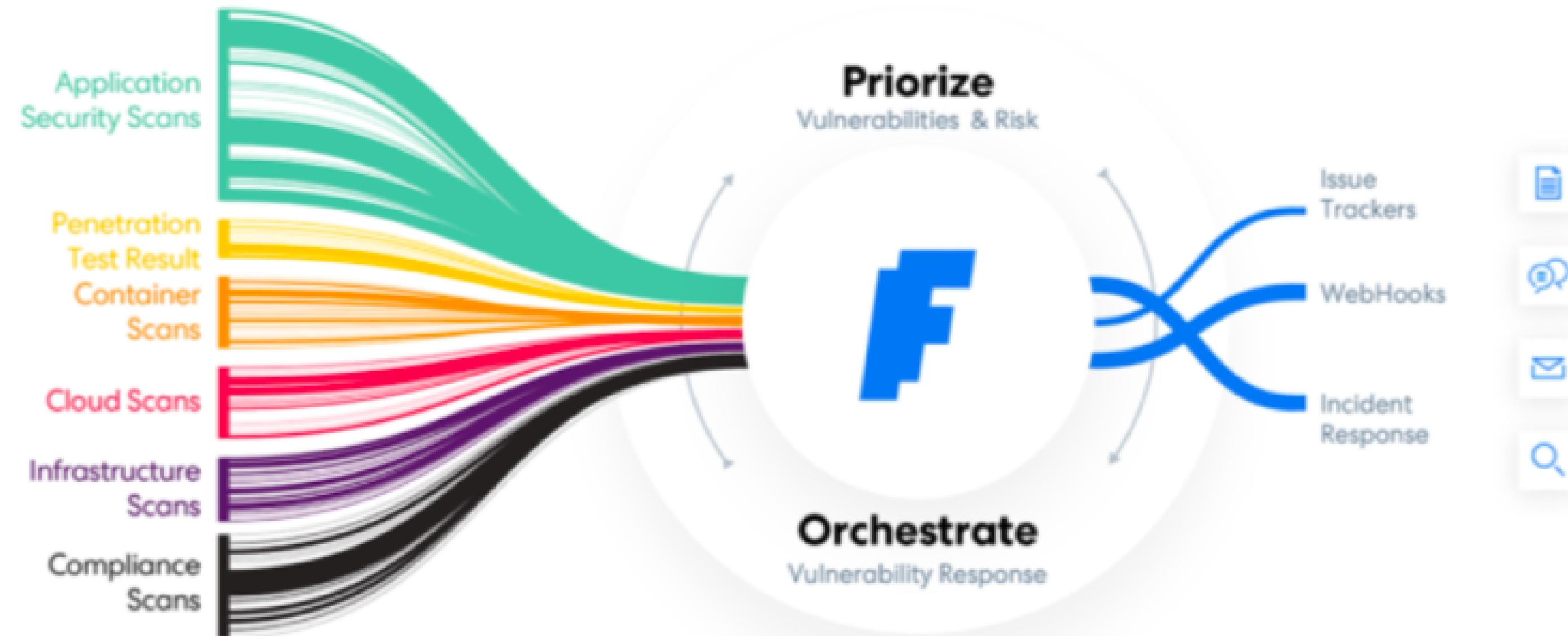
# Introduction to Faraday

What if you could automate daily tasks, like running your favorite scanners and actions based on findings?

Normalize and review results from different sources, manage, tag, track vulnerabilities as a team.



# Introduction to Faraday



# Integration & Flexibility



With more than +75 plugins, an easy-to-use REST API and a flexible scheme to develop your own Faraday Agents, our platform brings a unique alternative to create your own automated security pipelines into faraday's vulnerability management ecosystem.

