Task B: Interview Preparation Grid

COMM 3700

|  |
| --- |
| **Your name**:  Mohammad Al Jokhadar |

Instructions:

1. This interview preparation grid is focused on preparing you to answer behavioural style questions. In addition, the technical questions might need to be answered either with factual answers or a live demonstration.
2. Get a relevant entry level IT Job posting. The kind of job you would like to get upon graduation from the IT Diploma program.
3. Copy and paste a copy of the job posting within this document. Don’t put a link- it will expire.  
     
   [Zortech Solutions](https://www.linkedin.com/company/zortech/life)

[**XDR - Cyber Security**](https://www.linkedin.com/jobs/view/4015077205/?alternateChannel=search&refId=XVoSbbL2gRCkPJndedx%2FSg%3D%3D&trackingId=G0Cf%2F6JTGHwwo3Si77J8WA%3D%3D&trk=d_flagship3_search_srp_jobs)

Zortech Solutions · Toronto, ON (On-site)

SaveSave XDR - Cyber Security at Zortech Solutions

**About the job**

**Role: XDR - Cyber Security  
  
Location: Toronto, ON-Onsite  
  
Duration: Fulltime Permanent  
  
Required Skills And Responsibilities**

The job description for a Palo Alto XDR (Extended Detection and Response) role typically includes the following responsibilities:

* + 1. Deploying and managing Palo Alto XDR solutions: The XDR specialist is responsible for the installation, configuration, and maintenance of Palo Alto's XDR platform. This involves working with various teams to ensure proper setup and integration with existing security infrastructure.
    2. Monitoring and analyzing security events: The XDR specialist will monitor the XDR platform for security events, including threats, vulnerabilities, and anomalous activities. They will analyze the data and alerts generated by the system to identify potential security incidents.
    3. Incident response and investigation: In case of a security incident, the XDR specialist will be responsible for quickly and effectively responding to the incident. This involves taking appropriate actions to mitigate the impact, identifying the root cause, and conducting a thorough investigation to prevent similar incidents in the future.
    4. Threat hunting and intelligence: The XDR specialist should actively engage in threat hunting activities, proactively looking for signs of malicious activity or potential vulnerabilities within the network. They should stay up-to-date with the latest Security Threats and intelligence to enhance the organization's defense against evolving threats.
    5. Collaboration and communication: The XDR specialist will work closely with other teams, such as Network Security, system administrators, and the Security Operations Center (SOC), to ensure smooth integration and effective incident response. They should also effectively communicate any detected threats or incidents to appropriate stakeholders.
    6. Documentation and reporting: The XDR specialist will maintain accurate and up-to-date documentation of configurations, incidents, investigations, and any other relevant information. They should also prepare and present regular reports on security events, incidents, and overall system performance to management.
    7. Continuous improvement: The XDR specialist should actively seek opportunities to enhance the effectiveness and efficiency of the XDR platform and related security processes. This includes evaluating new features and updates, implementing best practices, and providing feedback to the vendor for product improvement..

1. Identify all the job posting skill requirements (both technical and non-technical)

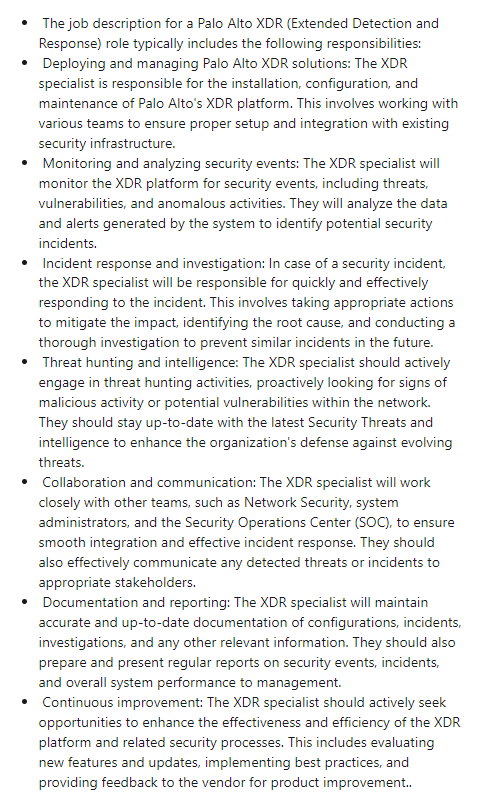
**Required Skills And Responsibilities**

