CSC 1

John Ryan Zelling Analyst

Jan 2017

Contents

CSC 1.0

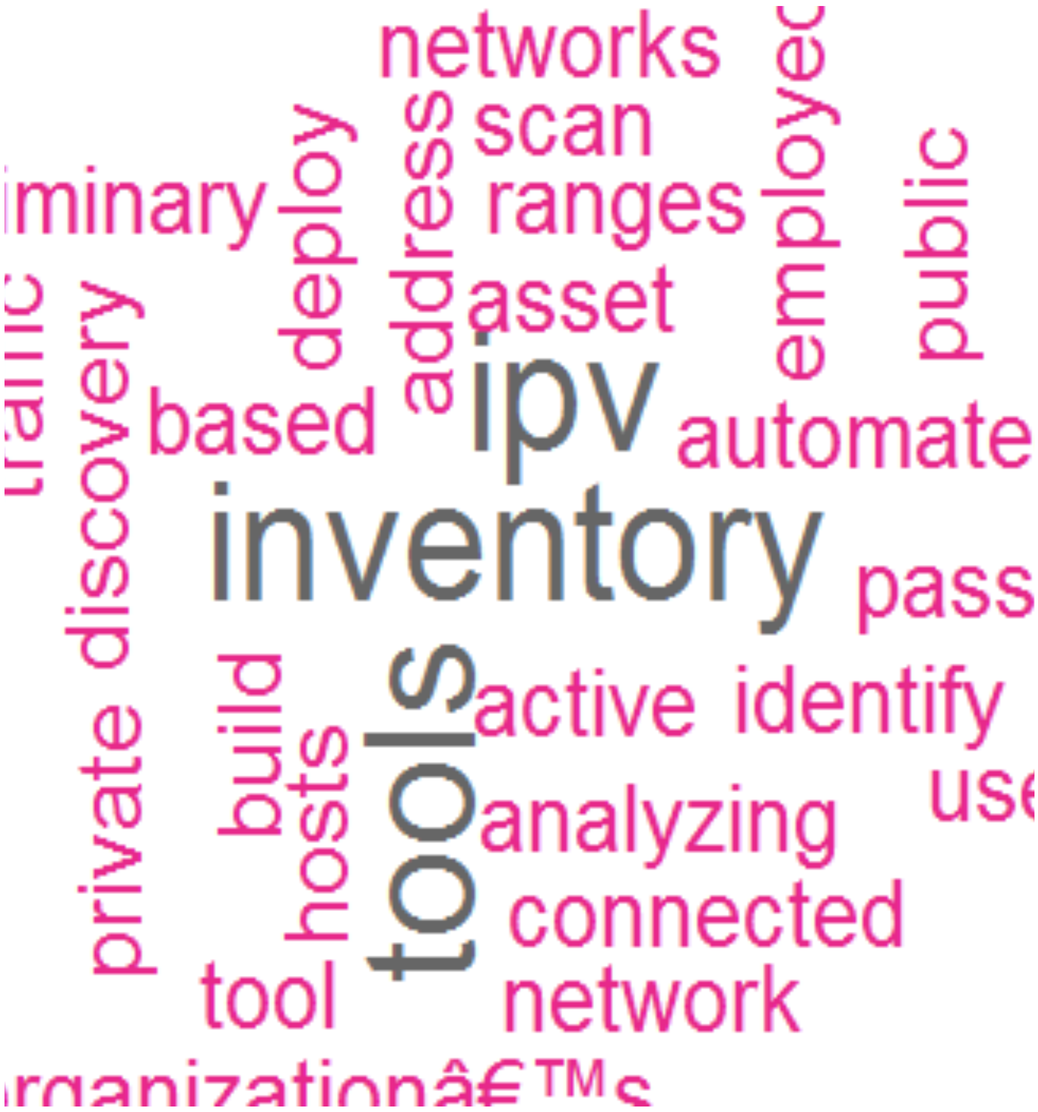
[1] “Critical Security Control #1: Inventory of Authorized and Unauthorized Devices”

[1]

