Name: \_Aryev P. Bhardwejj\_

Part A: Gathering domain information

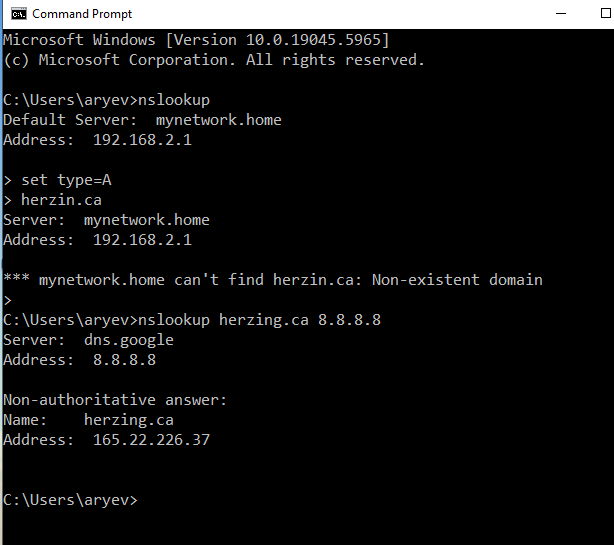
Use Open Source Intelligence (OSINT) tools **such as the ones below** to respond to questions in this section:

* MX ToolBox (<https://mxtoolbox.com/domain>)
* Whois Lookup (<https://whois.domaintools.com/>)
* Recon Cloud ([https://recon.cloud](https://recon.cloud/))
* For more tools, check OSINT Framework (<https://osintframework.com/>) and Nixintel’s resource list (https://start.me/p/rx6Qj8/nixintel-s-osint-resource-list)

NOTE: The information provided by the tools might vary, so it is up to the student to find the right tool in each case.

1. What is the IP associated with herzing.ca? And its location?

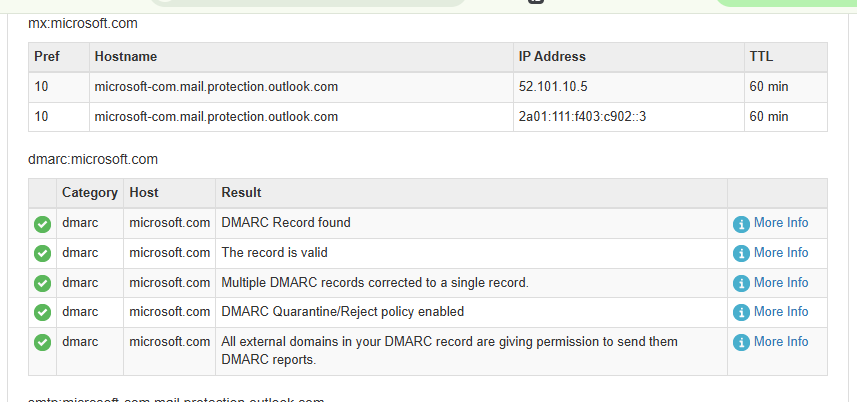
As shown below, the IP address of Herzing.ca is 165.22.226.37



This can be confirmed by using nslookup command in cmd prompt as shown in the screen shot.