## Scanners



## Connectors



## Modules



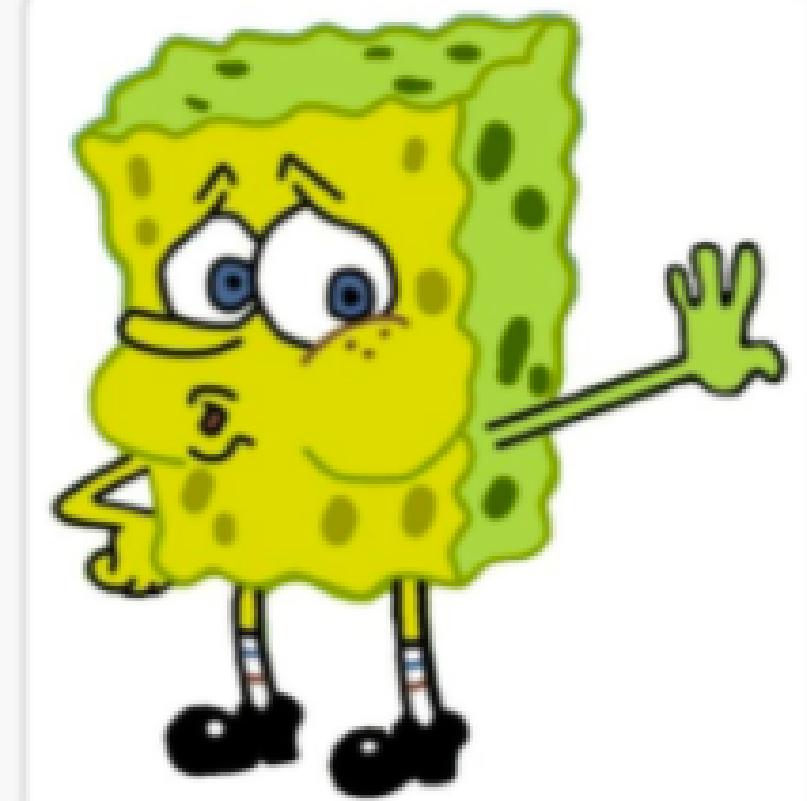
## Extenders



# Possibilities with Faraday

- Aggregate from different sources
  - Tools, Bug Bounties, Pentest
- Vulnerabilities can be processed using the same workflow
  - Triaging creates High Signal Output
  - Accountability and tracking of all vulnerabilities detected.
- Create Dashboard with actionable information
  - KPIs / SLAs
- Create Project so everyone in the team has access
- Use our APIs to automate as much as possible
- Understand Coverage
- Create standard workflows
- Asset tracking

Our “New” Users are  
Busy Engineers



# Benefits Faraday

- Automate repetitive team's actions and save time
- **Understand Attack Surface by Tracking assets and services**
- Visualize findings and get deeper understanding
- **Orchestrate risk detection methods and aggregate results**
- Vulnerability management ecosystem in one platform
- **Reduce mitigation time and compliance with your Time To Market**
- Increase team's maturity with collaboration and automation
- **Create Metrics while identifying and mitigating vulnerabilities**

# Introduction to Faraday

## Common use cases

- Consulting Services Companies
  - Red/Blue/Purple Teams
- Managed Security Service Providers.
  - Attack Surface
- CERTS
  - Vulnerability Management
- Internal Security Teams
  - Regression testing, Compliance, Scanning
- DevSecOps
  - Security Pipelines

