CSC 13

John Ryan Zelling Analyst

Jan 2017

Contents

CSC 13.0

[1] "Critical Security Control #13: Data Protection"

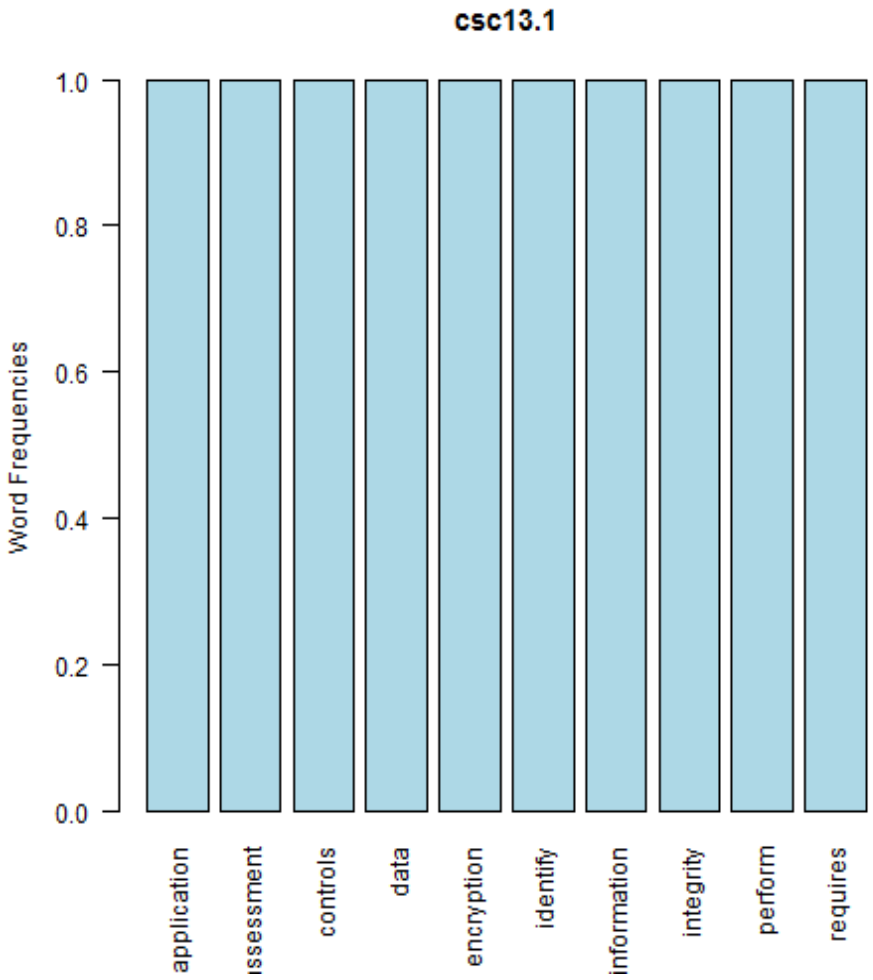
[1]

[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 13.1

[1] “application + assessment”

