CSC All

John Ryan Zelling Analyst

Jan 2017

Contents

CSC Combined

This document is generated using a program written for visualizing large files.

The Center for Internet Security Critical Security Controls Version 6.0 System Family

The Center for Internet Security (CIS) presents the CIS Controls for Effective Cyber Defense Version 6.0, a recommended set of actions that provide specific and actionable ways to stop today's most pervasive and dangerous cyber attacks.

The CIS Controls are a set of internationally recognized measures developed, refined, and validated by leading IT security experts from around the world. The CIS Controls represent the most important cyber hygiene actions every organization should implement to protect their IT networks. In fact, a study by the Australian government indicates that 85% of known vulnerabilities can be stopped by deploying the Top 5 CIS Controls. This includes:

- taking an inventory of IT assets,
- implementing secure configurations,
- patching vulnerabilities, and
- restricting unauthorized users.

The CIS Controls are especially relevant because they are updated by cyber experts based on actual attack data pulled from a variety of public and private threat sources. Version 6 incorporates recommended changes

from the cybersecurity community to reflect the latest technologies and threats. The new Controls include a new Control for "Email and Web Browser Protections," a deleted Control on "Secure Network Engineering," and a re-ordering to make "Controlled Use of Administration Privileges" higher in priority. This version also includes a new metrics companion guide.

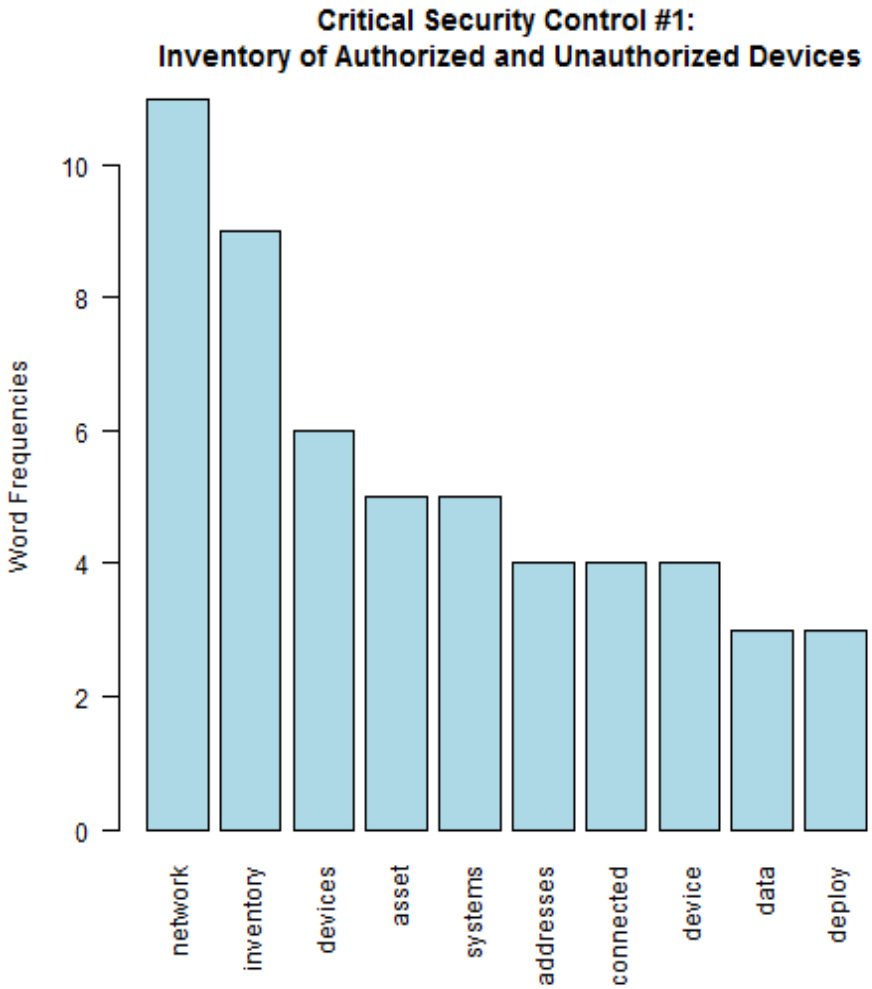
[1]