1. What is the DMARC policy for microsoft.com? What does it mean?

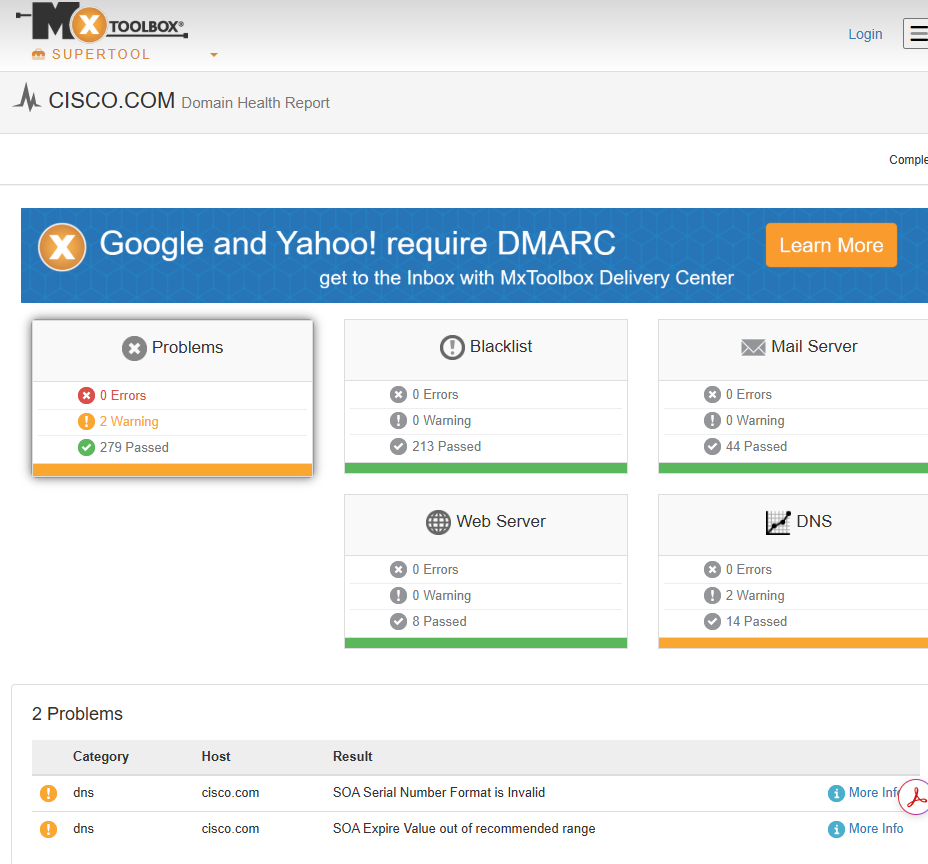
We checked the DMARC policy for microsoft.com on [https://mxtools.com](https://mxtools.com/) and received the following report:



This shows that microsoft.com has a very strict DMARC policy for its emails. They have a very strong ‘no fake allowed’ rule for emails that claim to be from microsoft.com. If an email isn’t perfectly legitimate and authorized by them, it won’t even reach your spam folder, it will be thrown away immediately by email server. They also keep a close eye on their email traffic with reports to make sure their system is working and to catch anyone trying to send fake emails.

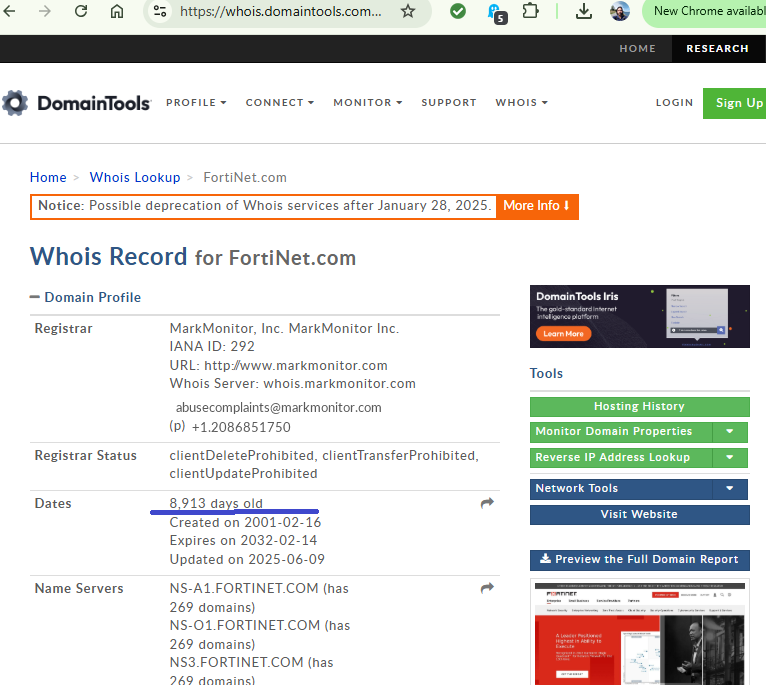
1. What two warnings are listed in the email health for cisco.com?