null device 1

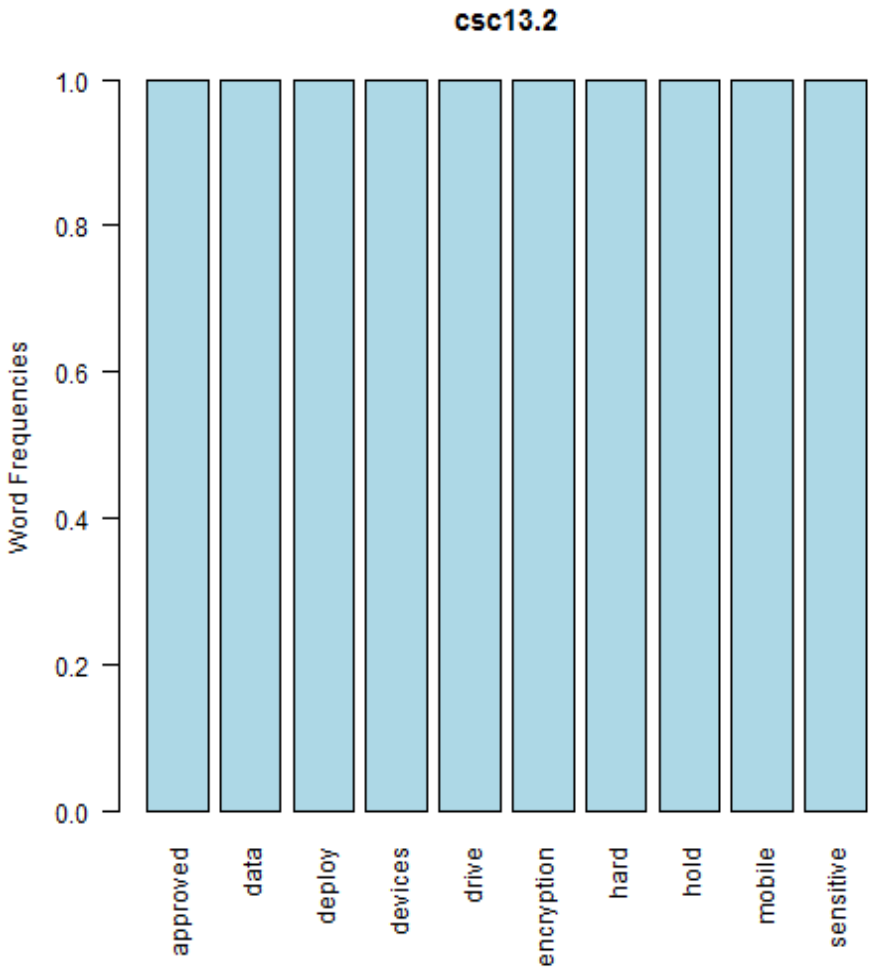


null device 1 [1] “Perform an assessment of data to identify sensitive information that requires the application of encryption and integrity controls”

CSC 13.2

[1] “approved + data”

