CSC 7

John Ryan Zelling Analyst

Jan 2017

Contents

CSC 7.0

[1] "Critical Security Control #7: Email and Web Browser Protections"

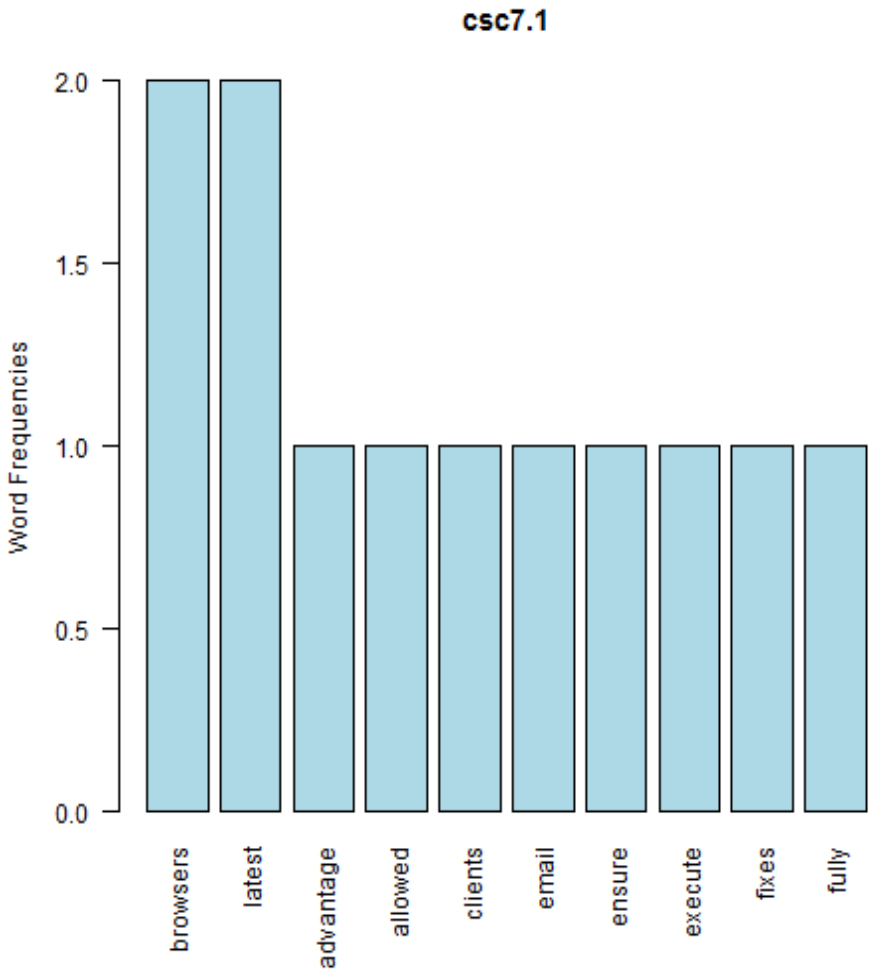
[1]

[1] [1] "To further clarify the Creative Commons license related to the CIS Critical Security Controls content, you are authorized to copy and redistribute the content as a framework for use by you, within your organization and outside of your organization for non-commercial purposes only, provided that (i) appropriate credit is given to CIS, and (ii) a link to the license is provided. Â Additionally, if you remix, transform or build upon the CIS Critical Security Controls, you may not distribute the modified materials. Users of the CIS Critical Security Controls framework are also required to refer to (http://www.cisecurity.org/critical-controls.cfm) when referring to the CIS Critical Security ControlsÂ in order to ensure that users are employing the most up to date guidance. Â Commercial use of the CIS Critical Security Controls is subject to the prior approval of The Center for Internet Security."