Checked on [https://mxtoolbox.com](https://mxtoolbox.com/) and found that there are two problems are listed for cisco.com as shown below:



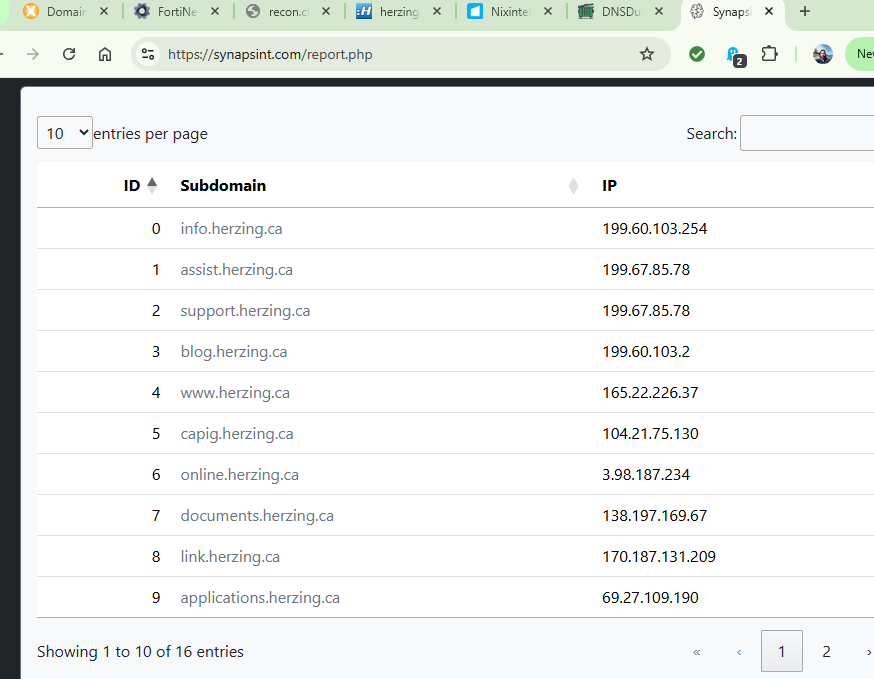
1. How old is the domain fortinet.com?

Checked for that information on whois.com and found that it is 8,913 days old

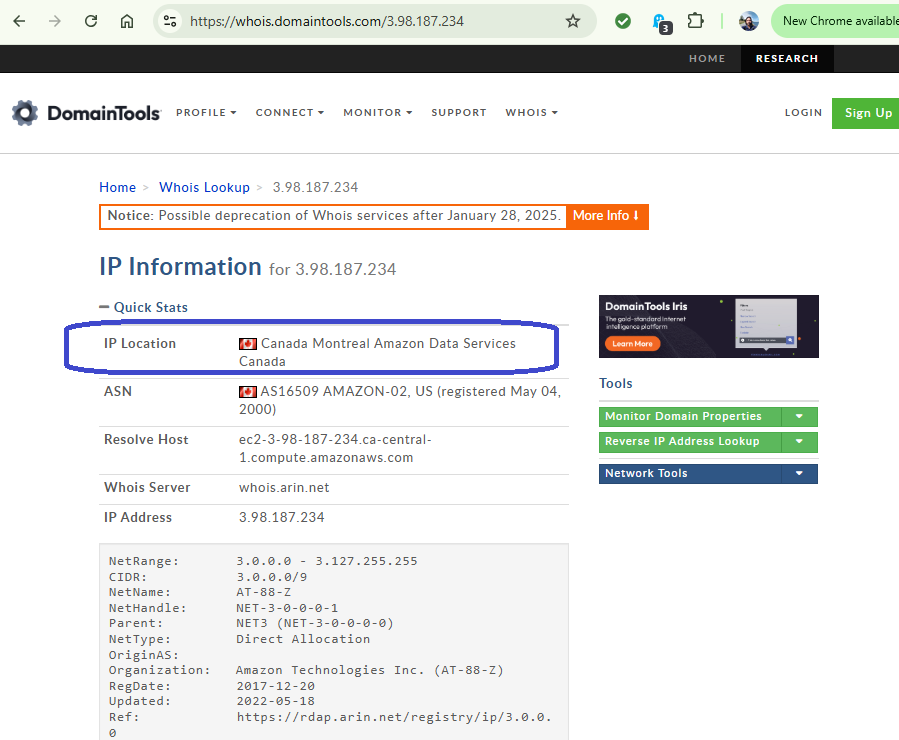


1. What subdomain is associated with herzing.ca? In which AWS region is it hosted?

These are the subdomains listed with Herzing.ca shown below:



AWS is located in Canada Montreal region as shown below:



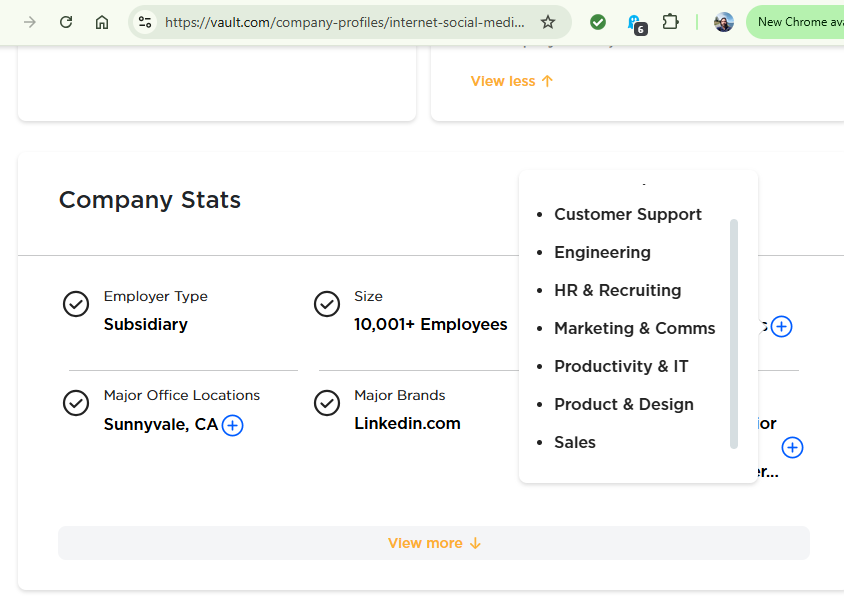
Part B: Gathering company and people information

Use **exclusively** the following tool to respond to questions in this section:

* Vault (<https://www.vault.com/>)
* Peepmail (<https://samy.pl/peepmail>)
* E-mail verifier (https://hunter.io/email-verifier)

1. Which two major departments LinkedIn begin with P?

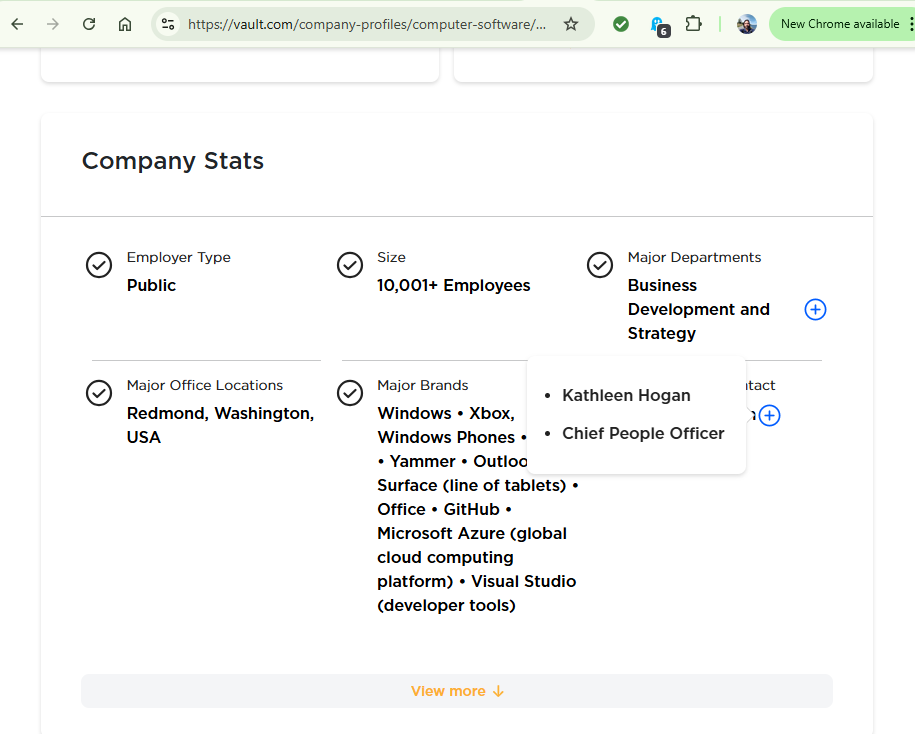
Using <https://www.vault.com/>, for linkedin, found the following 2 departments starting with ‘P’ are:

- Productivity & IT

- Product & design

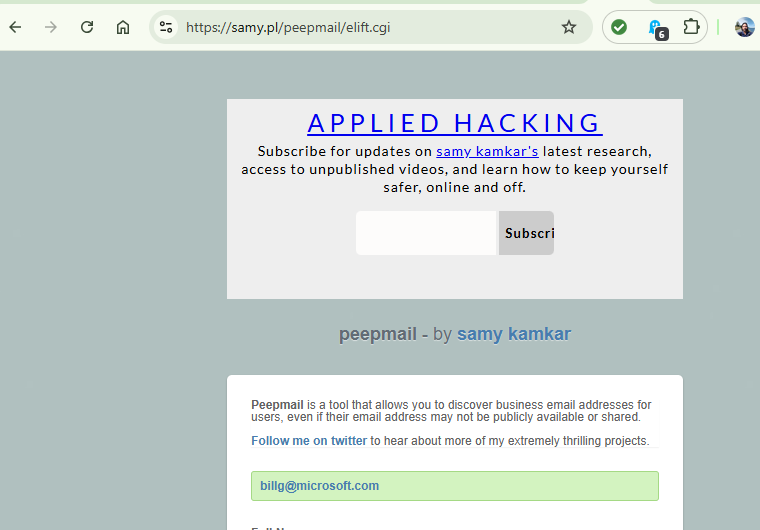
1. Who is listed as a contact for employment at Microsoft and what is this person’s position?

Using the same site: <https://vault.com/>, for Microsoft, found Kathleen Hogan, Chief People officer for employment contact



1. What is Bill Gate’s corporate email address? Verify it.

Bill Gate’s email address at Microsoft is: [billg@microsoft.com](mailto:billg@microsoft.com) as shown below



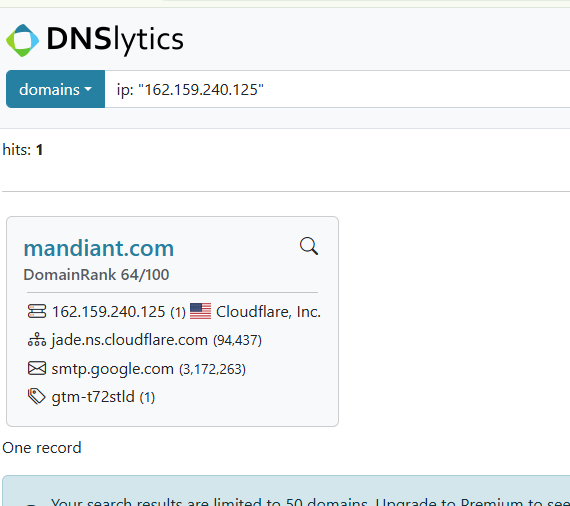
Part C: Gathering IP addresses information

Use **exclusively** the following tools to respond to questions in this section:

* IP Address Tools (<https://www.ipvoid.com/>)
* DNSlytics (https://dnslytics.com/)

