I. Introduction:

Glen Hub is an innovative video streaming startup that aims to provide a platform similar to Netflix for users to enjoy a wide range of video content. With a dedicated team of developers, Glen Hub has successfully developed a video streaming website and is now preparing for the next crucial steps of setting up offices and launching their website and services effectively.

Setting up offices and launching the website and services play a pivotal role in the success of Glen Hub. The office space serves as the central hub where the team can collaborate, innovate, and drive the growth of the company. It provides a physical presence for Glen Hub, enabling them to establish a professional image and enhance their credibility in the market.

Launching the website and services effectively is crucial for Glen Hub to attract and retain users. A well-executed launch ensures a seamless user experience, robust infrastructure, and scalability to meet the anticipated user base. By effectively setting up the offices and launching the website, Glen Hub can establish a strong foundation for growth and position itself as a leading player in the video streaming industry.

Throughout this research and analysis document, we will explore various aspects, including the internal network plan, hosting plan, threat analysis, and implementation budget, that will contribute to the successful setup of Glen Hub's offices and the launch of their website and services. By considering these factors comprehensively, Glen Hub will be equipped with the necessary insights and strategies to optimise their operations and provide an exceptional streaming experience to their users.

II. Internal Network Plan:

Reception Office:

- Router: To establish internet connectivity and manage network traffic.
- Switch: To connect multiple devices within the reception office, such as computers, printers, and other network devices.
- Wireless Access Point (WAP): To provide wireless connectivity for visitors and employees in the reception area.
- Computer: For receptionists to manage administrative tasks and handle customer interactions.
- Printer: To print necessary documents, visitor badges, or any other required paperwork.

Developer Workspace:

- Router: To provide internet connectivity and manage network traffic.
- Switch: To connect multiple devices within the developer workspace, including computers, servers, and other network equipment.
- Workstations: Computers or laptops for the developers to perform their tasks efficiently.
- Servers (if required): Depending on the requirements of the video streaming website, servers may be needed for hosting, content delivery, or other backend operations.
- Network Attached Storage (NAS) or File Server (if required): For storing and sharing development files and resources within the developer workspace.
- Network Cables: Ethernet cables to connect devices to the network infrastructure.

Director's Office:

- Router: To establish internet connectivity and manage network traffic.
- Switch: To connect devices within the director's office, such as computers, printers, and other network equipment.
- Computer: A workstation for the director to manage operations, communicate, and oversee the company's activities.
- Printer: To print necessary documents and reports for the director's office.
- Additional devices (common to all offices):

- Firewall: To protect the network from unauthorised access and potential threats.
- Network Attached Storage (NAS) or File Server: For shared file storage and collaboration among different offices and team members.
- VoIP Phone (if required): To facilitate internal and external communication through Voice over IP (VoIP) technology.
- UPS (Uninterruptible Power Supply): To provide power backup and protection against power outages.

Network Topologies:

Star Topology:

Advantages:

- Centralised management of the network through a central device (hub, switch, or computer).

- Easy addition of new devices to the network without disrupting the entire network.
- If one device fails, it doesn't affect the rest of the network, ensuring fault isolation.
- Provides better performance and faster data transfer rates compared to other topologies.
- Offers better security as data traffic is localised within each device's connection to the central device.

Disadvantages:

- Higher implementation cost, particularly when using a switch or router as the central network device.
- The performance and capacity of the network are dependent on the capabilities of the central device.
- If the central device fails, the entire network becomes inaccessible, resulting in network downtime.
- Increased reliance on the central device may create a single point of failure.

Overall, the star topology offers a reliable and scalable network setup. It simplifies network management, facilitates expansion, and provides better performance and fault isolation.

Ring topology:

Advantages:

- All data flows in one direction, reducing the chance of packet collisions and improving network performance.
- A network server is not required to control network connectivity between workstations, simplifying network management.
- Data can transfer between workstations at high speeds, as there are fewer hops for the data to traverse.
- Additional workstations can be added to the network without significantly impacting the network's performance or causing disruptions.

Disadvantages:

- If any individual connection in the ring is broken, the entire network is affected, leading to network downtime and potential data loss.
- The failure of a single workstation can disrupt the entire network, making it less fault-tolerant compared to other topologies.

- The hardware required to connect each workstation to the network, such as network cards and the cabling, can be more expensive than in other topologies.
- The data transmission speed in a ring topology may be slower compared to other topologies, as all data must pass through each workstation in the network.

It's important to consider these advantages and disadvantages when determining whether a ring topology is suitable for a particular network. Factors such as network size, reliability requirements, and budget constraints should be taken into account to make an informed decision.