# Automation

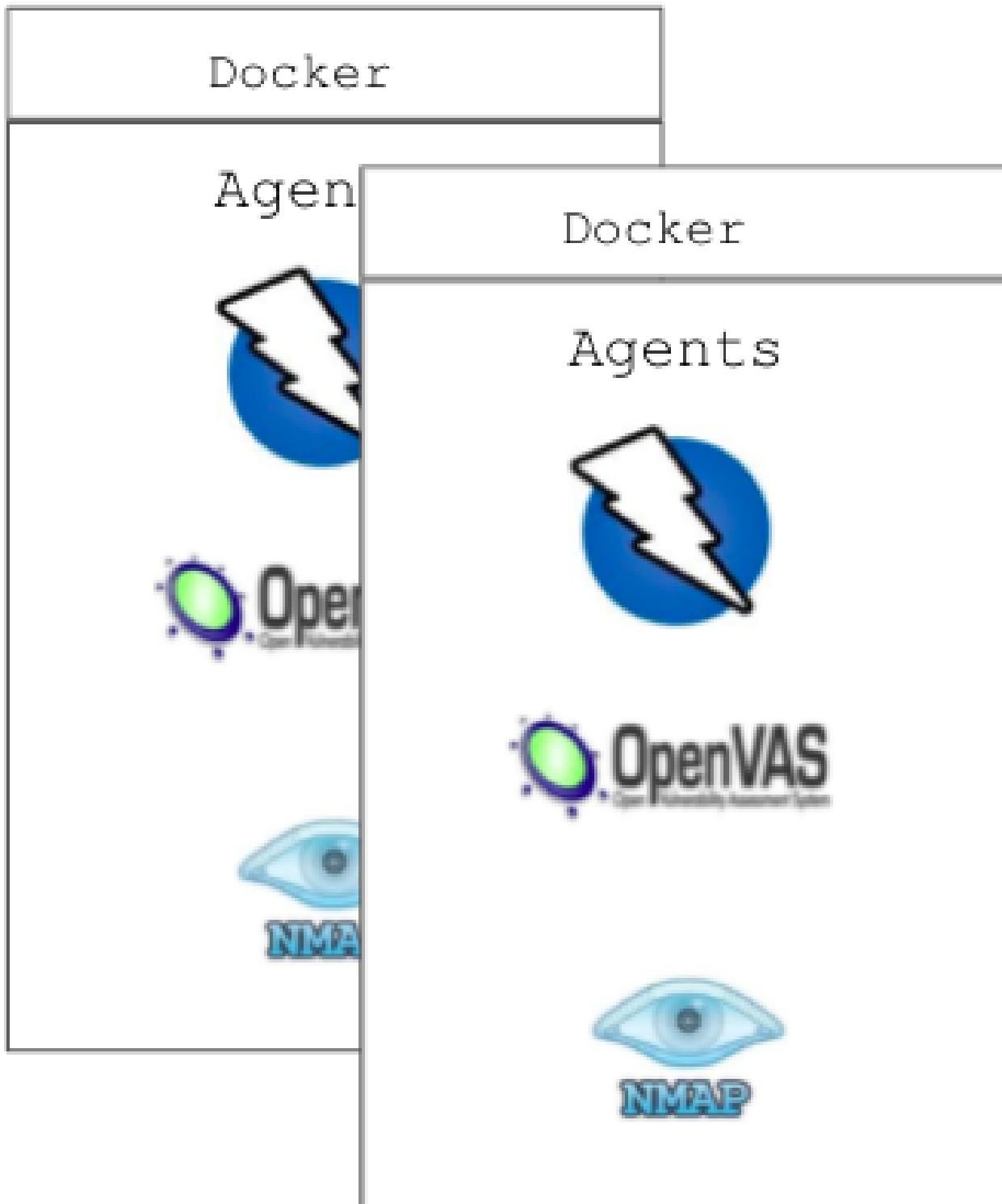
To make integrations with Faraday as easy as possible, we developed a project we called **Faraday Agent Dispatcher** that oversees handling the communication between the Faraday Server and your own agents.

The only thing you'll need to build your own integrations is a script (we call it an **Executor**) that prints to standard output every data you want to send to Faraday (hosts info, vulnerabilities, etc.) encoded in JSON.

There is no need to use complex APIs or communication methods, as all of this is abstracted by the Dispatcher. You just need to print JSON to standard out, and the Dispatcher will handle the rest!

[https://github.com/infobyte/faraday\\_agent\\_dispatcher](https://github.com/infobyte/faraday_agent_dispatcher)

# Automation with Agents



# Automate all The Things

- Faraday has a Server RESTful API by **default** running on 127.0.0.1:5985
- You can check all API endpoints with the command:

```
$ faraday-manage show-urls
```

- Or check out our Swagger:

