Create Your Own WordPress Plugin and Theme Repository

Boston WordPress Meetup // February 2025

BAIZMANDESIGN

Saul Baizman
https://baizman.design

Accessibility

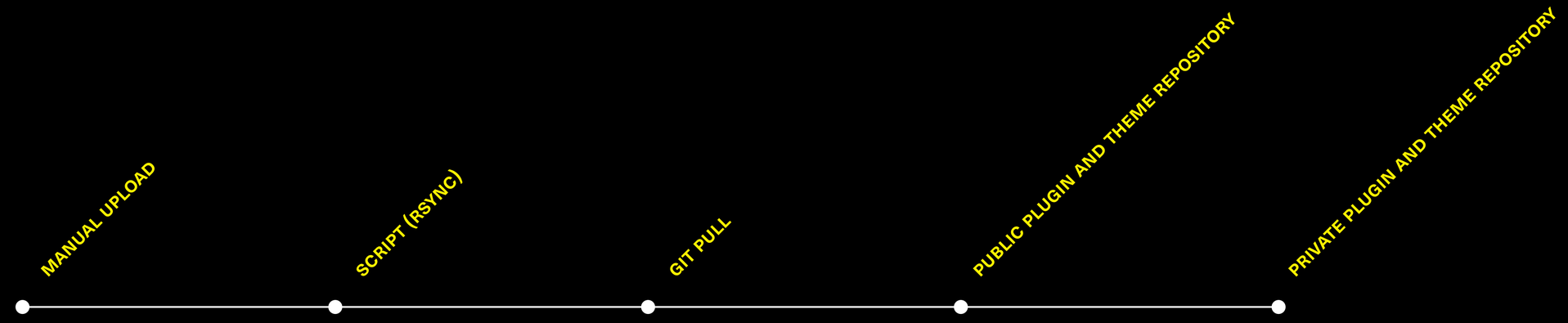
~~Composer~~

~~Object Oriented Programming~~

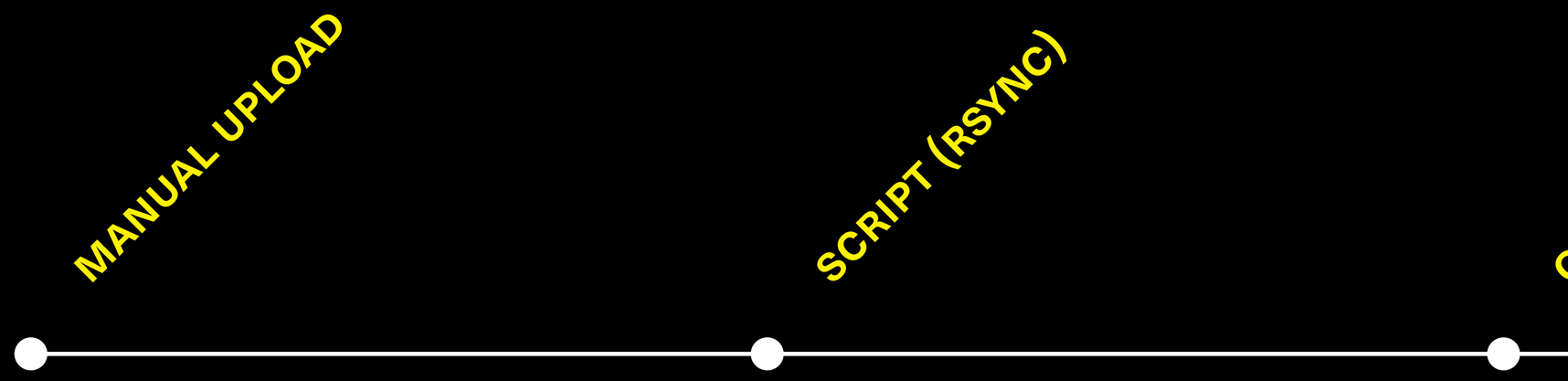
~~Docker~~

~~Advanced git~~

the continuum of deployment

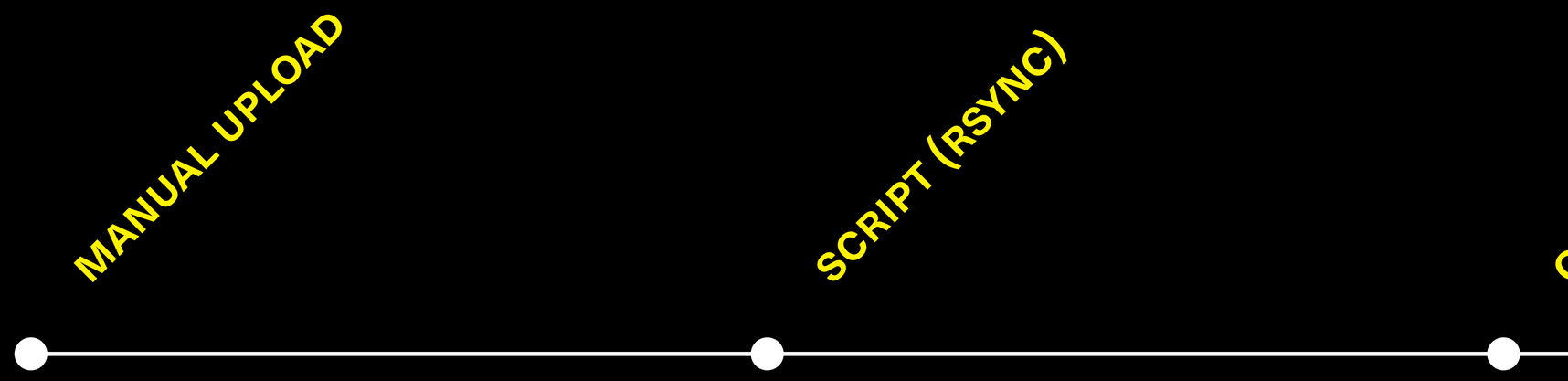


the continuum of deployment

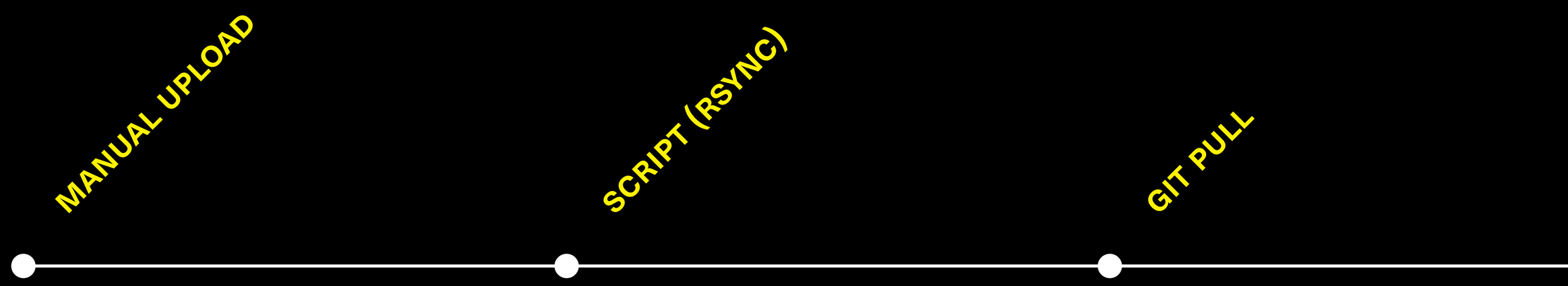


NETFLIX

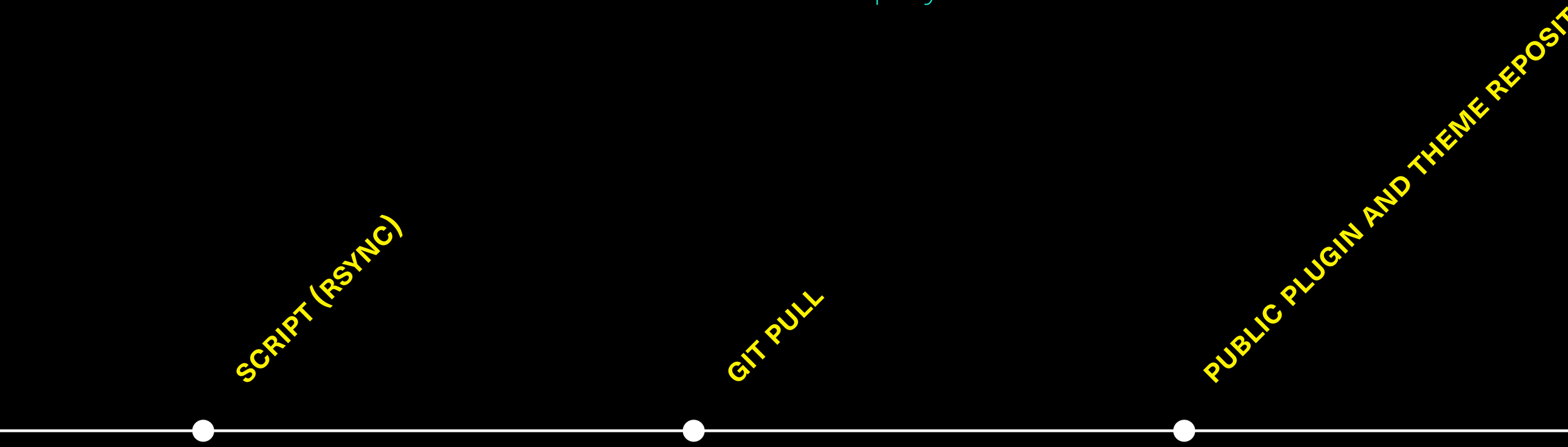
the continuum of deployment



the continuum of deployment



the continuum of deployment



Why not use `git pull`?

- Repo history is visible
- Repo may include developer-only files inappropriate on production
- Asset sizes are (much) smaller without a `.git` subdirectory and dev-only files
- Have to set up SSH access on every host
- Missed opportunity: you can standardize tests, QA, etc., via CI/CD
- Missed opportunity: automated versioning via `git tag` and substitutions
- Oh yeah, no nice dashboard notifications

Repo Lookout

Repo Lookout is a non-commercial project. We just want to make the web a safer place. You can support us on Ko-fi.

Find publicly exposed source code repositories

Repo Lookout is a large-scale security scanner, with a single purpose: **Find source code repositories that have been inadvertently exposed to the public** and report them to the domain's technical contact.

Accidentally exposed source code repositories often contain highly sensitive information that can be used for downstream attacks, such as data leakage and ransomware extortion. While the problem has been known and extensively documented for years,[1 2 3 4 5] our findings show that it is still prevalent.

Our goal is to combat this vulnerability by automatically detecting and reporting instances.

Further details and a bit of history can be found in this interview on our web hoster's blog.

URL index

The URL index for the scanning process is obtained from several sources:

- CommonCrawl builds and maintains an open repository of web crawling data.
- Tranco List is a research-oriented top site ranking hardened against manipulation.
- Chrome UX Report provides metrics for how real-world Chrome users experience the web.
- Certificate Transparency is an Internet security standard for monitoring and auditing the issuance of digital certificates.

