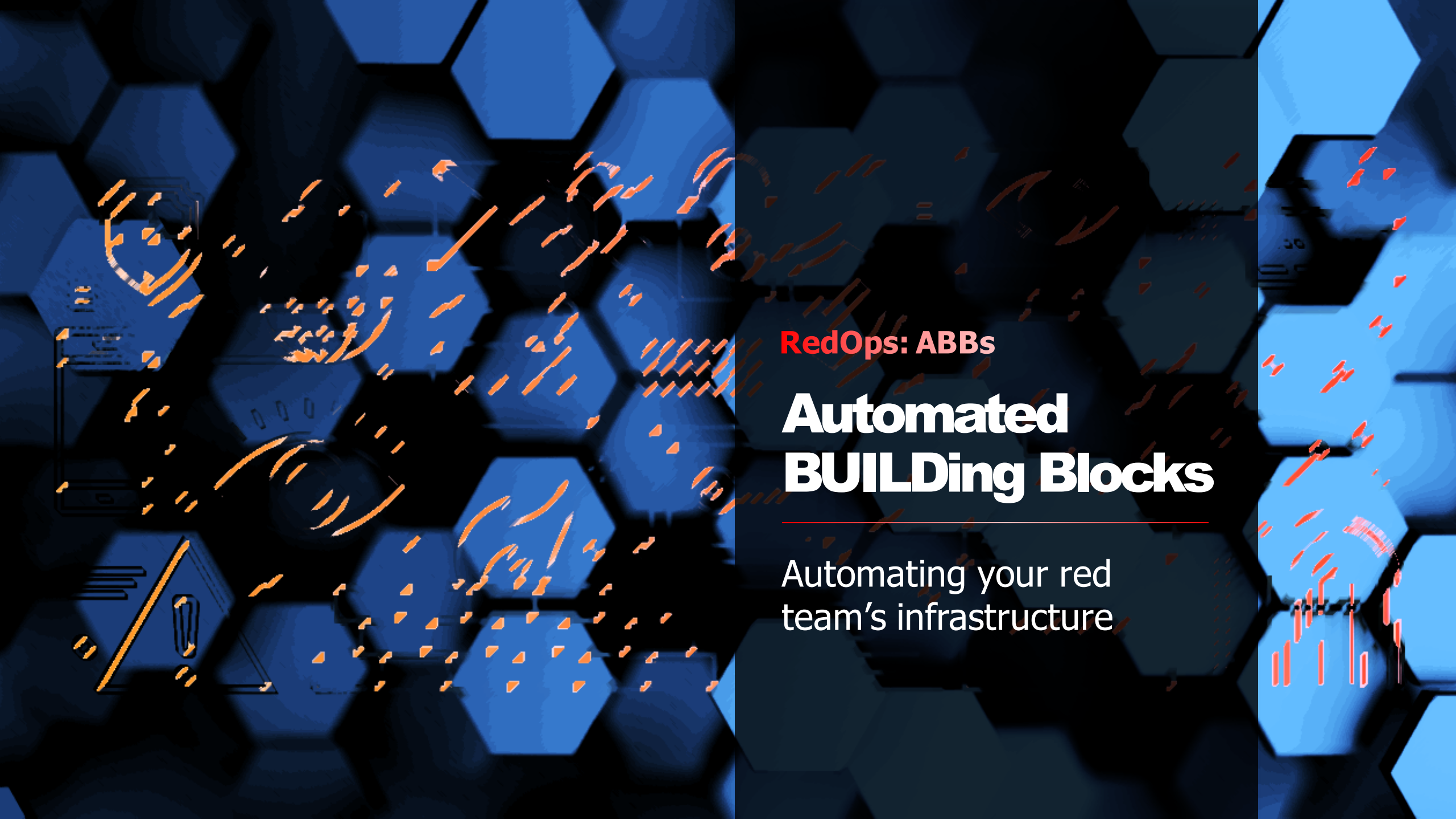




RedOps: ABBs

Automated BUILDing Blocks

Automating your red
team's infrastructure



whoami

Experience

IT/Security for 40...I mean 4 years... (:



Community

Professionally Evil

49th Security Division

Charlotte Hackers Anonymous



Work

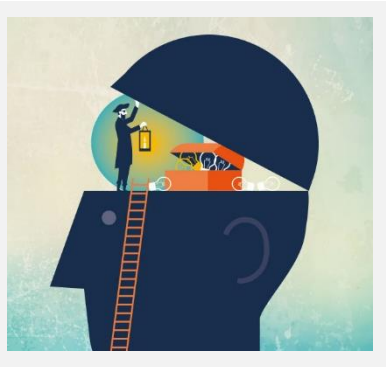
Pentester

Ops

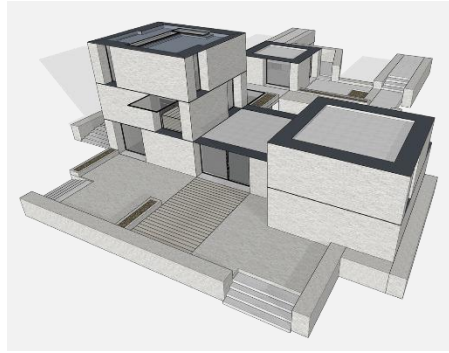
Developer



Class Outline



Introduction



High-level Overview



Basic Build



Build Pipeline

What is...



Pentesting



Kali Linux



Virtual Machine

What is...



DevOps



Automation



Successful Automation



This Workshop

- Primary Goal
- Objectives
- Our Perspective



Drivers

Why automate?



Who is this for?



Why automatic vs. manual?

