IRON CLOUD

SECURITY

"Protecting your digital assets with the strength of *Iron Cloud Security*."

Agenda

- Team Member Introductions
- Problem Domain & Project Overview
- Team Process & Documentation
- Application Demonstration
- Q&A

IRON CLOUD
SECURITY

Our Team

- Deontae Carter
- Emilio Cejo
- Sierra Maldonado
- Jordan Marshall

IRON CLOUD

SECURITY

Deontae Carter

CompTIA ITF+ CERTIFIED

CompTIA A+ CERTIFIED · CE

- Navy Veteran
- Dual Certified
- Passion for Cybersecurity Operations

Connect With Me LinkedIn

LinkedIn | Deontae Carter

Emilio Ceja

- Cybersecurity Professional, looking to enter multimedia industry.
- Defend against Hackers, and other related malicious Threat Actors.
- Performer and Athlete, Graduating class of 2020.

LinkedIn

CompTIA
ITF+
CERTIFIED

Sierra Maldonado

- US Navy Veteran, Seabee
- ITF+
- Six Sigma White belt in HR
- Accepted to ASU Pre-Vet Program
- Connect with me on linkedin!

Jordan Marshall

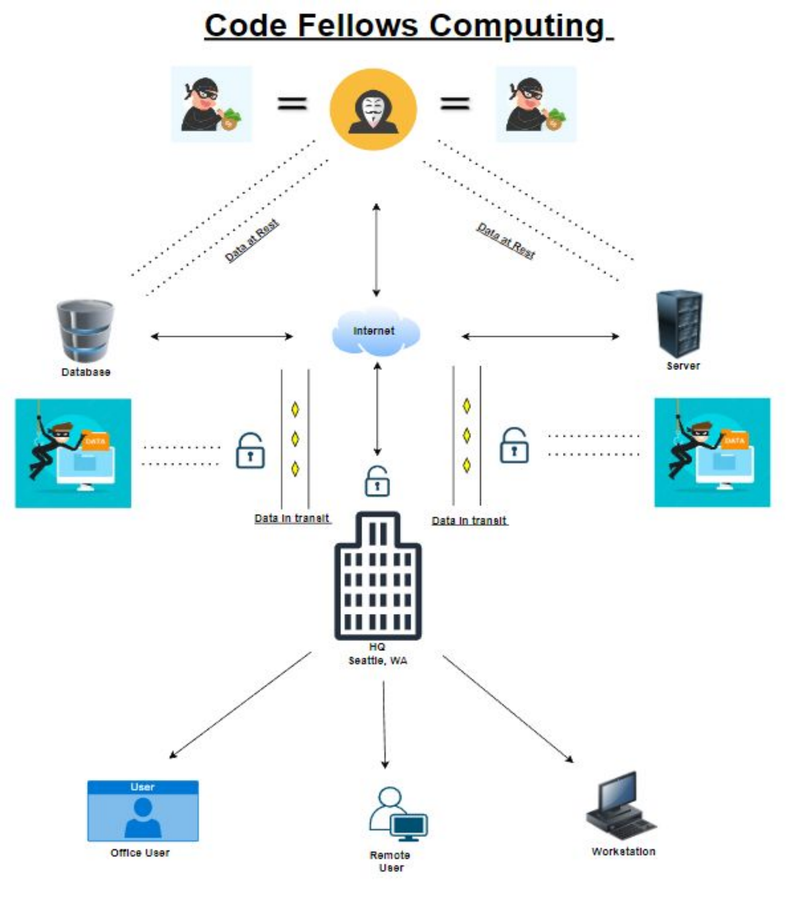
- USAF Medic
- Working in the healthcare field for the past 10 years.
- Newly Comp TIA ITF+ certified
- I chose cybersecurity to learn a new skill and my interest in the field
- No prior IT experience

Project Overview

- IAM Users: We will establish and configure Identity and Access Management (IAM) users
- Server Hardening and Data Protection: We will implement robust security measures to harden the servers, safeguarding them against potential vulnerabilities and threats.
- SIEM / Log Aggregation System: To proactively monitor and detect potential security incidents
- Cloud Monitoring: We will establish comprehensive cloud monitoring mechanisms to continuously monitor performance, and security of the infrastructure.

