Lab - Becoming a Defender

Objectives

Research and analyze what it takes to become a network defender.

Part 1: Conduct search of Certifications.

Part 2: Investigate positions available within cybersecurity

Background / Scenario

In our technology-centric world, as the world gets more connected, it also gets less safe. Cybersecurity is one of the fastest growing and most in-demand professions. Individuals in this field perform a wide variety of jobs including, but not limited to, consultation, investigation, and program management services to mitigate risks from both internal and external sources. Cybersecurity professionals are required to evaluate, design and implement security plans, conduct in-depth fraud investigation, perform security research and risk assessment, and propose solutions to potential security breaches.

Individuals with good security skills have a great earning potential. To be considered for one of these high paying jobs, it is very important to have the proper qualifications. Because of this, it is important to consider the industry certifications available for this career path. There are many certifications to choose from. Selecting the right certification(s) for you requires careful consideration.

Note: You can use the web browser in the virtual machine that was installed in a previous lab to research security-related issues. By using the virtual machine, you may prevent malware from being installed on your computer.

Required Resources

- PC or mobile device with internet access and virtual machine (optional).

Instructions

Step 1: Conduct search of Certifications.

a. Use your favorite search engine to conduct a search for the most popular cybersecurity-related certifications. List them below with the organization that provides the certification.

1. **Certified Information Systems Security Professional (CISSP) - (ISC)^2**
2. **Certified Ethical Hacker (CEH) - EC-Council**
3. **CompTIA Security+ - CompTIA**
4. **Certified Information Security Manager (CISM) - ISACA**
5. **Certified Information Systems Auditor (CISA) - ISACA**
6. **GIAC Security Essentials (GSEC) - Global Information Assurance Certification (GIAC)**
7. **Offensive Security Certified Professional (OSCP) - Offensive Security**
8. **Certified Cloud Security Professional (CCSP) - (ISC)^2**
9. **Certified Network Defender (CND) - EC-Council**
10. **Cisco Certified CyberOps Associate - Cisco**

b. Pick three certifications from the list above and provide more detail about the certification requirements and knowledge gained i.e.: vendor specific or neutral, number of exams to gain certification, exam requirements, topics covered etc.

Cisco Certified CyberOps Associate

- **Organization: Cisco**
- **Requirements: There are no formal prerequisites for taking the CyberOps Associate exam, but candidates should have a basic understanding of networking fundamentals, security concepts, and some experience working with Cisco technologies.**
- **Exam: The CyberOps Associate certification requires passing one exam, CBROPS 200-201 Understanding Cisco Cybersecurity Operations Fundamentals.**
- **Knowledge Gained: The certification covers the foundational skills needed for a Security Operations Center (SOC) Analyst role. Topics include Security Concepts, Security Monitoring, Host-Based Analysis, Network Intrusion Analysis, Security Policies and Procedures, Incident Response, and Data and Event Analysis. It focuses on Cisco cybersecurity solutions and technologies but also provides a solid understanding of general cybersecurity principles and practices applicable across various environments.**

Certified Information Systems Security Professional (CISSP)

- **Organization: (ISC)²**
- **Requirements: Candidates must have at least five years of cumulative, paid work experience in two or more of the eight domains of the CISSP Common Body of Knowledge (CBK). However, a four-year college degree or regional equivalent or an additional credential from the (ISC)² approved list can substitute for one year of experience.**
- **Exam: The CISSP exam consists of 100-150 multiple-choice and advanced innovative questions. Candidates have up to 3 hours to complete the exam.**
- **Knowledge Gained: CISSP is vendor-neutral and covers a broad range of cybersecurity topics across eight domains, including Security and Risk Management, Asset Security, Security Architecture and Engineering, Communication and Network Security, Identity and Access Management, Security Assessment and Testing, Security Operations, and Software Development Security.**

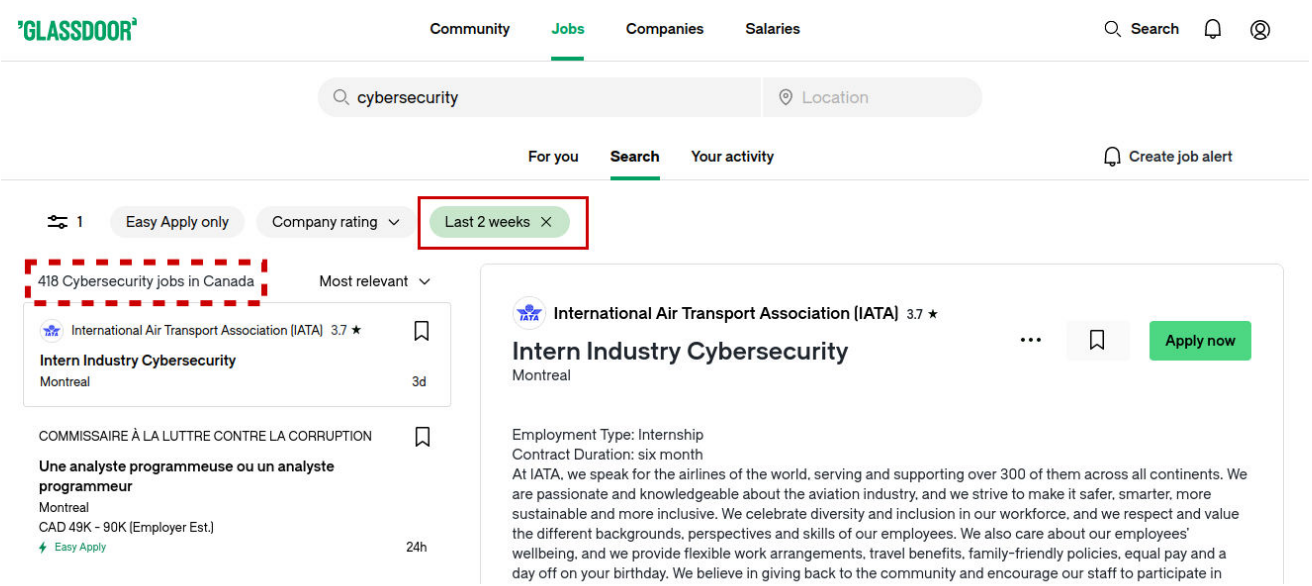
Certified Ethical Hacker (CEH)