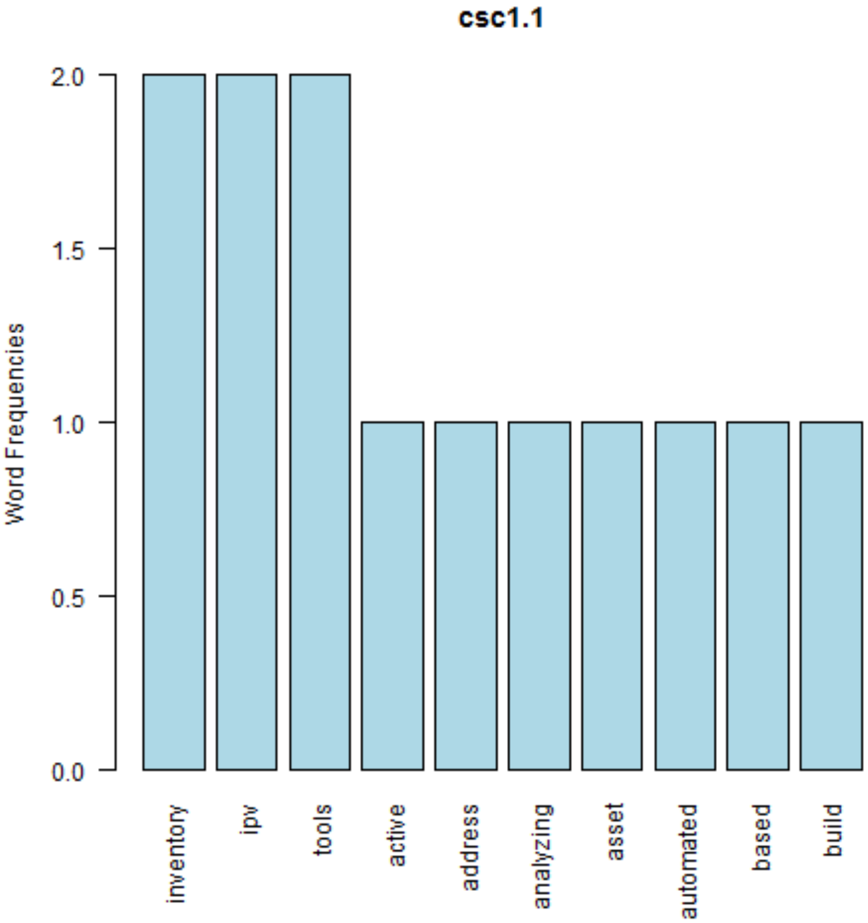
[1] [1] “To further clarify the Creative Commons license related to the CIS Critical Security Controls content, you are authorized to copy and redistribute the content as a framework for use by you, within your organization and outside of your organization for non-commercial purposes only, provided that (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 1.1

[1] “inventory + ipv”



