HITB SECCONF SIN-2021

SCALING UP OFFENSIVE PIPELINES

Gil Biton

Offensive Security Engineer, SYGNIA

@B1t0n_ B1t0n#4141 https://www.linkedin.com/in/gil-biton-a3a385101/ https://github.com/B1t0n

TRACK 1

CONTEXT

Red/Purple teaming became harder

Weaponization duration may take a lot of time and is also repetitive

Team collaboration can be lost

Memorizing and storing published tools or techniques may be complicated

CI/CD to **the rescue**

CI/CD pipelines concepts already adapted by the community with the goal of helping red teamers to automate tasks that are related to offensive tools weaponization.

We cannot automate an entire red team operation, but we can automate time consuming, repetitive red team tasks in different methods.

THE NEED

Our evolving team of adversaries required a CI/CD framework to answer specific needs

Simplicity

Modularity

Automated

Collaborative

Self-managed

On-demand

WHY USING **GITLAB** AS CI/CD FOR **OFFENSIVE PIPELINES?**

Simplicity

Self-managed

On-demand

What is GitLab?

“GitLab is the open DevOps platform, delivered as a single application. This makes GitLab unique and creates a streamlined software workflow, unlocking your organization from the **constraints of a pieced together toolchain**. Learn how GitLab offers unmatched visibility and **higher levels of efficiency** in a single application across the **DevOps lifecycle**.

GitLab started as an open source project to help teams **collaborate on** software development. GitLab's mission is to provide a place where everyone can contribute. Each team member **uses our product internally** and directly impacts the company roadmap. This exceptional approach works because we're a team of passionate people who want to see each other, the company, and the broader GitLab community succeed and we have the platform to make that possible.”