null device 1

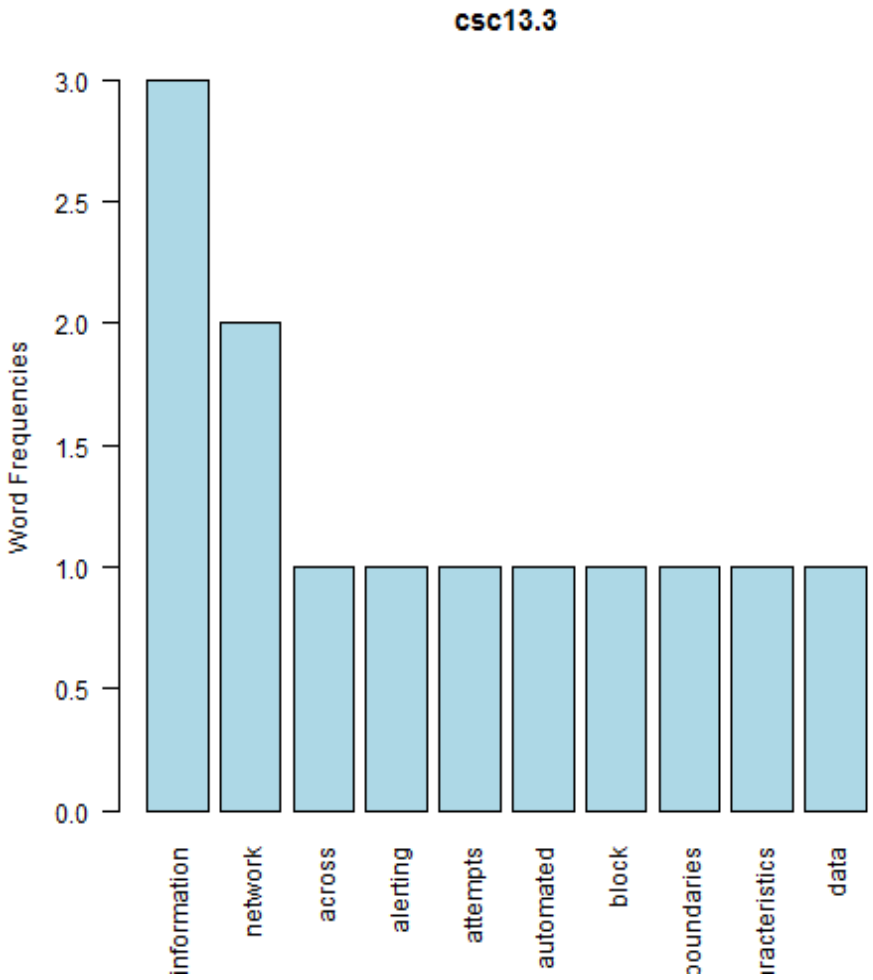


null device 1 [1] “Deploy approved hard drive encryption software to mobile devices and systems that hold sensitive data.”

CSC 13.3

[1] “information + network”

null device 1

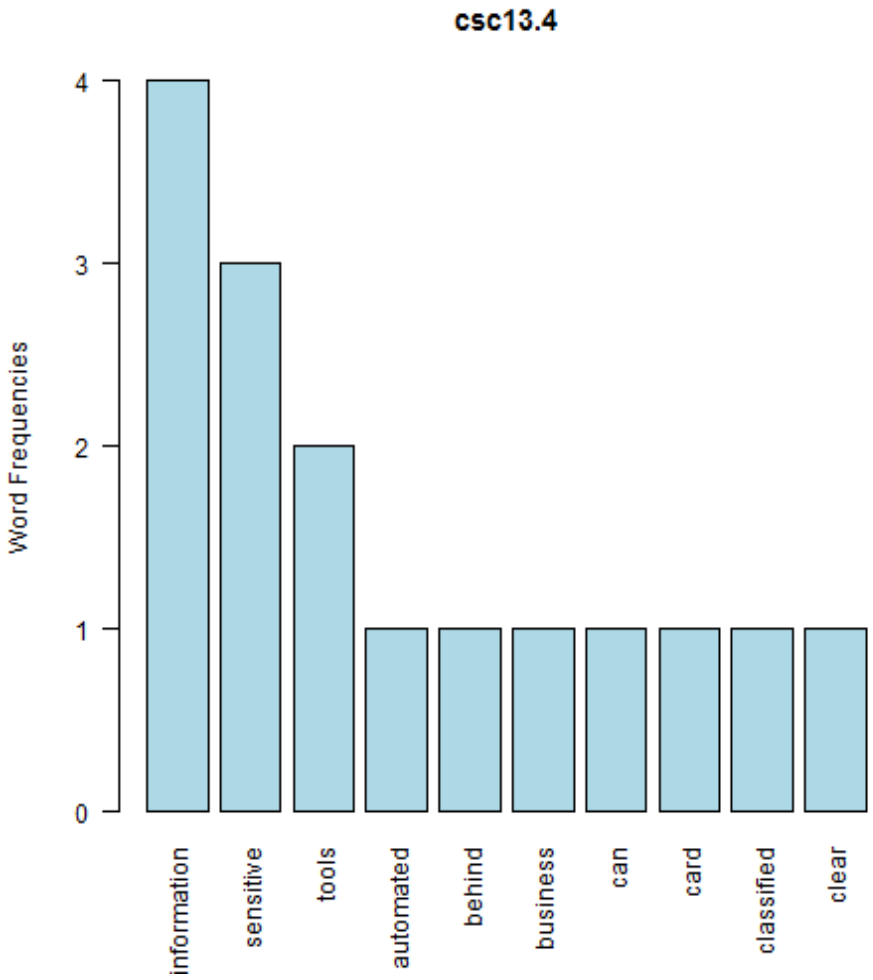


null device 1 [1] “Deploy an automated tool on network perimeters that monitors for sensitive information (e.g., personally identifiable information), keywords, and other document characteristics to discover unauthorized attempts to exfiltrate data across network boundaries and block such transfers while alerting information security personnel.”

