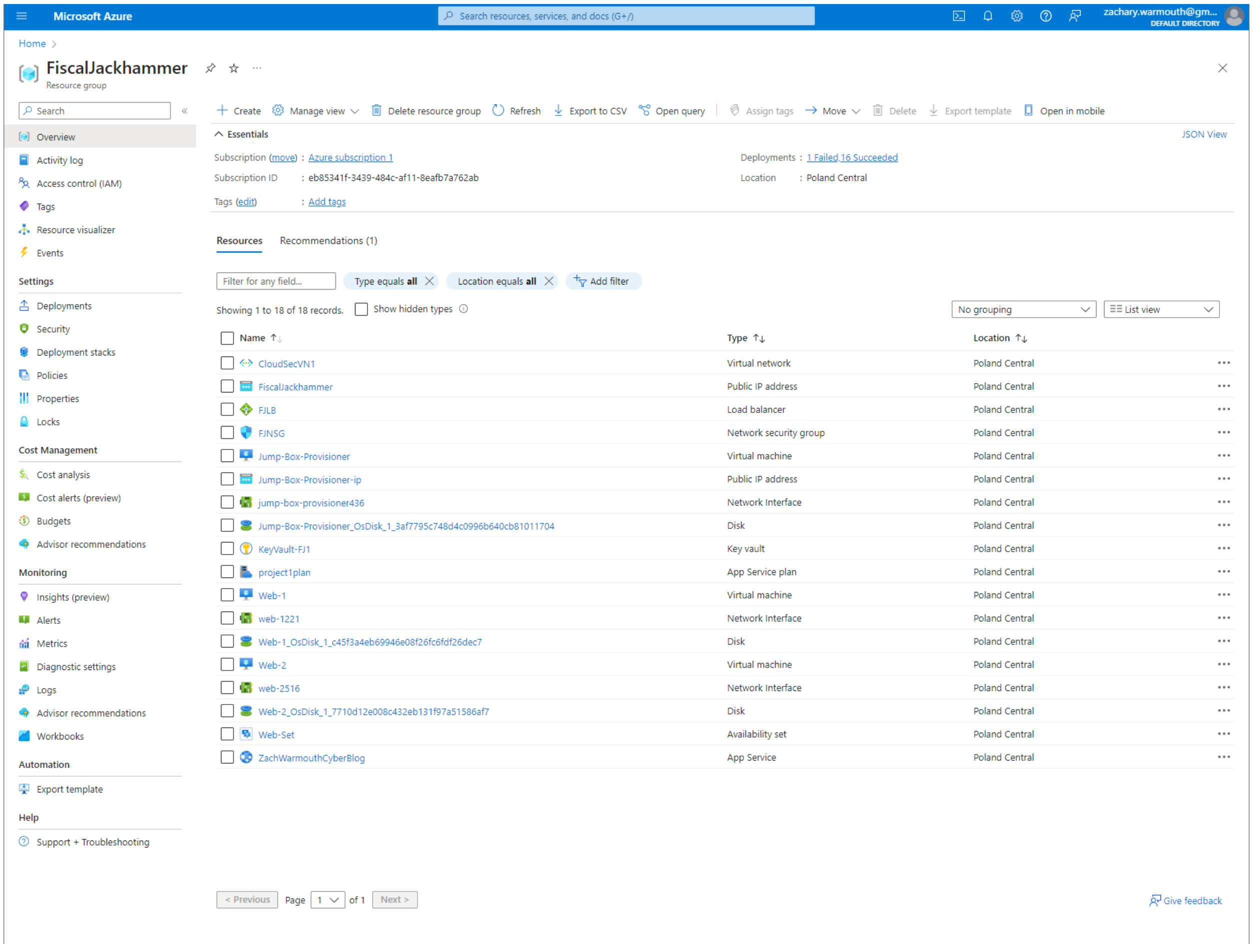
Cybersecurity Bootcamp Web Application/Cloud Security:

Build, secure, and protect a cloud application hosting a cyber blog using Microsoft Azure.