Transmission media:

Ring Topology:

- Coaxial Cable: Historically, coaxial cables were commonly used in ring topologies. However, with the advent of Ethernet technology, their use has become less prevalent.

Star Topology:

- Ethernet Cable (Twisted Pair): The most common transmission media used in star topologies is Ethernet cable, specifically twisted pair cables. There are two main types:

- Unshielded Twisted Pair (UTP): UTP cables are widely used for short to medium-length connections within office environments. They are inexpensive and suitable for lower-speed Ethernet networks.
- Shielded Twisted Pair (STP): STP cables provide better protection against electromagnetic interference (EMI) and are used in environments where there is a higher chance of interference, such as industrial settings.

It's important to note that the choice of transmission media may depend on factors such as the network's speed requirements, distance between devices, electromagnetic interference, and budget considerations.

III. <u>Hosting Plan:</u>

Southern Africa is a region with a growing population and increasing internet penetration. GlenHub expects to have 1,200,000 users in Southern Africa by the end of their first year of operation. Here are some factors to consider regarding the user base in Southern Africa:

- Population and Internet Penetration: Assess the population size and internet penetration rates in each country within Southern Africa. Consider factors such as access to affordable internet services and the availability of smartphones and other devices.
- Demographic Analysis: Analyse the demographic profile of the target audience in Southern Africa. Consider factors such as age groups, income levels, language preferences, and cultural preferences for video content.
- Market Research: Conduct market research specific to Southern Africa to understand the demand for video streaming services. Explore user preferences, popular genres, and content consumption habits in the region.
- Competition Analysis: Evaluate the existing competition in the video streaming market in Southern Africa. Identify key players, their market share, and unique offerings. Understand the challenges and opportunities in capturing the target audience.

The Midwest region of the United States comprises several states, including Illinois, Indiana, Iowa, Kansas, Michigan, Minnesota, Missouri, Nebraska, North Dakota, Ohio, South Dakota, and Wisconsin. GlenHub expects to have 500,000 users in the Midwest region by the end of their first year. Consider the following aspects related to the user base in the Midwest:

- Population and Internet Connectivity: Analyse the population density and internet connectivity rates in the Midwest states. Consider the availability of high-speed internet infrastructure and the penetration of broadband services.

- Demographic Considerations: Understand the demographic characteristics of the target audience in the Midwest. Consider factors such as age groups, income levels, educational background, and preferences for video content.

- Market Analysis: Conduct market analysis to determine the demand for video streaming services in the Midwest region. Identify trends, preferences, and consumption patterns of the target audience.

- Competitor Landscape: Evaluate the competition in the video streaming market in the Midwest. Identify key players, their market share, and their strengths and weaknesses. Assess opportunities to differentiate GlenHub's services and capture the market.

I have decided that I’ll be using **AWS** as my hosting

There are several compelling reasons for choosing Amazon Web Services (AWS) for web hosting. Here are the key advantages of using AWS for hosting GlenHub's video streaming website:

- Broad Platform Support: AWS supports a wide range of content management systems (CMS) and programming languages. Whether you prefer WordPress, Drupal, Joomla, or other CMS platforms, AWS provides SDKs and tools for popular programming languages such as Java, Ruby, PHP, Node.js, and .NET. This flexibility allows you to use your preferred CMS and programming language for website development.

- Data Centers Worldwide: AWS has a global infrastructure with data centres located in various regions worldwide. This means you can choose the geographic location for hosting your website and ensure proximity to your target audience. AWS allows you to host your website or use a Content Delivery Network (CDN) to deliver content efficiently to users in any part of the world with just a few clicks.

- Scalability: Website traffic can vary significantly, and AWS offers scalable infrastructure to handle fluctuations in demand. Whether you experience low traffic during quiet periods or sudden spikes in traffic due to marketing campaigns or social media sharing, AWS can automatically scale resources up or down to match your needs. This ensures that your website remains accessible and performs optimally, regardless of traffic fluctuations.

- Flexible Pricing Model: AWS offers a flexible pricing model that allows you to pay for the resources you use, without any upfront costs or long-term contracts. You can choose between pay-as-you-go pricing, where you pay only for the resources consumed, or fixed monthly pricing for predictable workloads. This flexibility enables cost optimization and aligns with your specific hosting requirements and budget.

- AWS Website Solutions: For GlenHub's video streaming website, the "Simple Website Hosting" option is suitable. This solution is ideal for low to medium traffic websites with multiple authors and frequent content changes, such as marketing websites, content websites, or blogs. It provides a simple starting point for website development, and while cost-effective, it requires IT administration of the web server.