CSC 7.1

[1] “browsers + latest”

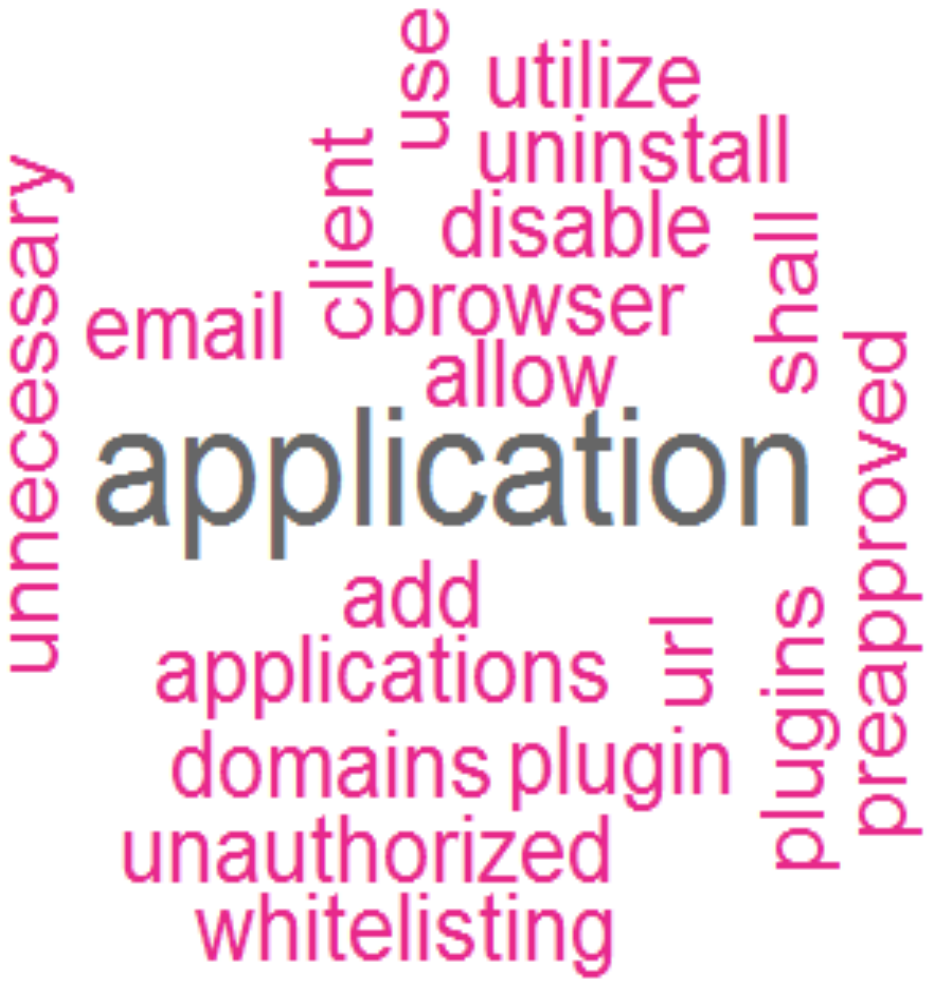
null device 1



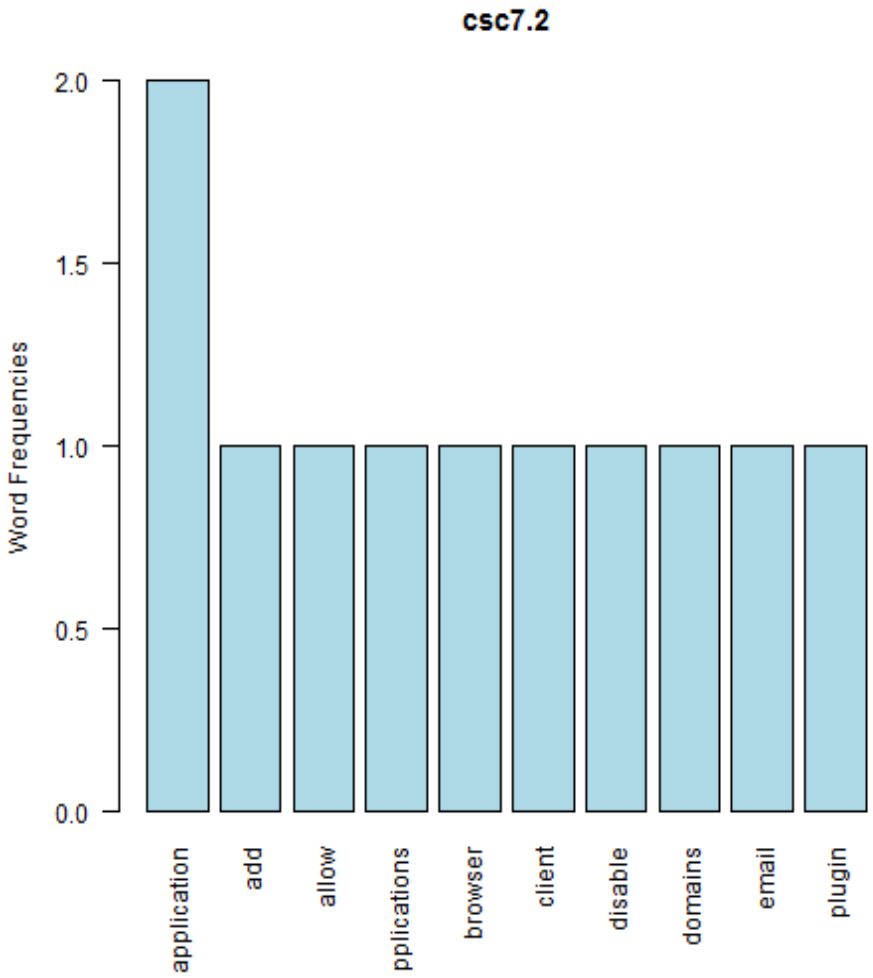
null device 1 [1] “Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers provided by the vendor in order to take advantage of the latest security functions and fixes.”

CSC 7.2

[1] “application + add”