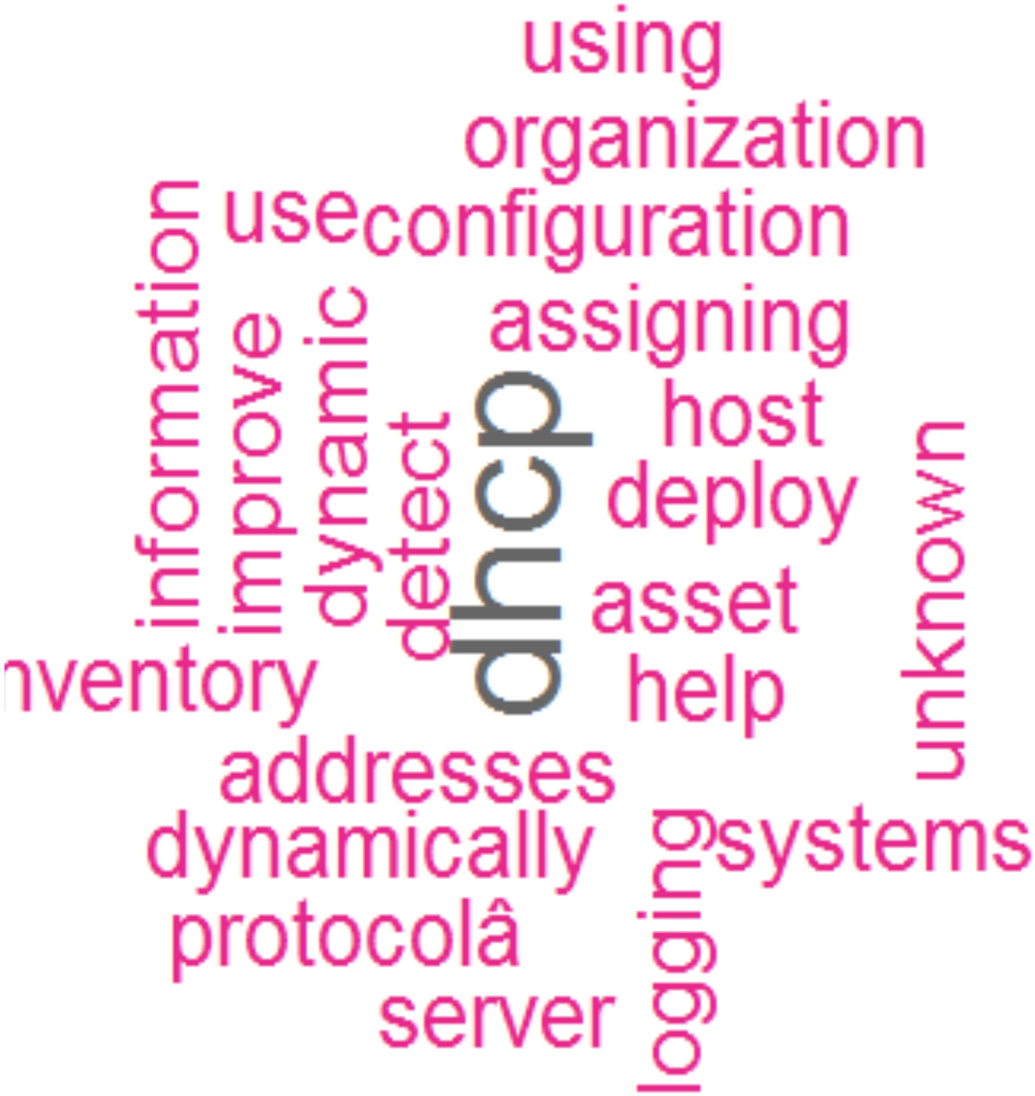
null device 1



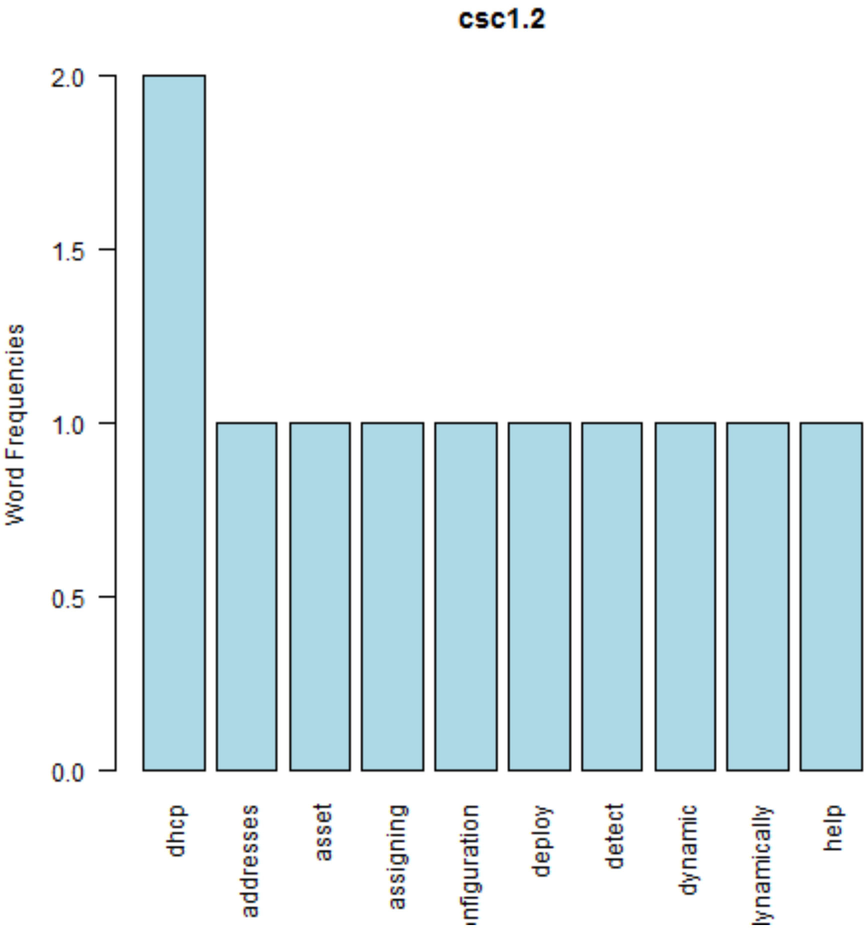
null device 1 [1] "Deploy an automated asset inventory discovery tool and use it to build a preliminary inventory of systems connected to an organizationâ s public and private network(s). Both active tools that scan through IPv4 or IPv6 network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed."

CSC 1.2

[1] “dhcp + addresses”