[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.x

[1] “network + inventory”

null device 1

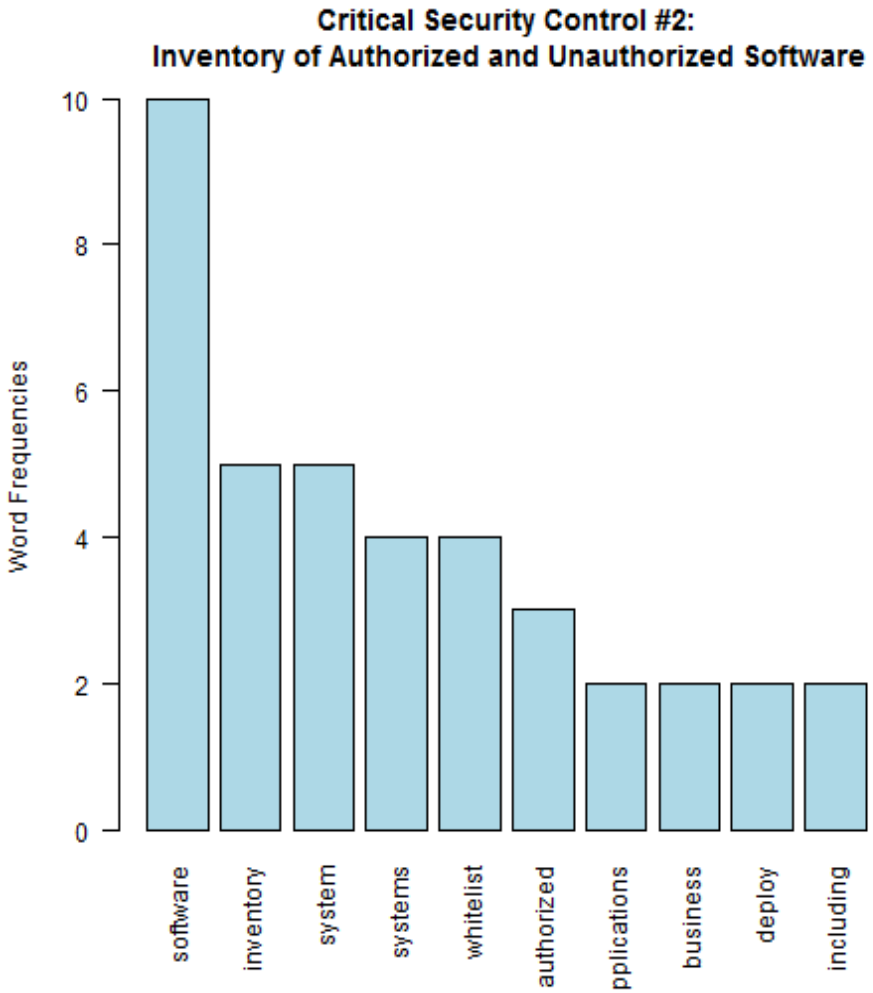


null device 1

CSC 2.x

[1] “software + inventory”