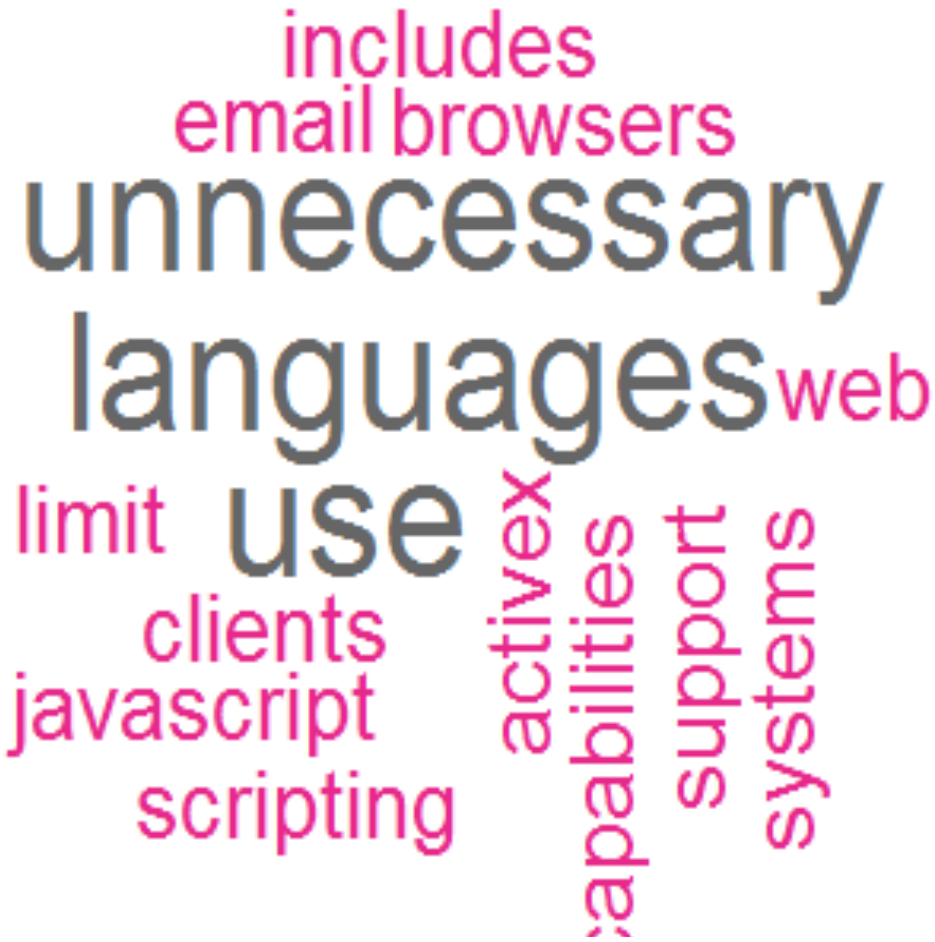
null device 1



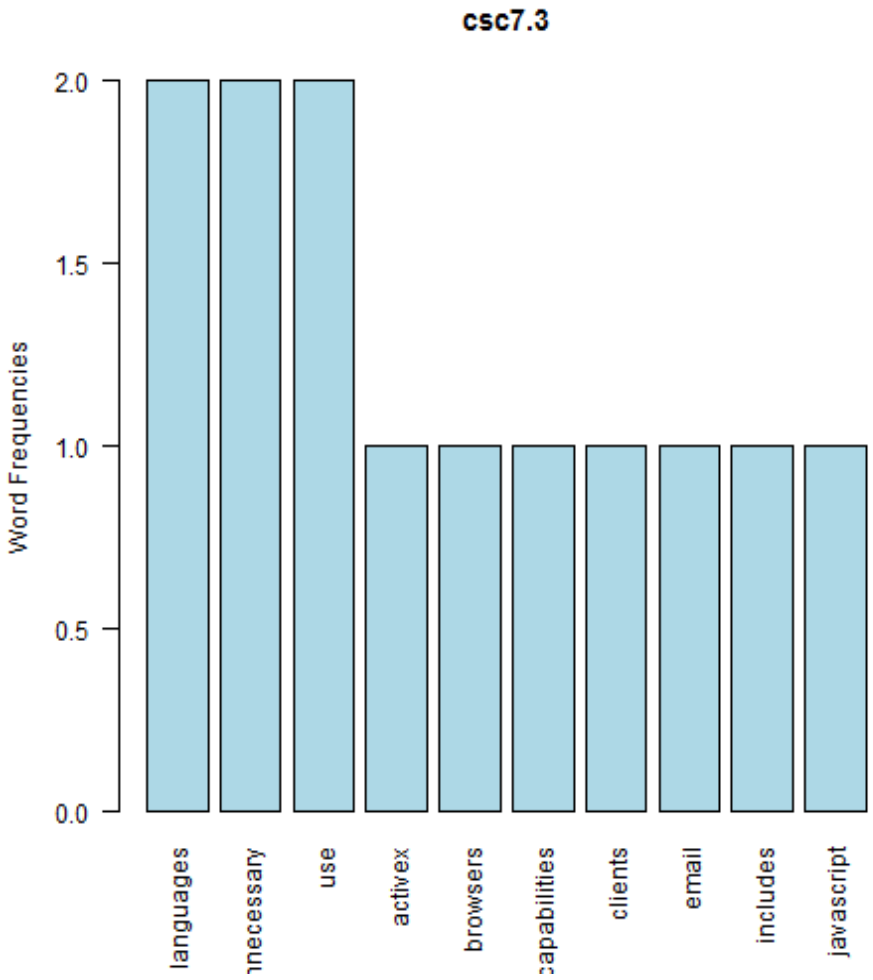
null device 1 [1] “Uninstall or disable any unnecessary or unauthorized browser or email client plugins or add-on applications. Each plugin shall utilize application / URL whitelisting and only allow the use of the application for pre-approved domains.”

CSC 7.3

[1] “languages + unnecessary”



