Cybersecurity

Project 1 Technical Brief

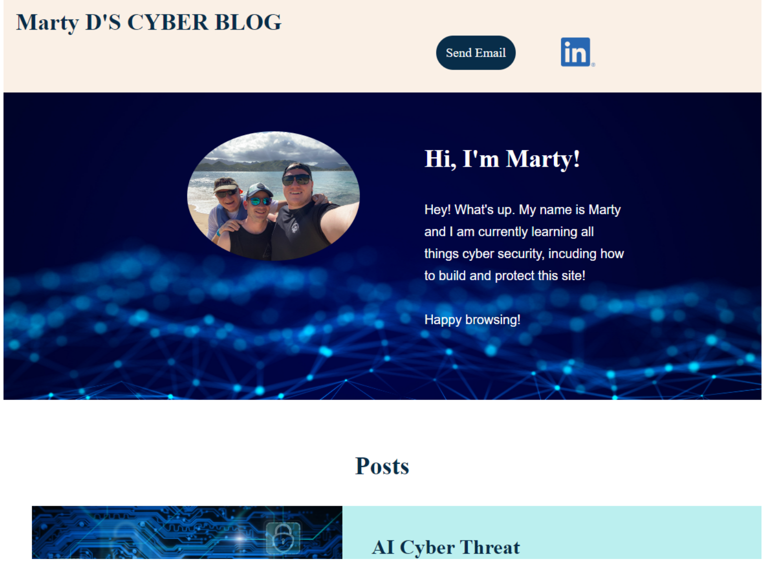
Make a copy of this document before you begin. Place your answers below each question. This completed document will be your deliverable for Project 1. Submit it through Canvas when you're finished with the project at the end of the week.

Your Web Application

Enter the URL for the web application that you created:

```
https://cybersec-mdblog.azurewebsites.net/
```

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


Marty D'S CYBER BLOG

Hi, I'm Marty!

Hey! What's up. My name is Marty and I am currently learning all things cyber security, incuding how to build and protect this site!

Happy browsing!

Posts

AI Cyber Threat

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?

```
https://cybersec-mdblog.azurewebsites.net/
```

Networking Questions

1. What is the IP address of your webpage?

```
20.211.64.13
```

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

```
Redmond, WA, US, 98052
```

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

```
Non-authoritative answer:
cybersec-mdblog.azurewebsites.net    canonical name =
waws-prod-sy3-091.sip.azurewebsites.windows.net.
waws-prod-sy3-091.sip.azurewebsites.windows.net    canonical name =
waws-prod-sy3-091-a15c.australiaeast.cloudapp.azure.com.

Authoritative answers can be found from:
australiaeast.cloudapp.azure.com
    origin = ns1-06.azure-dns.com
    mail addr = msnhst.microsoft.com
    serial = 10001
    refresh = 900
    retry = 300
    expire = 604800
    minimum = 60
```

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?

```
In this specific situation the stack refers to the backend technology used
to run the web app. This handles the logic, data and communication.
A stack can work on either the front on backend but in this case the runtime
stack selected was referring to the backend tech.
```

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

```
Inside that directory lies all the raw images, styles, formatting and design
assets that provide the space for the raw data and ensure its presented in a
digestible way. Coloured shapes, images, fonts, styles, spacing, margins
etc…
```

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

```
The assets directory provides visual assets for the website to assist with
presentation and formatting.
```

Day 2 Questions

Cloud Questions

1. What is a cloud tenant?

Cloud tenancy is the most basic form of SaaS. In essence it is the remote hosting of an organization's operations. Cloud tenancy can come in the forms of single or multi tenancy, each with their own benefits, with advantages for single tenancy leaning towards major corporations who have the resources and managerial process to warrant the extra effort and security, and smaller enterprises favoring the multi-tenancy to reduce their responsibility in maintenance, security and cost. Single tenancy means that the entity has singular ownership, use and control of SaaS resources they have attained, meaning they also have full responsibility to manage and maintain it. Multi-tenancy is a SaaS where resources are shared and therefore the burden and responsibility are lessened. It is worth noting that multi-tenancy still has security and privacy for their data, they just don't have the same level of control over the security measures.

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

An access policy is important as it determines who can access your keys, secrets and certificates which ultimately underpin a significant part of your security and without proper attention would lead to your information and systems being compromised.

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

Certificates establish the identity of the user and protect the traffic between the client and the server. These are used to authenticate the server content prior to it being served to the client/user.

Secrets provide secure storage for information such as passwords or API keys and are encrypted. This feature is simply to centralize and secure sensitive information that may need to be recalled by the user at a later time.

A key is a string of data that is used to encrypt or decrypt data. They are essentially used as a way to protect information from general access while using mediums of transport that aren't 100% secure. There are two types of keys, symmetric and asymmetric. Symmetric uses the same key to encrypt and decrypt data. Asymmetric uses a private key to decrypt and a public key to encrypt, this way others can send information to the user using their public key to encrypt it and the user can decrypt it using their private key.