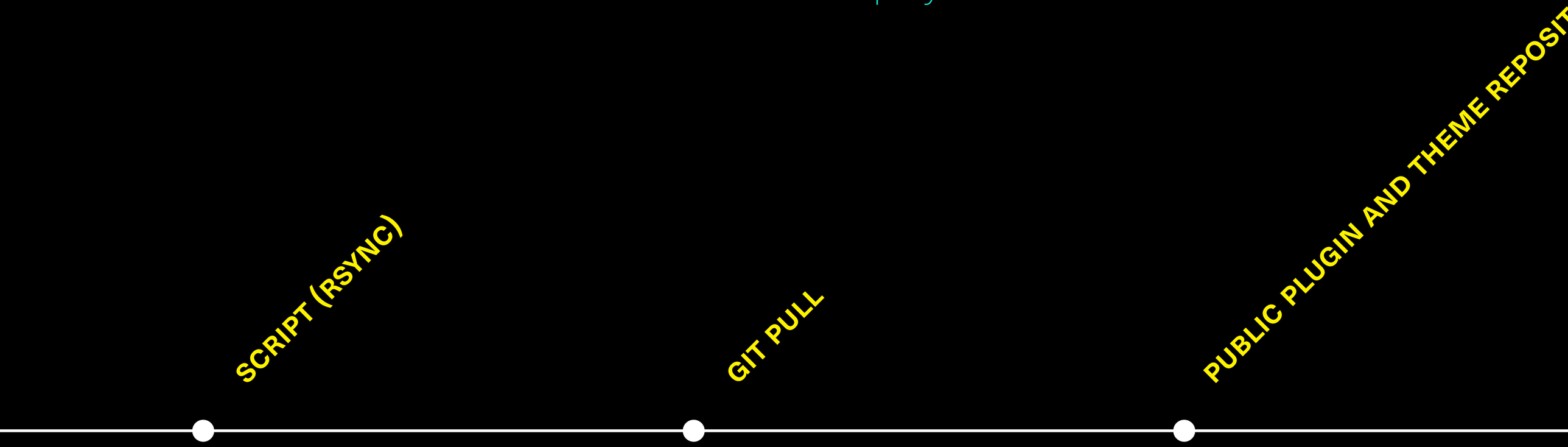
Statistics

Including our most recent security scan on February 17, 2025, we have scanned **16,128,527,757 URLs** on **1,960,758,395 domains**. A total of **1,327,240 publicly exposed source code repositories** have been found to date.

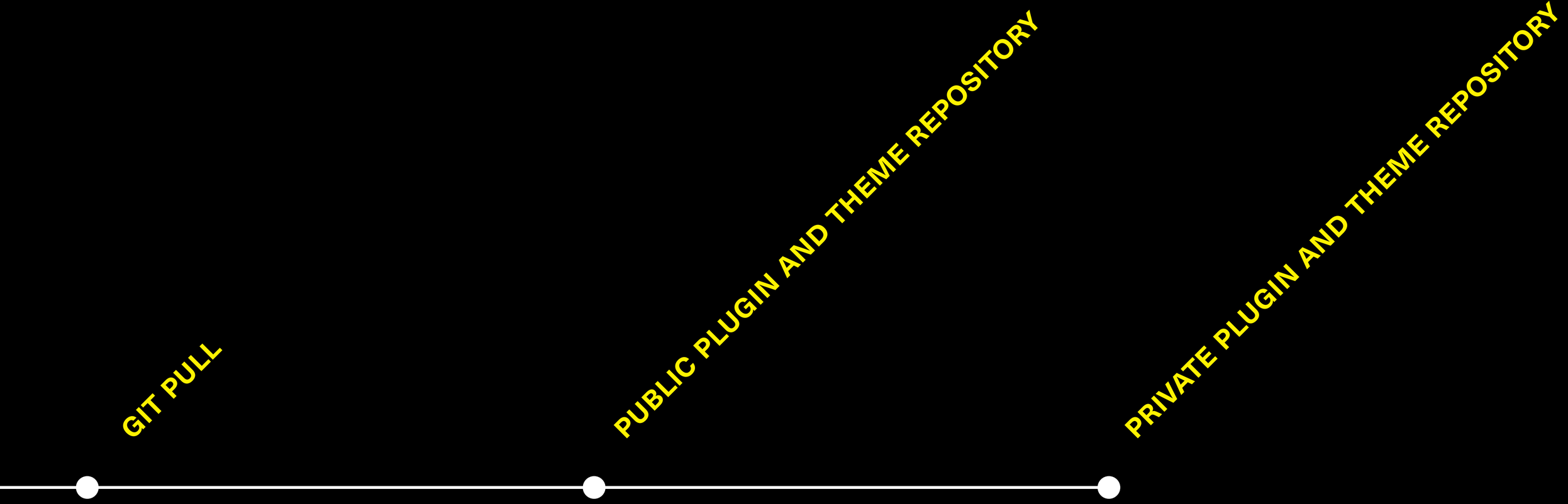
As a result, *Repo Lookout* sent **747,231 emails** to the technical contact, of which **520,916 emails** were successfully delivered.

Copyright 2022–24
Crissy Field GmbH

the continuum of deployment



the continuum of deployment



the continuum of deployment

There is a new version of WP Activity Log available. View version 5.3.1 details or update now.

Baizman Design

Deactivate

A plugin for the Baizman Design website.