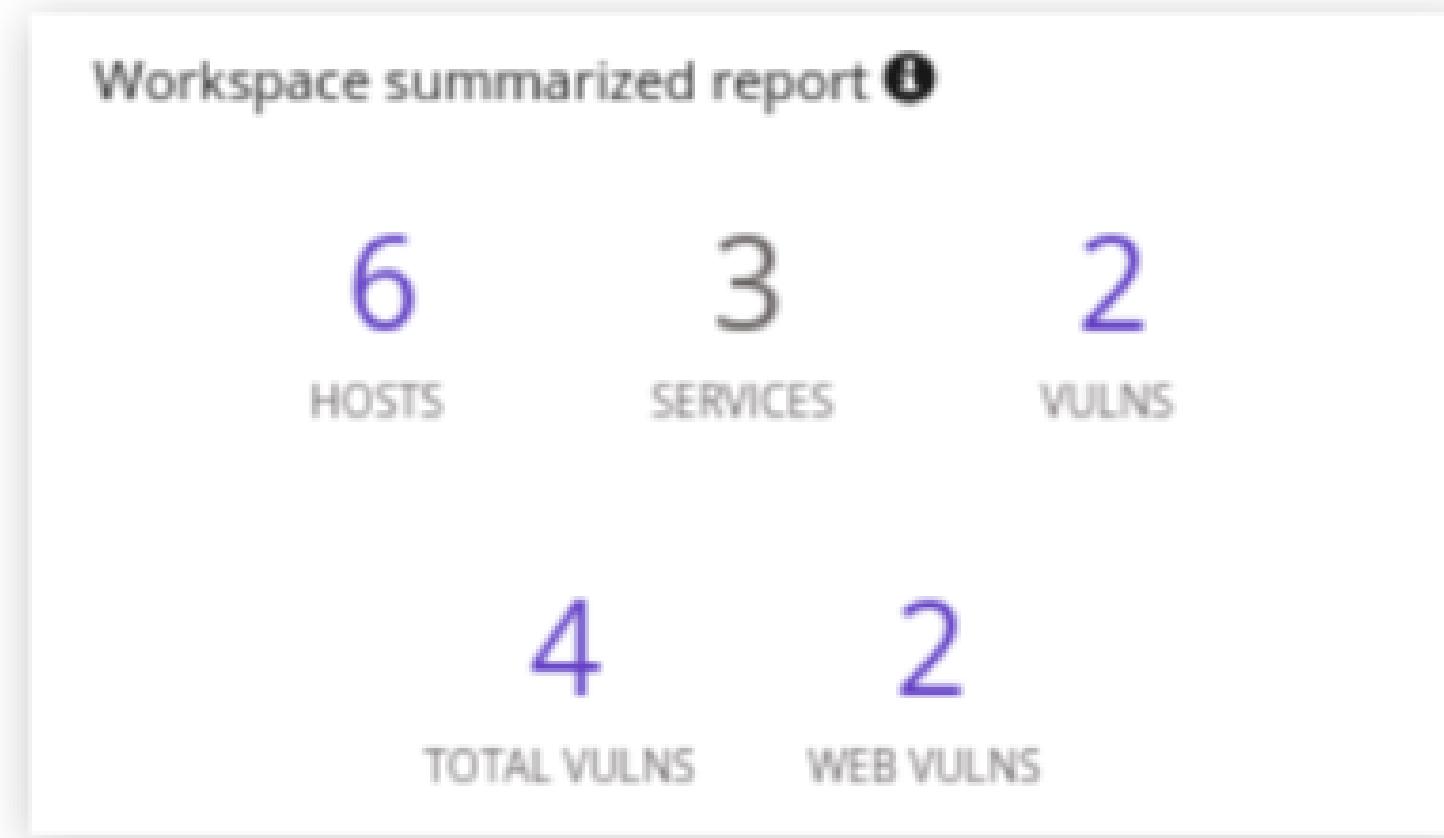
```
https://api.faradaysec.com/
```

```
{
  "params": "*",
  "path": "./git/config",
  "name": "GIT Config Disclosure",
  "type": "VulnerabilityWeb",
  - metadata: {
      update_user: null,
      update_controller_action: "*",
      creator: "faraday_csv",
      create_time: "2021-07-03T07:26:43.997864+00:00",
      update_action: 0,
      owner: "faraday",
      update_time: "2021-07-03T07:26:43.997869+00:00",
      command_id: 13
    },
    _id: 2062,
  - service: {
      status: "open",
      summary: "(443/tcp) https",
      ports: 443,
      name: "https",
      version: "",
      protocol: "tcp",
      _id: 195
    }
  ...
}
```

# Faraday in each phase

## Discovery

When a process is discovering network hosts, all this information can be aggregated in Faraday. All this information will be summarized in the platform.