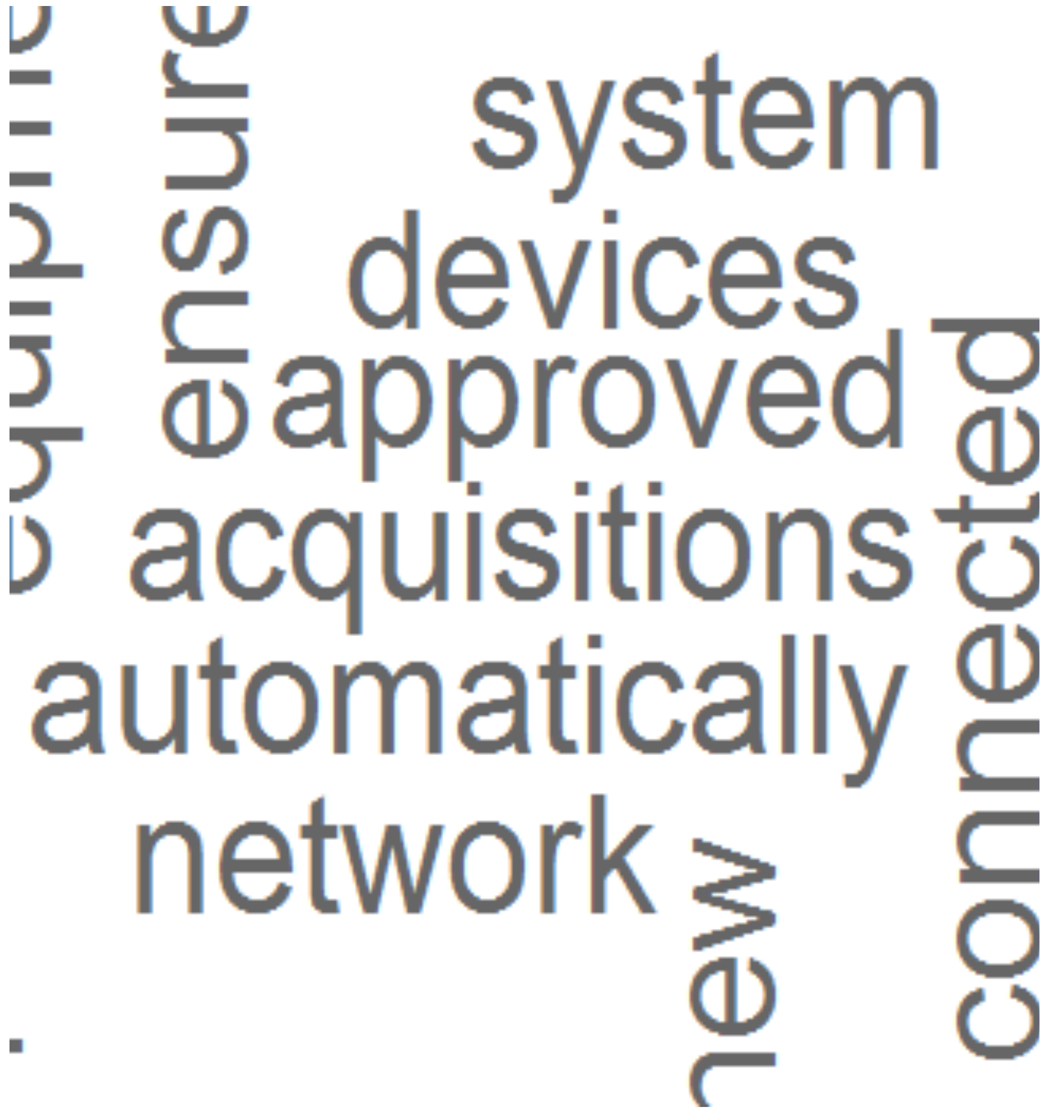
null device 1



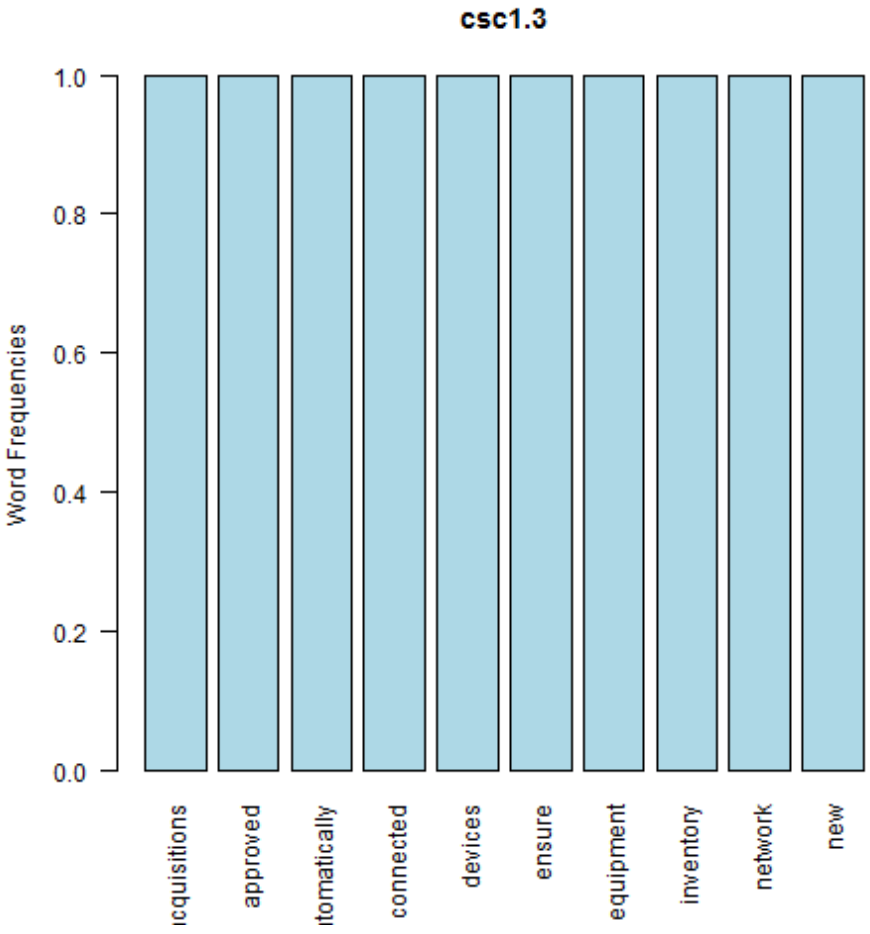
null device 1 [1] “If the organization is dynamically assigning addresses using DHCP, then deploy dynamic host configuration protocolÂ (DHCP) server logging, and use this information to improve the asset inventory and help detect unknown systems.”