*Site currently offline – see below for cloud architecture used.



FiscalJackhammer
Resource group

Essentials

Subscription (move) : Azure subscription 1

Subscription ID : eb85341f-3439-484c-af11-8eafb7a762ab

Tags (edit) : Add tags

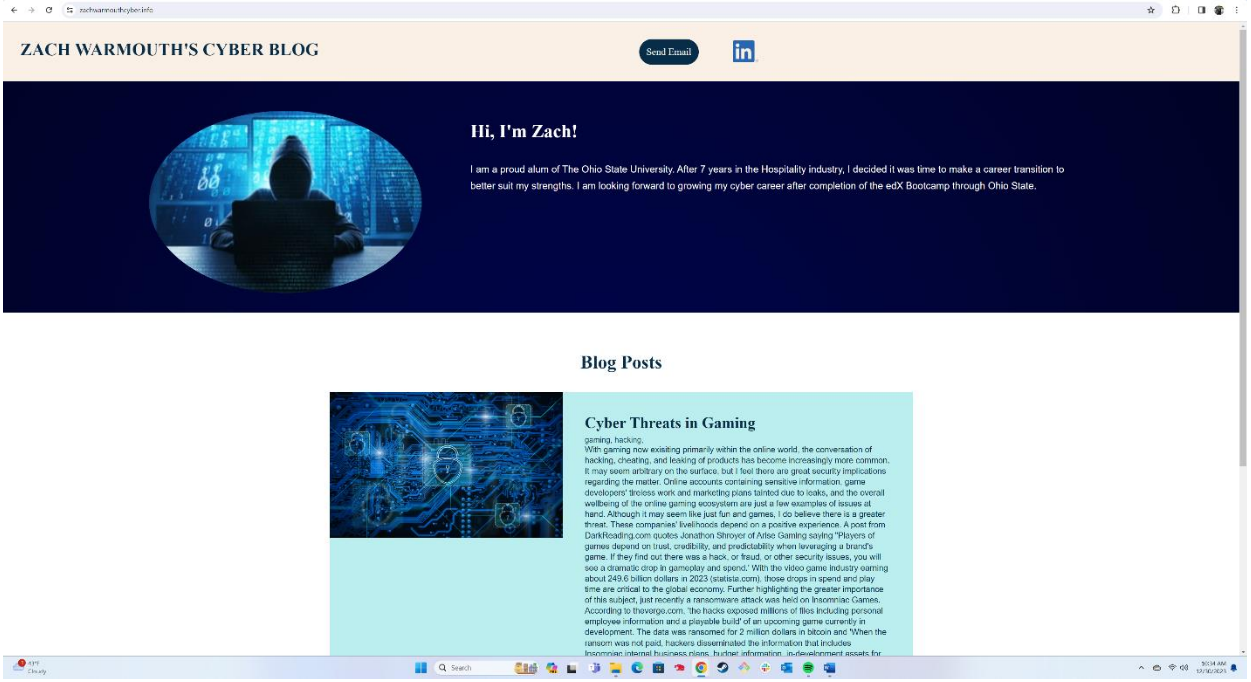
Deployments : 1 Failed, 16 Succeeded

Location : Poland Central

Type equals **all** Location equals **all**

Showing 1 to 18 of 18 records. □ Show hidden types

Name	Type	Location
CloudSecVN1	Virtual network	Poland Central
FiscalJackhammer	Public IP address	Poland Central
FJLB	Load balancer	Poland Central
FJNSG	Network security group	Poland Central
Jump-Box-Provisioner	Virtual machine	Poland Central
Jump-Box-Provisioner-ip	Public IP address	Poland Central
jump-box-provisioner436	Network Interface	Poland Central
Jump-Box-Provisioner_OsDisk_1_3af7795c748d4c0996b640cb81011704	Disk	Poland Central
KeyVault-FJ1	Key vault	Poland Central
project1plan	App Service plan	Poland Central
Web-1	Virtual machine	Poland Central
web-1221	Network Interface	Poland Central
Web-1_OsDisk_1_c45f3a4eb69946e08f26fc6fdf26dec7	Disk	Poland Central
Web-2	Virtual machine	Poland Central
web-2516	Network Interface	Poland Central
Web-2_OsDisk_1_7710d12e008c432eb131f97a51586af7	Disk	Poland Central
Web-Set	Availability set	Poland Central
ZachWarmouthCyberBlog	App Service	Poland Central



ZACH WARMOUTH'S CYBER BLOG

Hi, I'm Zach!