null device 1

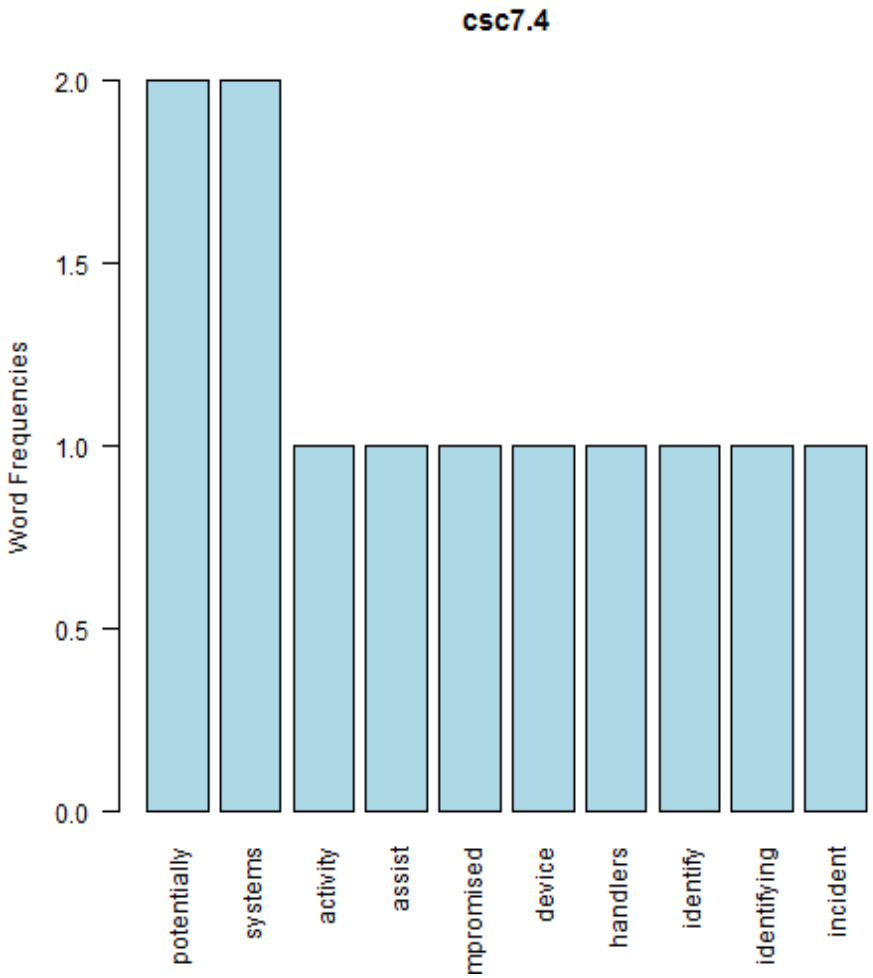


null device 1 [1] “Limit the use of unnecessary scripting languages in all web browsers and email clients. This includes the use of languages such as ActiveX and JavaScript on systems where it is unnecessary to support such capabilities.”

CSC 7.4

[1] “potentially + systems”