Comparison

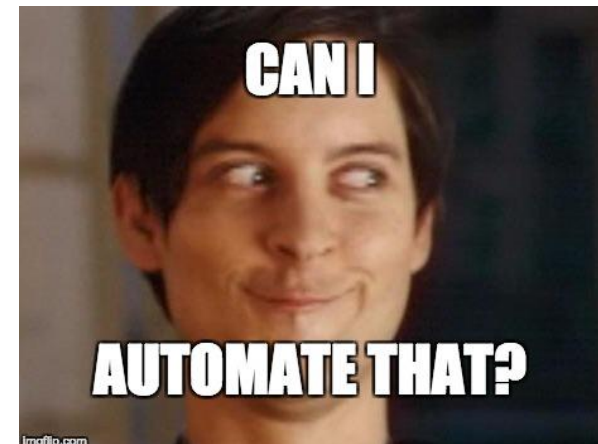
Automatic

- Idempotency
 - Repeatable
 - Consistent
 - Time re-gained



Manual

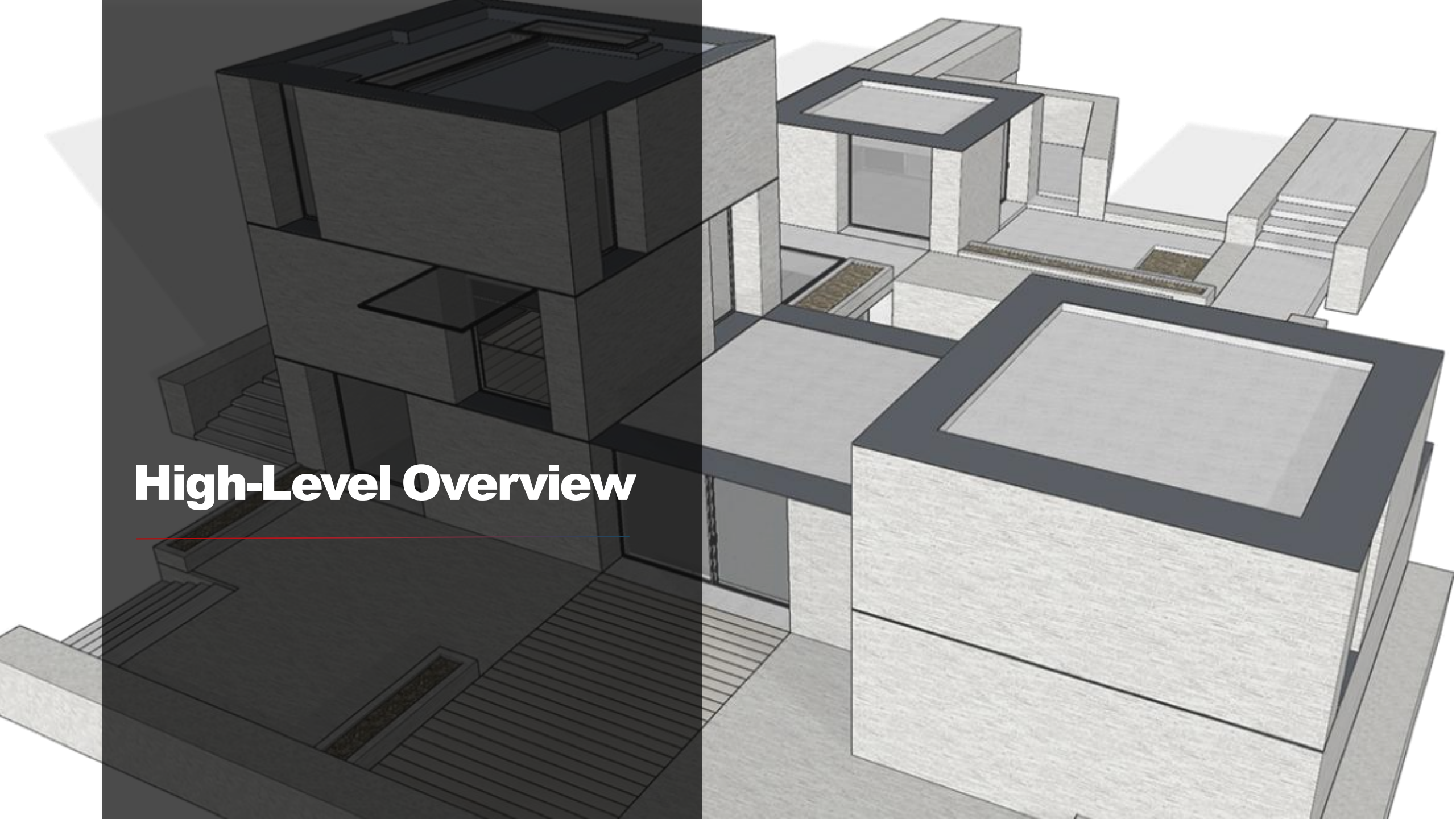
- Human error
- Time consumption
 - Remember your preferences



A still life photograph of a breakfast scene. A white ceramic cup filled with coffee sits on a matching saucer. Steam rises from the cup. Next to the cup are two chocolate chip cookies. In the background, two golden-brown croissants are visible. The entire scene is set on a rustic wooden surface. In the foreground, some coffee beans are scattered. The image has a dark, moody atmosphere with soft lighting.

BREAK

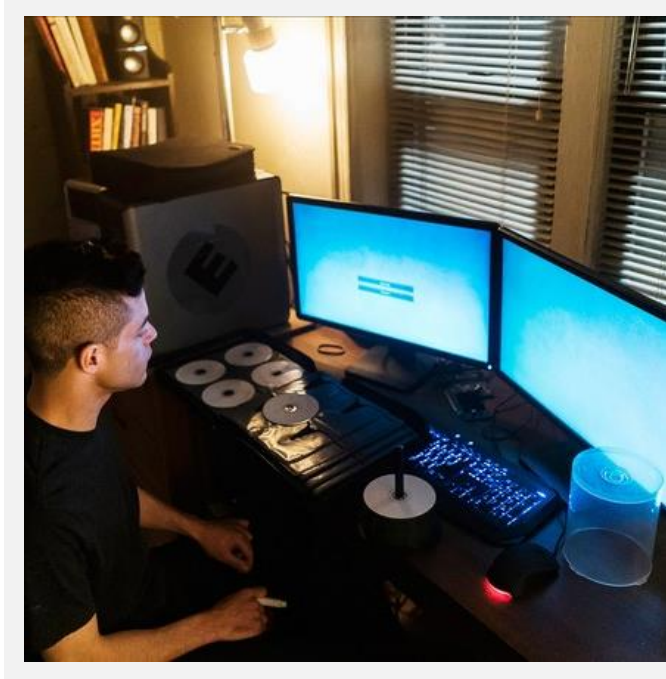
Let's take a quick 5 – 10 min break



High-Level Overview

Different Users

- Consumer
- Custom (framework)
- Contributor



Consumer



Vagrantfile



GitHub



Customization

Custom (framework)



This Workshop



Alterations

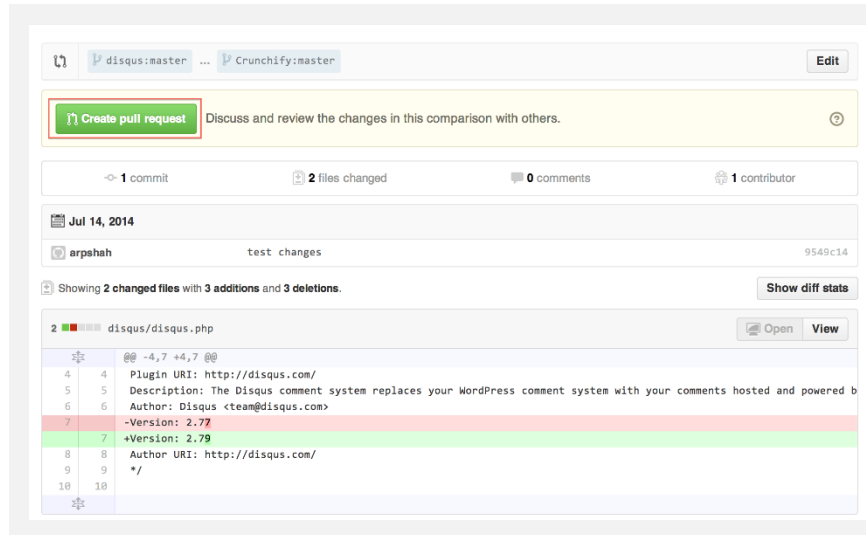


Modularity

Contributor



Find Bugs



Want a feature?

```
/**
 * Simple HelloButton() method.
 * @version 1.0
 * @author john doe <doe.j@example.com>
 */
HelloButton()
{
    JButton hello = new JButton( "Hello, wor
    hello.addActionListener( new HelloBtnList

    // use the JFrame type until support for t
    // new component is finished
    JFrame frame = new JFrame( "Hello Button"
    Container pane = frame.getContentPane();
    pane.add( hello );
    frame.pack();
    frame.show(); // display the fra
}
```