By choosing AWS for hosting, GlenHub can benefit from the reliability, scalability, and global presence of the AWS infrastructure. Additionally, managing the web server, DNS, and networking can be done conveniently from a single AWS console, providing a unified and efficient management experience.

Overall, AWS offers a robust and flexible hosting platform that can meet the needs of GlenHub's video streaming website, ensuring reliable performance, scalability, and cost efficiency.

Scalability, Reliability and Cost Implications:

When considering AWS hosting for GlenHub's video streaming website, it's important to evaluate the scalability, reliability, and cost implications of the hosting solution. Let's discuss each of these factors:

Scalability:
AWS provides excellent scalability options that allow your hosting infrastructure to grow or shrink based on demand. This is particularly important for a video streaming website that may experience varying levels of traffic. With AWS, you can leverage services such as Amazon EC2 (Elastic Compute Cloud) and Auto Scaling to automatically adjust the number of server instances based on traffic patterns. This ensures that your website can handle increased user load during peak times and scale down during quieter periods, providing a seamless user experience.

Reliability:
AWS is renowned for its high level of reliability. The AWS infrastructure is designed to offer robustness and minimise downtime. AWS achieves this through its multiple availability zones (AZs) within each region, which provide redundancy and fault tolerance. If one AZ experiences an issue, the traffic can be automatically redirected to another AZ, ensuring continuous availability of your website. Additionally, AWS offers various database options, such as Amazon RDS (Relational Database Service) and Amazon DynamoDB, which provide reliable and scalable storage for your video content and other data.

Cost Implications:
AWS offers flexible pricing options that can help manage costs effectively. With pay-as-you-go pricing, you are billed based on the resources you consume, allowing you to align costs with your actual usage. This is particularly beneficial for a startup like GlenHub, as you can start small and incrementally increase resources as your user base and demand grow. Additionally, AWS provides cost optimization tools and recommendations to help you optimise your infrastructure and control expenses.

IV. Threat Analysis:

Four major networking threats that Glen Hub should be aware of are:

1. **Malware and Viruses:** Malicious software and viruses can infiltrate the network, compromise devices, and steal or corrupt data. They can spread through infected files, email attachments, or compromised websites.

2. **Data Breaches**: Unauthorised access to sensitive user data can lead to data breaches, resulting in the exposure of personal information, financial loss, and damage to the company's reputation.

3. **DDoS Attacks:** Distributed Denial of Service (DDoS) attacks aim to overwhelm the network infrastructure by flooding it with a massive amount of traffic. This can lead to service disruptions, website downtime, and loss of user trust.

4. **Unauthorised Access**: Internal and external actors may attempt to gain unauthorised access to the network, compromising sensitive data, disrupting operations, or exploiting vulnerabilities.

Malware and viruses:

- Malware is short for "malicious software" and encompasses various types of threats like viruses, spyware, worms, and Trojans.
- A computer virus is a type of malware that infects a computer by attaching itself to executable files or documents.
- Viruses can corrupt or delete files, alter system settings, and steal sensitive information.
- Viruses require human interaction or social engineering to spread, such as opening infected email attachments or downloading infected files.
- Practising safe computing habits, such as being cautious of email attachments and downloading files from trusted sources, can help prevent virus infections.
- Implementing robust antivirus and antimalware solutions is crucial to protect against malware and viruses.
- Regularly updating software and operating systems helps patch vulnerabilities that malware can exploit.
- Security awareness training for employees educates them about the risks of malware and how to avoid infection.

- Conducting regular system scans and backups helps detect and mitigate malware infections.
- Using firewalls and intrusion detection systems adds an extra layer of protection against malware threats.
- Employing strong access controls and authentication mechanisms enhances network security.
- Staying informed about the latest malware threats and trends allows for proactive defence against evolving attack methods.

Data Breaches:

- A data breach refers to a security incident where unauthorised individuals gain access to sensitive or confidential data.
- It involves the compromise of personal or corporate information, such as Social Security numbers, bank account details, customer records, intellectual property, or financial data.
- Data breaches can occur through cyberattacks, but not all cyberattacks result in data breaches, and not all data breaches are caused by cyberattacks.
- The focus of data breaches is on the compromise of data confidentiality.
- Examples of data breaches include ransomware attacks that encrypt customer data and demand a ransom, as well as physical theft of storage devices or documents containing sensitive information.
- Data breaches pose significant risks, including financial losses, reputational damage, legal and regulatory consequences, and potential harm to individuals whose personal data is exposed.
- Preventing data breaches requires implementing robust cybersecurity measures, such as strong access controls, encryption, regular security audits, and employee training.
- Incident response plans should be in place to detect, contain, and mitigate the effects of a data breach.