CSC 13.4

[1] “information + sensitive”

null device 1

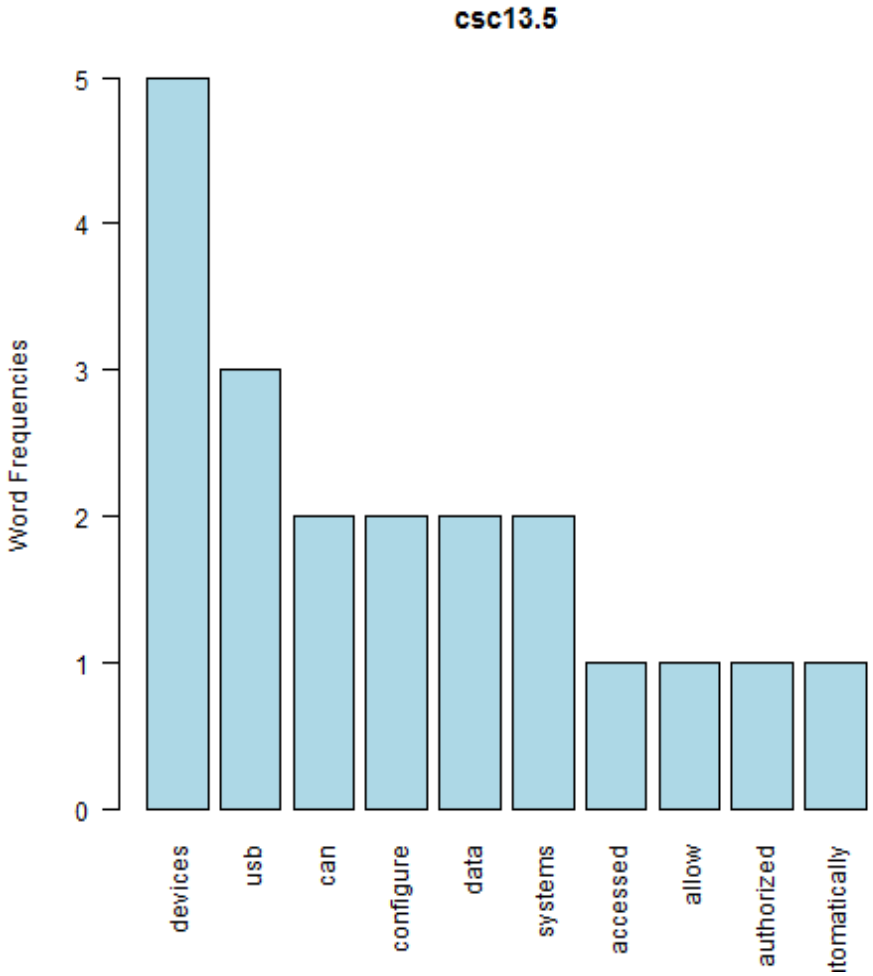


null device 1 [1] “Conduct periodic scans of server machines using automated tools to determine whether sensitive data (e.g., personally identifiable information, health, credit card, or classified information) is present on the system in clear text. These tools, which search for patterns that indicate the presence of sensitive information, can help identify if a business or technical process is leaving behind or otherwise leaking sensitive information.”