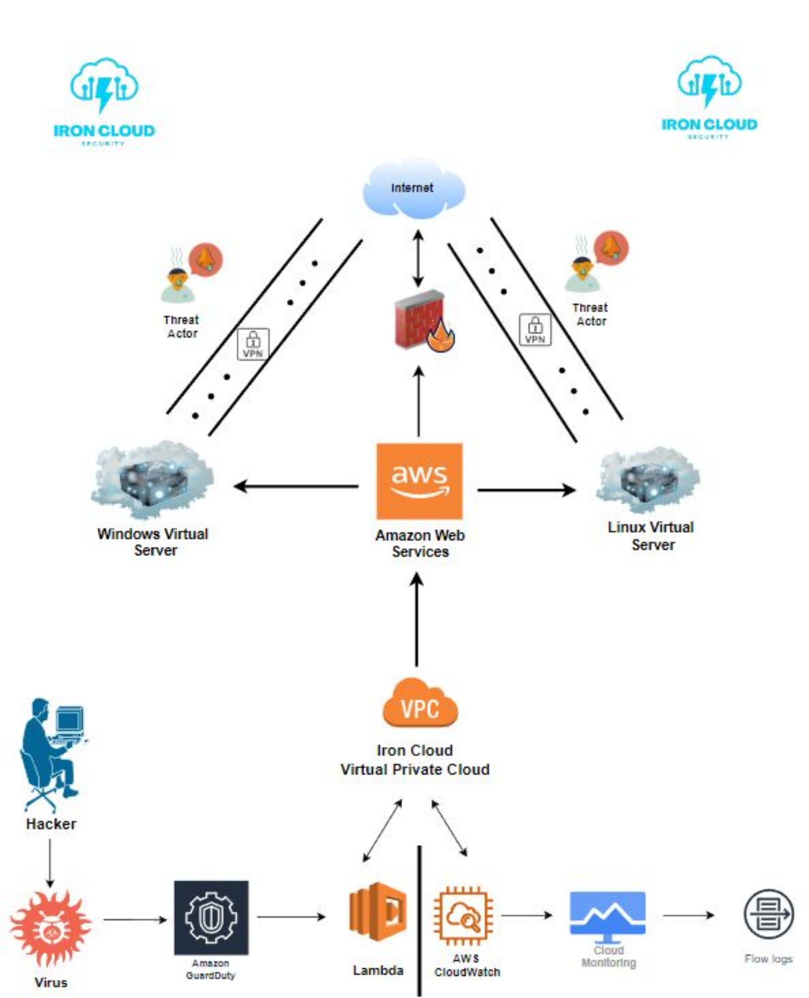
IRON CLOUD
SECURITY

Problem Domain

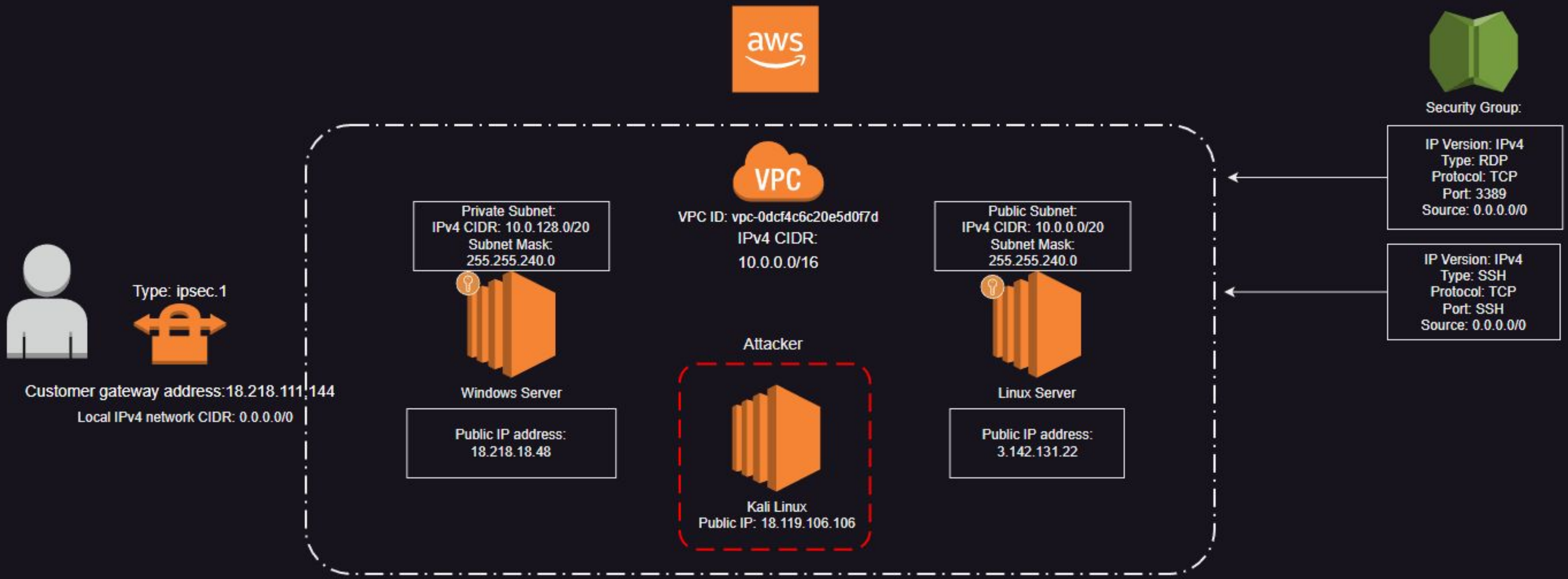


Iron Cloud has been contracted to improve the cybersecurity processes and systems for the client company, Code Fellows Computing. The client has a vulnerable cloud infrastructure that lacks security compliance and employs insecure networking methods.

