



# Cybersecurity

## Project 1 Technical Brief

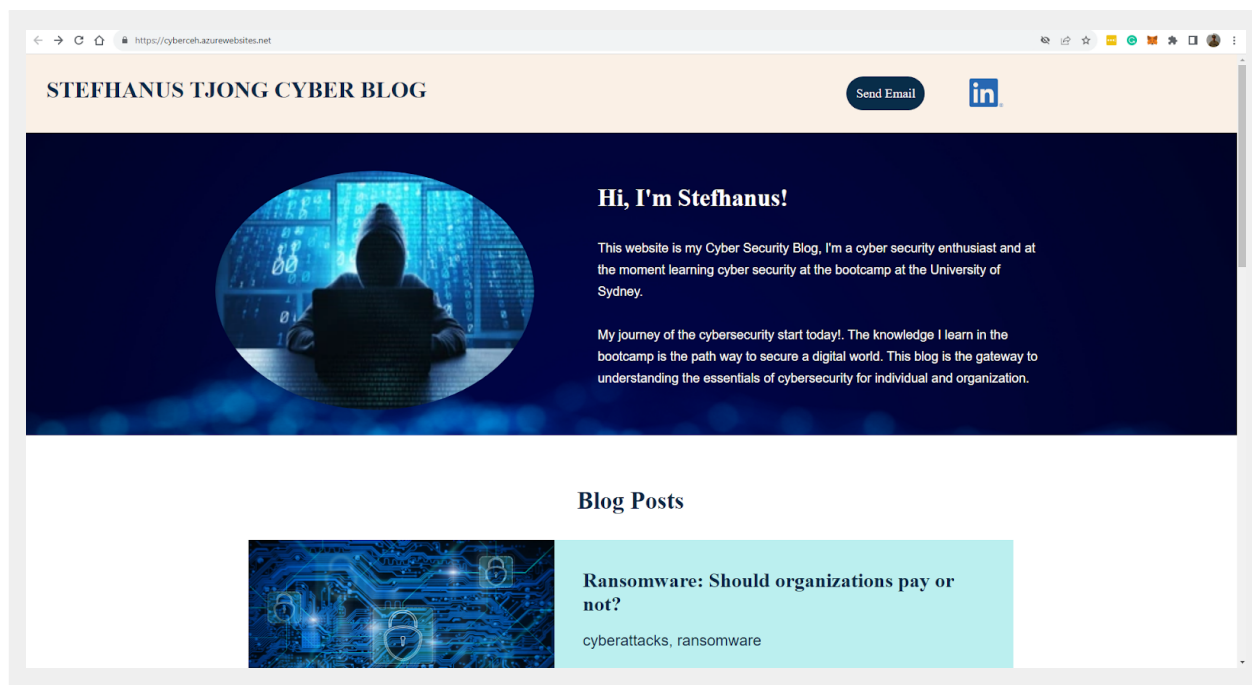
Make a copy of this document before you begin. Place your answers below each question. This completed document will be your deliverable for Project 1. Submit it through Canvas when you're finished with the project at the end of the week.

### Your Web Application

Enter the URL for the web application that you created:

<https://cyberceh.azurewebsites.net/>

Paste screenshots of your website created (Be sure to include your blog posts):





## Ransomware: Should organizations pay or not?

cyberattacks, ransomware

While some experts don't think companies should ever pay ransomware demands, others say it is not such a clear-cut issue. Whether they pay or not, these cyberattacks can create crisis situations for business leaders. The bad actors now know that your system is insecure and that you will pay a ransom. There is no one-size-fits-all answer, as each situation can have unique circumstances.

### Reason for paying:

There may be scenarios where payment is necessary or advisable.

*Data Recovery:* Paying the ransom might be the fastest way to regain access to encrypted data.

*Business Continuity:* Paying the ransom might seem like a quick way to restore normal operations.

*Risk Assessment:* Paying the ransom against potential financial losses and reputational damage.

### Reason for not paying:

*No Guarantees:* There is no guarantee you will regain access to your information, nor prevent it from being sold or leaked online. Paying ransom does not guarantee that the attackers will provide the decryption key or that the data will be fully recovered. Attackers might disappear or demand more money.

*Availability Of Backups:* Organizations that have fully backup copies of the data affected by the ransomware generally don't need to pay a ransomware demand.

*Encouraging Further Attacks:* Paying ransom can make an organization a more attractive target for future attacks as the attackers know you are willing to pay for the ransom.

*Funding Criminal Activities:* Paying ransoms indirectly supports cybercriminal activities and encourages them to continue targeting organizations.



## How could quantum computing affect



## How could quantum computing affect cybersecurity?

### cybersecurity, quantum computing

Large-scale quantum computers will create new opportunities for improving cybersecurity but can also create exposures. Quantum computing presents challenges and opportunities for the cybersecurity sector.

Quantum computers have the potential to break some of the encryption methods that are currently considered secure. However, they can also be used to develop new encryption techniques based on quantum principles, such as quantum key distribution and post-quantum cryptography. These methods could provide stronger security against attacks by classical and quantum computers.