null device 1

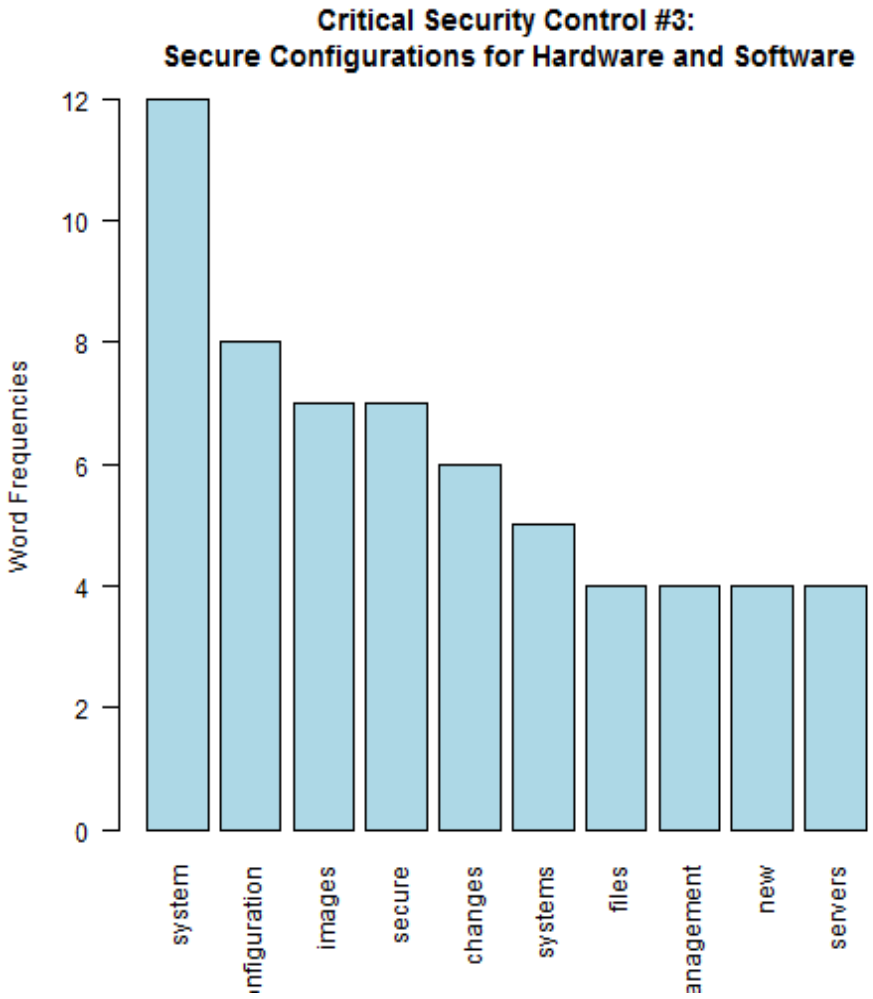


null device 1

CSC 3.x

[1] “system + configuration”