* **Deploying and managing Palo Alto XDR solutions**: The XDR specialist is responsible for the installation, configuration, and maintenance of Palo Alto's XDR platform. This involves working with various teams to ensure proper setup and integration with existing security infrastructure.
* **Monitoring and analyzing security events**: The XDR specialist will monitor the XDR platform for security events, including threats, vulnerabilities, and anomalous activities. They will analyze the data and alerts generated by the system to identify potential security incidents.
* **Incident response and investigation**: In case of a security incident, the XDR specialist will be responsible for quickly and effectively responding to the incident. This involves taking appropriate actions to mitigate the impact, identifying the root cause, and conducting a thorough investigation to prevent similar incidents in the future.
* **Threat hunting and intelligence**: The XDR specialist should actively engage in threat hunting activities, proactively looking for signs of malicious activity or potential vulnerabilities within the network. They should stay up-to-date with the latest Security Threats and intelligence to enhance the organization's defense against evolving threats.
* **Collaboration and communication**: The XDR specialist will work closely with other teams, such as Network Security, system administrators, and the Security Operations Center (SOC), to ensure smooth integration and effective incident response. They should also effectively communicate any detected threats or incidents to appropriate stakeholders.
* **Documentation and reporting**: The XDR specialist will maintain accurate and up-to-date documentation of configurations, incidents, investigations, and any other relevant information. They should also prepare and present regular reports on security events, incidents, and overall system performance to management.
* **Continuous improvement**: The XDR specialist should actively seek opportunities to enhance the effectiveness and efficiency of the XDR platform and related security processes. This includes evaluating new features and updates, implementing best practices, and providing feedback to the vendor for product improvement..

1. Take a screen shot of the job posting section that has required skills and paste in this document for future reference. (Links expire, so do a screenshot)

A screenshot of a computer

Description automatically generated

  
A screenshot of a computer

Description automatically generated

1. Put the skills in the left most column. (one skill per row).
2. Think about what knowledge or experiences you have that addresses that skill requirement.