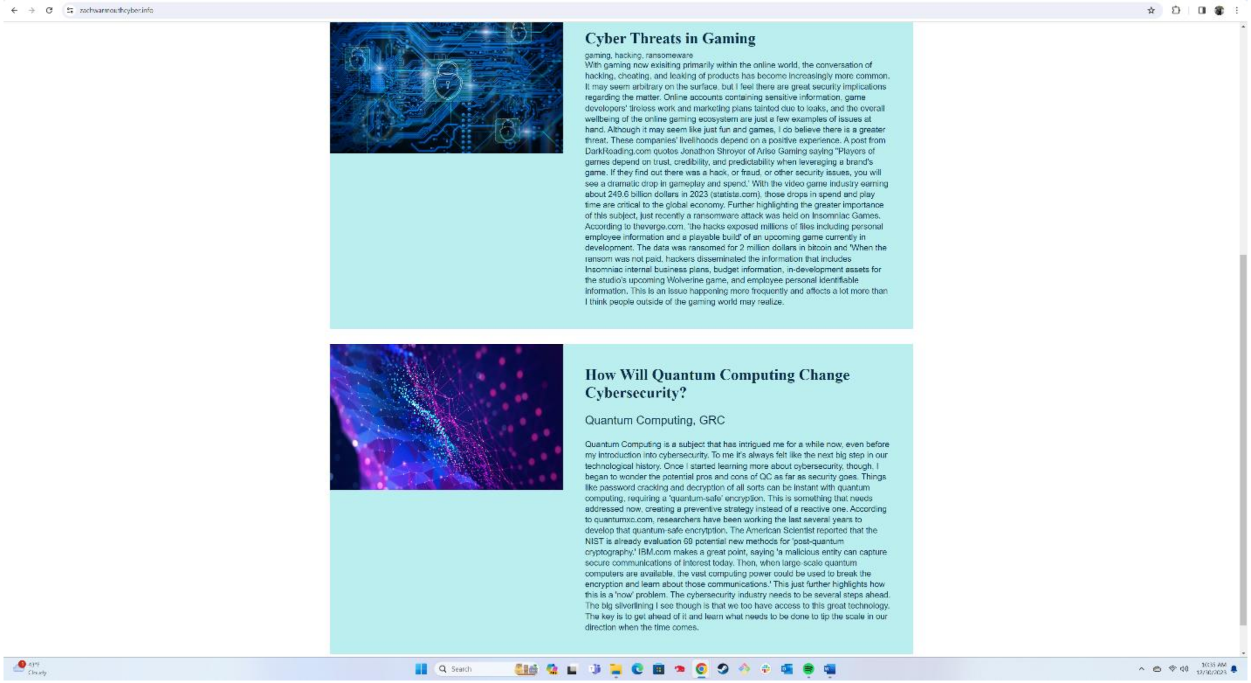
I am a proud alum of The Ohio State University. After 7 years in the Hospitality industry, I decided it was time to make a career transition to better suit my strengths. I am looking forward to growing my cyber career after completion of the edX Bootcamp through Ohio State.