CSC 1.3

[1] "acquisitions + approved"



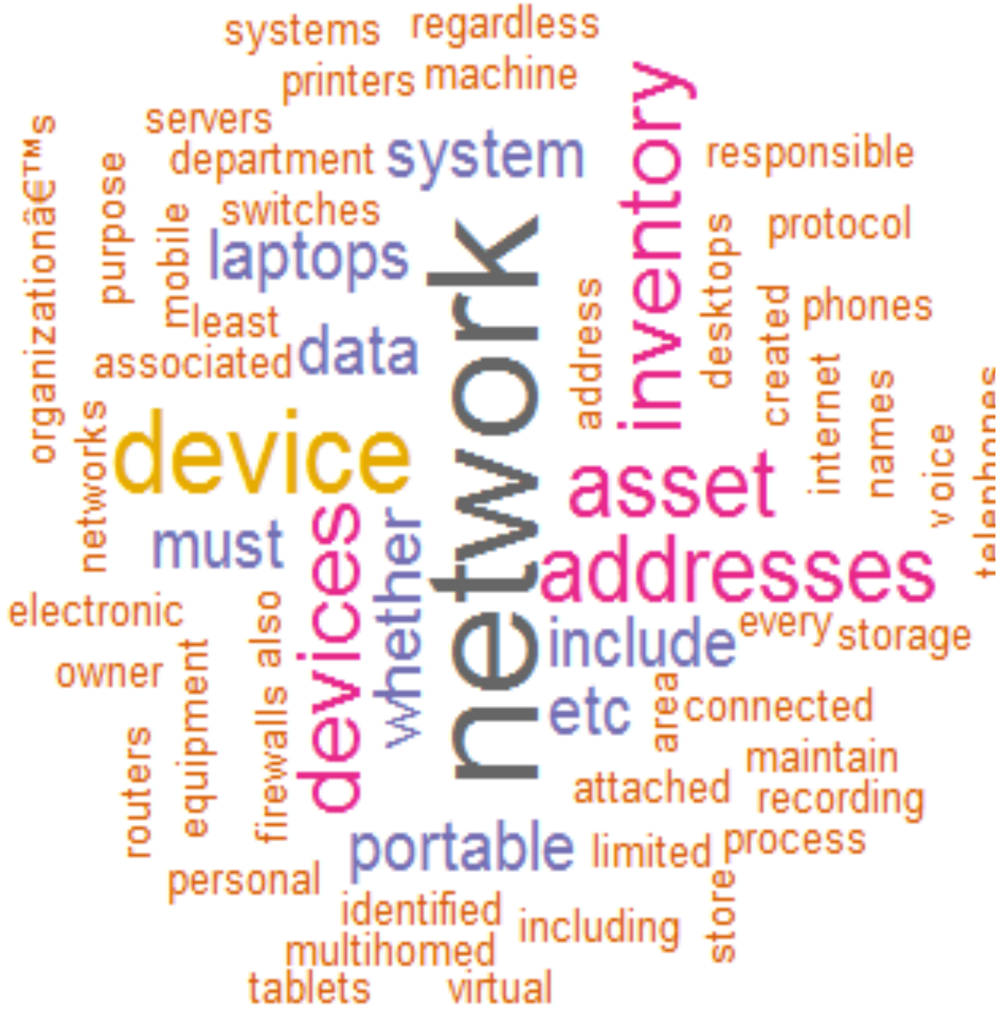
null device 1



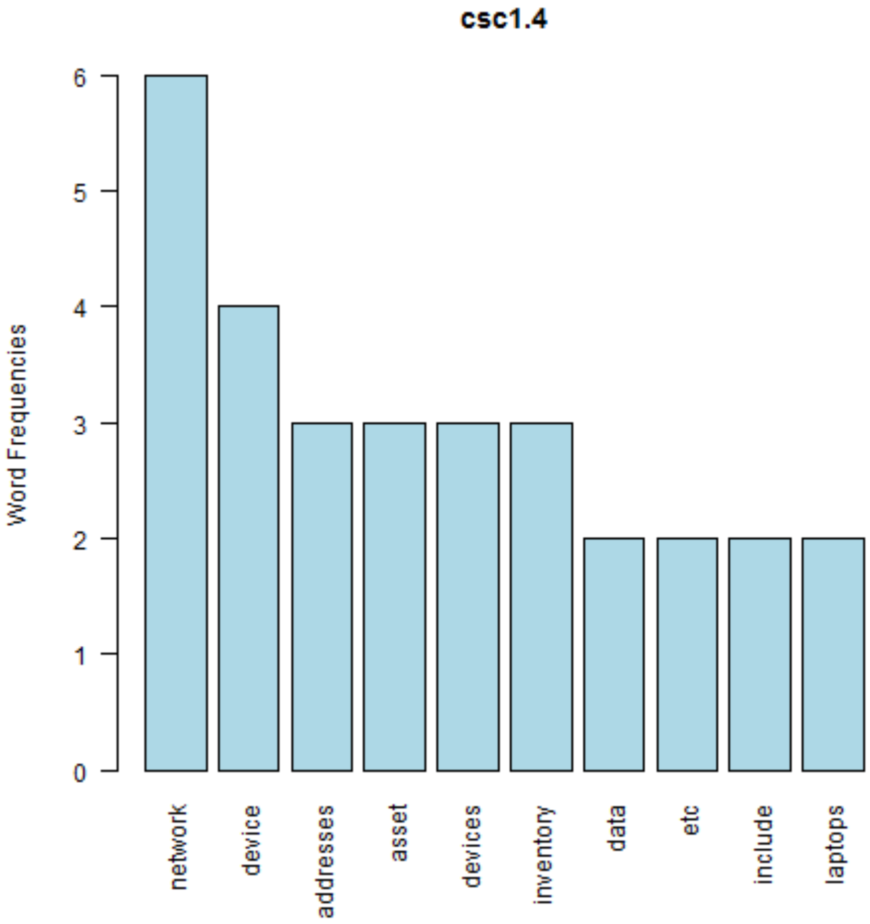
null device 1 [1] “Ensure that all equipment acquisitions automatically update the inventory system as new, approved devices are connected to the network.”

CSC 1.4

[1] “network + device”