# Managing Vulnerabilities

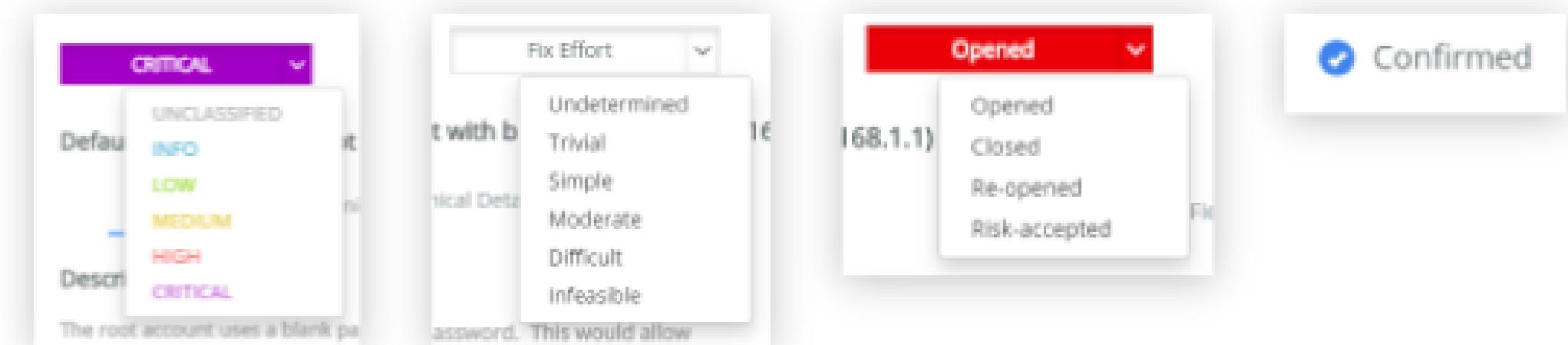
## Vulnerability Life Cycle

The screenshot shows a web-based vulnerability management tool. At the top, there's a navigation bar with tabs: 'Jobs' (selected), 'Vulns', 'Hosts', 'Credentials', 'Tasks', and a search bar with placeholder 'Enter keywords'. Below the navigation is a table listing vulnerabilities:

Severity	Type	Count	Plugin Name	Host	Description
CRITICAL	Weak Credentials	0	(1111/tcp) no...	192.168.1.1	(metasploit found)
CRITICAL	Weak Credentials	0	(22/tcp) ssh	192.168.1.1	(metasploit found)
HIGH	SSH Protocol Version Sup...	0	(22/tcp) ssh	192.168.10.45	This plugin deter...
HIGH	SSH Server Type and Versi...	0	(22/tcp) ssh	192.168.10.45	It is possible to ob...
INFO	SSL Certificate Expiry	0	(25/tcp) smtp	192.168.10.45	This script checks

A modal window is open for the first item in the list, showing a detailed view of the 'Weak Credentials' issue. The modal has tabs: 'General' (selected), 'Fix Details', 'Timeline', 'Comments', and 'Attachments'. The 'General' tab displays the following information:

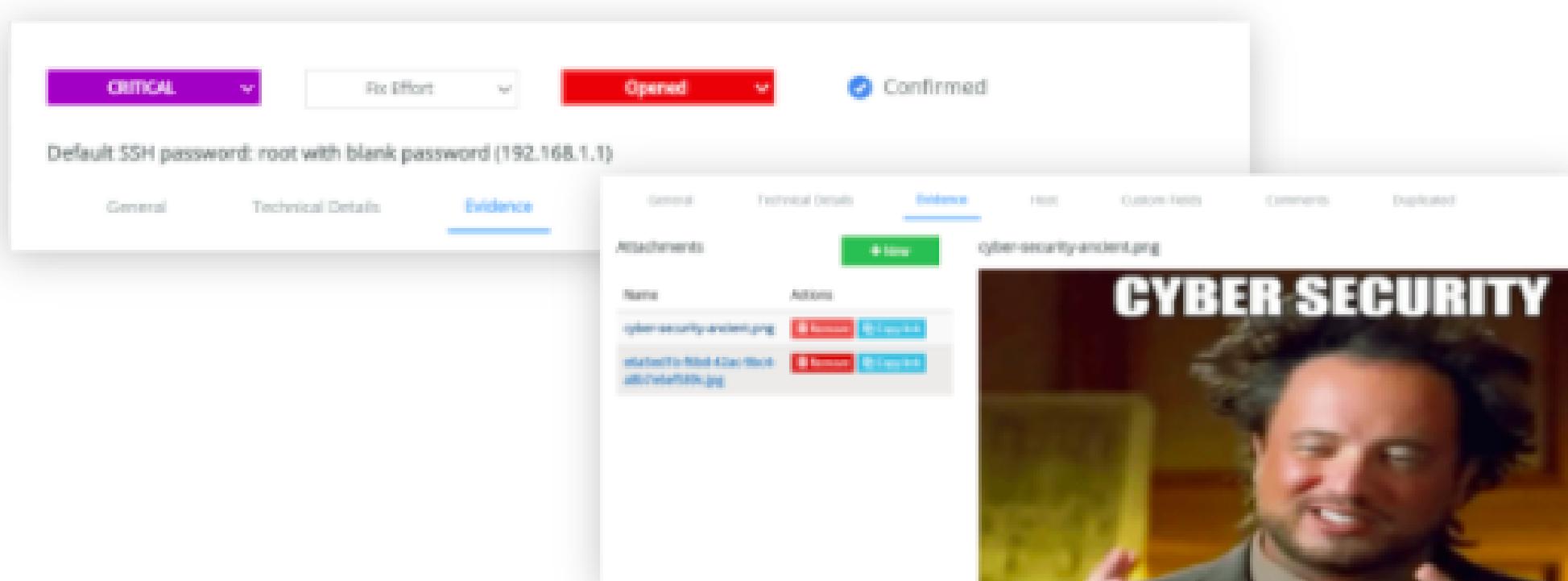
**Severity:** CRITICAL  
**Description:** The root account uses a blank password. This would allow anyone logging into the machine via SSH anduttle complete control having obtained the service.  
**Resolution:** Use the passwd command to set a more secure root password. A good password should consist of a mix of upper- and lower-case characters, numbers, and punctuation and should be at least 8 characters long. You may also want to disable root login via SSH, which you can do by specifying the following in your configuration file: /etc/