Source: https://about.gitlab.com/what-is-gitlab/

Modularity

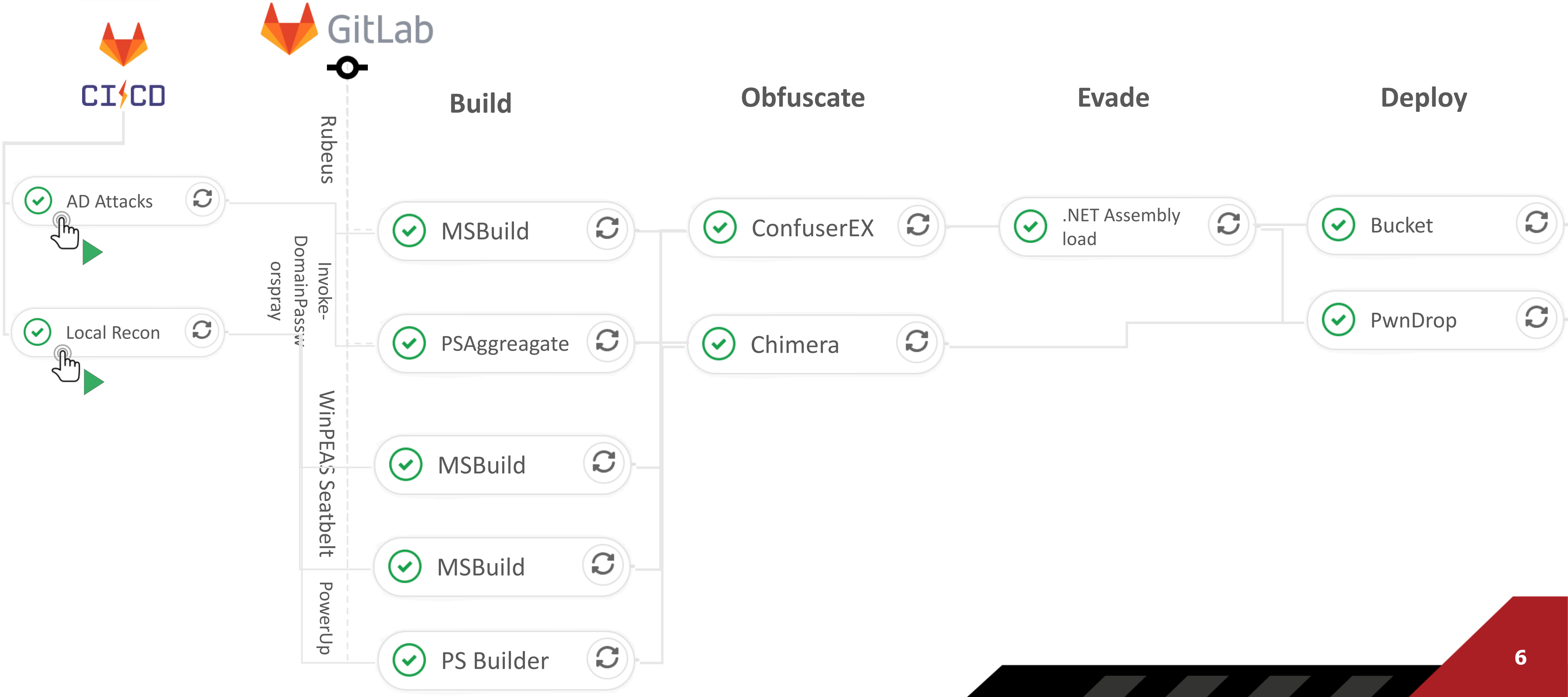
Automated

Collaborative

WHY USING **GITLAB** AS CI/CD FOR **OFFENSIVE PIPELINES?**

- Version Control
- Rich RESTful API
- Detailed documentation
- Gitlab CI/CD
  - YAML format recipes
  - Docker, K8s integration for running job
  - Rule based job triggering
  - Multi-pipeline support
- And many more to explore!