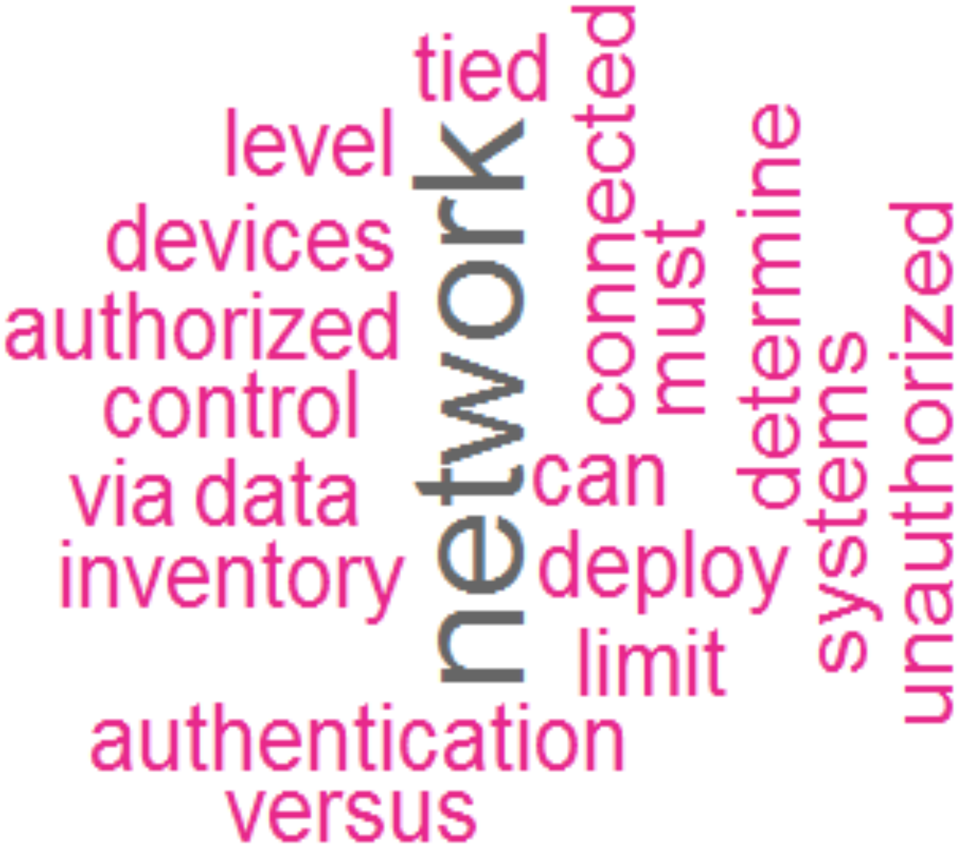
null device 1



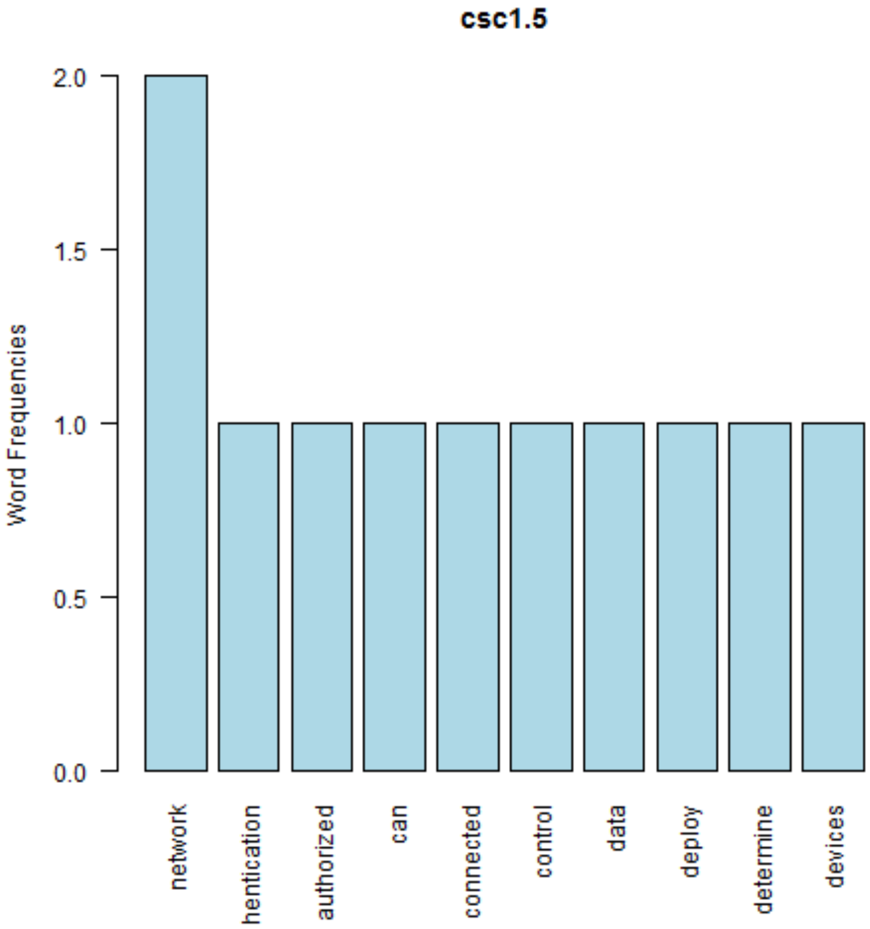
null device 1 [1] “Maintain an asset inventory of all systems connected to the network and the network devices themselves, recording at least the network addresses, machine name(s), purpose of each system, an asset owner responsible for each device, and the department associated with each device. The inventory should include every system that has an Internet protocol (IP) address on the network, including but not limited to desktops, laptops, servers, network equipment (routers, switches, firewalls, etc.), printers, storage area networks, Voice Over-IP telephones, multi-homed addresses, virtual addresses, etc. The asset inventory created must also include data on whether the device is a portable and/or personal device. Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store or process data must be identified, regardless of whether they are attached to the organizationâ s network.”