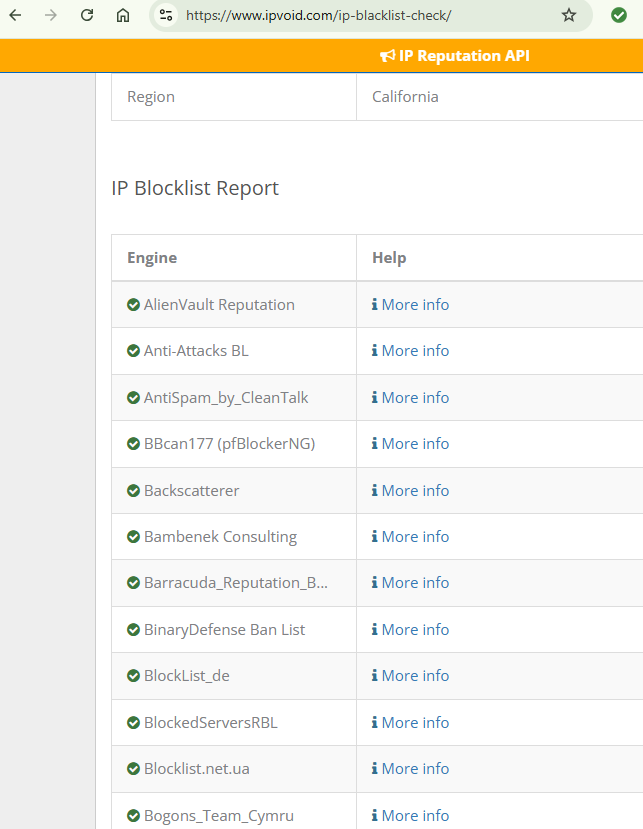
1. Which well known company appears when looking for the reverse IP resolution of 162.159.240.125?

The name mandiant.com shows when looking for a reverse IP address lookup on DNSlytics.com



1. Is this IP blocklisted? Capture a screenshot of the result.

On <https://www.ipvoid.com/>, it doesn’t shows as blocked as shown below (all check marks show)