Blog Posts

Cyber Threats in Gaming

gaming, hacking,

With gaming now exisiting primarily within the online world, the conversation of hacking, cheating, and leaking of products has become increasingly more common. It may seem arbitrary on the surface, but I feel there are great security implications regarding the matter. Online accounts containing sensitive information, game developers' tireless work and marketing plans tainted due to leaks, and the overall wellbeing of the online gaming ecosystem are just a few examples of issues at hand. Although it may seem like just fun and games, I do believe there is a greater threat. These companies' livelihoods depend on a positive experience. A post from DarkReading.com quotes Jonathon Shroyer of Arise Gaming saying "Players of games depend on trust, credibility, and predictability when leveraging a brand's game. If they find out there was a hack, or fraud, or other security issues, you will see a dramatic drop in gameplay and spend.' With the video game industry earning about 249.6 billion dollars in 2023 (statista.com), those drops in spend and play time are critical to the global economy. Further highlighting the greater importance of this subject, just recently a ransomware attack was held on Insomniac Games. According to theverge.com, 'the hacks exposed millions of files including personal employee information and a playable build' of an upcoming game currently in development. The data was ransomed for 2 million dollars in bitcoin and 'When the ransom was not paid, hackers disseminated the information that includes Insomniac internal business plans, budget information, in-development assets for