null device 1

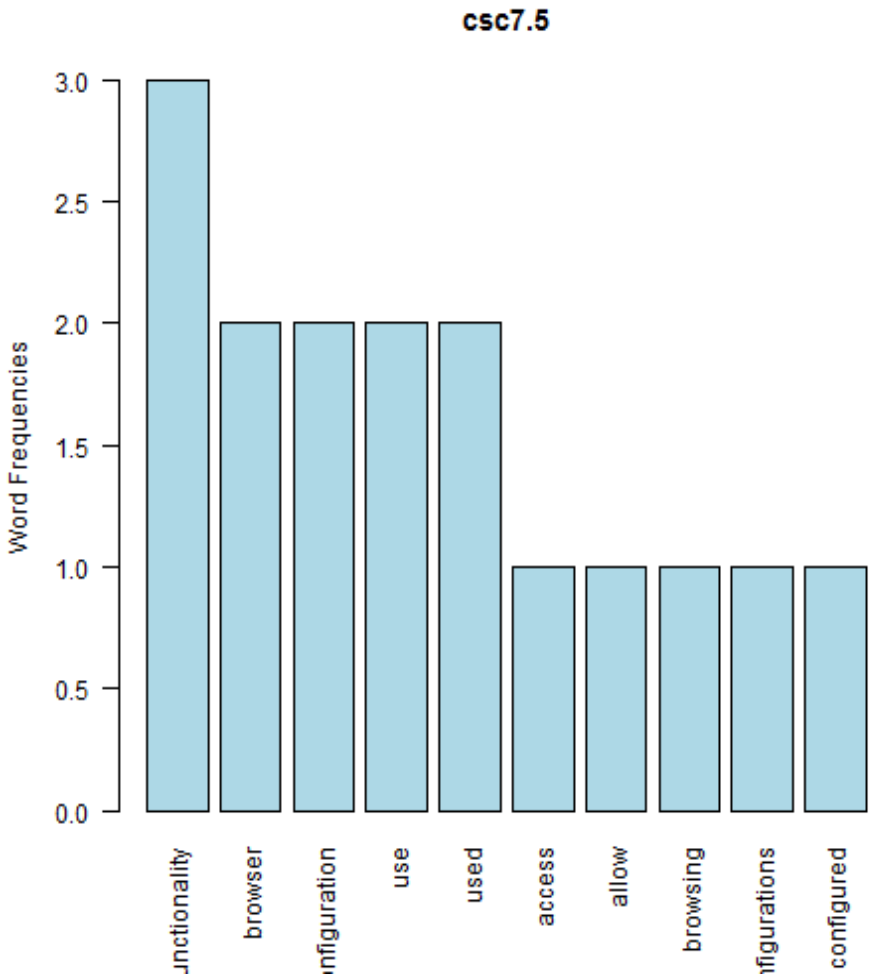


null device 1 [1] “Log all URL requests from each of the organization’s systems, whether onsite or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.”

CSC 7.5

[1] “functionality + browser”

null device 1

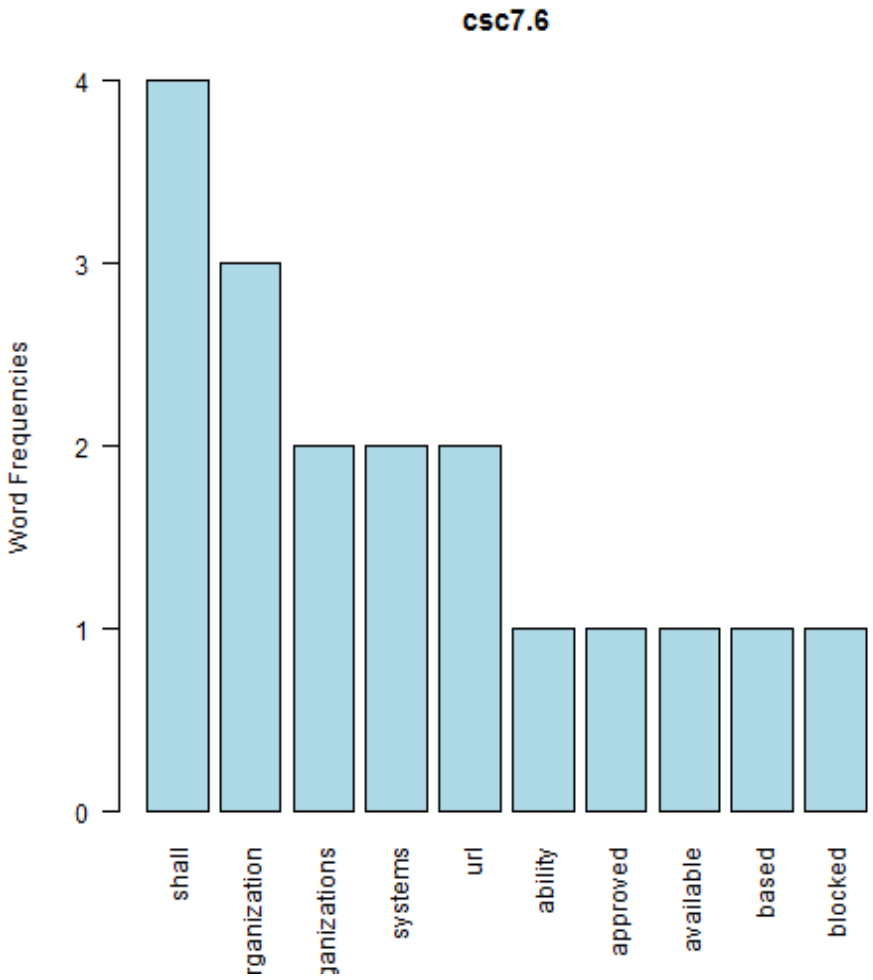


null device 1 [1] “Deploy two separate browser configurations to each system. One configuration should disable the use of all plugins, unnecessary scripting languages, and generally be configured with limited functionality and be used for general web browsing. The other configuration shall allow for more browser functionality but should only be used to access specific websites that require the use of such functionality.”