# Managing Vulnerabilities

## Vulnerability Life Cycle

Add evidence to any finding, allowing easier verification by OPs



The screenshot shows a web-based application for managing vulnerabilities. At the top, there are dropdown menus for 'CRITICAL' (selected), 'Fix Effort' (dropdown), 'Opened' (selected), and 'Confirmed'. Below this, a summary message reads: 'Default SSH password: root with blank password (192.168.1.1)'. The main content area has tabs for 'General', 'Technical Details', and 'Evidence'. The 'Evidence' tab is currently selected, indicated by a blue underline. Under the 'Evidence' tab, there is a section titled 'Attachments' with a green 'Add New' button. A table lists two attachments: 'cyber-security-incident.png' and 'relatedTo-Bugfix-Doc-Work-att1-Verifiable.jpg'. The first attachment is shown as a thumbnail image of a man with a beard and the text 'CYBER SECURITY'.

# faraday-cli

## Vulnerabilities in your terminal

```
kali㉿kali:~$ faraday-cli
```

```
Server: https://avjxdzfi.de Faraday> workspace dashboard accessible wp-config
[ws:test_ws]> █
```

WORKSPACE	SUMMARY	SEVERITIES	ACTIVITY	General	Technical Details	Evidence
group	hosts: 30 services: 76 vulns: 1247	critical: 0 high: 1 med: 34 low: 0	Nessus (report) found 29 hosts, 75 services and 1241 vulns (0/1/1) nuclei (report) found 1 hosts, 1 services and 4 vulns (0/1/1)			
present	hosts: 34 services: 35 vulns: 247	critical: 1 high: 4 med: 27	faraday_csv (report) found 34 hosts, 35 services and 246 vulns (0/1/1)			

# faraday-cli

# Vulnerabilities in your terminal

kali㉿kali:~\$ faraday-cli stats severity

Gathering data

# Severity stats (test\_ws)

critical high med low info unclassified

Host	Critical	High	Med	Low	Info	Unclassified	Total
host-7.example.com	15	25	10	5	10	10	152
host-2.example.com	10	15	10	5	10	10	102
host-8.example.com	15	45	45	10	10	10	344
wins2012r2d.example.com	10	10	10	10	10	10	167
wins2016s.example.com	0	10	10	10	10	10	136
centos7sx64.example.com	0	0	0	0	0	4	4
wins2019d.example.com	0	0	5	5	10	10	116
host-5.example.com	0	0	5	5	10	10	112
192.168.1.14	0	0	0	0	0	9	9

# faraday-cli

# Vulnerabilities in your terminal

- You can install it on any box running Python
  - It will help you manage your Faraday Server remotely.
  - Upload results from your favorite Tools.
  - Pull information from your Faraday Server
  - Automate your security workflows.
  - Helper for CI/CD

# What we know so far?

- We can't kill ALL the bugs, but we can definitely kill a few
- You can't fully protect a computer, but you can at least make it expensive to attack.
- Can we elevate baseline security by automating all the things?
- Content creation for scanners is difficult to scale  
Using offensive methodologies creates high signal but does not scales
- Security should be an enabler
- Security is a **culture** not a tool