Docs

Basic Build



Basic Build - Tools



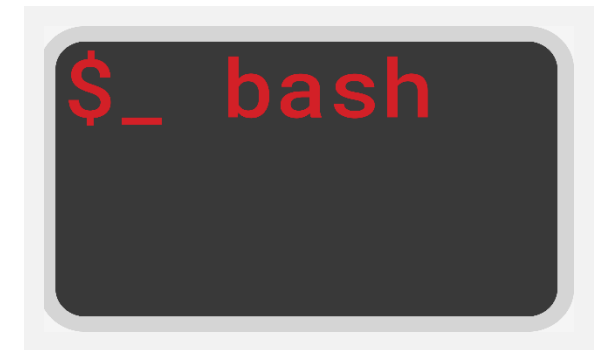
Packer



Vagrant



VirtualBox



Shell Scripts

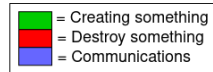
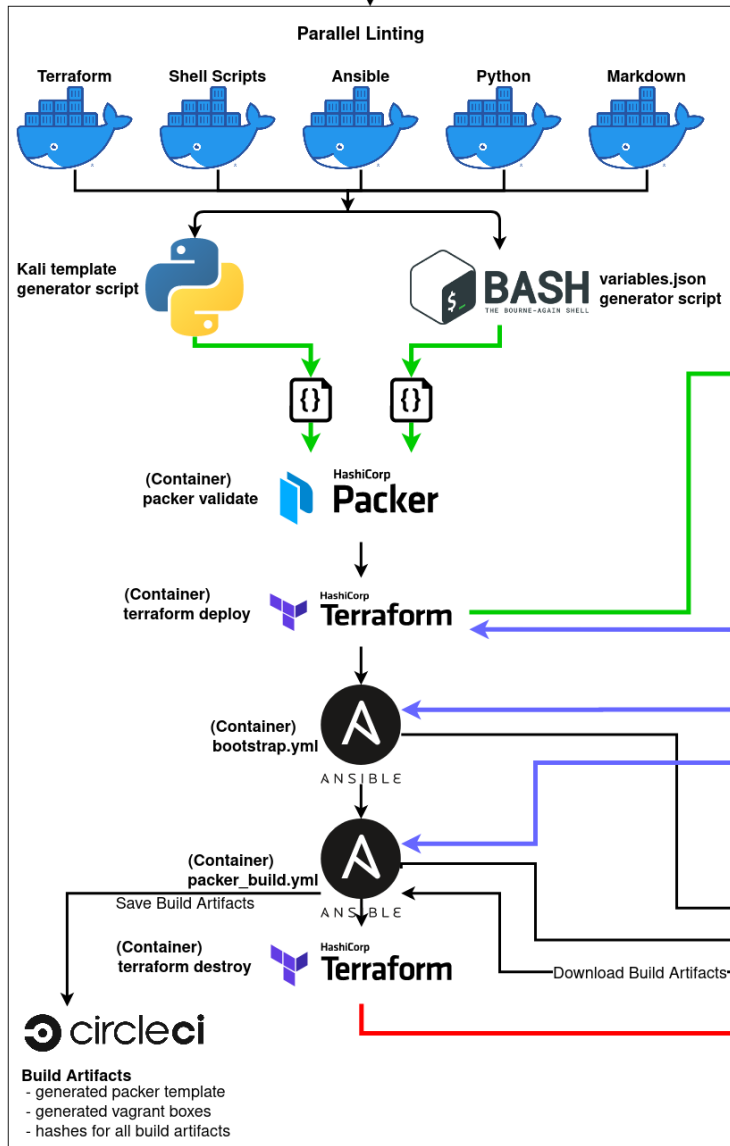
Basic Build – Kali Auto Installation