1. Check the HTTP headers of www.herzing.ca and capture a screenshot or copy the text.

The following is the text for HTTP header for herzing.ca  
  
HTTP/1.1 301 Moved Permanently

Server: nginx

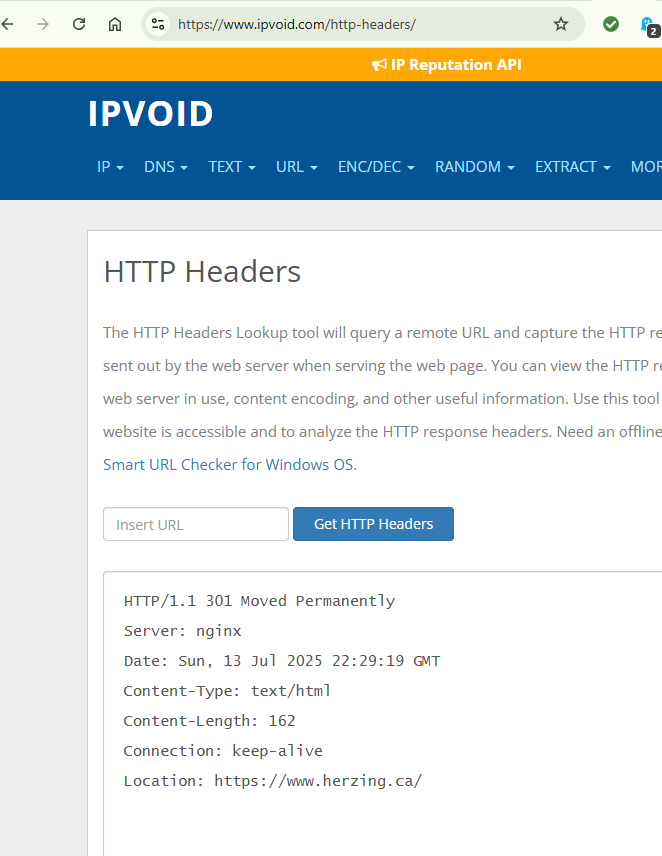
Date: Sun, 13 Jul 2025 22:29:19 GMT

Content-Type: text/html

Content-Length: 162

Connection: keep-alive

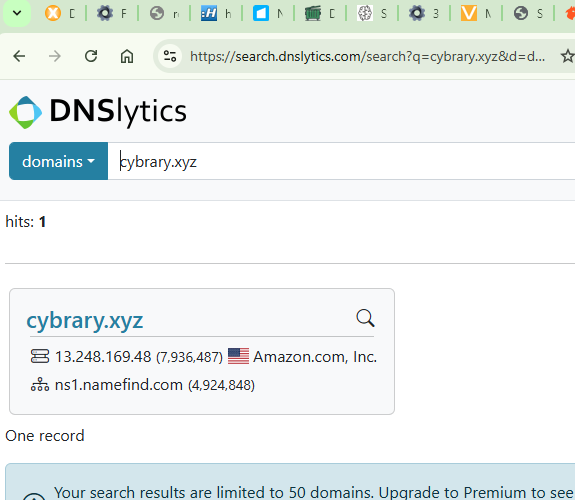
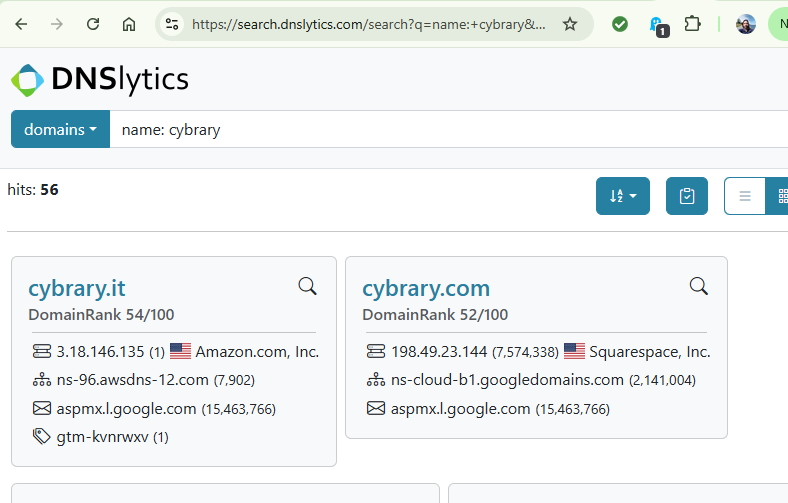
Location: https://www.herzing.ca/



Part D: Fostering your skills

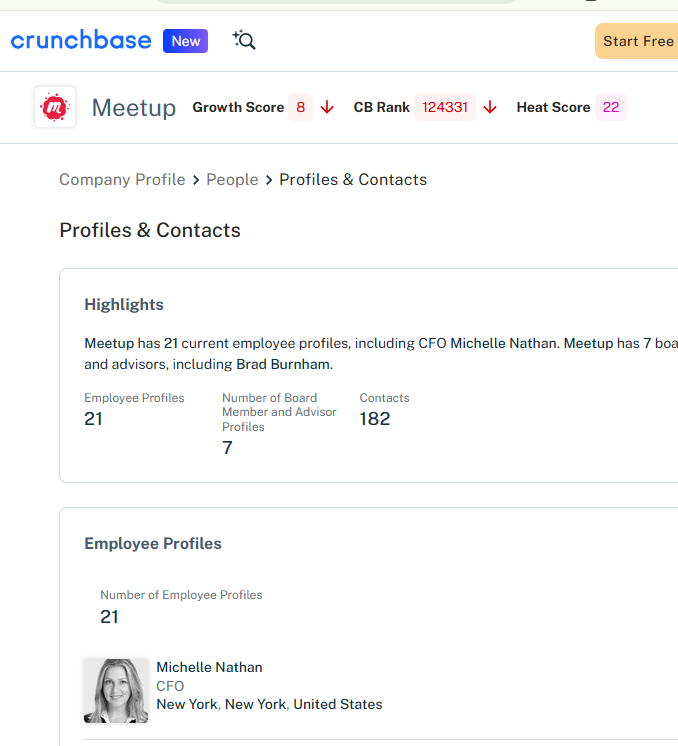
1. You are about to send a sophisticated phishing email to all employees of Cybrary. What spoofed domain your message should come from? Check if the same domain but in the .xyz TLD is available (add a screenshot).