CSC 13.5

[1] “devices + usb”

null device 1

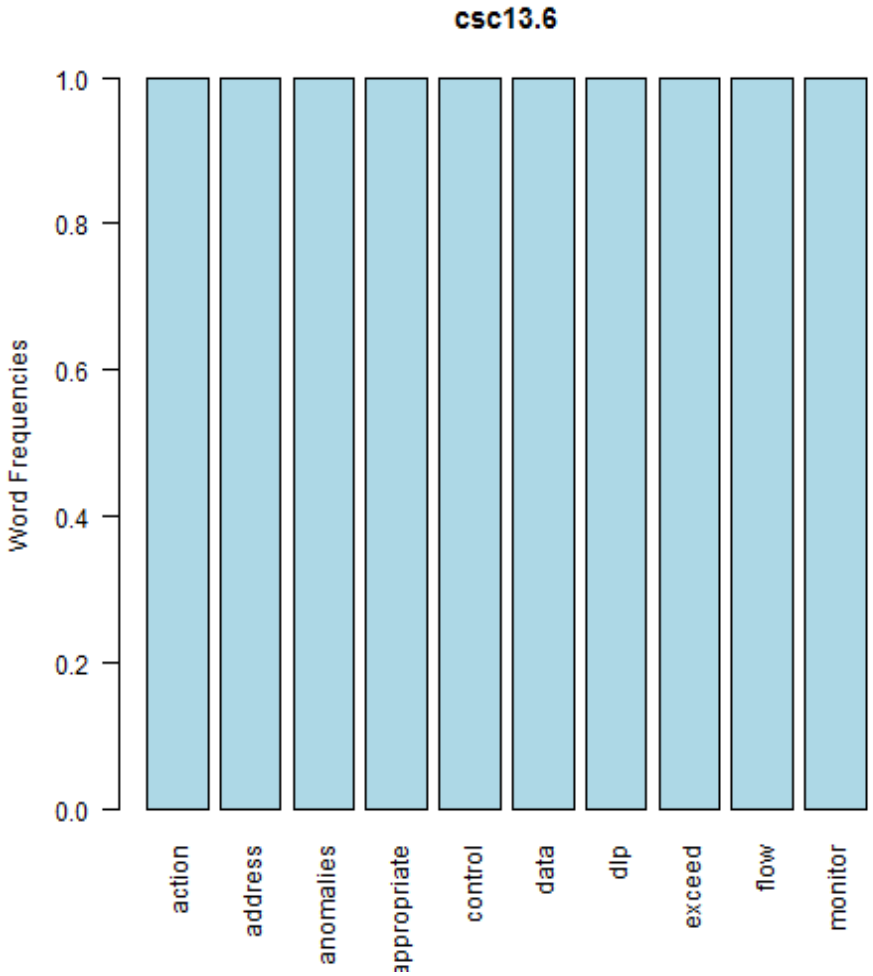


null device 1 [1] “If there is no business need for supporting such devices, configure systems so that they will not write data to USB tokens or USB hard drives. If such devices are required, enterprise software should be used that can configure systems to allow only specific USB devices (based on serial number or other unique property) to be accessed, and that can automatically encrypt all data placed on such devices. An inventory of all authorized devices must be maintained.”

CSC 13.6

[1] “action + address”