Cyber Threats in Gaming

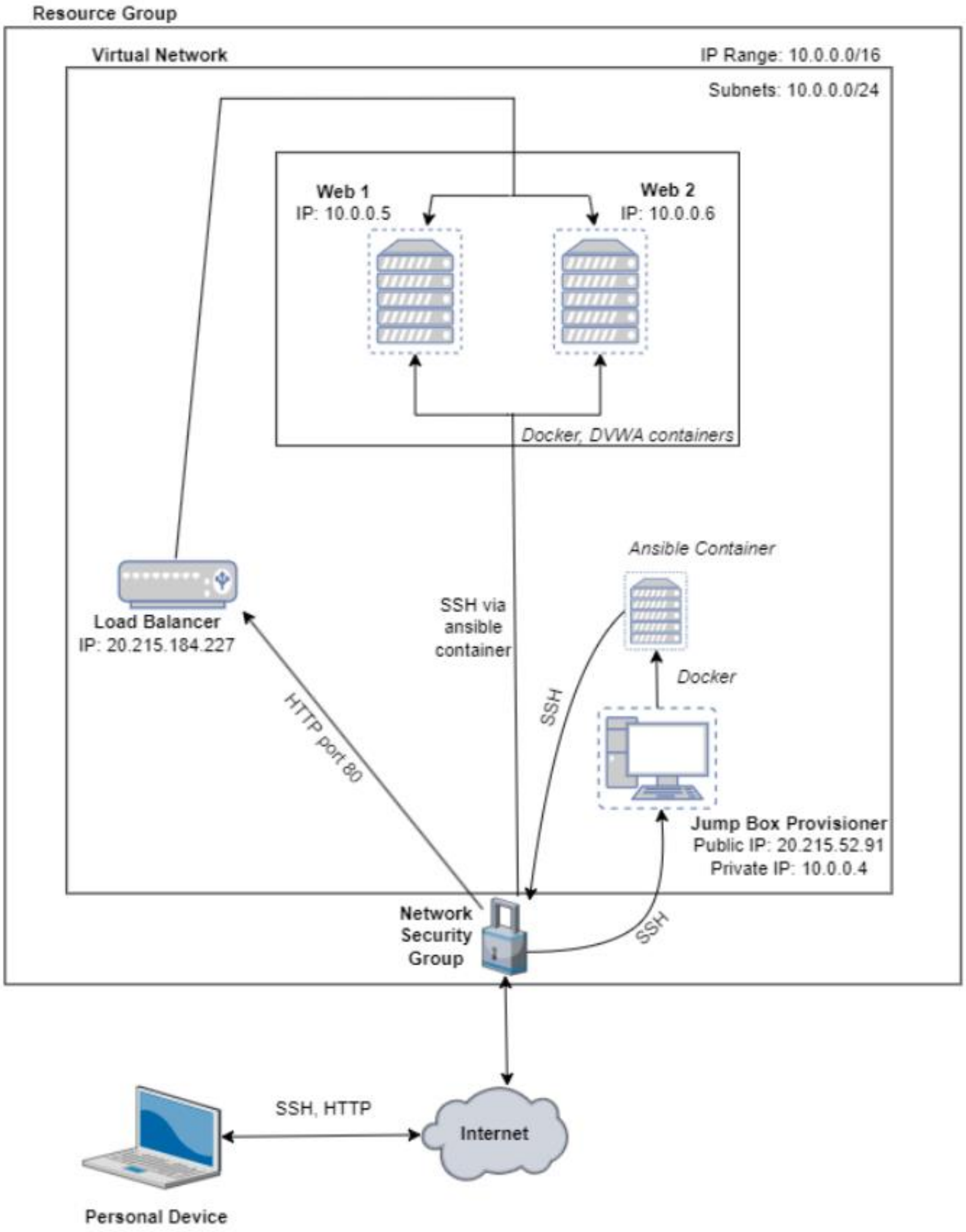
gaming, hacking, ransomeware

With gaming now exisiting primarily within the online world, the conversation of hacking, cheating, and leaking of products has become increasingly more common. It may seem arbitrary on the surface, but I feel there are great security implications regarding the matter. Online accounts containing sensitive information, game developers' tireless work and marketing plans tainted due to leaks, and the overall wellbeing of the online gaming ecosystem are just a few examples of issues at hand. Although it may seem like just fun and games, I do believe there is a greater threat. These companies' livelihoods depend on a positive experience. A post from DarkReading.com quotes Jonathon Shroyer of Arise Gaming saying "Players of games depend on trust, credibility, and predictability when leveraging a brand's game. If they find out there was a hack, or fraud, or other security issues, you will see a dramatic drop in gameplay and spend.' With the video game industry earning about 249.6 billion dollars in 2023 (statista.com), those drops in spend and play time are critical to the global economy. Further highlighting the greater importance of this subject, just recently a ransomware attack was held on Insomniac Games. According to theverge.com, 'the hacks exposed millions of files including personal employee information and a playable build' of an upcoming game currently in development. The data was ransomed for 2 million dollars in bitcoin and 'When the ransom was not paid, hackers disseminated the information that includes Insomniac internal business plans, budget information, in-development assets for the studio's upcoming Wolverine game, and employee personal identifiable information. This is an issue happening more frequently and affects a lot more than I think people outside of the gaming world may realize.

How Will Quantum Computing Change Cybersecurity?

Quantum Computing, GRC

Quantum Computing is a subject that has intrigued me for a while now, even before my introduction into cybersecurity. To me it's always felt like the next big step in our technological history. Once I started learning more about cybersecurity, though, I began to wonder the potential pros and cons of QC as far as security goes. Things like password cracking and decryption of all sorts can be instant with quantum computing, requiring a 'quantum-safe' encryption. This is something that needs addressed now, creating a preventive strategy instead of a reactive one. According to quantumxc.com, researchers have been working the last several years to develop that quantum-safe encrytption. The American Scientist reported that the NIST is already evaluation 69 potential new methods for 'post-quantum cryptography.' IBM.com makes a great point, saying 'a malicious entity can capture secure communications of interest today. Then, when large-scale quantum computers are available, the vast computing power could be used to break the encryption and learn about those communications.' This just further highlights how this is a 'now' problem. The cybersecurity industry needs to be several steps ahead. The big silverlining I see though is that we too have access to this great technology. The key is to get ahead of it and learn what needs to be done to tip the scale in our direction when the time comes.


Resource Group
Virtual Network
IP Range: 10.0.0.0/16
Subnets: 10.0.0.0/24
Web 1
IP: 10.0.0.5
Web 2
IP: 10.0.0.6
Docker, DVWA containers
Ansible Container
Load Balancer
IP: 20.215.184.227
SSH via
ansible
container
SSH
Docker
HTTP port 80
Jump Box Provisioner
Public IP: 20.215.52.91
Private IP: 10.0.0.4
Network
Security
Group
SSH
SSH, HTTP
Internet
Personal Device