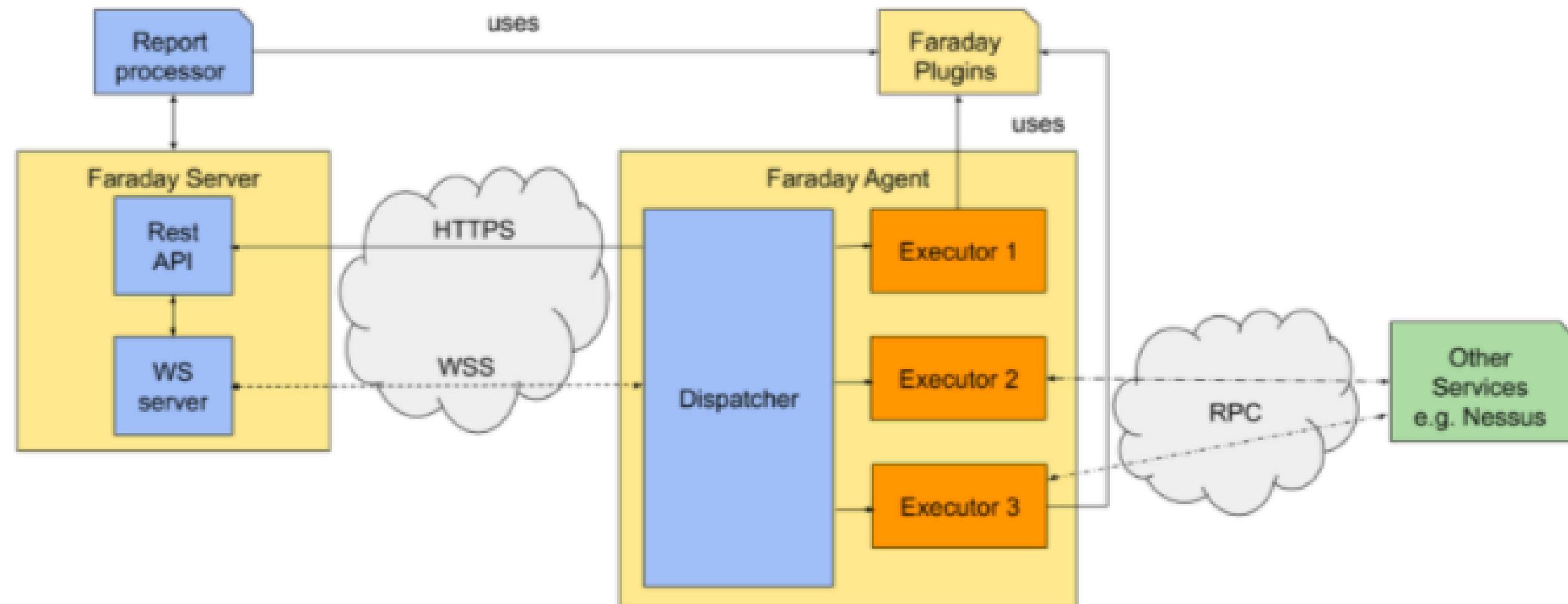
Thanks for your time  
**Questions?**

# Stack



- Python
- Python-Flask
- AngularJS
- PostgreSQL
- HTML5

# Agents Architecture



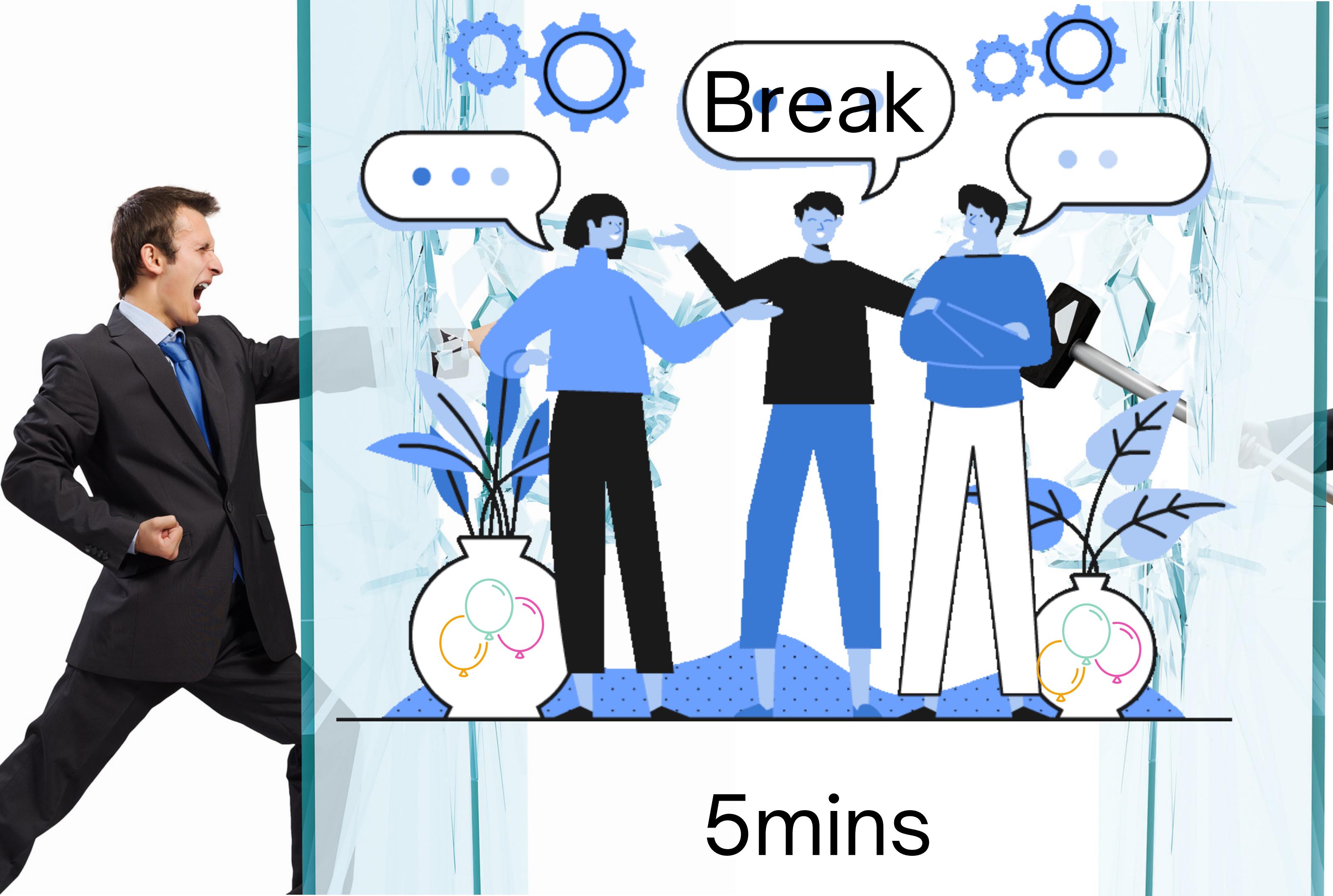
<https://docs.agents.faradaysec.com/technical/arch/>

The screenshot shows the Faraday tool interface. On the left, there is a sidebar with a tree view of the current session, showing various vulnerabilities and services. The main area has a search bar at the top with the text "git config disclosure". Below the search bar, there are two tabs: "Vulnerabilities" (selected) and "Services". The "Vulnerabilities" tab shows a table with columns: ID, Title, Status, and Created. One row is highlighted in yellow, showing the title "Git Config Disclosure (HTTP)" and the status "Confirmed". To the right of this table, there is a detailed view of the selected vulnerability. The title is "Git Config Disclosure (HTTP)". The status is "Confirmed". The description is "Search for the pattern @gitconfig in passed URLs". The resolution is "No resolution was found". The created date is "2021-07-03T07:26:43.997864+00:00". The updated date is "2021-07-03T07:26:43.997869+00:00". The command ID is 13. The service table shows a single row for "https" with port 443, status open, and summary "(443/tcp) https".

