Who *really* needs admin rights?

CSC 4: Controlled Use of Administrative Privileges

Controlled Use of Administrative Privileges **The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.**	
Maintain Inventory of Administrative Accounts	Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.
Change Default Passwords	Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.
Ensure the Use of Dedicated Administrative Accounts	Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.
Use Unique Passwords	Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.
Use Multi-Factor Authentication for All Administrative Access	Use multi-factor authentication and encrypted channels for all administrative account access.
Use Dedicated Workstations For All	Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.
Limit Access to Script Tools	**Limit access to scripting tools (such as Microsoft® PowerShell and Python) to only administrative or development users with the need to access those capabilities.**
Log and Alert on Unsuccessful Administrative Account Login	Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.

http://www.cisecurity.org/controls/

Limit access to Script Tools

CSC 4: Controlled Use of Administrative Privileges

Binary	Functions	Type
Atbroker.exe	Execute	Binaries
Bash.exe	Execute, AWL bypass	Binaries
Bitsadmin.exe	Alternate data streams, Download, Copy, Execute	Binaries
Certutil.exe	Download, Alternate data streams, Encode, Decode	Binaries
Cmd.exe	Alternate data streams	Binaries
Cmdkey.exe	Credentials	Binaries
Cmstp.exe	Execute, AWL bypass	Binaries
Control.exe	Alternate data streams	Binaries
Csc.exe	Compile	Binaries
Cscript.exe	Alternate data streams	Binaries
Dfsvc.exe	AWL bypass	Binaries
Diskshadow.exe	Dump, Execute	Binaries
Dnscmd.exe	Execute	Binaries

Credit to LOLBAS Living Off The Land Binaries And Scripts - (LOLBins and LOLScripts)