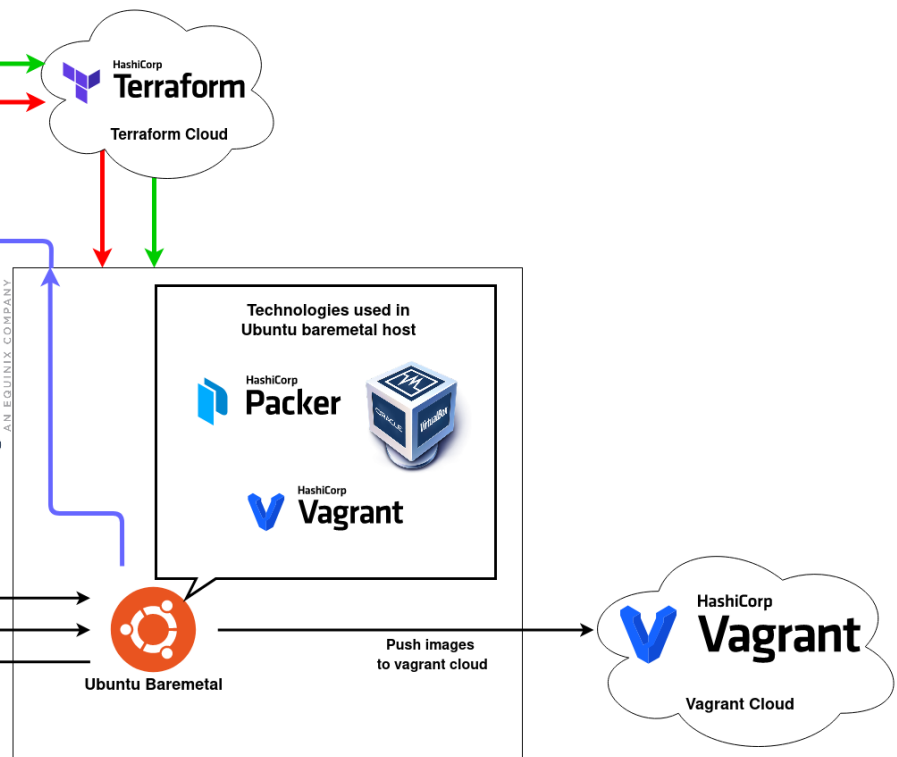
Build Pipeline



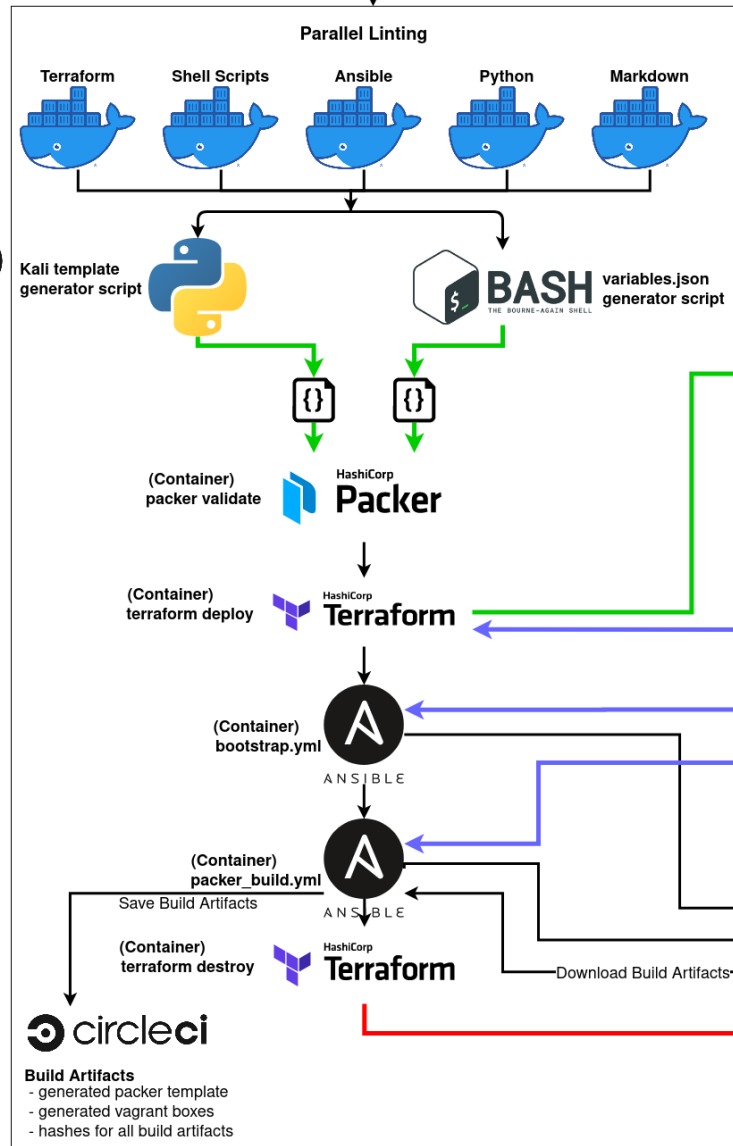
circleci



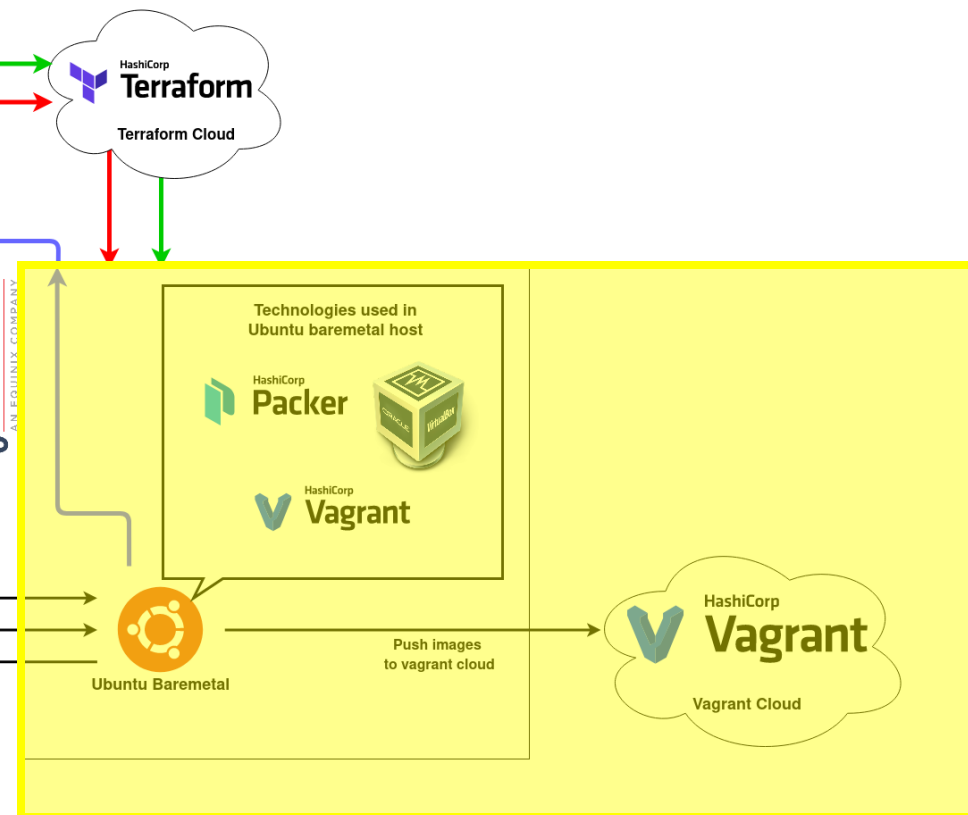
packet
AN EQUINIX COMPANY



circleci



= Creating something
= Destroy something
= Communications



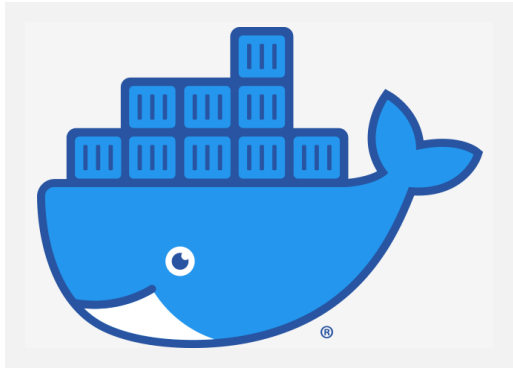
Basic Build - Tools

	Basic Build	Advanced (Build Pipeline)	Future Features
Packer	✓		
Vagrant	✓		
Bash	✓		
Docker			
Python			
Terraform			
Ansible			
Virtual Box	✓		
VM Ware			
Hyper-V			
KVM/QEMU			

Build Pipeline - Tools

	Basic Build	Advanced (Build Pipeline)	Future Features
Packer	✓	✓	
Vagrant	✓	✓	
Bash	✓	✓	
Docker		✓	
Python		✓	
Terraform		✓	
Ansible		✓	
Virtual Box	✓	✓	
VM Ware			
Hyper-V			
KVM/QEMU			