CSC 7.6

[1] “shall + organization”

null device 1

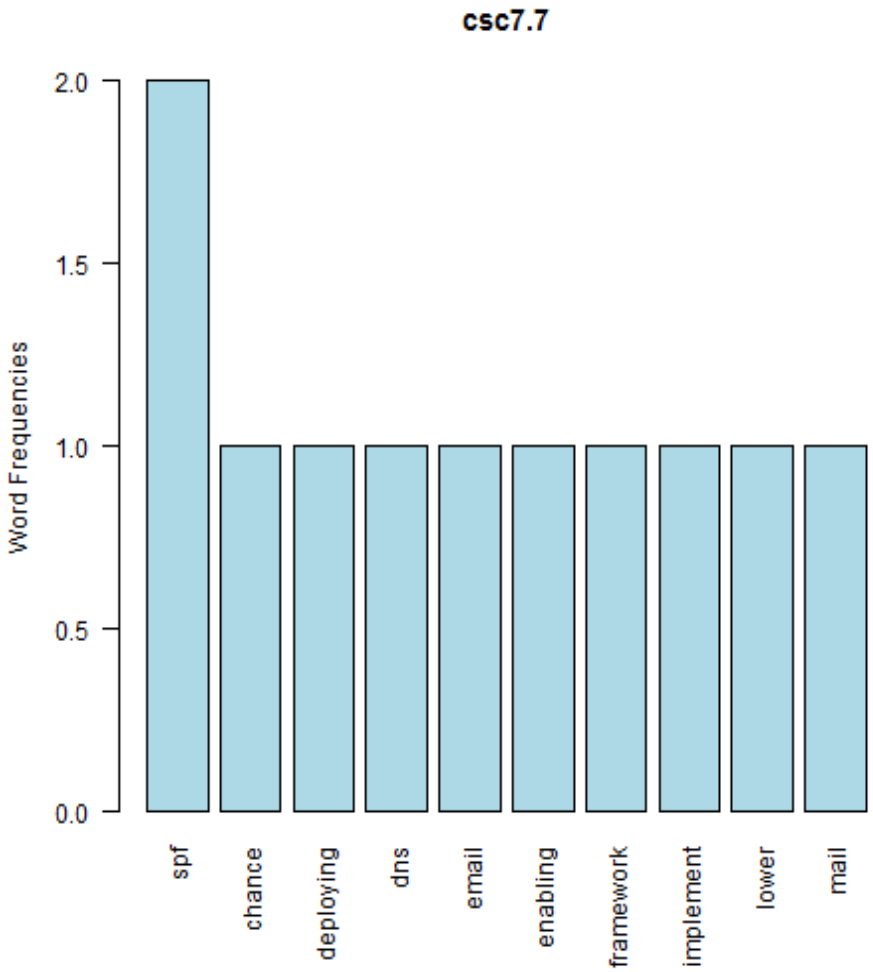


null device 1 [1] "The organization shall maintain and enforce network based URL filters that limit a system's ability to connect to websites not approved by the organization. The organization shall subscribe to URL categorization services to ensure that they are up-to-date with the most recent website category definitions available. Uncategorized sites shall be blocked by default. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not."

CSC 7.7

[1] “spf + chance”