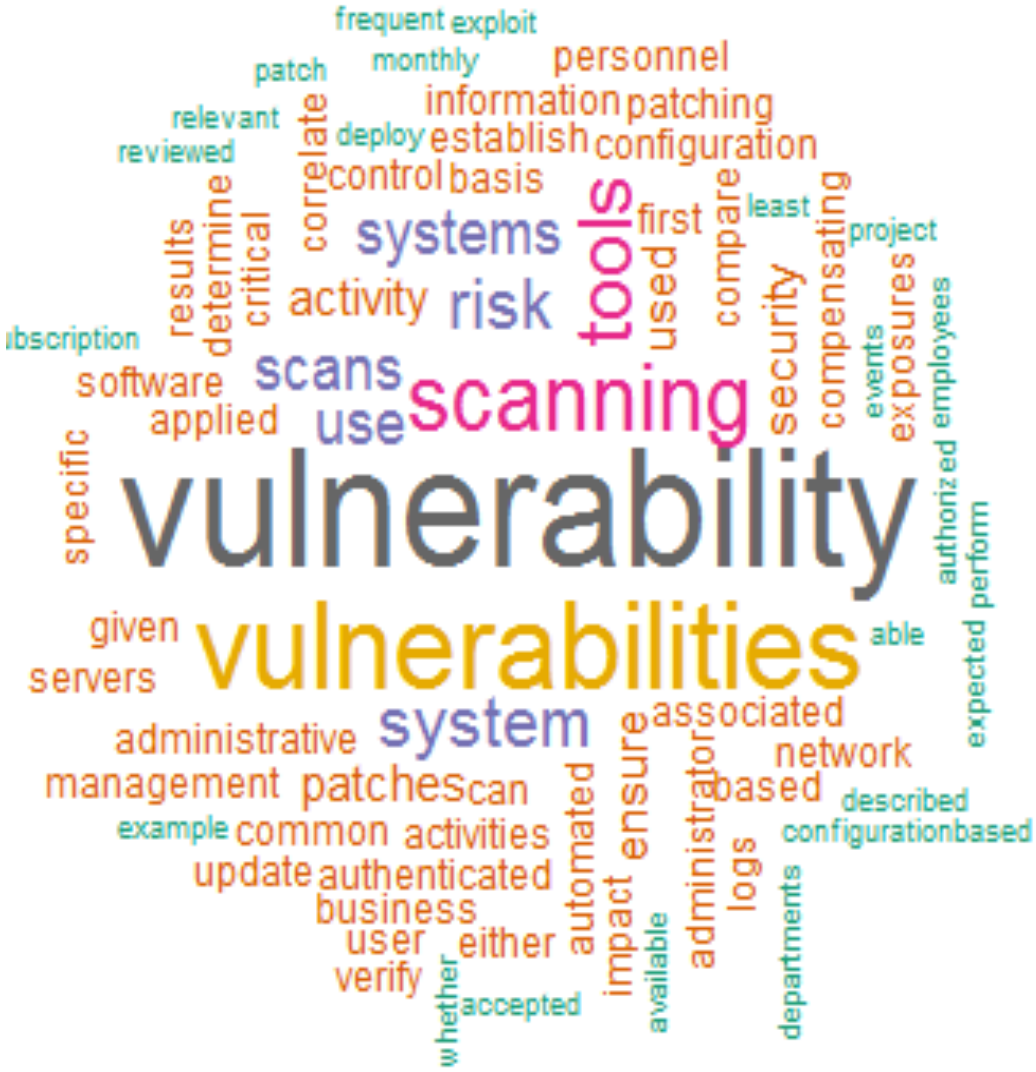
null device 1



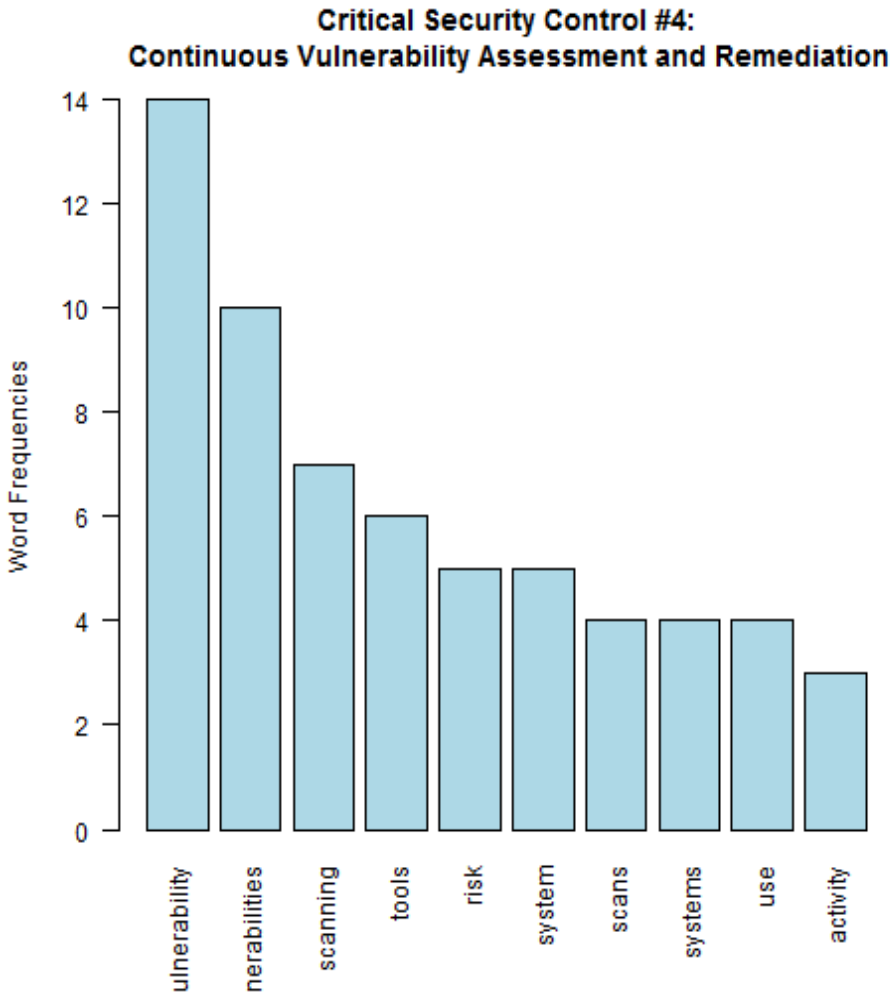
null device 1

CSC 4.x

[1] “vulnerability + vulnerabilities”