Network Topology



Network Chart



Security Group:

IP Version: IPv4
Type: RDP
Protocol: TCP
Port: 3389
Source: 0.0.0.0/0

IP Version: IPv4
Type: SSH
Protocol: TCP
Port: SSH
Source: 0.0.0.0/0

VPC ID: vpc-0dcf4c6c20e5d0f7d
IPv4 CIDR:
10.0.0.0/16

Private Subnet:
IPv4 CIDR: 10.0.128.0/20
Subnet Mask:
255.255.240.0

Windows Server

Public IP address:
18.218.18.48

Public Subnet:
IPv4 CIDR: 10.0.0.0/20
Subnet Mask:
255.255.240.0

Linux Server

Public IP address:
3.142.131.22

Attacker

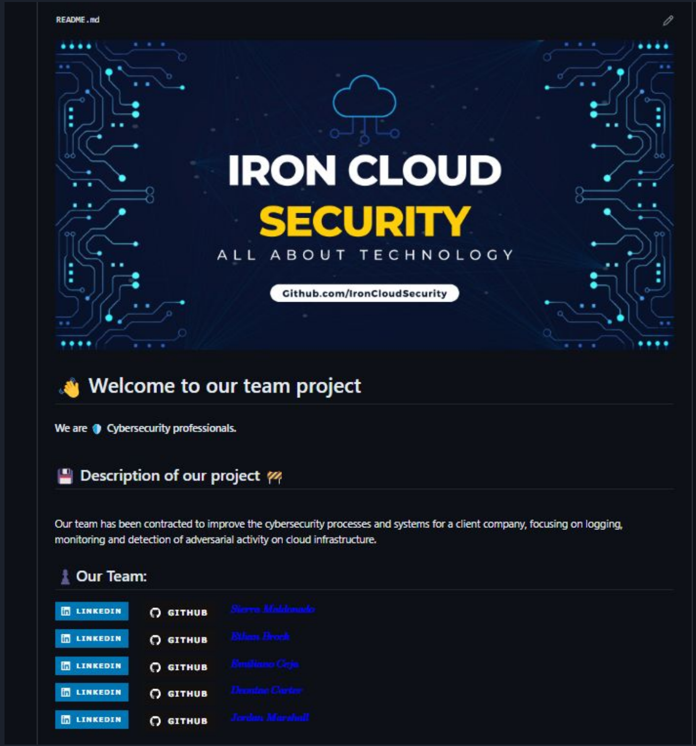
Kali Linux
Public IP: 18.119.106.106

Type: ipsec.1

Customer gateway address:18.218.111.144
Local IPv4 network CIDR: 0.0.0.0/0

Process & Documentation

IRON CLOUD
SECURITY



README.md

IRON CLOUD
SECURITY
ALL ABOUT TECHNOLOGY
Github.com/IronCloudSecurity

👋 Welcome to our team project

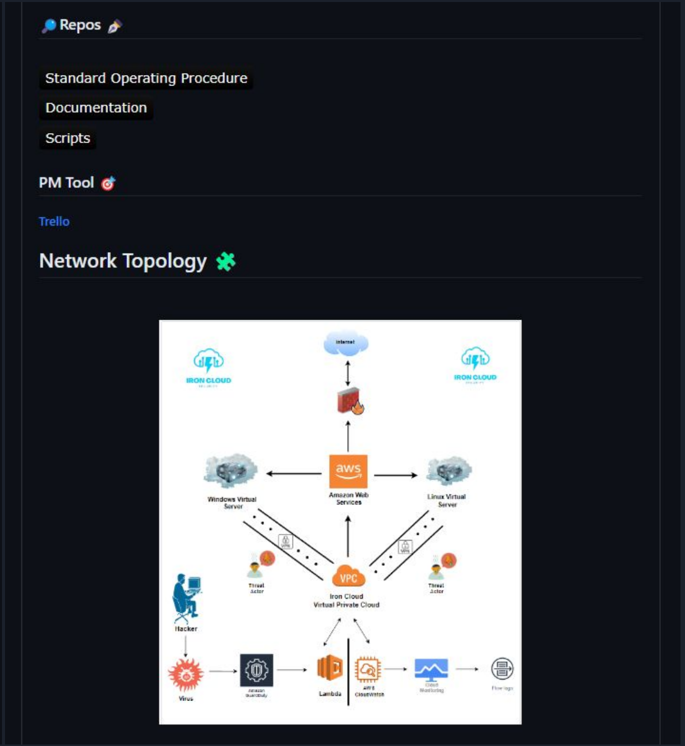
We are 🛡 Cybersecurity professionals.

💾 Description of our project 🚧

Our team has been contracted to improve the cybersecurity processes and systems for a client company, focusing on logging, monitoring and detection of adversarial activity on cloud infrastructure.

♟ Our Team:

LINKEDIN	GITHUB	Sierra Maldonado
LINKEDIN	GITHUB	Ethan Brock
LINKEDIN	GITHUB	Emiliano Ceja
LINKEDIN	GITHUB	Deontae Carter
LINKEDIN	GITHUB	Jordan Marshall



🔎 Repos 🖍

Standard Operating Procedure

Documentation

Scripts

PM Tool 🎯

Trello

Network Topology 🧩

Demo

Resources & Thanks

Special thanks to our fellow students and our instructors!

Questions?

IRON CLOUD

SECURITY