OFFENSIVE PIPELINE EXAMPLE



CI/CD

GitLab

Build

Obfuscate

Evade

Deploy

AD Attacks

Local Recon

Rubeus

Invoke-
DomainPassw
orspray

WinPEAS Seatbelt

PowerUp

MSBuild

PSAggreagate

MSBuild

MSBuild

PS Builder

ConfuserEX

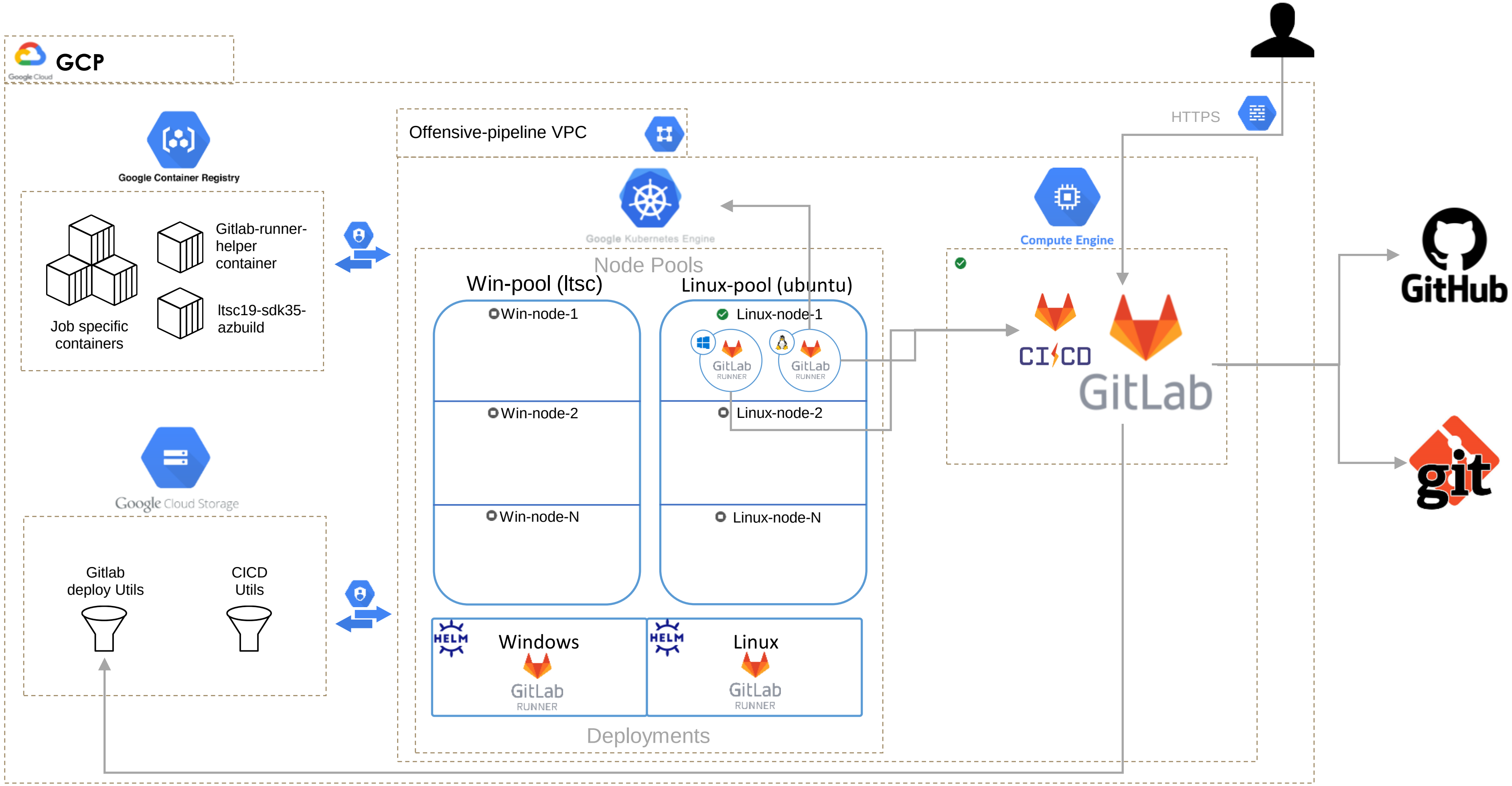
Chimera

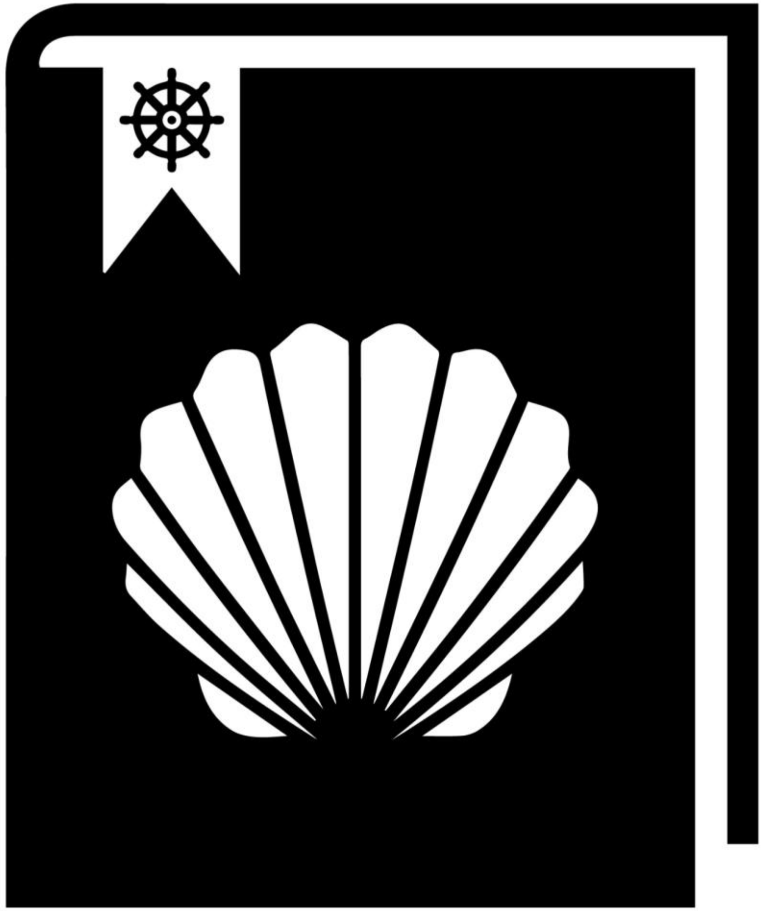
.NET Assembly load

Bucket

PwnDrop

ARCHITECTURE

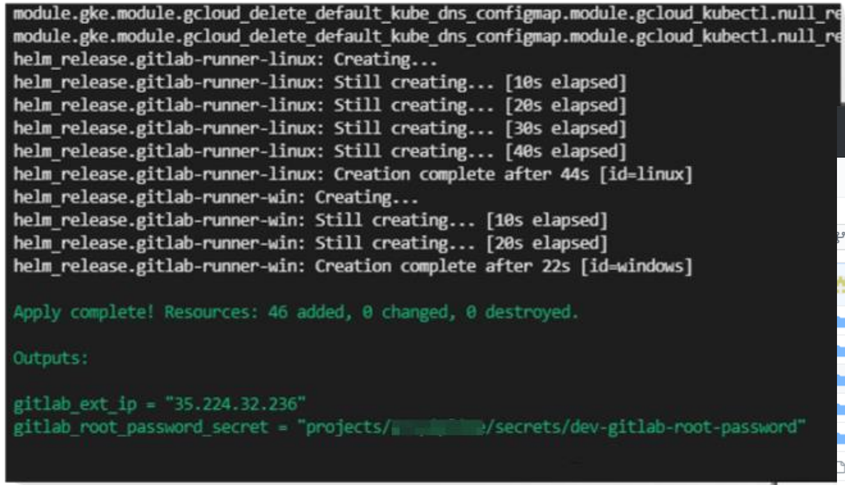




SCALLOPS

GETTING STARTED

- Refer to the framework's Github repository at: https://github.com/SygniaLabs/ScallOps
- Configure the Terraform variables and authenticate to your GCloud.
- Deploy the framework and wait to receive the Gitlab external IP.
- For additional Information refer to the README.

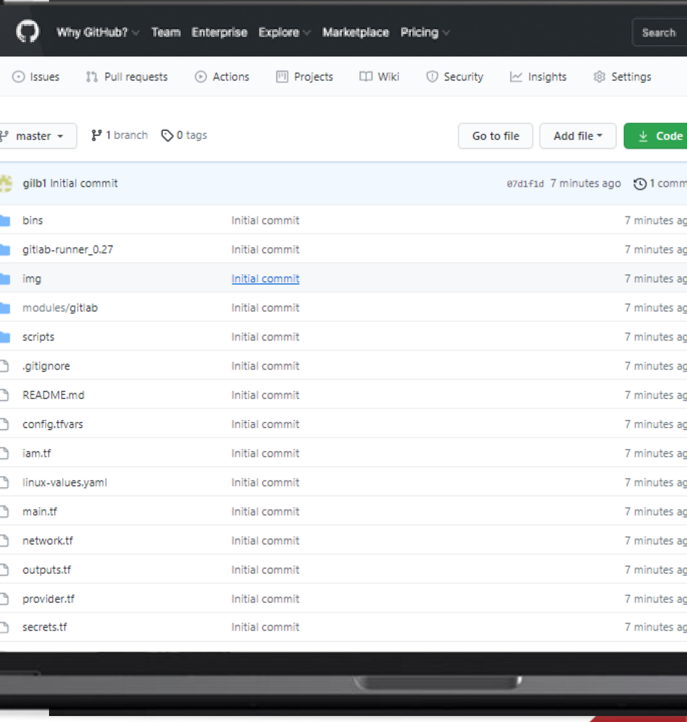


```
module.gke.module.gcloud_delete_default_kube_dns_configmap.module.gcloud_kubectl.null_re
module.gke.module.gcloud_delete_default_kube_dns_configmap.module.gcloud_kubectl.null_re
helm_release.gitlab-runner-linux: Creating...
helm_release.gitlab-runner-linux: Still creating... [10s elapsed]
helm_release.gitlab-runner-linux: Still creating... [20s elapsed]
helm_release.gitlab-runner-linux: Still creating... [30s elapsed]
helm_release.gitlab-runner-linux: Still creating... [40s elapsed]
helm_release.gitlab-runner-linux: Creation complete after 44s [id=linux]
helm_release.gitlab-runner-win: Creating...
helm_release.gitlab-runner-win: Still creating... [10s elapsed]
helm_release.gitlab-runner-win: Still creating... [20s elapsed]
helm_release.gitlab-runner-win: Creation complete after 22s [id=windows]

Apply complete! Resources: 46 added, 0 changed, 0 destroyed.

Outputs:

gitlab_ext_ip = "35.224.32.236"
gitlab_root_password_secret = "projects/[redacted]/secrets/dev-gitlab-root-password"
```



