task 6

(30/08/23):Understanding CIS Policy version 7and write about them

CIS Controls Version 7 is a prioritized set of 20 cybersecurity best practices developed by the Center for Internet Security (CIS). It is a consensus-based framework that is designed to help organizations of all sizes protect themselves against the most common cyber threats.

The CIS Controls are organized into three categories:

1. **Basic Controls:** These controls are considered essential for any organization that wants to establish a baseline level of cybersecurity.
2. **Foundational Controls:** These controls build on the Basic Controls and provide additional protection against more sophisticated threats.
3. **Organizational Controls:** These controls are designed to help organizations implement and manage their security programs effectively.

The CIS Controls are not a one-size-fits-all solution. Organizations should implement the controls that are most relevant to their specific needs and environment. However, the CIS Controls provide a good starting point for any organization that is looking to improve its cybersecurity posture.

Here is a brief overview of each of the CIS Controls Version 7:

Basic Controls

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Secure Configuration of Hardware and Software
4. Continuous Vulnerability Management
5. Controlled Use of Administrative Privileges
6. Maintenance, Monitoring, and Analysis of Audit Logs
7. Email and Web Browser Protections

8. Malware Defenses
9. Limited and Controlled Network Access
9. Data Loss Prevention

Foundational Controls

1. Account Management
2. Security Awareness and Training
3. Asset Management
4. Incident Response and Management
5. Penetration Testing and Red Team Activities
6. Secure Development and Deployment
7. Backup and Recovery
8. Supply Chain Management
9. Risk Management
10. Threat Intelligence

The CIS Controls are a valuable resource for any organization that is serious about cybersecurity. By implementing the CIS Controls, organizations can significantly reduce their risk of being compromised by cyberattacks.

Benefits of Implementing CIS Controls Version 7

There are many benefits to implementing CIS Controls Version 7, including:

- Reduced risk of cyberattacks
- Improved compliance with regulatory requirements
- Increased customer confidence
- Reduced costs associated with cybersecurity incidents
- Improved overall security posture

How to Implement CIS Controls Version 7

The first step in implementing CIS Controls Version 7 is to assess your current security posture. This will help you to identify which controls you need to implement and which ones you already have in place. Once you have completed your assessment, you can begin to implement the controls that you need.

There are a number of resources available to help you implement CIS Controls Version 7. The CIS website provides a variety of resources, including documentation, tools, and training. There are also a number of third-party vendors that offer products and services to help organizations implement CIS Controls.

Conclusion

CIS Controls Version 7 is a valuable resource for any organization that is serious about cybersecurity. By implementing the CIS Controls, organizations can significantly reduce their risk of being compromised by cyberattacks.