DDoS Attacks:

- A distributed denial-of-service (DDoS) attack is a malicious act that aims to disrupt the normal functioning of a targeted server, service, or network by flooding it with a massive volume of Internet traffic.

- DDoS attacks are orchestrated using networks of compromised computers and devices, known as botnets, which are controlled remotely by the attacker.
- Infected machines, including computers and IoT devices, become part of the botnet and are used to generate attack traffic.
- The attacker sends instructions to the bots, directing them to send a barrage of requests to the target's IP address, overwhelming its resources and causing a denial-of-service to legitimate traffic.
- DDoS attacks can make it difficult to distinguish between attack traffic and normal traffic since the bots involved are genuine Internet devices.
- These attacks can disrupt online services, render websites inaccessible, and impact the availability of network services.
- DDoS attacks can be financially motivated, politically driven, or simply carried out as acts of vandalism.
- Countermeasures for mitigating DDoS attacks include implementing network infrastructure defences such as firewalls, load balancers, and traffic filtering systems.
- Employing rate limiting, traffic profiling, and anomaly detection techniques can help identify and block suspicious traffic patterns associated with DDoS attacks.

Unauthorised Access:

- Unauthorised access refers to the act of gaining entry to a website, program, server, service, or any system without proper authorization or using someone else's account or credentials.
- It can occur when an individual repeatedly attempts to guess a password or username until they successfully gain access to an account that does not belong to them.
- Unauthorised access can also happen when a user tries to access restricted areas or sensitive information within a system without the necessary permissions.
- System administrators often employ security measures such as alerts to detect and notify them of unauthorised access attempts, allowing them to investigate and take appropriate actions.
- To prevent unauthorised access, many secure systems implement measures like account lockouts after multiple failed login attempts.
- Unauthorised access poses a significant risk to the security and confidentiality of systems, as it can lead to data breaches, unauthorised modifications, theft of sensitive information, and other malicious activities.

- Countermeasures to mitigate unauthorised access include strong authentication methods (such as two-factor authentication), access control mechanisms, regular security audits, and user education on secure practices.
- Employing robust password policies, implementing role-based access control, and regularly monitoring and reviewing access logs can also help prevent unauthorised access incidents.
- It is crucial for organisations to maintain up-to-date security practices, promptly patch vulnerabilities, and establish incident response plans to address any unauthorised access incidents swiftly and effectively.

Countermeasures:

- Implement strong and unique passwords for all accounts and regularly update them.
- Enable two-factor authentication (2FA) to add an extra layer of security.
- Regularly update and patch software, operating systems, and applications to fix vulnerabilities.
- Utilise a reliable antivirus and anti-malware solution and keep it up to date.
- Employ a robust firewall to monitor and filter incoming and outgoing network traffic.
- Implement intrusion detection and prevention systems (IDPS) to identify and block malicious activities.
- Use encryption techniques to protect sensitive data in transit and at rest.
- Regularly back up critical data and ensure backups are stored securely offsite.
- Educate employees about safe browsing habits, phishing attacks, and social engineering tactics.
- Establish strong access controls and permissions, granting users only the necessary privileges.
- Monitor network traffic and system logs for any suspicious activities or unauthorised access attempts.
- Conduct regular security audits and penetration testing to identify and address vulnerabilities.
- Develop an incident response plan to quickly and effectively respond to security incidents.
- Stay informed about the latest security threats and best practices through industry resources and security advisories.

V. Implementation Budget:

VI. Conclusion:

In conclusion, for Glen Hub's success, it is vital to prioritise a well-planned internal network, a reliable hosting infrastructure, robust security measures, and careful budget considerations. The internal network should be designed to meet the specific needs of each office room, utilising suitable network topologies and transmission media. When considering the hosting infrastructure, the expected user base and video content volume should be taken into account, exploring options from cloud providers like Oracle and AWS. Implementing strong security measures is crucial to protect against malware, data breaches, DDoS attacks, and unauthorised access. Lastly, allocating a realistic budget that covers hosting costs, security measures, and potential scalability needs is essential. By addressing these key factors, Glen Hub can ensure a seamless and secure video streaming experience while setting a strong foundation for its growth and success.

Referencing:

ComputerHope, n.a. https://www.computerhope.com. (Accessed 15 June 2023)

FOSCO, n.a. https://www.fiberoptics4sale.com (Accessed 15 June 2023)

aws, n.a.https://aws.amazon.com. (Accessed 15 June 2023)

DigiCert, n.a. https://www.digicert.com. (Accessed 15 June 2023)

IBM. n.a. https://www.ibm.com. (Accessed 15 June 2023)

Cloudflare. N.a. https://www.cloudflare.com. (Accessed 15 June 2023)