Build Pipeline Tools



Docker



Python

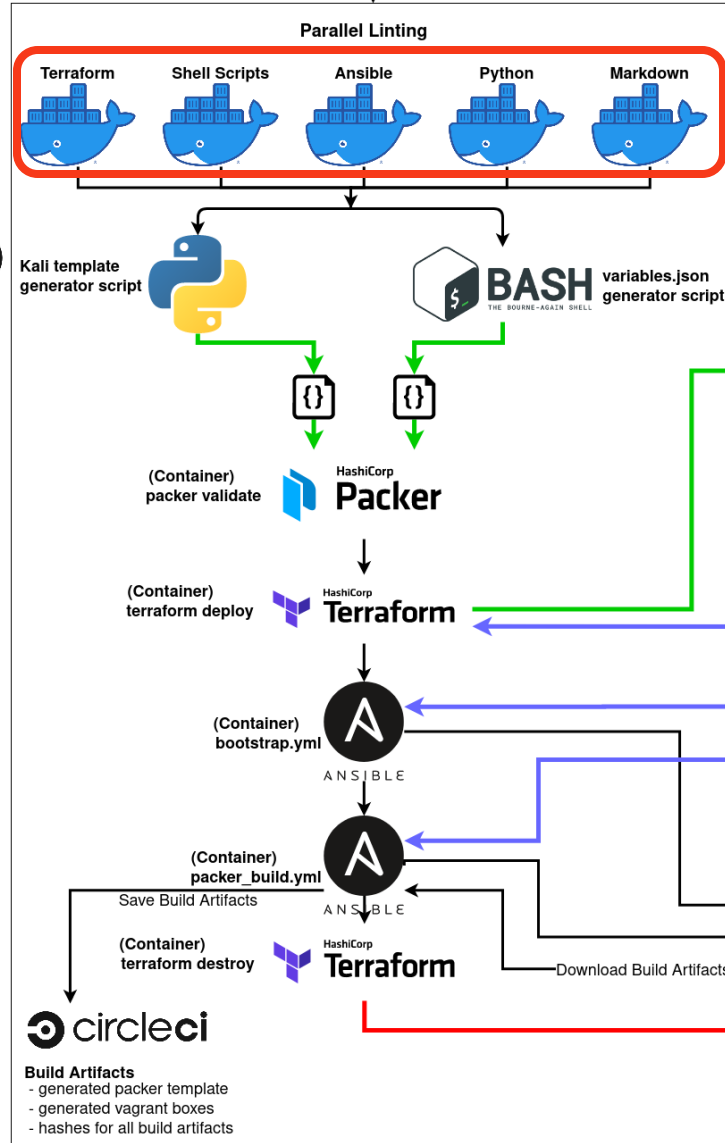


Terraform



Ansible

circleci

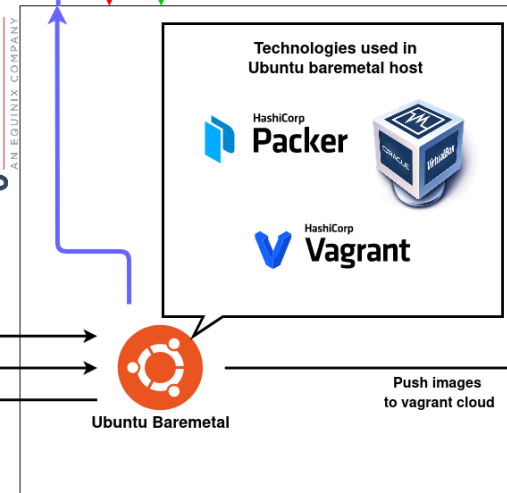


= Creating something
 = Destroy something
 = Communications

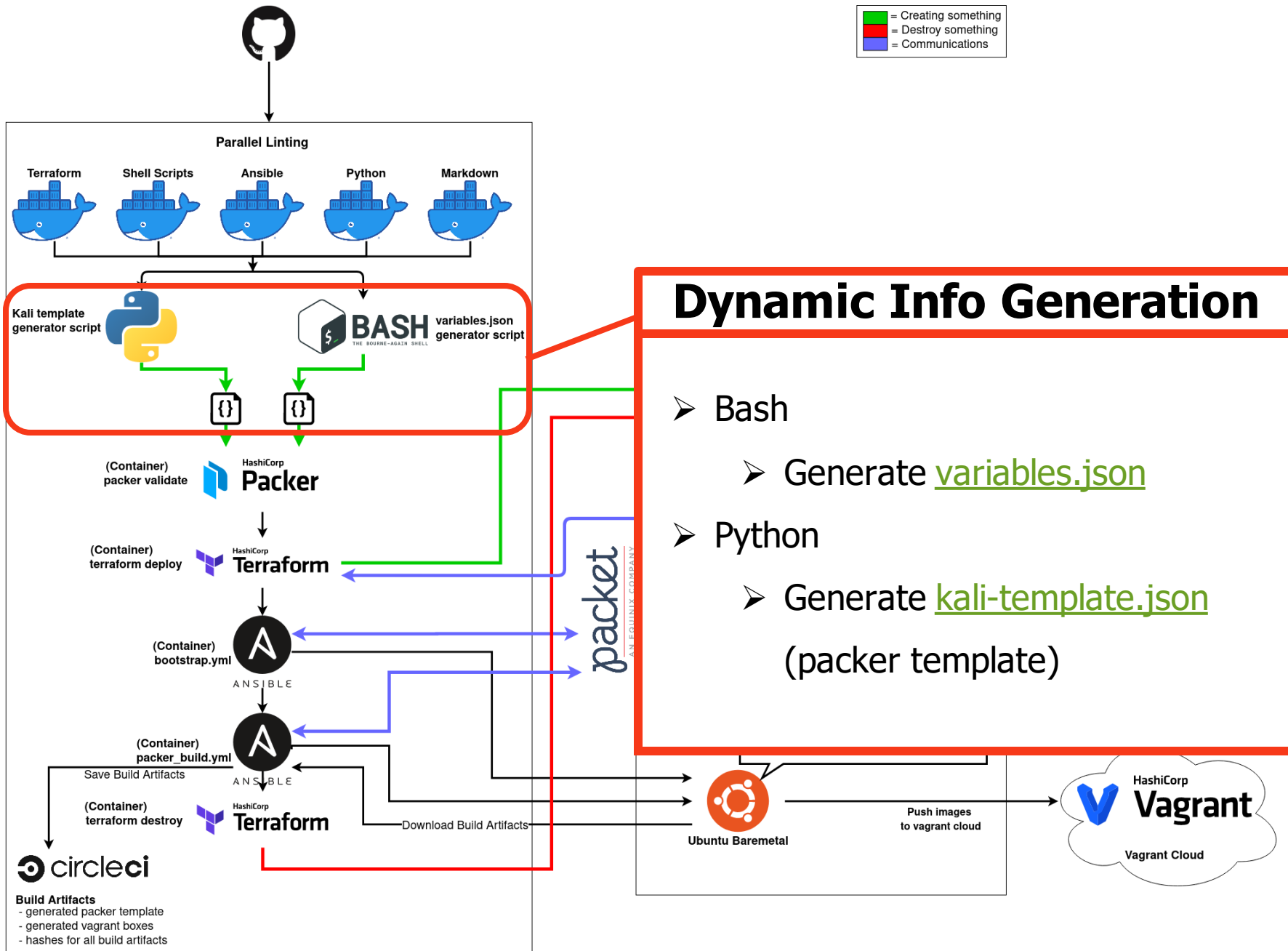
Linting

- shellcheck
- markdownlint
- ansible-lint
- terraform

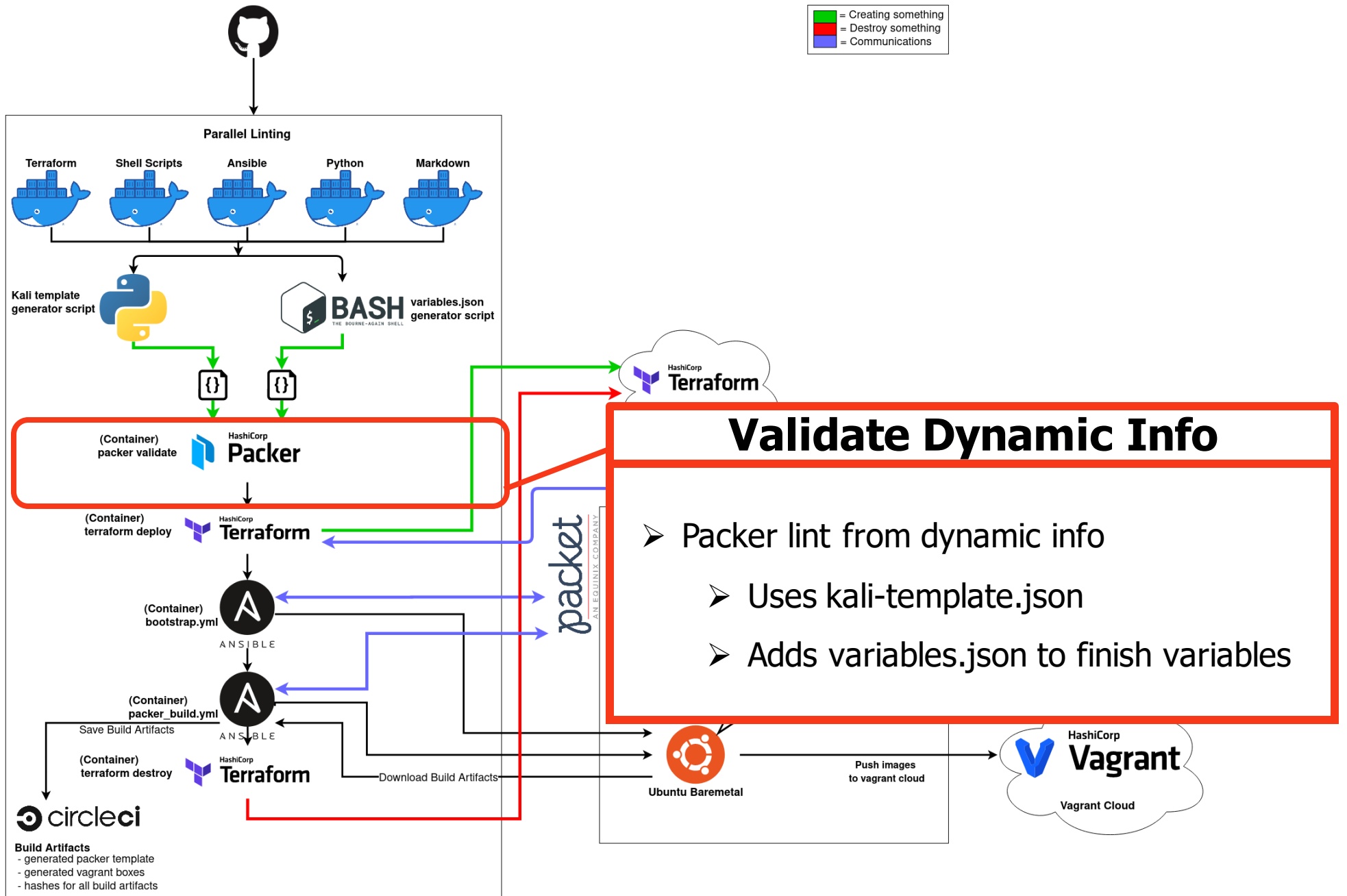
packet
AN EQUINIX COMPANY



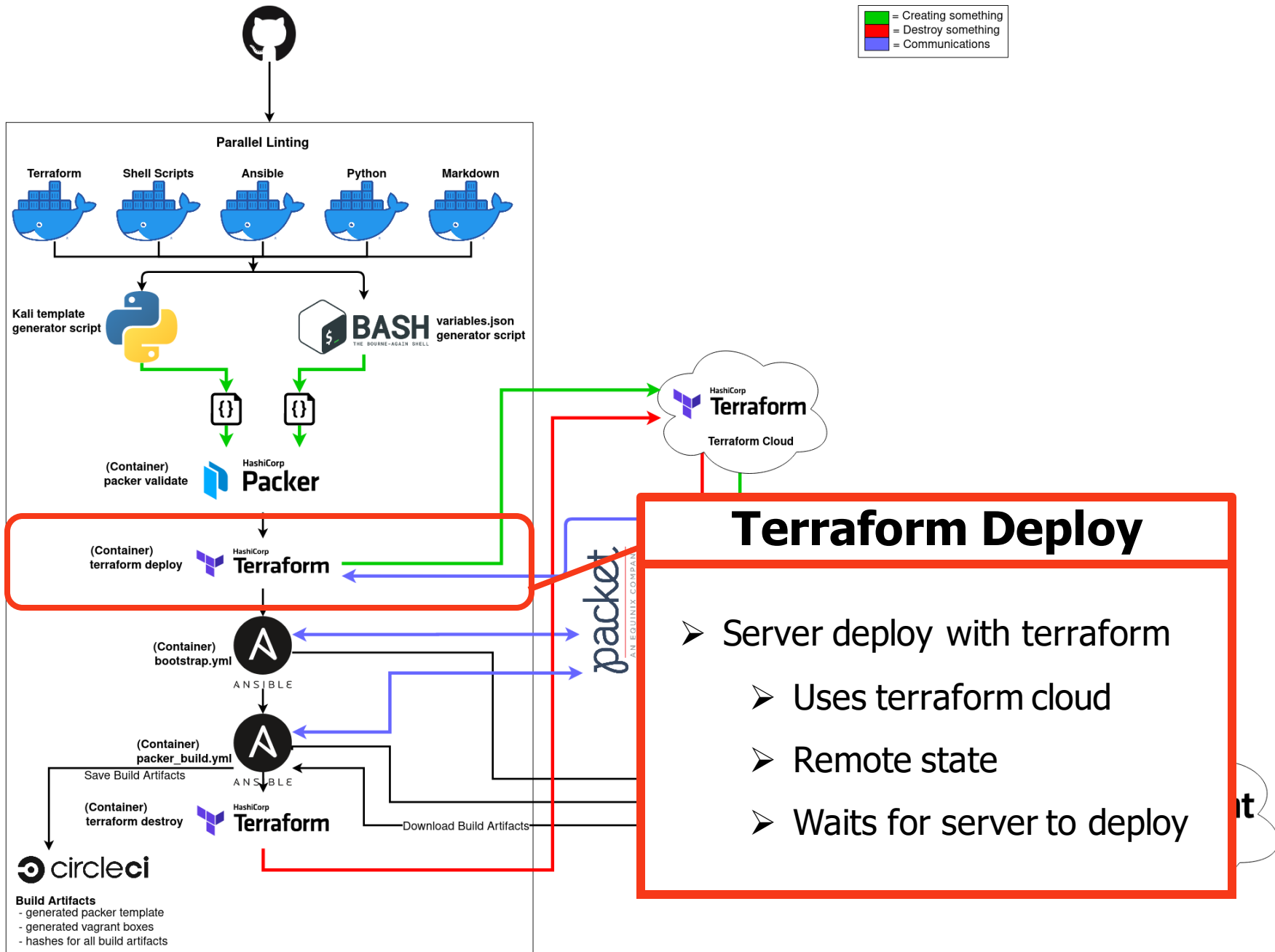
circleci

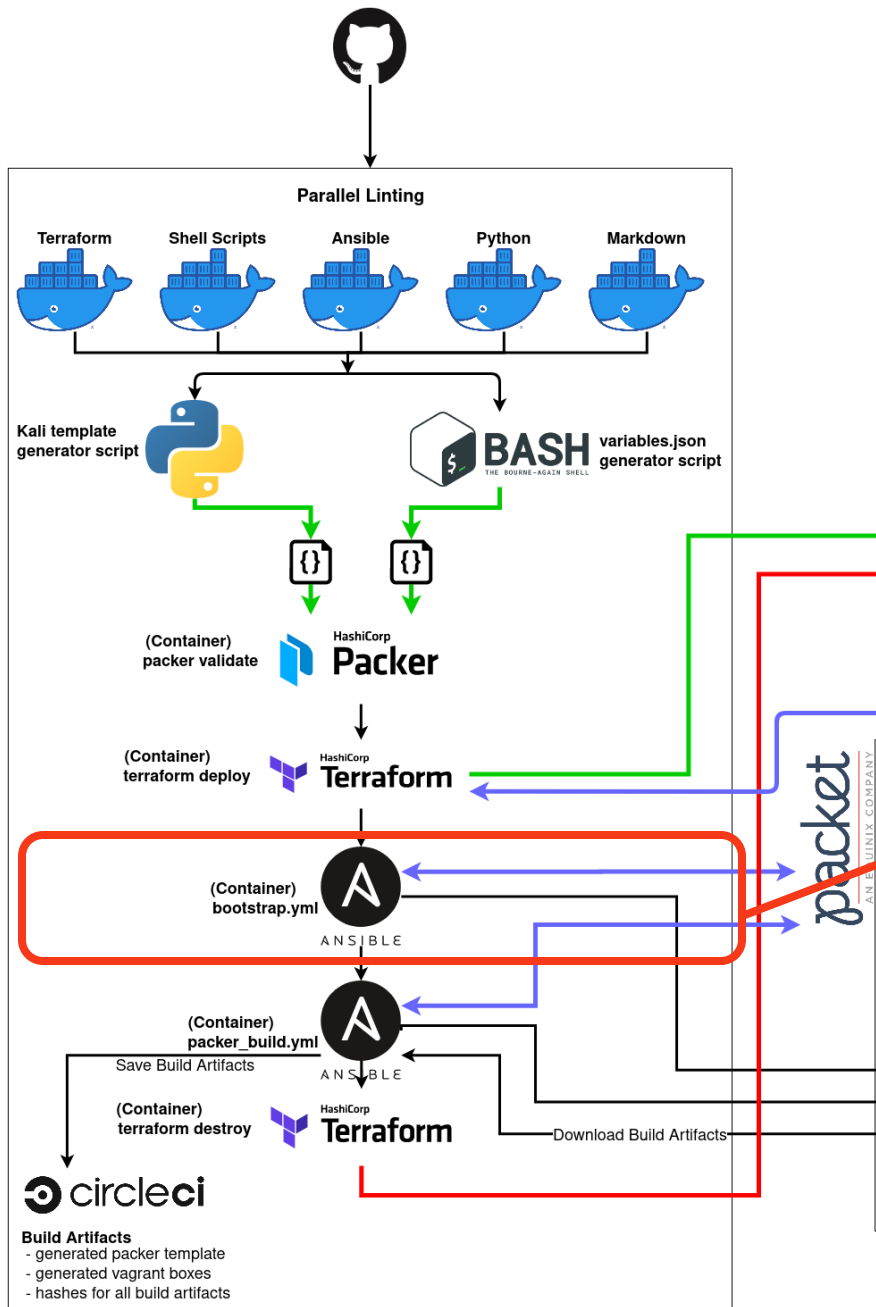


circleci



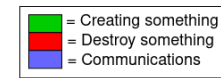
circleci





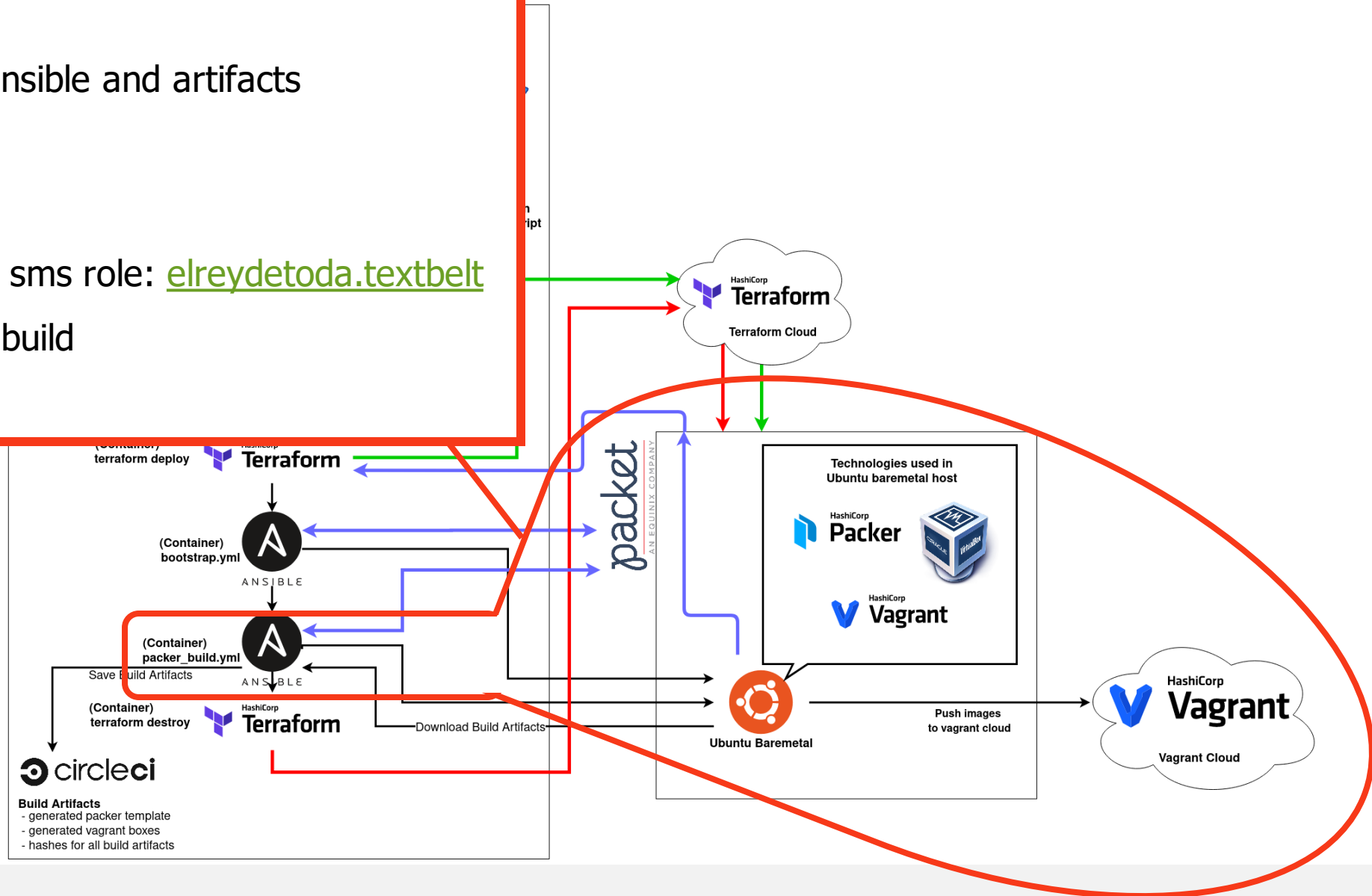
Server Provision

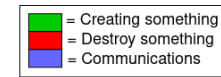
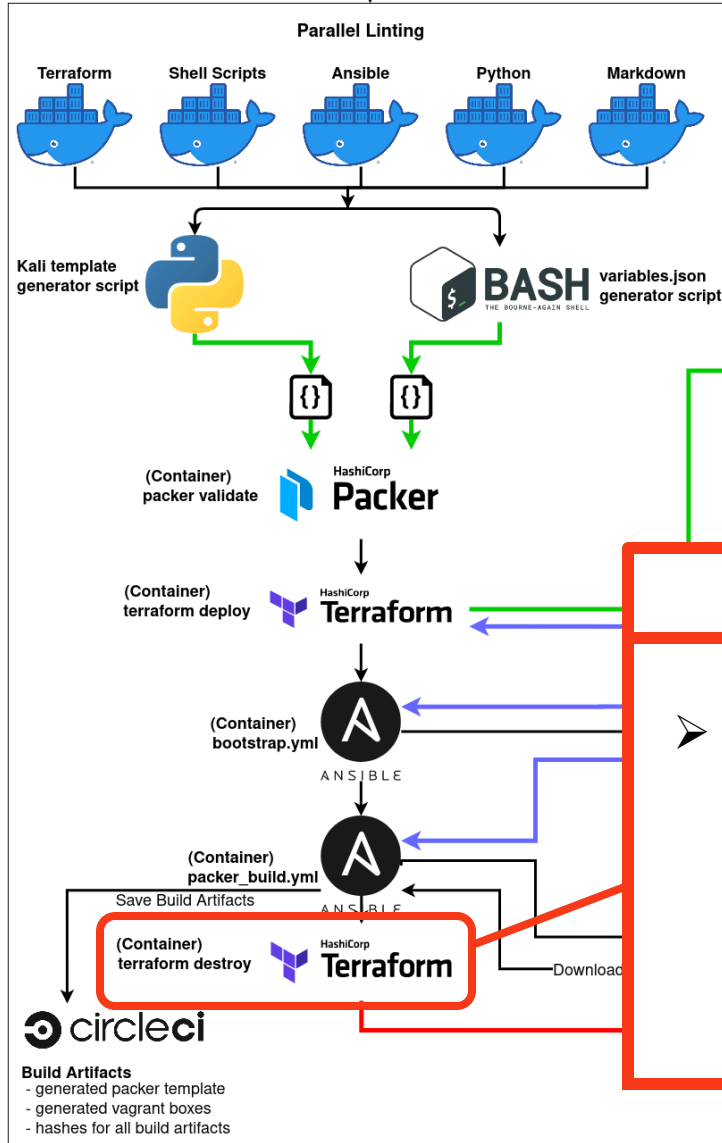
- Server provision with ansible
- Ansible collection: [elreydetoda.virtualization](https://github.com/elreydetoda/ansible-collection-virtualization)
 - Hypervisors
 - Build tools
 - Packer
 - Vagrant
- UFW OpenSSH only