null device 1

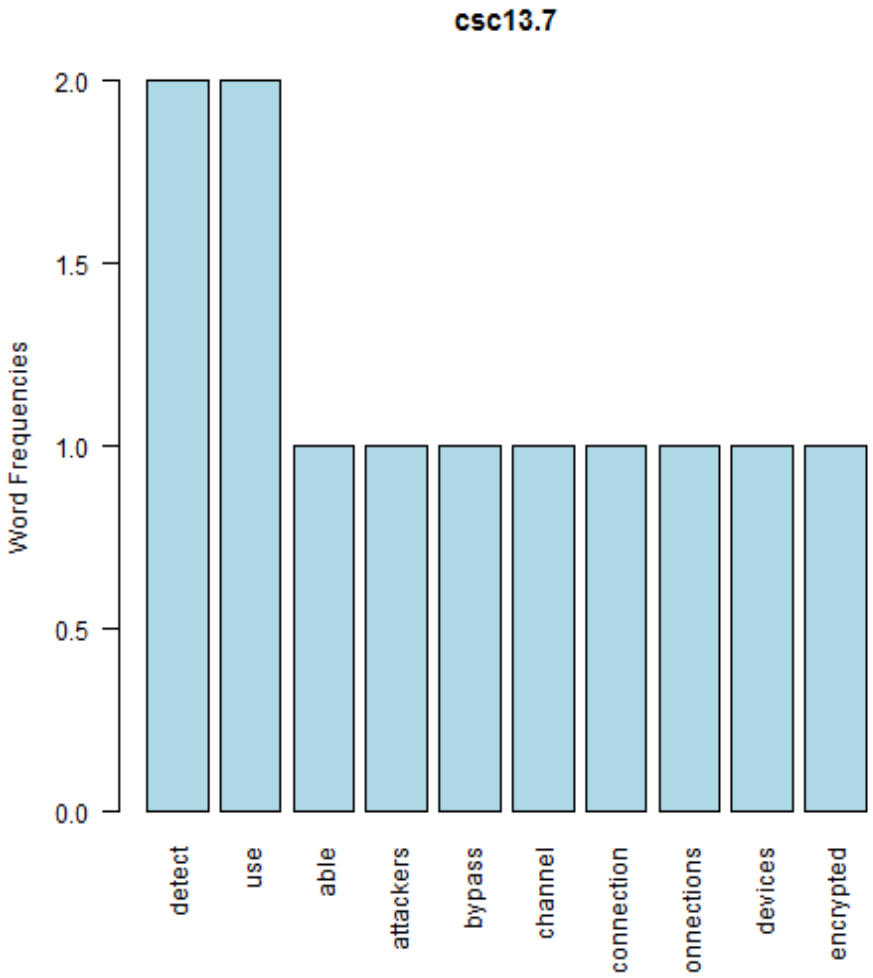


null device 1 [1] "Use network-based DLP solutions to monitor and control the flow of data within the network. Any anomalies that exceed the normal traffic patterns should be noted and appropriate action taken to address them."

CSC 13.7

[1] “detect + use”

null device 1

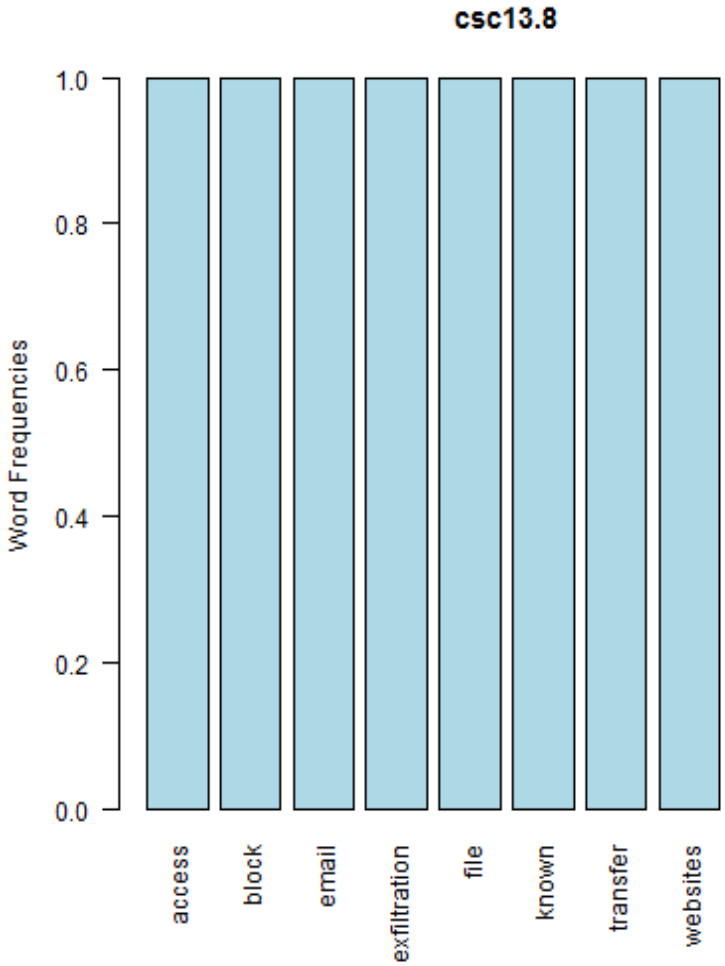


null device 1 [1] “Monitor all traffic leaving the organization and detect any unauthorized use of encryption. Attackers often use an encrypted channel to bypass network security devices. Therefore it is essential that organizations be able to detect rogue connections, terminate the connection, and remediate the infected system.”