- **Organization: EC-Council**
- **Requirements: There are no specific requirements to sit for the CEH exam. However, it's recommended that candidates have a strong understanding of networking concepts and some experience in information security.**
- **Exam: The CEH exam consists of 125 multiple-choice questions and candidates have 4 hours to complete it.**
- **Knowledge Gained: CEH focuses on the tools and techniques used by hackers to penetrate and exploit systems, but from an ethical perspective. Topics covered include Footprinting and Reconnaissance, Scanning Networks, Enumeration, System Hacking, Malware Threats, Sniffing, Social Engineering, Denial of Service, Session Hijacking, Hacking Web Servers, Wireless Networks, and more. CEH is more hands-on and practical compared to other certifications.**

Step 2: Investigate positions available within cybersecurity

Glassdoor is one of the largest job sites worldwide. Using your browser of choice, access glassdoor.com and search to find cybersecurity jobs available that were posted within the last two weeks. Adjust the search as you would like. You can search for jobs in your area or an area that you would like to live and work in.

a. How many new job listings were posted within the last two weeks?



418 Cybersecurity jobs in Canada

International Air Transport Association (IATA) 3.7 ★
Intern Industry Cybersecurity
Montreal
3d

COMMISSAIRE À LA LUTTRE CONTRE LA CORRUPTION
Une analyste programmeuse ou un analyste programmeur
Montreal
CAD 49K - 90K (Employer Est.)
Easy Apply
24h

International Air Transport Association (IATA) 3.7 ★
Intern Industry Cybersecurity
Montreal

Employment Type: Internship
Contract Duration: six month
At IATA, we speak for the airlines of the world, serving and supporting over 300 of them across all continents. We are passionate and knowledgeable about the aviation industry, and we strive to make it safer, smarter, more sustainable and more inclusive. We celebrate diversity and inclusion in our workforce, and we respect and value the different backgrounds, perspectives and skills of our employees. We also care about our employees' wellbeing, and we provide flexible work arrangements, travel benefits, family-friendly policies, equal pay and a day off on your birthday. We believe in giving back to the community and encourage our staff to participate in

b. What is the salary range for the top 10 listings?

The salary range for the top 10 listings ranges from $60,000 to $100,000.

c. What are the most common qualifications required by employers?

Bachelor's degree in Computer Science, Information Technology, Cybersecurity, or related field.

Strong analytical and problem-solving skills.

Hands-on experience with cybersecurity tools and technologies, such as firewalls, intrusion detection/prevention systems, antivirus software, and SIEM (Security Information and Event Management) platforms.

Understanding of networking concepts, protocols, and technologies.

Knowledge of operating systems, especially Windows and Linux.

d. What industry certifications are required by these employers?

Relevant certifications such as CompTIA Security+, Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), or Cisco Certified CyberOps Associate.

e. Do any of the certifications match the ones that you found in Step 1a?

Yes, certifications like CompTIA Security+, CISSP, CEH, and Cisco CyberOps Associate match the qualifications employers often seek for cybersecurity associates.

f. Investigate online resources that allow you to legally test your hacking skills. These tools allow a novice with limited cyber security experience to sharpen their penetration testing skills. One such site is Google Gruyere (Web Application Exploits and Defenses). What kinds of challenges can you find?

At Google Gruyere, users can find various challenges designed to test their skills in web application security. Some of the challenges available on the platform include:

- **Cross-site scripting (XSS): Users can learn about and practice exploiting and defending against XSS vulnerabilities, where malicious scripts are injected into web pages viewed by other users.**

- **Cross-site request forgery (CSRF): Challenges related to CSRF vulnerabilities allow users to understand how attackers can trick authenticated users into unknowingly executing malicious actions on a web application.**

- **SQL injection: Users can learn about SQL injection vulnerabilities by attempting to manipulate SQL queries through input fields to gain unauthorized access to a database.**

- **File upload vulnerabilities: Challenges related to file upload vulnerabilities involve exploiting flaws in web applications that allow attackers to upload and execute malicious files.**

- **Authentication and session management flaws: Users can explore challenges related to authentication and session management vulnerabilities, such as weak passwords, session fixation, and session hijacking.**