Cryptography Questions

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

Self signed certificates have a few advantages:

1. The issuer has complete control over the cert and its properties. Settings such as expiration dates and naming conventions.
2. There is a substantial increase in privacy as it is not issued by a 3rd party and therefore does not expose the entity’s information to 3rd parties.
3. It's low cost.
4. It's faster.

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

The most obvious disadvantage is the lack of trust from most web browsers and OSs. This means that users will likely encounter warnings which will discourage traffic.

There are some other downsides such as not being able to rely on a provider for their support, expertise and services which may result in poor management of certificates. If you don't know what you are doing you may end up making yourself not only less likely to be available to your average user but more vulnerable to attackers.

3. What is a wildcard certificate?

A wildcard certificate is a cert that secures not only the primary domain but a site's subdomains. This is ultimately quite helpful as it reduces the amount of certificates required, saving both time/money and makes it easier to manage. Time is money, friend.

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 is an outdated protocol and has known vulnerabilities. This makes it undesirable and insecure as a certificate protocol. This is not isolated to Azure and in fact most modern web browsers have done away with supporting this protocol.

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, because the SSL cert has been assigned by a well known and reputable company that should have a robust system for allocating SSL certs and therefore it is more than likely a secure certificate.

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

Wednesday, 28 December 2022 at 08:12:39

Through to

Saturday, 23 December 2023 at 08:12:39

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

I don't have an intermediate certificate.

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

Yes. My root certificate is “Bitdefender Personal CA.Net-Defender”.

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

Yes it does.

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

DigiCert Global Root CA

Day 3 Questions

Cloud Security Questions

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

The Azure Web App Gateways and the Azure Front Door are similar in that they are both load balancers that reside on layer 7 of the OSI model. They both can be customized with web application firewall rules, provide support for http and https protocols and provide availability/scalability of web apps.

The differences are primarily in what they specialize in, specifically web app gateways are designed for web app workloads, whereas the azure front door is designed for global workloads and can only perform path-based load balancing. Front doors don't work on a VM or container whereas the web app gateway does. Web app gateways can perform url based routing and ssl offloading for multiple web apps, whereas azure front door focuses on load balancing/global routing while also managing failover on backend services.

These services actually can be used together with the Azure Front Door literally being at the front, and the Azure Web Application Gateway running behind it to assist with managing the load on apps/vms/containers. This allows for 100% TLS/SSL offloading.

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 essentially when the ssl based encryption occurs prior to reaching the webserver and typically at a designated point (load balancers) that is designed to efficiently do this.

The advantages to doing this is that:

- You centralize your SSL and TLS certificates
- Which can in turn increase your efficiency and security
- You remove the workload from the web servers, freeing them up to perform their dedicated purpose
- Enhances scalability, serviceability, management and troubleshooting.

3. What OSI layer does a WAF work on?

A WAF works on layer 7 (application) of the OSI model.

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

An SQL injection attack is an attack on a database by exploiting the query function.

A WAF rule designed to protect against an SQL injection attack by detecting and responding to SQL attack keywords, special characters, symbols, patterns and operators.

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?

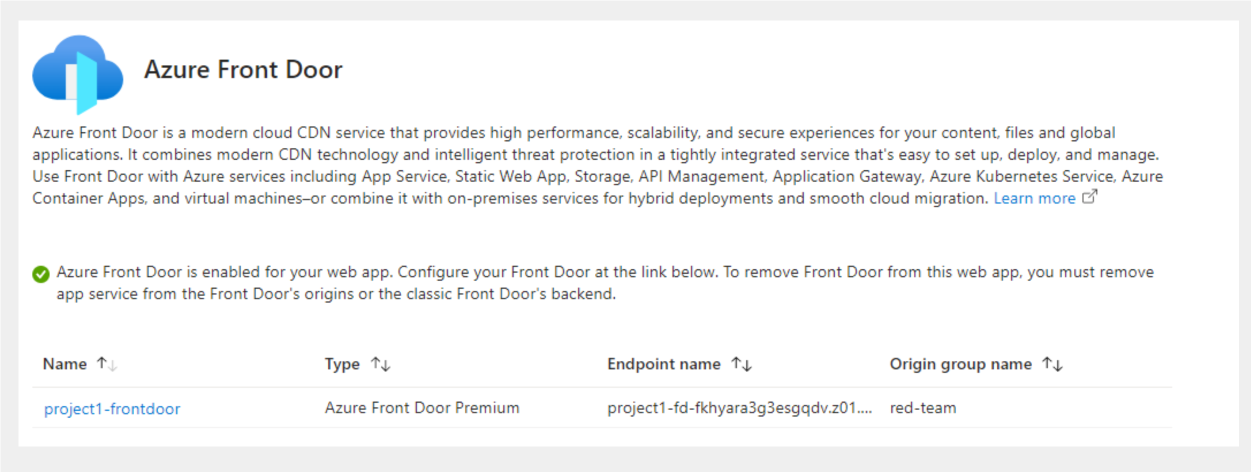
Yes. The security of my database would be made more vulnerable without the additional layer of protection afforded by the WAF rules that are attributed to the Azure Front Door as the likelihood of an SQL injection attack being detected would be reduced. It is possible that the other rules I have configured may prevent attacks, however best practice would recommend that I have many layers of security.