Version 1.1.13 | By Saul Baizman | View details

Enable auto-updates

Enable auto-updates

Terminal — tmux — 80×24

```
$ wp @remote-host plugin update my-awesome-plugin
Downloading update...
Unpacking the update...
Installing the latest version...
Removing the old version of the plugin...
Plugin updated successfully.
+-------------------+-------------+-------------+---------+
| name              | old_version | new_version | status  |
+-------------------+-------------+-------------+---------+
| my-awesome-plugin | 1.0.0       | 1.0.1       | Updated |
+-------------------+-------------+-------------+---------+
Success: Updated 1 of 1 plugins.
```

[0] 1:zsh- 2:zsh 3:zsh 4:zsh* macbookair | 21.27

There is no off-the-shelf solution for you to build your own plugin and theme repository. Umm, what do I do?

How to Configure Self-Hosted Updates for Your Private Plugins

Prepare update server

Plugin update information

Push the update

Updated on March 10, 2022

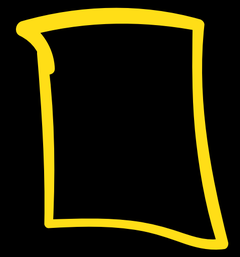
In this tutorial I will show you how to develop a custom update repository for your private plugin. It will be helpful if you're developing plugins for sale.

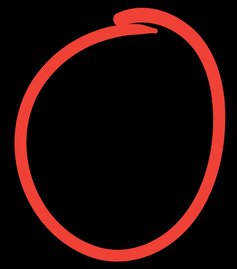
We are not going to use any ready or bloated PHP-libraries for that, only two filter hooks `plugins_api` and `site_transient_update_plugins` and transient cache, that's all.

You can also download the full code as a ready plugin from my GitHub.

And remember if you need some custom coding help, you can always get in touch with me and my team.

PLUGIN / THEME





PRIVATE
REPOSITORY
SERVER

```
{
   "name": "Your Plugin",
   "slug": "your-plugin-slug",
   "author": "your name",
   "version": "1.2.1",
   "package": "https://private-repository-server.org/your-plugin-slug.zip"
   ...
}
```

`update_themes_{$hostname}` (since 6.1)

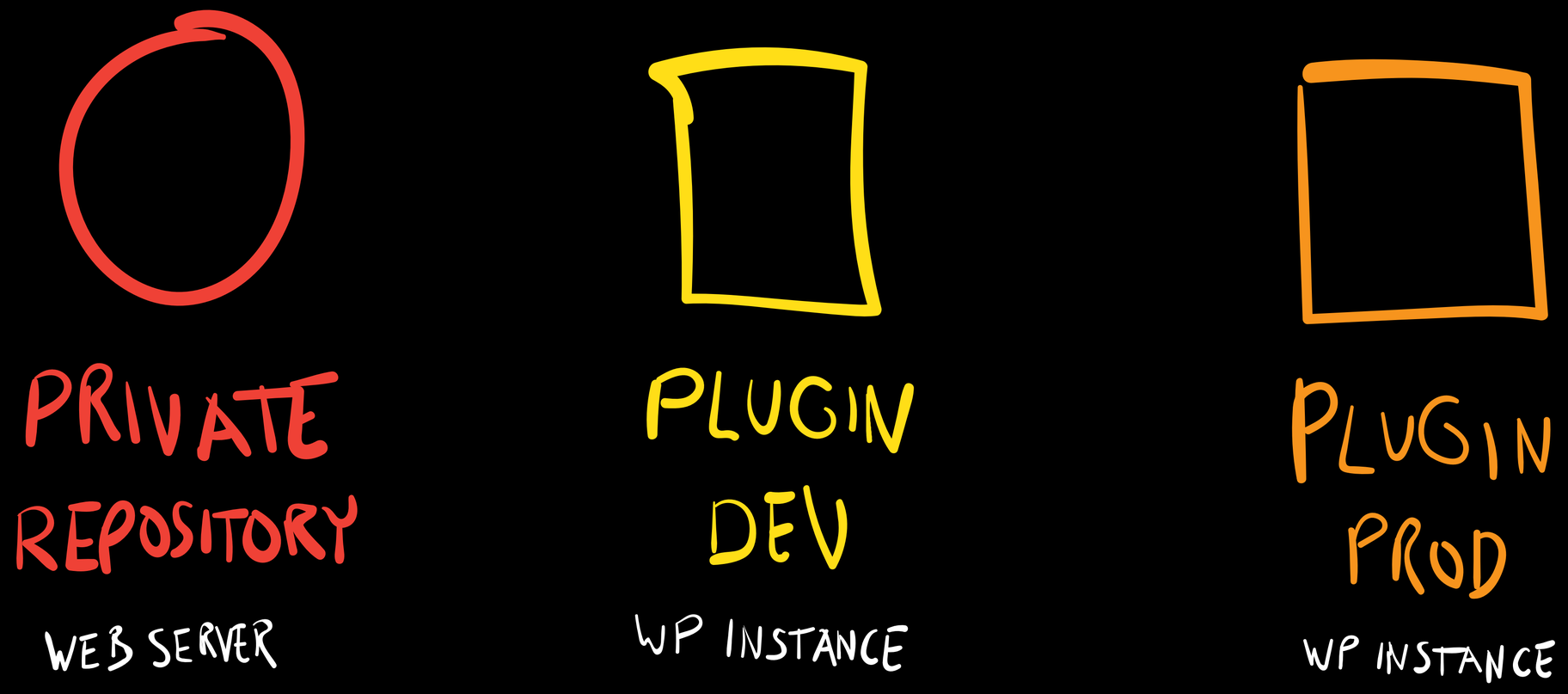
`update_plugins_{$hostname}` (since 5.8)