Cybrary.xyz is not available as shown below



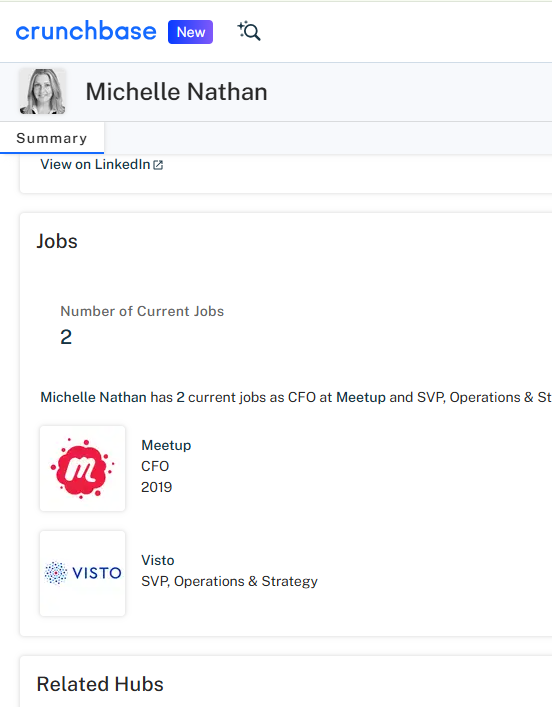
1. You need to send a spear phishing pretending to come from the Chief Financial Officer of Meetup. Who is that? Paste a screenshot with your findings.

CFO of Meetup.com is Michelle Nathan as shown below



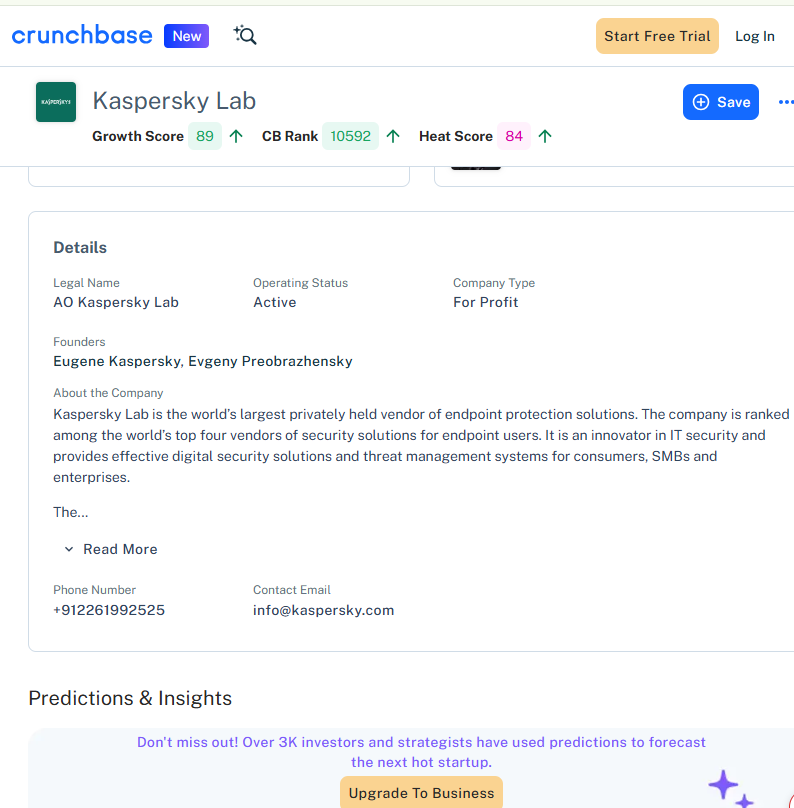
1. That person turns out to have another role at another organization according to Crunchbase. Check this out and capture a screenshot of your findings.

Michelle Nathan has two jobs as shown below



1. You need to call an employee at the HQ of Kaspersky. What number would you dial? Find out using Crunchbase and paste your findings.

Kaspersky Lab phone number is **+912261992525** as shown below



1. If this employee received an email from another employee and the headers showed the IP address 103.212.98.54, would it be suspicious? Why?

IP geolocation lookup shows that this is based in Hong Kong. So if one doesn’t knows anyone in Hong Kong and has no business associates in Hong Kong, it would be considered suspicious.