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?

Technically a WAF rule alone would not prevent someone from Canada accessing our web app if the WAF rule was using IP based triggers to determine a machine's geographic location and restricting access. Services such as VPNs change your IP address and would trick a system that only looks at your IP address into thinking you were accessing the web servers from a different location than the one you are in.

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

    a. Azure Front Door enabled



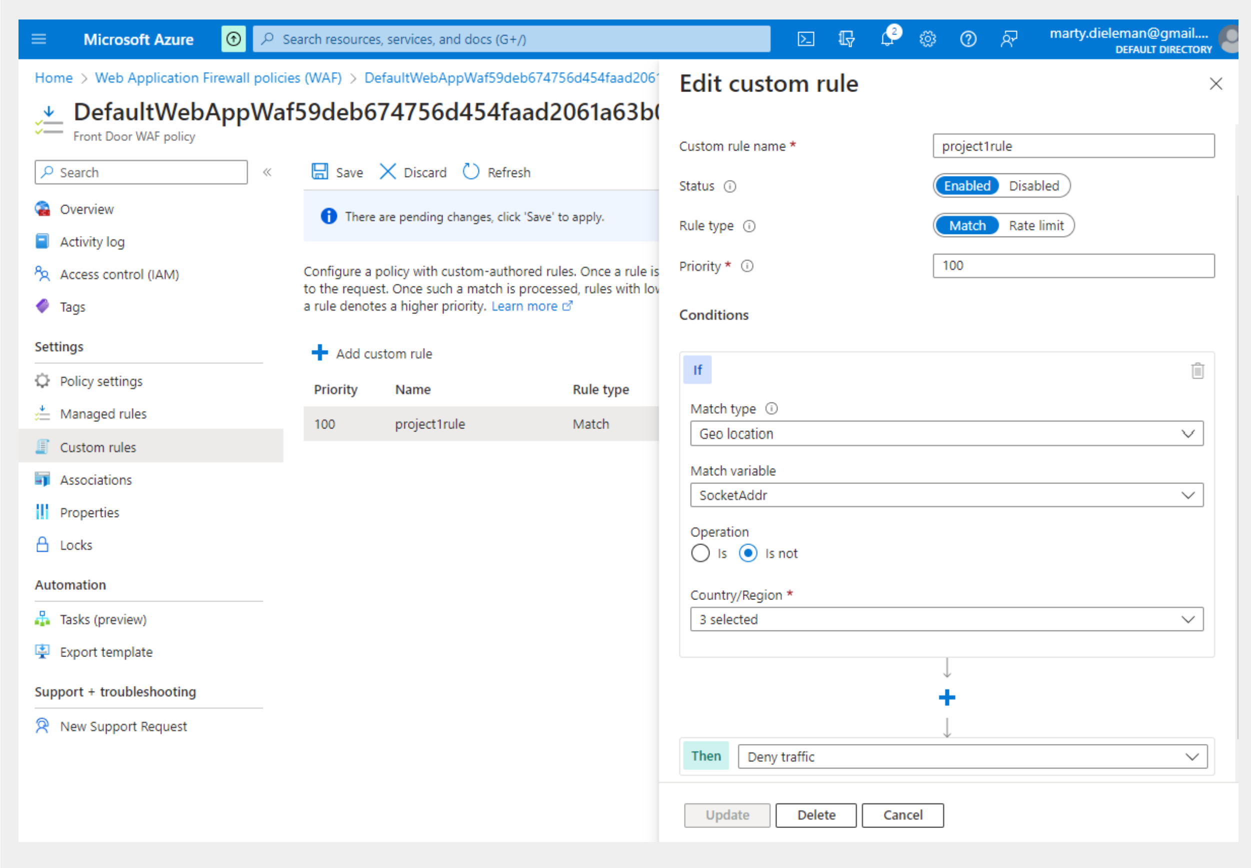
Azure Front Door

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 ↑↓
project1-frontdoor	Azure Front Door Premium	project1-fd-fkhyara3g3esgqdv.z01....	red-team

b. A WAF custom rule



Home > Web Application Firewall policies (WAF) > DefaultWebAppWaf59deb674756d454faad206

DefaultWebAppWaf59deb674756d454faad2061a63b(

Front Door WAF policy

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

Configure a policy with custom-authored rules. Once a rule is
to the request. Once such a match is processed, rules with lov
a rule denotes a higher priority. Learn more

Priority	Name	Rule type
100	project1rule	Match

Edit custom rule

Custom rule name * project1rule

Status: Enabled [✓] Disabled

Rule type: Match [✓] Rate limit

Priority * 100

Conditions

If

Match type: Geo location

Match variable: SocketAddr

Operation: ○ Is ● Is not

Country/Region * 3 selected

Then: Deny traffic

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.*

- ***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**