Quantum computers can generate truly random numbers using quantum processes, which could enhance the security of various applications that rely on random number generation, such as encryption keys and authentication tokens.

Quantum computing may also create new exposures, such as the ability to quickly solve the difficult math problems that are the basis of some forms of encryption. Quantum cybersecurity will wield the power to detect and deflect quantum cyberattacks before they cause harm.

The advent of quantum computing will lead to changes to encryption methods. Currently, the most widely used asymmetric algorithms are based on difficult mathematical problems, such as factoring large numbers, which can take thousands of years on today's most powerful supercomputers.

Future quantum computers may be able to break asymmetric encryption solutions that base their security on integer factorization or discrete logarithms. To help withstand brute-force attacks, key sizes should be doubled to support the same level of protection. New vulnerabilities and attack vectors specific to quantum technologies might emerge. Cybersecurity experts would need to develop new strategies and tools to address these challenges.

Quantum computers could potentially solve certain mathematical problems that many cryptographic protocols much faster than normal computers. This could be used to crack encryption methods that are currently considered secure.

Quantum computers could undermine the security of digital signatures, which are used to verify the authenticity of documents and messages. This might lead to identity theft, unauthorized access, and falsified digital certificates.

## Day 1 Questions

### General Questions

1. What option did you select for your domain (Azure free domain, GoDaddy domain)?

Azure free domain

## 2. What is your domain name?

cyberceh.azurewebsites.net

## Networking Questions

### 1. What is the IP address of your webpage?

20.211.64.16

### 2. What is the location (city, state, country) of your IP address?

City: Sydney

State: New South Wales

Country: Australia

### 3. Run a DNS lookup on your website. What does the NS record show?

Server: h268a

Address: fe80::1

Non-authoritative answer:

cyberceh.azurewebsites.net canonical name =

waws-prod-sy3-101.sip.azurewebsites.windows.net

waws-prod-sy3-101.sip.azurewebsites.windows.net canonical name =

waws-prod-sy3-101-06a2.australiaeast.cloudapp.azure.com

australiaeast.cloudapp.azure.com

primary name server = ns1-06.azure-dns.com

responsible mail addr = msnhst.microsoft.com

serial = 10001

refresh = 900 (15 mins)

retry = 300 (5 mins)

expire = 604800 (7 days)

default TTL = 60 (1 min)

## Web Development Questions

1. When creating your web app, you selected a runtime stack. What was it? Does it work on the front end or the back end?

The runtime stack was PHP8.0 and it works on the back end.

2. Inside the `/var/www/html` directory, there was another directory called assets. Explain what was inside that directory.

The assets directory contains 2 directories: css and images.

css directory contains 2 files:

- style.css
- Style.css.bak

CSS is a stylesheet language used for describing the presentation and formatting of web pages. CSS files define how elements on a web page should be displayed, including their layout, colours, fonts, and other visual aspects.

images directory contains 6 files:

- Background.jpg
- Image1.jpg
- Image2.jpg
- LinkedIn-logo.png
- RobertSmith-profile.jpg
- Readme

Images (.jpg) files can be used for the images for web pages or specific sections of the page and the image can be made to be clickable to point to the specific web page.

3. Consider your response to the above question. Does this work with the front end or back end?

Front end

## Day 2 Questions

### Cloud Questions

1. What is a cloud tenant?

A cloud tenant is an individual, organization, or entity that uses the services, resources, and infrastructure provided by a cloud computing provider.

2. Why would an access policy be important on a key vault?

An access policy plays a critical role in securing a key vault by controlling who can access, manage, and manipulate the sensitive information stored within it, access policies contribute to maintaining the confidentiality, integrity, and availability of the stored data and keys.

3. Within the key vault, what are the differences between keys, secrets, and certificates?

Keys in a key vault are used for cryptographic operations, such as encryption, decryption, signing, and verification, secrets are anything that we want to tightly control access to, such as API keys, passwords, certificates, or cryptographic keys and certificates are used for authentication, encryption, and secure communications.

### Cryptography Questions

1. What are the advantages of a self-signed certificate?

The advantages of using self-signed certificates are free, easy to generate and don't require interaction with a certificate authority (CA). This makes them useful for testing, development, or setting up secure communication in a local or isolated environment quickly.

2. What are the disadvantages of a self-signed certificate?

The disadvantages of using self-signed certificates are a lack of trust,

having no validation from a third-party authority, leading to warning messages when users attempt to access the website, has security vulnerabilities that make them unsuitable for many production and public-facing applications.

### 3. What is a wildcard certificate?

A wildcard certificate is a certificate that is used to secure multiple subdomains of a single domain with a single certificate.

### 4. When binding a certificate to your website, Azure only provides TLS versions 1.0, 1.1, and 1.2. Explain why SSL 3.0 isn't provided.

SSL 3.0 isn't provided because it has been found to be vulnerable to several serious security vulnerabilities, making it unsafe to use.

### 5. After completing the Day 2 activities, view your SSL certificate and answer the following questions:

- a. Is your browser returning an error for your SSL certificate? Why or why not?

