Avecto

The First Six Critical Security Controls as recommended by SANS

About the Center for Internet Security (CIS) and the 20 Critical Controls

Introduced in 2008 in response to extreme data losses in the US, the 20 Critical Security Controls prioritizes a list of measures that are effective in improving risk posture against real-world threats.

The project was initially developed by SANS, but in 2013 the management of the Controls was transferred to the Council on CyberSecurity (the Council) and then in 2015 to the Center for Internet Security (CIS).

Derived from the most common attack patterns and vetted across government and industry bodies, the 20 Critical Controls focus on a small number of actionable controls with immediate benefits, aiming for a "must do first" philosophy. The CIS Critical Security Controls are an example of the principle of Pareto's Law whereby 80% of the impact comes from 20% of the effort.

Notable changes in 6.0 update

Controlled use of administrative privileges was increased in priority from Control 12 to Control 5 in recognition of the number of attacks exploiting overprivileged accounts.

A new control (7) was introduced for email and web browser protections in response.

The "First Six CIS Controls" as recommended by SANS

To provide a direct starting point for organizations, SANS highlights the "First Six" Controls as the basics to prevent disruptive attacks, with high impact and immediate benefits:

CIS Control #1: Inventory of Authorized and Unauthorized Devices

CIS Control #2: Inventory of Authorized and Unauthorized Software

The first two Controls call for organizations to know which endpoints need to be protected and be aware of the software running on them. SANS notes that it's not uncommon for security teams to "find devices and software that are either not visible to or not managed by IT operations". Only authorized devices should be granted access, and only authorized software is installed and can execute.

How Defendpoint can help

Defendpoint can help with devising a list of authorized software and versions for each type of systems (server, desktop, laptop etc.). There is a requirement that this list is monitored through file integrity checking tools, but where this list is stored in a Defendpoint policy, we could digitally sign the configuration to maintain integrity. Application whitelisting, which Defendpoint can deliver, is also mentioned, as well as file integrity (system files are given as examples - which least privilege achieves without monitoring).

Avecto

CIS Control #3: Secure Configurations for Hardware and Software...

Define and apply a secure baseline configuration to all devices, and to ensure they are updated with the necessary security patches. Ensuring the configuration is continually managed will avoid a security “decay” as new vulnerabilities are reported. If not, attackers will find opportunities to exploit both networkaccessible services and client software.

How Defendpoint can help

Defendpoint allows you to maintain your gold standard build by providing the most granular, flexible approach to policy design. This means that configurations scale easily with a firewall style engine for management and clear, logical process flows.

Avecto leverages existing infrastructure and integrates tightly with Microsoft Group Policy or McAfee ePO - or alternatively utilize Avecto’s own iC3 cloud infrastructure based on Azure. In addition, all employees become standard users, ensuring a safe, clean and secure environment.

CIS Control #4: Continuous Vulnerability Assessment and Remediation

In order to minimize the window of opportunity for attackers, organizations must continuously “acquire, assess, and take action” on the latest information to identify vulnerabilities and remediate. Organizations that fail to scan for vulnerabilities and are not proactive in addressing them “face a significant likelihood of having their computer systems compromised”.

How Defendpoint can help

With Defendpoint you can quickly distribute update packages for third-party applications without the need for administrative privileges. Defendpoint complements your patching strategy by ensuring proactive and holistic defense in depth.

CIS Control #5: Controlled Use of Administrative Privileges

Removing administrative rights from end users is a vital step in improving security by ensuring that PCs and servers cannot be compromised as it is a “primary method” for attackers. Preventing unknown processes from running with administrative privileges limits the damage that can be done should a PC be compromised by malware, as well as reducing the risk of data loss and misconfiguration.

Microsoft’s built-in User Account Control (UAC) offers some control over user access but lacks flexibility and adds extra administrative burden.

How Defendpoint can help

Defendpoint provides enterprises with an effective solution to ensure minimum impact for end users, for maximum productivity gain. It allows all Windows users to operate as standard users across desktops and servers, with admin rights applied directly to applications, tasks and scripts. Defendpoint’s privilege management capability allows you to remove admin rights from all users, even sysadmins in the data centre. Its flexible approach allows users to carry out their job function without restriction, while providing an effective security solution with low maintenance overheads and implementation costs.

CIS Control #6: Maintenance, Monitoring and Analysis of Audit Logs

Collect, manage, and analyse audit logs of events that could help detect understand, or recover from an attack. Without audit logs it is possible for attacks to remain unnoticed for months or years, causing irreversible damage.

How Defendpoint can help

This control describes how audit data should include data, timestamp and other characteristics and that it should be in a standardized format - Defendpoint’s event output can do this. It also talks about weekly reports/reviews for anomalies in the data - our enterprise reporting and some of the discovery dashboards (or custom reports) could offer or support this. Use of a SIEM tool is also mentioned. This is something Defendpoint can feed into, and its application characteristics can help to prioritize the events within the system.

About Avecto

Avecto is a leader in Privilege Elevation and Delegation Management. Since 2008, the company has enabled over 8 million users to successfully work without admin rights, enabling many of the world’s biggest brands to achieve the balance between overlocked and underlocked environments.

Avecto’s Defendpoint software has been deployed in the most highly regulated industries, enabling organizations to achieve compliance, gain operational efficiency and stop internal and external attacks.