```
{
  "params": "",
  "path": "./.git/config",
  "name": "Git Config Disclosure",
  "type": "VulnerabilityWeb",
  - metadata: {
      update_user: null,
      update_controller_action: "",
      creator: "faraday_csv",
      create_time: "2021-07-03T07:26:43.997864+00:00",
      update_action: 0,
      owner: "faraday",
      update_time: "2021-07-03T07:26:43.997869+00:00",
      command_id: 13
    },
    _id: 2062,
  - service: {
      status: "open",
      summary: "(443/tcp) https",
      ports: 443,
      name: "https",
      version: "",
      protocol: "tcp",
      _id: 195
    }
}
```

# Q&A | Discussion





5mins

# Wrap Up

HOWTO



## Remember!

- Re-Search
- Be short and clear
- Re-mind
- Q&A over Slack

Linkedin: @fedek

GOUP Slack: @Federico Kirschbaum



# Federico Kirschbaum



**Join Us!**

**HTTPS://GOUPAZ.COM**

**HTTPS://METABOB.COM**

- 1** Community Managers
- 2** Tech Writers
- 3** In/Out Ambassadors
- 4** Marketing Creators & Editors
- 5** Course Creators
- 6** Project Creators

# Thank You

## Culture

#egoless #collaborative #competent #decentralized #scalable #fun

## Open source

#creator #contributor

## Diversity

#age #gender #location #economics #religion #politicalview

How can we do  
better?