gilb1 Initial commit 07d1f1d 7 minutes ago 1 comm

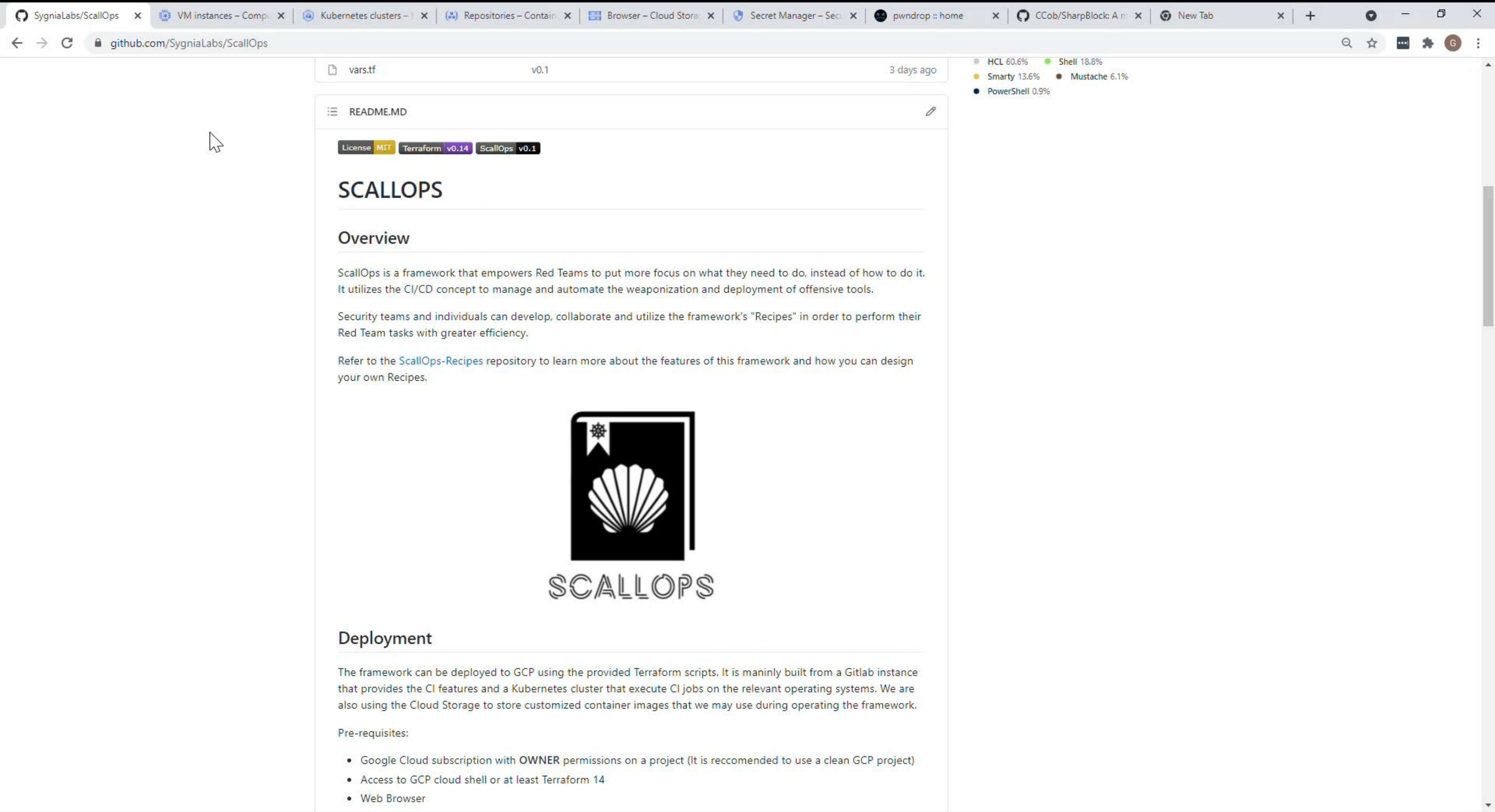
bins	Initial commit	7 minutes ag
gitlab-runner_0.27	Initial commit	7 minutes ag
img	Initial commit	7 minutes ag
modules/gitlab	Initial commit	7 minutes ag
scripts	Initial commit	7 minutes ag
.gitignore	Initial commit	7 minutes ag
README.md	Initial commit	7 minutes ag
config.tfvars	Initial commit	7 minutes ag
iam.tf	Initial commit	7 minutes ag
linux-values.yaml	Initial commit	7 minutes ag
main.tf	Initial commit	7 minutes ag
network.tf	Initial commit	7 minutes ag
outputs.tf	Initial commit	7 minutes ag
provider.tf	Initial commit	7 minutes ag
secrets.tf	Initial commit	7 minutes ag