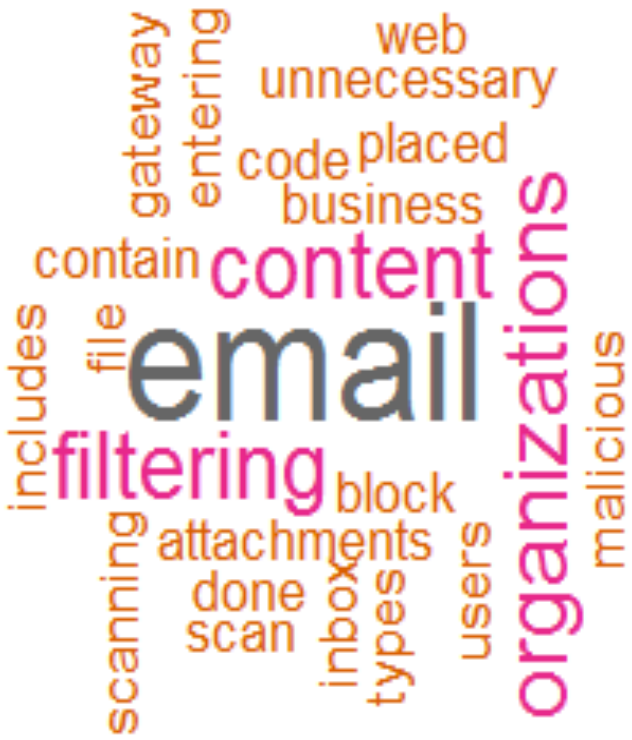
null device 1



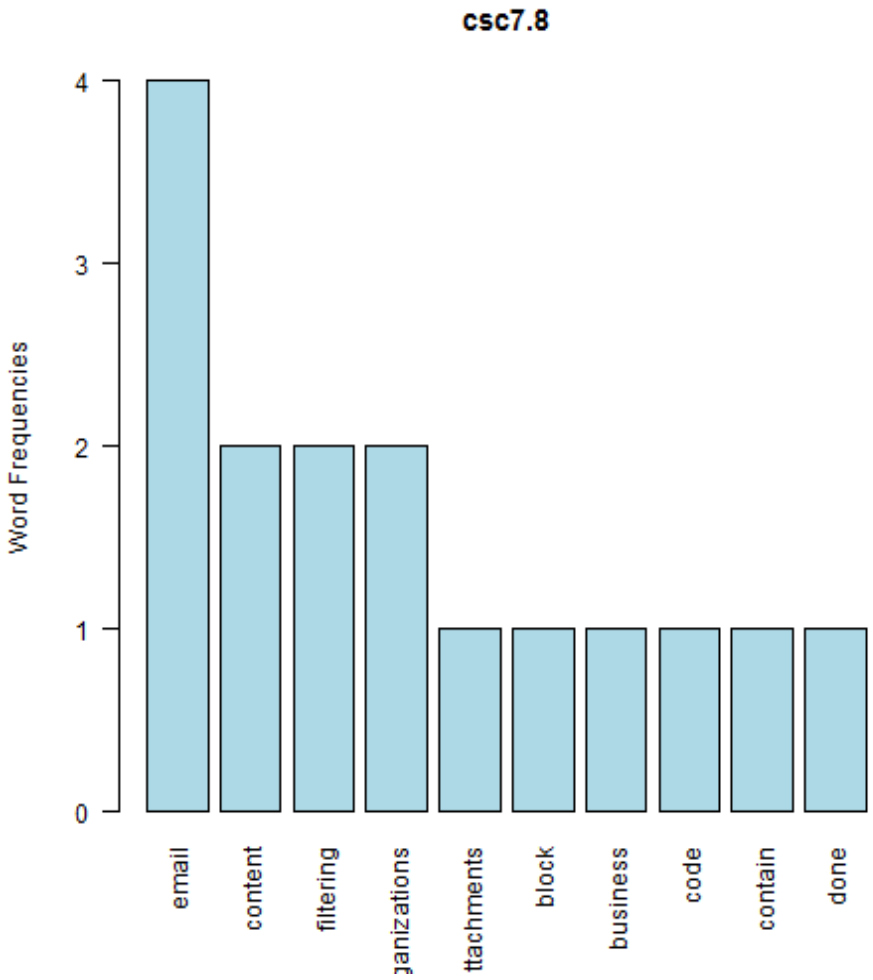
null device 1 [1] “To lower the chance of spoofed e-mail messages, implement the Sender Policy Framework (SPF) by deploying SPF records in DNS and enabling receiver-side verification in mail servers.”

CSC 7.8

[1] “email + content”



null device 1



null device 1 [1] “Scan and block all e-mail attachments entering the organization’s e-mail gateway if they contain malicious code or file types that are unnecessary for the organization’s business. This scanning should be done before the e-mail is placed in the user’s inbox. This includes e-mail content filtering and web content filtering.”