SecHack365

セキュリティ演習環境構築ツール

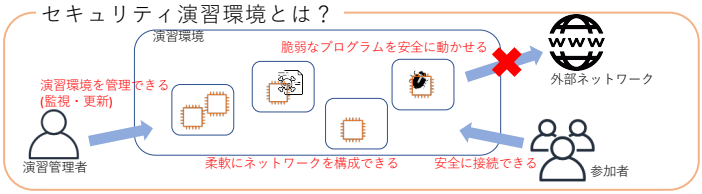
開発駆動コース 仲山ゼミ 寺嶋友哉

Motivation

セキュリティ演習の構築・運用をシンプルに!

Background

セキュリティ演習環境とは？



セキュリティ演習環境構築の課題

複雑で考えることが多い
設計・安全性の確保・管理・コスト etc..
→ 設計不備
大変さ

専門家(詳しい人)がいないと気軽かつ安全に演習ができない!

KAKOI

Concept

演習環境構築の複雑さと考えることを減らして簡単に!

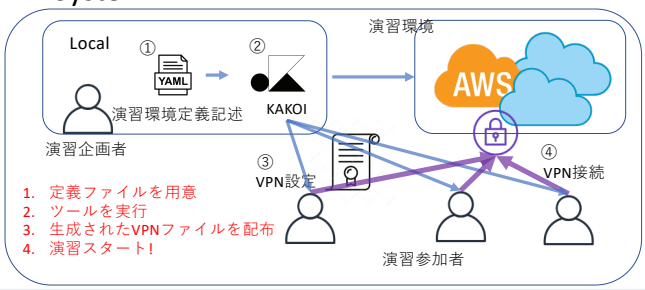
構成のテンプレート化・自動生成

設計の考慮事項 構築時の手順 DOWN

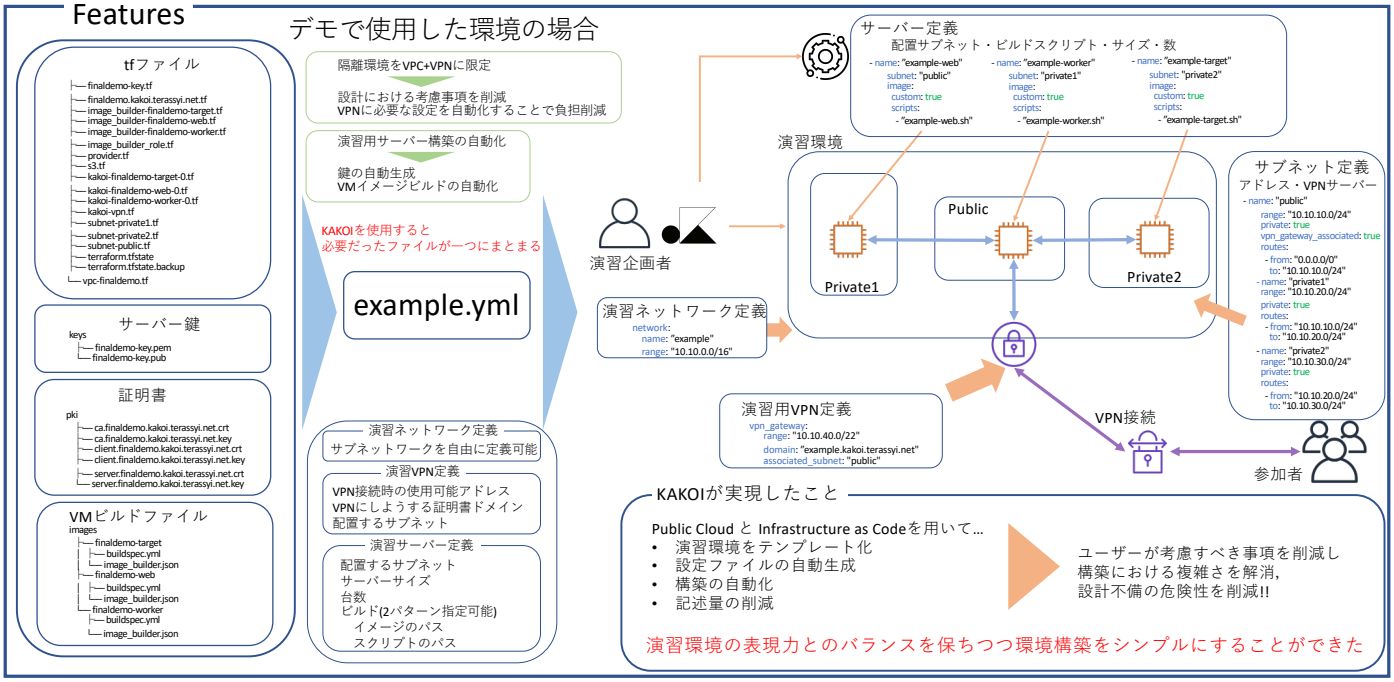
安全性 環境の再現性 UP

Public Cloud ✖ Infrastructure as Code

System



Features



KAKOIが実現したこと

Public Cloud と Infrastructure as Codeを用いて...
- 演習環境をテンプレート化
- 設定ファイルの自動生成
- 構築の自動化
- 記述量の削減

→ ユーザーが考慮すべき事項を削減し
構築における複雑さを解消,
設計不備の危険性を削減!!

演習環境の表現力とのバランスを保ちつつ環境構築をシンプルにすることができた

Use

Setup

1. ビルド(Required Go >= 1.13)
```
$ git clone https://github.com/terassyi/kakoi
$ cd kakoi
$ sudo ./setup.sh
```
2. AWS Credentialファイル作成

Command

Init: VMビルド	$ kakoi init -p example.yml
Create: 演習インフラ作成	$ kakoi create -p example.yml
Destroy: 演習インフラ破壊	$ kakoi destroy -p .kakoi

Procedure

1. 演習環境の定義記述をyamlで記述
2. Initコマンドで使用するイメージをビルド
3. Createコマンドで演習環境を構築
4. 生成されるVPN接続ファイルを配布して演習開始
5. 終了したらDestroyコマンドで環境を破壊

Future Work

演習環境管理・検証機能サポート
- 演習環境へのssh機能
- 構築時の環境検証機能

シナリオ作成支援機能サポート
- 演習に使用する脆弱性の管理機能
- バージョン指定でのソフトウェアインストール機能

他のクラウドへの対応
- 使用できるプラットフォームの追加

演習環境構築・運用の複雑さを解消しより気軽かつ安全に演習を実施することができるように開発を継続

NICT 国立研究開発法人 情報通信研究機構

Icon: https://www.flaticon.com/, https://aws.amazon.com/jp/architecture/icons/

https://github.com/terassyi/kakoi