update_plugins_{$hostname}

```
<?php
/**
 * Plugin Name:   My Private Plugin
 * Plugin URI:    https://github.com/baizman-design/my-private-plugin/
 * Description:   A private plugin for a client website.
 * Version:       1.0.0
 * Author:        Saul Baizman
 * Author URI:    https://baizmandesign.com
 * Update URI:    https://private-repository-server.org
 */
```

update_plugins_private-repository-server.org

The hook is only fired once per domain.


PRIVATE REPOSITORY
WEB SERVER
PLUGIN DEV
WP INSTANCE
PLUGIN PROD
WP INSTANCE

I couldn’t use a local website as the private repository due to an SSL issue.

JSON response:


```
{
  "my-private-plugin": {
    "name": "My Private Plugin",
    "slug": "my-private-plugin",
    "package": "https://private-repository.baizmandesign.com/my-private-plugin.zip",
    "version": "1.0.1",
    "autoupdate": "true"
  }
}
```

Transient data is refreshed “occasionally.”

have a good way to reproduce the "issue" I've raised. How do we proceed?

danielbachhuber added state:approved and removed state:unconfirmed on Feb 11, 2024

danielbachhuber on Feb 11, 2024 Member

Oh, I see. I assumed `wp_update_plugins()` always made the outbound HTTP request. It looks like it bails early if there was a "recent" check: https://github.com/WordPress/wordpress-develop/blob/44a2073816ba8c474f598c348e4d334696b495e4/src/wp-includes/update.php#L385-L388

Today I learned!

`wp core check-update` has a `--force-check` flag, so let's add the same to `wp plugin list` and `wp theme list`. We can forcefully trigger the update check by deleting the `update_plugins` transient when the flag is present.

When writing tests, you can write a test value to the `update_plugins` transient that persists when the flag isn't present, and gets updated when the flag is present.

baizmandesign on Feb 12, 2024 Author

@danielbachhuber I like the idea of adding a `--force-check` flag to the `plugin list` and `theme list` commands. (Part of me thinks this should be the default behavior and not require an extra flag, but I also understand why you would want WP CLI to mirror the behavior of the web interface.)

When this is implemented, can I simply configure my `wp-cli/config.yml` to always pass this flag to the list commands? I

Update notifications do not appear when the plugin/theme is disabled.

Download the code and slides:
https://github.com/baizman-design/boston-wordpress-meetup-202502

Next steps

- Use git tags for versioning (via git string substitution).
- Exclude developer files (via `.gitattributes` and “export-ignore”).
- Connect JSON version value to VCS (GitHub, Bitbucket, etc.) via their REST API.
- Add CI/CD to upload ZIP archive to the private repository server.
- Add CI/CD to push updates to WordPress via WP CLI + Docker.
- Refactor JSON response to use OOP and add support for themes.
- Populate “view details” modal window (description, installation, changelog, etc.).
- Work around one hostname per asset issue.

Questions?

Thank you.

BAIZMANDESIGN