Build Process

- Build with ansible and artifacts
- Build
 - Rsync
 - Ansible sms role: [elreydetoda.textbelt](https://github.com/elreydetoda/textbelt)
 - Packer build
- Artifact(s)





Terraform Destroy

- Server deploy with terraform
 - Uses terraform cloud
 - Remote state
 - Waits for server to destroy





Let's get set up!

Your Turn

elrey.casa/auto-kali-w

Workshop Instructions

Services

You will need to go to each of these websites and sign up for an account to each of them, and just so you know all of these websites are either free to use as an individual, optional, or I have a voucher to give you to make it free for up to \$50. This will allow you to interact with their services, and leverage them for automation. This is only required for the build path that we will be using during the workshop, and we are using this as the lowest common denominator in case people don't have access to decently powerful processing machines.

Required (for workshop) - all free/voucher|

- Github - <https://github.com/join>
- CircleCI - <https://circleci.com/signup/> (uses Github account for login)
- Terraform Cloud - <https://app.terraform.io/signup/account>
- Vagrant Cloud - <https://app.vagrantup.com/account/new>
- Packet - <https://app.packet.net/signup>
 - This is the service that you will be given the voucher for

Optional

- TextBelt - <https://textbelt.com/purchase/?generateKey=1>
 - This service is used to text you at vital points of the build process to inform you as to what is happening in your build.

A white ceramic cup filled with a frothy coffee beverage sits on a matching saucer. The cup is placed on a rustic wooden surface. To the right of the cup, there are two golden-brown croissants and two chocolate chip cookies. Steam is rising from the cup, suggesting it is hot. The background is dark and out of focus.