CSC 13.8

[1] “access + block”

null device 1



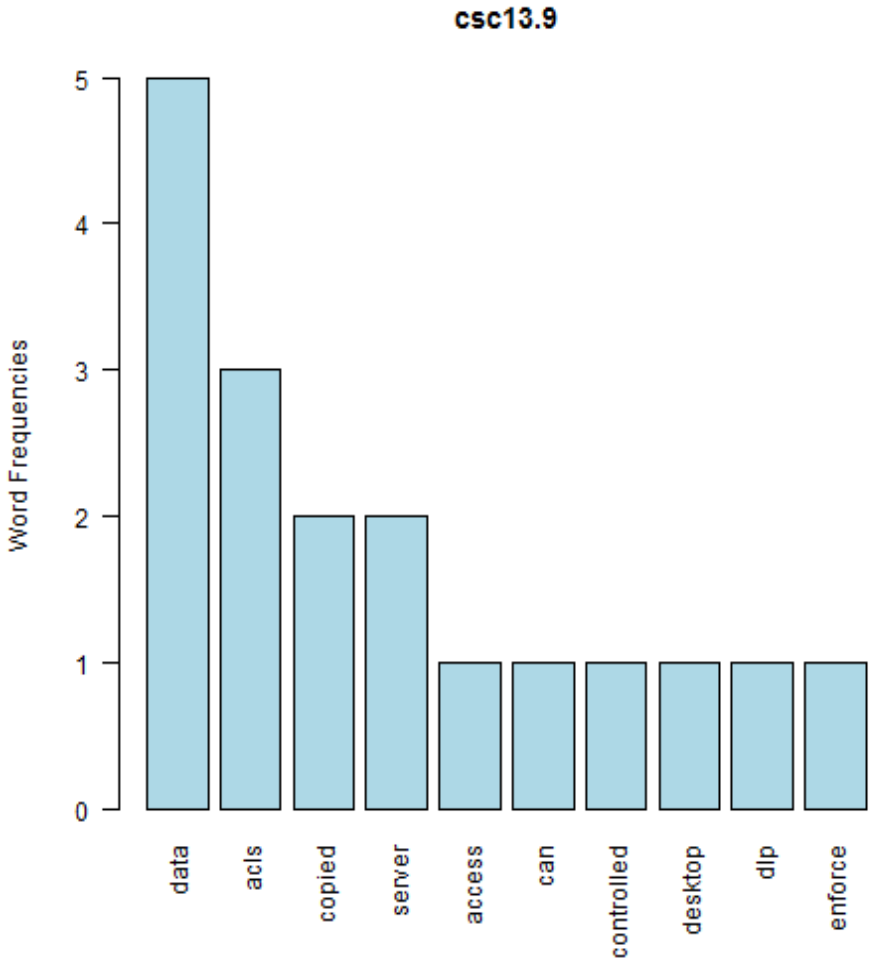
null device 1 [1] “Block access to known file transfer and e-mail exfiltration websites.”
2

[2]http://www.sei.cmu.edu/reports/13tn012.pdf

CSC 13.9

[1] “data + acls”

null device 1



null device 1 [1] “Use host-based data loss prevention (DLP) to enforce ACLs even when data is copied off a server. In most organizations, access to the data is controlled by ACLs that are implemented on the server. Once the data have been copied to a desktop system, the ACLs are no longer enforced and the users can send the data to whomever they want.”