CSC 1.5

```
[1] “network + authentication”
```



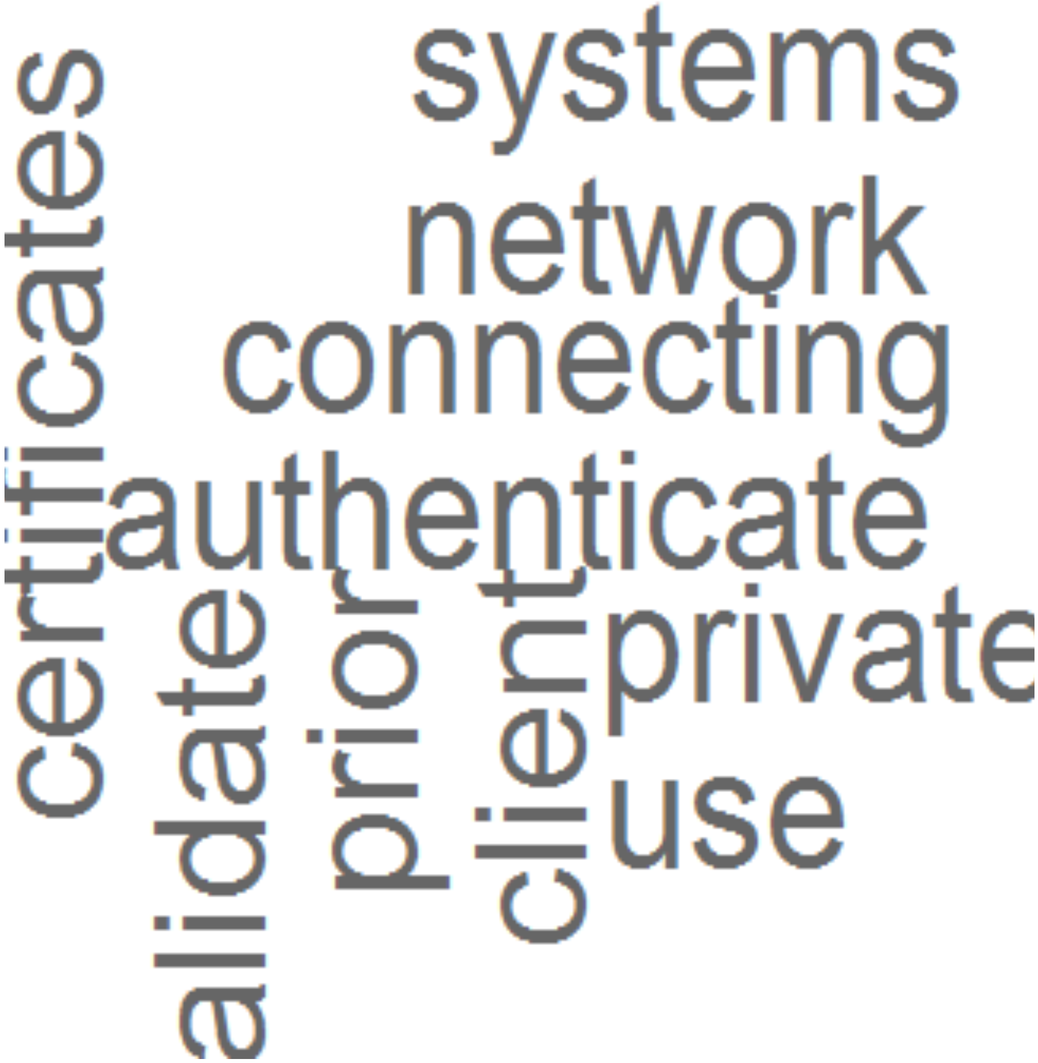
```
null device 1
```



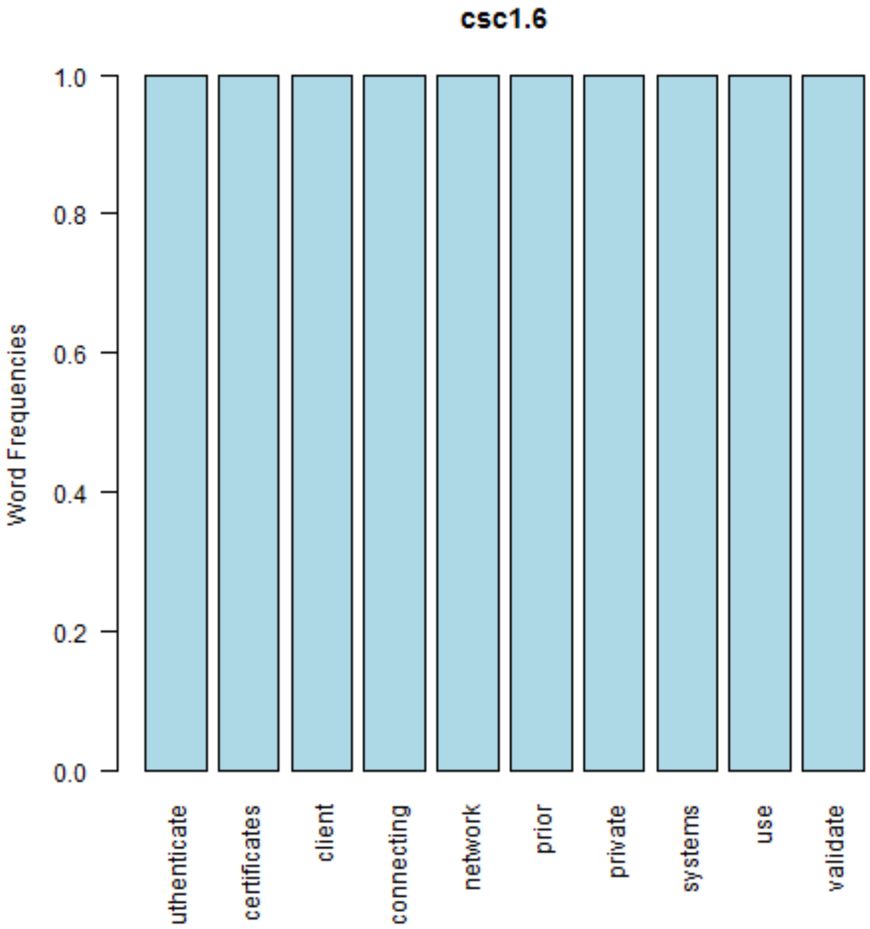
null device 1 [1] “Deploy network level authentication via 802.1x to limit and control which devices can be connected to the network. The 802.1x must be tied into the inventory data to determine authorized versus unauthorized systems.”

CSC 1.6

[1] “authenticate + certificates”



null device 1



null device 1 [1] “Use client certificates to validate and authenticate systems prior to connecting to the private network.”