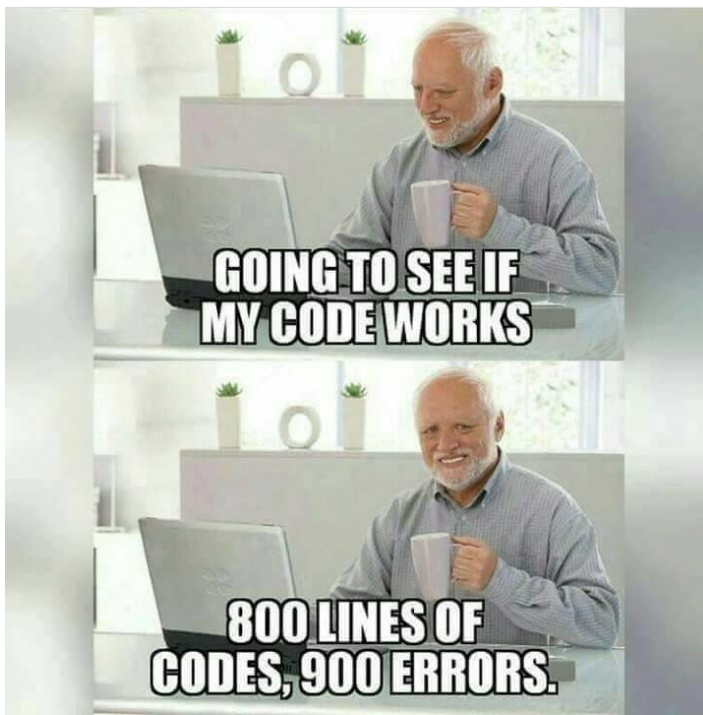
BREAK

Let's take a quick 5 – 10 min break

elrey.casa/auto-kali-w



Stages of Building



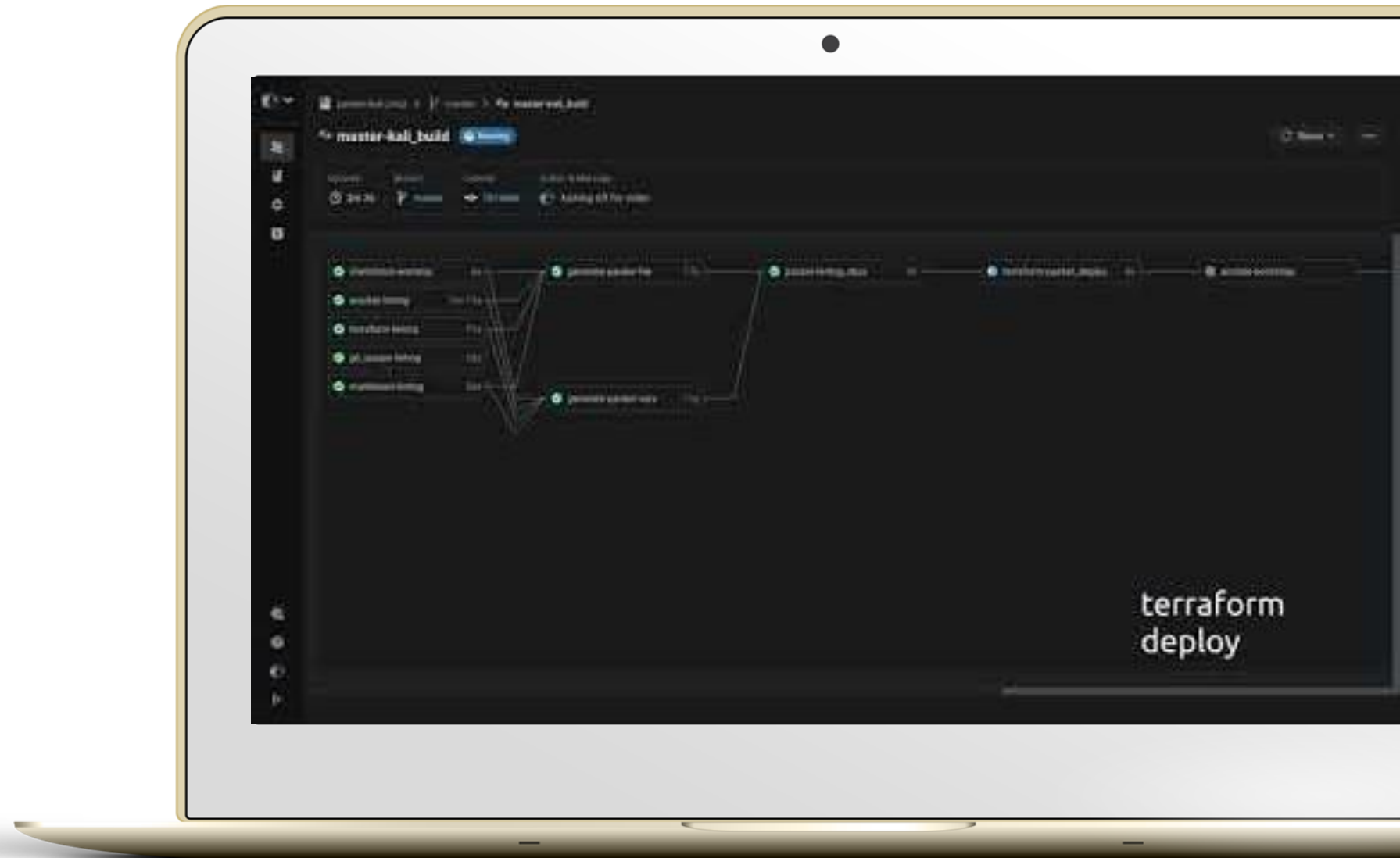
Because everything always works on the first try, right?



When your code compiled successfully after 10 try but you didn't change anything ...



Build Pipeline Recording



YOU AUTOMATED YOUR AUTOMATION!

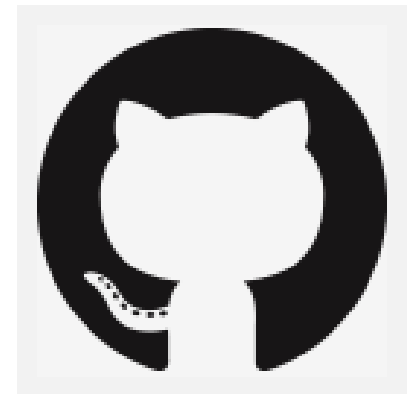
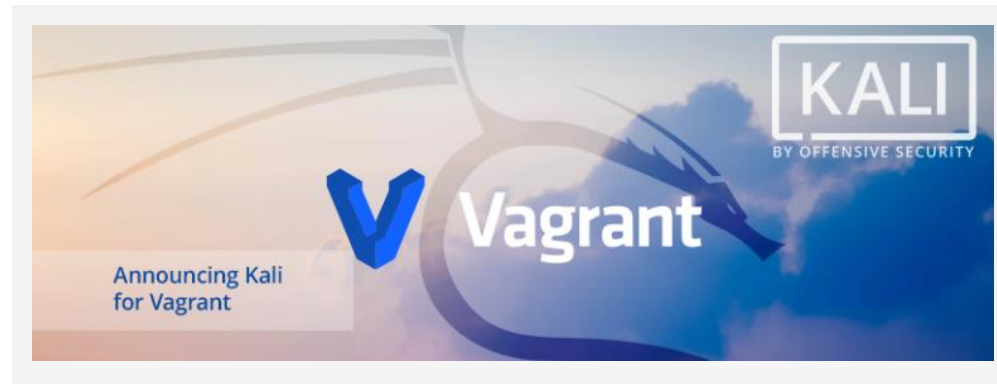


Future Features

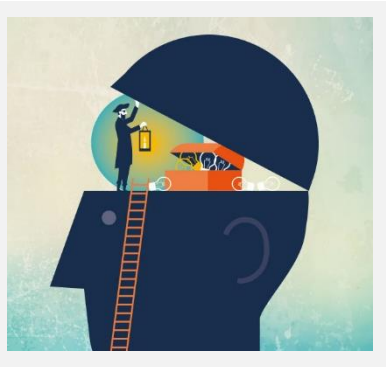
	Basic Build	Advanced (Build Pipeline)	Future Features
Packer	✓	✓	✓
Vagrant	✓	✓	✓
Bash	✓	✓	✓
Docker		✓	✓
Python		✓	✓
Terraform		✓	✓
Ansible		✓	✓
Virtual Box	✓	✓	✓
VM Ware			✓
Hyper-V			✓
KVM/QEMU			✓

Clarifications

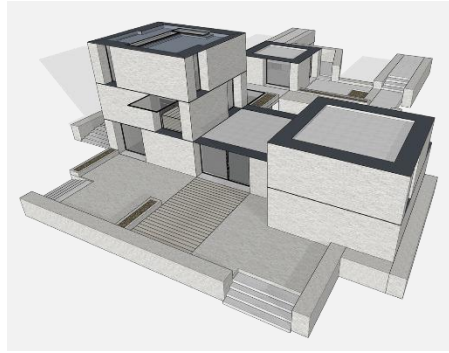
- Pentester vs Red Teamer
- My project
- Get Involved



Foundation Complete



Introduction



High-level Overview



Basic Build



Build Pipeline

Resources

- [Tracking RedOps](#)
- Get Involved
- [Image Credit Srcs](#)
- [Pentesting vs Red Team](#)