The 18 CIS Critical Controls for Cybersecurity

You may have heard of the CIS Critical Security Controls. But what are they, and who are they for?

In this post, we'll give you an introduction to the CIS Critical Security Controls and explain how they can help your organization improve its cybersecurity posture.

What are the CIS Critical Security Controls?

The CIS Critical Security Controls are a framework of best practices for cybersecurity. They were created by the Center for Internet Security, and they're designed to help organizations of all sizes improve their cybersecurity posture.

The main purpose of the CIS Critical Security Controls is to help organizations prioritize their actions. They were created to assist organizations in quickly defining the foundation of their defenses, allocating their limited resources to actions that would yield quick, high-value results, before concentrating their attention and resources on other business risks.

The CIS Security Controls were created in 2008 through a collaboration that included businesses, governmental organisations, educational institutions, and people from every sector of the ecosystem (cyber analysts, vulnerability finders, solution providers, users, consultants, policy-makers, executives, academia, auditors, etc.). These skilled volunteers drew from their first-hand experiences to develop the best possible defensive measures against cyberattacks.

The controls are based on the principle of defense-in-depth, which means that you should use multiple layers of security to protect your systems. The controls are also modular, which means that you can pick and choose the ones that are most relevant to your organization. They’re also continuously updated and improved to account for the latest cybersecurity threats and techniques.

Who are the CIS Controls for?

The CIS Critical Security Controls are for everyone. No, really—they are.

Even if you're not in IT, you should be aware of these controls. Why? Because they can help protect your business from cyberattacks. In fact, they're designed to do just that.

In an endeavour to establish secure, dependable standards of protection for IT systems and cybersecurity programmes from data breaches, the CIS established frameworks that have an impact on everyone from individuals to corporations and governments. They were created to assist organizations in quickly defining the foundation of their defenses, allocating their limited resources to actions that would yield quick, high-value results, before concentrating their attention and resources on other risk issues that were particular to their business or mission.

Thousands of enterprises worldwide have implemented the CIS Controls to help protect themselves and their business interests. These controls are also supported by a vast number of security solution vendors, and consultants.

The 18 CIS Security Controls

There are a total of 18 CIS Controls. These 18 controls are made to prevent the great majority of threats that are currently being seen, in addition to providing the structure for automation and systems management that will benefit cyber security well into the future.

1. Inventory and Control of Enterprise Assets
2. Inventory and Control of Software Assets
3. Data protection
4. Secure Configuration of Enterprise Assets and Software
5. Account Management
6. Access Control Management
7. Continuous Vulnerability Management
8. Audit Log Management
9. Email and Web Browser Protections
10. Malware Defenses
11. Data recovery
12. Network Infrastructure Management
13. Network Monitoring and Defense
14. Security Awareness and Skills Training
15. Service Provider Management
16. Application Software Security
17. Incident Response Management
18. Penetration Testing
19.

CIS Control 1 - Inventory and Control of Hardware Assets

- Identify devices on your organization’s network, keep them updated, and maintain an inventory of assets that store or process information.

This first control's primary objective is to obtain a complete picture of all the company's assets. These assets include end-user devices, including portable and mobile ones, network devices, non-computing/Internet of Things (IoT) devices, and servers connected to the network physically, virtually, remotely, and/or within cloud environments. Maintaining an inventory of all the assets helps to get an accurate idea of what needs to be monitored and protected, in addition to identifying unauthorized use of assets.

CIS Control 2 - Inventory and Control of Software Assets

- Automate the documentation of all software using software inventory tools

This control ensures that all software on the network including operating systems and applications are actively managed, to prevent the unauthorized installation and execution of any software.

CIS Control 3 - Data Protection

- Establish procedures and technology safeguards to recognise, categorize, handle data securely, keep it, and discard it.

Install an automated system on network perimeters that keeps an eye out for unauthorized transfers of sensitive data, stops those transfers, and notifies information security specialists.

CIS Control 4 - Secure Configuration of Enterprise Assets and Software

- Maintain all approved operating systems and software according to established, standardized security configuration criteria.

Configuration errors are one of the most common causes of data loss and system compromise. In fact, they're expected to be the root of 99 percent of firewall breaches in 2023. When improperly configured network devices and applications might expose security flaws and interfere with company operations. Using security automation can help to make your IT assets more secure and easier to monitor.

CIS Control 5 - Account Management

- Use the necessary processes and tools to manage authorization for user accounts including admin accounts and service accounts to access the enterprise assets.

Attackers can utilize privileged and dormant user accounts to infiltrate your network. Keeping these accounts under control and to a minimum can help safeguard your network and data from unauthorized access.

CIS Control 6 - Access Control Management

- Use the required processes and tools to create, assign, and revoke access privileges for users, administrators, and services to enterprise assets.

Access management defends your business against potential security breaches by controlling who has access to what within your organization. Granting too many privileges to one user or a group of users creates more opportunities for attack. Limiting access to only the resources required can help to reduce the attack surface of your organization.

CIS Control 7 - Continuous Vulnerability Management

- Use a reliable vulnerability scanning tool to keep an eye on your network's systems, find any flaws, and patch them as necessary.

In order to address, remediate, and minimize vulnerabilities and reduce the potential for security breaches, create a strategy to monitor and assess vulnerabilities throughout the business infrastructure. Additionally, keep an eye out for the latest threat and vulnerability information in public and private industry sources.

CIS Control 8 - Audit Log Management

- Make sure that local logging is activated and that the proper logs are aggregated into a centralized log management system for evaluation.

Tracking and analyzing security events makes it difficult for attackers to conceal their activity and whereabouts. Security logs are the perfect starting point for your investigation, and are a critical component of any security solution. Having access to complete logs can help you understand which systems were affected during an incident, and what actions were taken by the attacker while they were active.