Behavioural Answers

| Skills shown  [choose 1,summarize] | Story/Nugget  Nugget | Situation  [summarize] | Your Action(s)  [Lots of specific detail, step by step] | Result  [choose 1, summarize] |
| --- | --- | --- | --- | --- |
| Tech skill, communicate, manage information, use numbers, solve problems, work with others, participate in projects, positive attitude, be responsible, be adaptable**, learn continuously**, work safely | The project I am working on, which is called OpenCorporation | . This project utilizes different components as a requirement : Kubernetes (for load balancing across systems), Git ( for Version Control and Collaboration) and NixOS Operating System(which is the foundation for this project). I have committed myself to continuously learn about every part of the project, how it works, and how it fits in as a part of the whole. | I have studied the Python programming language at NSCC, and I am grateful for that, as it is an essential part of my project. I have spent my summer learning about Git, Kubernetes, Python and Penetration Testing (to make sure my project is secure), all while recovering from my bone surgery. I continue to walk my path in the project, as it continues to grow! | Improvement in Efficacy, Speed, **Reliability** **( in the sense of feeling that I have enough knowledge to do what I must !)**, Ease of Use, Flexibility, Status, Aesthetic Appeal, Emotion, Cost |
| Tech skill, communicate, manage information, use numbers, solve problems, **work with others**, participate in projects, positive attitude, be responsible, be adaptable, learn continuously, work safely | During my time with the Kraken Cryptocurrency Exchange, I have worked on a research project with others to find potential new clients for the Exchange. | When I heard about the creation of the project, I immediately volunteered to join the team, as it gave me a new challenge, which involved my critical thinking. | I compiled a list of organizations in the Persian Gulf region, and worked with a fellow colleague in analyzing how our Sales team might approach them, and which points that they should discuss. I have utilized Open Source Intelligence ( such as the organization’s website, and members of the staff/leadership team from LinkedIn, Indeed, etc). The end result was well-written dossiers on each organization, the organization’s key players, and the points to focus on. | **Improvement in Efficacy**, Speed, Reliability, Ease of Use, Flexibility, Status, Aesthetic Appeal, Emotion, **Cost** |
| Tech skill, **communicate**, manage information, use numbers, solve problems, work with others, participate in projects, positive attitude, be responsible, be adaptable, learn continuously, work safely | During my time with CRM Group, which involved Archaeological Test Excavations, I had to communicate with the management team and the individual about his actions. | I have worked with an individual who disregarded instructions about proper sifting to look for possible artefacts, and simply did not want to complete the sifting process. We worked as a two-person team. | My co-worker would throw away all of the material-to-be-sifted away, risking the loss of potential artefacts (which is why we were there in the first place). I communicated with him regarding his actions, explained the potential loss of artefacts to him, and he proceeded to continue with his actions. I communicated with the management team about his actions. | **Improvement in Efficacy**, Speed, Reliability, Ease of Use, Flexibility, Status, Aesthetic Appeal, Emotion, Cost |

Technical Answers

|  |  |  |
| --- | --- | --- |
| Tech Skill | Question | Answer |
| Monitoring and analyzing security events | If you are to look out for intrusions, what would be your method of Security Event Detection? | Throughout my time studying Cybersecurity at NSCC, we were tasked with a variety of cybersecurity attacks in a lab environment. We detected the success of out endeavors by using a browser plugin called FoxyProxy. Another method was to use the *journalctl* command on Linux-based systems involving the running service we are protecting, or by checking the logging messages in http servers that we are attacking. |
| Vulnerability Assessment | If you are tasked with identifying vulnerabilities in our organization’s website , could you tell us the approach you would take to do so ? | My approach would be to gather as much information as possible about your organization’s externally-facing apparatus , such as your organization’s websites. Then, I would create a script that would utilize the gobuster command to identify the Domain Name Servers used by your organization’s infrastructure, then use the *nmap* command to detect the versions of running services on the targets that I have identified from the *gobuster* command. Afterwards, I would have *nmap* produce the results to a file that I would use to create a report identifying the vulnerable services. |
| Incident Response and Investigation | Hypothetically, assume that we were contracted by a client that had the misfortune of a major hack. Could you describe your methodology in investigating and responding to the incident? | The first thing I would do is check their systems’ logs, and through disc forensics/hashing, I would check the data assets for any modifications that could have done by the attackers to maintain persistence. After identifying the point of entry for the attackers, I would isolate it from the rest of the network, and check the organization’s backup infrastructure for any signs of modification/alteration to the running services or stored data. As a part of my process, I would do a vulnerability assessment on the affected system/s to detect/block any intrusion attempts by the same party or other parties. |
| Ethical Hacking | If you were to attack our organization, what would you say would be the most likely point of entry? | Since your organization provides Palo Alto’s Security Event Monitoring and Response services, I would say that the weakest link would most likely be your personnel. Phishing attacks or Spear-Phishing attacks are most common nowadays. Hypothetically, the attackers would go on sites like LinkedIn or Indeed, and view information on your personnel such as email addresses and personal information to custom-design a Phishing email that would entice your employees to click on the link provided within it. I would not be surprised to see Artificial Intelligence being used to creatively mimic the styling of your organization’s internal emails to achieve their goal. |