Understanding the 18 CIS Critical Security Controls: Your Roadmap for Cybersecurity Excellence

In the ever-evolving landscape of cybersecurity, staying ahead of threats is paramount.

To assist organizations across the globe improve their cyber posture, information security training nonprofit Center for Internet Security (CIS) develops comprehensive cybersecurity guidelines called CIS Critical Security Controls.

Formerly known as SANS Critical Security Controls (SANS Top 20), these recommended cyber defense best practices have been refined and consolidated into its eighth version, and enhanced to address the latest and most pervasive threats to systems and software.

Consider this helpful guide a primer in CIS Controls Version 8 outlining their importance in bolstering a robust cybersecurity posture.

The Evolution: SANS Top 20 to CIS Controls

The Critical Security Controls encompassed within this latest version represent several phases of refinement.

Originally dubbed the SANS Top 20, these protocols were designed to provide organizations with a structured approach to cybersecurity.

Recognizing the need for adaptability and efficiency in the face of evolving cyber threats, they underwent a transformation and were officially adopted as the CIS Critical Security Controls.

CIS Controls Version 8 signifies a shift in perspective. Rather than organizing controls based on who manages the devices, Version 8 restructures them around activities.

In this paradigm, the focus shifts away from physical devices, fixed boundaries, and isolated security measures. The result is a consolidation of controls from 20 to 18, each designed to address critical aspects of cybersecurity.

The 18 CIS Critical Security Controls: Your Respective Guide

Let's dive into a primer of CIS Controls Version 8, where each control represents a crucial pillar in your cyber defense.

CIS Control 1: Inventory & Control of Enterprise Assets

Maintain an accurate inventory of authorized and unauthorized devices to reduce attack surface.

Importance: You can't protect what you don't know exists. Asset management forms the foundation of cybersecurity.

CIS Control 2: Inventory & Control of Software Assets

Regularly assess and manage software assets to mitigate vulnerabilities.

Importance: Unmanaged software can be a vector for attacks. Keeping a software inventory is key.

CIS Control 3: Data Protection

Implement measures to safeguard sensitive data, including encryption and access controls.

Importance: Data is a valuable asset. Protecting it is essential for compliance and reputation.

CIS Control 4: Secure Configuration of Enterprise Assets & Software

Establish and maintain secure configurations for hardware and software to minimize vulnerabilities.

Importance: Weak configurations are low-hanging fruit for attackers. Proper setup is crucial.

CIS Control 5: Account Management

Monitor and manage user accounts to detect and respond to suspicious activities.

Importance: Unauthorized access can lead to breaches. Effective account management is the first step.

CIS Control 6: Access Control Management

Similarly, it is extremely important to ensure proper user authentication and access control measures are in place to prevent unauthorized access.

Importance: Unauthorized access can lead to breaches. Proper access controls are an essential defense layer.

CIS Control 7: Continuous Vulnerability Management

Identify, assess, and remediate vulnerabilities in systems and software on an ongoing basis.

Importance: Vulnerabilities are gateways for attackers. Timely patching is critical.

CIS Control 8: Audit Log Management

Implement comprehensive audit log management to track and investigate security incidents.

Importance: Logs are your trail of breadcrumbs. Efficient log management assists incident response.

CIS Control 9: Email & Web Browser Protections

Implement protections to safeguard email and web browsing from cyber threats.

Importance: Phishing and web threats are common attack vectors.

CIS Control 10: Malware Defenses

Strengthen defenses against malware attacks, including prevention and remediation.

Importance: Malware can disrupt operations. Effective defenses mitigate risks and include real-time detection for rapid response.

CIS Control 11: Data Recovery

Establish and test data backup and recovery procedures to ensure data availability.

Importance: Data loss can be catastrophic. Recovery readiness is a safeguard!

CIS Control 12: Network Infrastructure Management

Secure network configurations and architectures to defend against network-based attacks.

Importance: Network vulnerabilities can be exploited. Proper management mitigates risks.

CIS Control 13: Network Monitoring & Defense

Implement measures to detect and prevent network-based attacks at the perimeter.

Importance: Early detection is crucial. Monitoring enhances proactive defense.

CIS Control 14: Security Awareness & Skills Training

Educate employees about cybersecurity risks and best practices through training programs.

Importance: Employees are both your first line of defense and potential risks. Training mitigates human errors.

CIS Control 15: Service Provider Management

Manage and assess relationships with third-party service providers to ensure security standards are met.

Importance: Outsourced services introduce risks. Effective management ensures compliance.

CIS Control 16: Application Software Security

Ensure the security of application software through secure coding practices, testing, and patch management.

Importance: Applications have vulnerabilities. Keeping them up to date helps prevent exploitation.

CIS Control 17: Incident Response Management

Develop and maintain an incident response plan to effectively respond to and recover from security incidents.

Importance: Incidents are inevitable. Effective, real-time response minimizes damage.

CIS Control 18: Penetration Testing

Conduct penetration testing to identify and proactively address vulnerabilities.

Importance: Testing helps uncover weaknesses. Proactive mitigation improves security.

Why CIS Controls Matter

CIS Critical Security Controls provide a structured and comprehensive framework for organizations of all sizes and cybersecurity maturity levels.

By adopting these controls, organizations can significantly enhance their security posture, reduce vulnerabilities, and better defend against a wide range of cyber threats.

In today's interconnected landscape, knowledge and proactive measures are your greatest allies.

CIS Controls serve as a blueprint for excellence in cybersecurity, empowering organizations to navigate the complex cybersecurity landscape with confidence and resilience.

Stay informed, stay secure, and consider alignment with CIS Critical Security Controls a critical step on your roadmap.

Cybersafe Solutions is a leading MSSP leveraging CIS Critical Security Controls and other industry standards to help organizations bolster a robust cybersecurity posture, mitigate risks, and defend against evolving threats. To learn more about partnering with Cybersafe to enhance your security, contact us today.