CIS Control 9 - Email and Web Browser Protections

- Enhance threat detection and protection against email and web-based threats.

Every day, we send millions of emails for various purposes. They are one of the most common attack vectors of the present day. An email with a virus or a phishing attack can lead to a data breach and loss of sensitive information. Not just email, but other web based attacks are also on the rise as our reliance on the internet grows. At present, websites encounter an average of 94 attacks per day. As a result, it is essential to exercise caution in web-based environments.

CIS Control 10 - Malware Defenses

- Use centrally managed anti-malware software to continuously monitor and protect all workstations and servers within the company.

This security control is used to prevent and manage the installation, propagation, and execution of malicious code, scripts or apps on enterprise assets. Malware can steal, encrypt, or delete your data, change or hijack fundamental computer operations, and spy on your online behavior without your knowledge or consent, making it one of the biggest threats to your security.

CIS Control 11 - Data Recovery

- Build and maintain data recovery procedures that help to restore compromised assets to their original, pre-incident state.

These security practices can include regularly backing up all system data and key systems, protecting, and isolating the backed up data, and periodically testing data recovery procedures. Effective data backup and recovery can prevent accidental data loss or corruption. Moreover, Making sure you have a recent backup of your data in a secure location will help you avoid having to pay a steep ransom to get access to it again after a ransomware attack.

CIS Control 12 - Network Infrastructure Management

- Network devices must be established, implemented, and actively managed in order to stop attackers from taking advantage of weak network services and access points.

Securing the network is currently one of the most pressing challenges that security professionals face. Businesses must regularly review and change configurations, access control, and traffic flows to improve network security. You can detect security issues by thoroughly documenting every element of your network infrastructure and keeping an eye out for unauthorized changes.

CIS Control 13 - Network Monitoring and Defense

- Maintain thorough network surveillance and defense against security threats across the network infrastructure.

This security control addresses how to gather and analyze the information needed to spot breaches, filter traffic, manage access control, gather traffic flow logs, and send out notifications about security incidents.

CIS Control 14 - Security Awareness and Skills Training

- Create and manage a security awareness programme to impact employee behavior and ensure that they have the necessary training to minimize cybersecurity threats to the company.

As per the latest statistics, 82% of data breaches involve some form of human error. Despite being the cause for most breaches and security incidents, this is a concern that is barely addressed. This CIS control emphasizes the role of security awareness training in preventing data breaches, compliance penalties, identity theft, and other damages.

CIS Control 15 - Service Provider Management

- Assess service providers who handle sensitive data or are in charge of a company's vital IT systems to make sure they are protecting the systems and the data they handle properly.

This security measure pertains to third-party-managed data, systems, and procedures. It’s common for organizations to hire third-party service providers to help manage and support their operations and it's also common for these service providers to have access to company data. However, any flaw in your vendor's security infrastructure could be a direct threat to your organization. Monitoring your supply chain is an essential part of any comprehensive security strategy today. For example, Evolve's Automated Supply Chain Monitoring service lets you automatically gather and generate intelligence about your supply chain to spot potential threats that could be used to disrupt your business.

CIS Control 16 - Application Software Security

- Manage the security life cycle of software that has been developed in-house, hosted, or bought in order to avoid, identify, and fix security flaws before they have an impact on the business.

Attackers love to exploit unpatched security flaws in your software and/or applications. Finding and fixing flaws early on in the software development life cycle is crucial to ensure the safety of your systems.

CIS Control 17 - Incident Response Management

- Build and maintain an incident response capability to help you be ready for, recognize an attack coming, and react rapidly to it.

No business is immune to cyberattacks. Without an incident response plan in place, you risk missing a breach of your network until it’s too late.

CIS Control 18 - Penetration Testing

- Evaluate the efficiency and resilience of your network and assets by finding and exploiting weaknesses just like an attacker would.

In a dynamic IT environment and with a threat landscape that is just as dynamic, it isn’t enough if you have all the security controls in place. You also need to test your defenses regularly. Both internal and external pen tests can help you gauge the effectiveness of your security controls, identify security gaps, and fix them as needed.

CIS Controls and Other Security Standards

So how do they work with other security standards?

The Critical Security Controls are designed to complement other widely known frameworks. And while CIS controls cannot replace other frameworks like NIST, they do make it easier to apply them and are cross-compatible with them.

For instance, The CIS Controls are identified as one of the "informative references" in the NIST Framework for Improving Critical Infrastructure Cybersecurity, which enables users to implement the Framework using an already established, and widely accepted technique.

That implies that as a starting point, an organization could establish CIS measures to ensure fundamental security. Following that, you can implement the NIST Cybersecurity Framework, the ISO 27000 series, and related standards, and even comply with regulatory standards such as the PCI-DSS or HIPAA.

Conclusion

The CIS Critical Security Controls are a prioritized list of measures that organizations can take to mitigate cyber risks. They are based on the most common attacks that occur in the real world, so they're essentially a playbook of best practices.

If you're responsible for cybersecurity in your organization, then you need to be familiar with the CIS Critical Security Controls. And if you're not, then now is the time to learn about them.

Secure Your Organization with Threat Intelligence

At Threat Intelligence, we're specialists in penetration testing and automated security capabilities such as incident response, supply chain monitoring, DNS sinkholing, cyber threat intelligence, endpoint detection and response, and much more.

Our services have been used by organizations - big and small, government and private - across the globe. We combine world-class expertise with cutting-edge technology to bring you the best in cybersecurity. To learn more about our solutions visit www.threatintelligence.com or schedule a demo of our products at no cost to your company.