DIFFICULTIES – Almost Killers

- Gitlab lacks support for Windows build pods in Kubernetes executor (https://gitlab.com/gitlab-org/gitlab-runner/-/issues/4014)

- Google Kubernetes Engine (GKE) windows node images are provisioned with pre-installed Windows Defender that deletes your binaries upon compilation

DEMO



SCALLOPS

Overview

ScallOps is a framework that empowers Red Teams to put more focus on what they need to do, instead of how to do it. It utilizes the CI/CD concept to manage and automate the weaponization and deployment of offensive tools.

Security teams and individuals can develop, collaborate and utilize the framework's "Recipes" in order to perform their Red Team tasks with greater efficiency.

Refer to the ScallOps-Recipes repository to learn more about the features of this framework and how you can design your own Recipes.

Deployment

The framework can be deployed to GCP using the provided Terraform scripts. It is maninly built from a Gitlab instance that provides the CI features and a Kubernetes cluster that execute CI jobs on the relevant operating systems. We are also using the Cloud Storage to store customized container images that we may use during operating the framework.

Pre-requisites:

- Google Cloud subscription with **OWNER** permissions on a project (It is reccomended to use a clean GCP project)
- Access to GCP cloud shell or at least Terraform 14
- Web Browser

CLOUD COSTS

- Idle
  - Gitlab Instance: 51.46$ / month
  - Linux node: 24.46$ / month
  - Storage (depends on images volume): 100GB - 2$ / month
  - Secret manager: 0.06$ /month
  - GKE: One Zonal cluster is free per billing account
  - Total: 78$ https://cloud.google.com/products/calculator/#id=8cb8ce23-5ff1-4e7a-a3b4-da2df464bfff
- Per Job
  - Linux: Same as idle since system already up. When scaled 0.09$ per hour for each running node.
  - Windows: ~0.12$ on the first job (30 mins), and additional 0.006 for an average build job (2 mins).

* Note that jobs which are executed simultaneously, can use the same node resources, resulting them in using the same credit.

ADDITIONAL THOUGHTS

- Community driven framework (e.g. Cobalt-Strike Agressor script).

- Speeding up the task completion arousing a different problem – Data processing.

- We are not planning on shifting from the use of C2 but do use them in conjunction.

REFERENCES

- CI/CD guides:
  - CI/CD concept: https://hackernoon.com/understanding-the-basic-concepts-of-cicd-fw4k32s1
  - Gitlab CI docs: https://docs.gitlab.com/ee/ci/
  - Gitlab CI Runner K8s executor: https://docs.gitlab.com/runner/executors/kubernetes.html
- Infrastructure references
  - Terraform & GCloud: https://registry.terraform.io/providers/hashicorp/google/latest/docs
  - GKE: https://cloud.google.com/kubernetes-engine/docs/concepts/kubernetes-engine-overview
  - Container registry access: https://cloud.google.com/container-registry/docs/access-control
  - Helm Charts: https://helm.sh/docs/topics/charts/
  - Kaniko: https://github.com/GoogleContainerTools/kaniko
- Issues:
  - K8s windows exec support: https://gitlab.com/gitlab-org/gitlab-runner/-/issues/4014

CREDITS

- @OlegLerner – For helping with the framework design and presentation
- @paranoid314 - For the design and build of great recipes
- @Anyone else!

HITB SECCONF SIN-2021

Thank You for Joining Us

Join our Discord channel to discuss more or ask questions

https://discord.gg/dXE8ZMvU9J

@B1t0n_

B1t0n#4141

https://www.linkedin.com/in/gil-biton-a3a385101/

https://github.com/B1t0n