No error, because Azure set up a secure SSL certificate and this is a trusted certificate which has been approved by a CA which most browsers trust.

- b. What is the validity of your certificate (date range)?

Issued On  
Friday, 10 March 2023 at 14:05:55  
Expires On  
Monday, 4 March 2024 at 14:05:55

- c. Do you have an intermediate certificate? If so, what is it?

Yes, it's a Microsoft Azure TLS Issuing CA 02

- d. Do you have a root certificate? If so, what is it?

Yes, it's a DigiCert Global Root G2

e. Does your browser have the root certificate in its root store?

Yes.

f. List one other root CA in your browser's root store.

Go Daddy Root Certificate Authority - G2

## Day 3 Questions

### Cloud Security Questions

1. What are the similarities and differences between Azure Web Application Gateway and Azure Front Door?

Similarities:

- Both reside in front of your web application in order to protect it.
- They work on the Application Layer (7) of the OSI model.
- Their primary solution is a load balancer.
- They can incorporate a web application firewall (WAF) to protect against web vulnerability attacks.
- They have additional features such as URL path-based routing and SSL/TLS termination.

Differences:

- The Web Application Gateway is more regional and is best suited to protect a web application in a single region in your cloud.
- The Azure Front Door is more global and is better suited when you have a variety of regions in a cloud environment.

2. A feature of the Web Application Gateway and Front Door is "SSL Offloading." What is SSL offloading? What are its benefits?

SSL offloading is the process of removing the SSL-based encryption from incoming traffic to relieve a web server of the processing burden of



decrypting and/or encrypting traffic sent via SSL. The benefits of SSL offloading are to improve the performance and efficiency of web servers.

3. What OSI layer does a WAF work on?

Layer 7.

4. Select one of the WAF managed rules (e.g., directory traversal, SQL injection, etc.), and define it.

SQL injection is the injection of malicious SQL code into an application, allowing the attacker to view or modify a database.

5. Consider the rule that you selected. Could your website (as it is currently designed) be impacted by this vulnerability if Front Door wasn't enabled? Why or why not?

No, because the WAF managed rules will detect and block malicious SQL code injection attacks.

6. Hypothetically, say that you create a custom WAF rule to block all traffic from Canada. Does that mean that anyone who resides in Canada would not be able to access your website? Why or why not?

No, it does not mean someone who resides in Canada would not be able to access my website. The WAF is blocking IP addresses originating from Canada, but if someone who resides in Canada uses a VPN, they can mask their IP address to a completely different location and that would allow them to bypass the custom WAF rule and access my website.

7. Include screenshots below to demonstrate that your web app has the following:

a. Azure Front Door enabled

Microsoft Azure


Upgrade

Search resources, services, and docs (G+)

Home > App Services > cyberceh | Networking >

# Azure Front Door

Microsoft Azure



## Azure Front Door

Azure Front Door is a modern cloud CDN service that provides high performance, scalability, and secure experiences for your content, files and global applications. It combines modern CDN technology and intelligent threat protection in a tightly integrated service that's easy to set up, deploy, and manage. Use Front Door with Azure services including App Service, Static Web App, Storage, API Management, Application Gateway, Azure Kubernetes Service, Azure Container Apps, and virtual machines—or combine it with on-premises services for hybrid deployments and smooth cloud migration. [Learn more](#)

✔

Azure Front Door is enabled for your web app. Configure your Front Door at the link below. To remove Front Door from this web app, you must remove app service from the Front Door's origins or the classic Front Door's backend.

Name ↑↓	Type ↑↓	Endpoint name ↑↓	Origin group name ↑↓
<a href="#">project1-FrontDoor</a>	Azure Front Door Premium	Project1-FD-cketahb9fyaxbrh5.z01....	Red-Team

b. A WAF custom rule

DefaultWebAppWaff597840393954025959d3158c0d4327f | Custom rules ☆ ...

Front Door WAF policy

Search

Save Discard Refresh

There are pending changes, click 'Save' to apply.

Configure a policy with custom-authored rules. Once a rule is matched, the corresponding action defined in the rule is applied to the request. Once such a match is processed, rules with lower priorities are not processed further. A smaller integer value for a rule denotes a higher priority. [Learn more](#)

+ Add custom rule

Priority	Name	Rule type	Action	Status
100	Project1rule	Match	Block	Enabled

Overview

Activity log

Access control (IAM)

Tags

Settings

Policy settings

Managed rules

**Custom rules**

Associations

Properties

Locks

Automation

Tasks (preview)

Export template

Help

New Support Request

## Disclaimer on Future Charges

Please type “**YES**” after one of the following options:

- Maintaining website after project conclusion:*** I am aware that I am responsible for any charges that I incur by maintaining my website. I have reviewed the [guidance](#) for minimizing costs and monitoring Azure charges. **YES**
- Disabling website after project conclusion:*** I am aware that I am responsible for deleting all of my project resources as soon as I have gathered all of my web application screen shots and completed this document. **YES**