null device 1

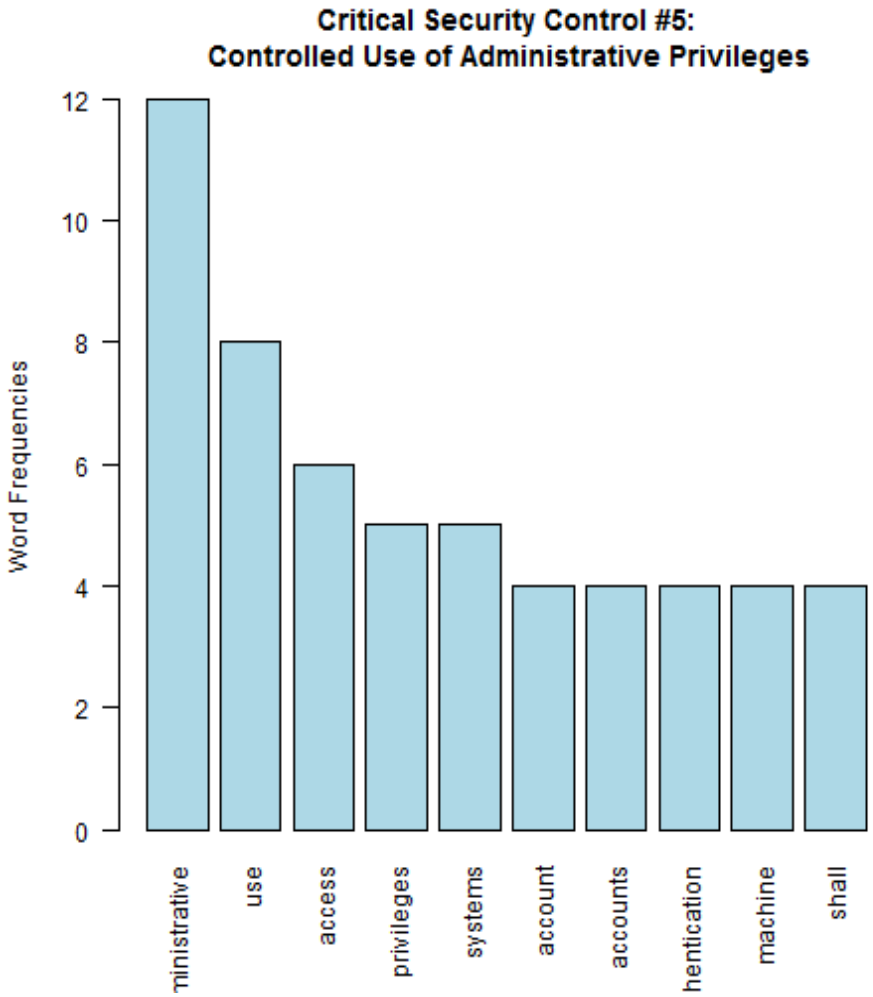


null device 1

CSC 5.x

[1] “administrative + use”

null device 1

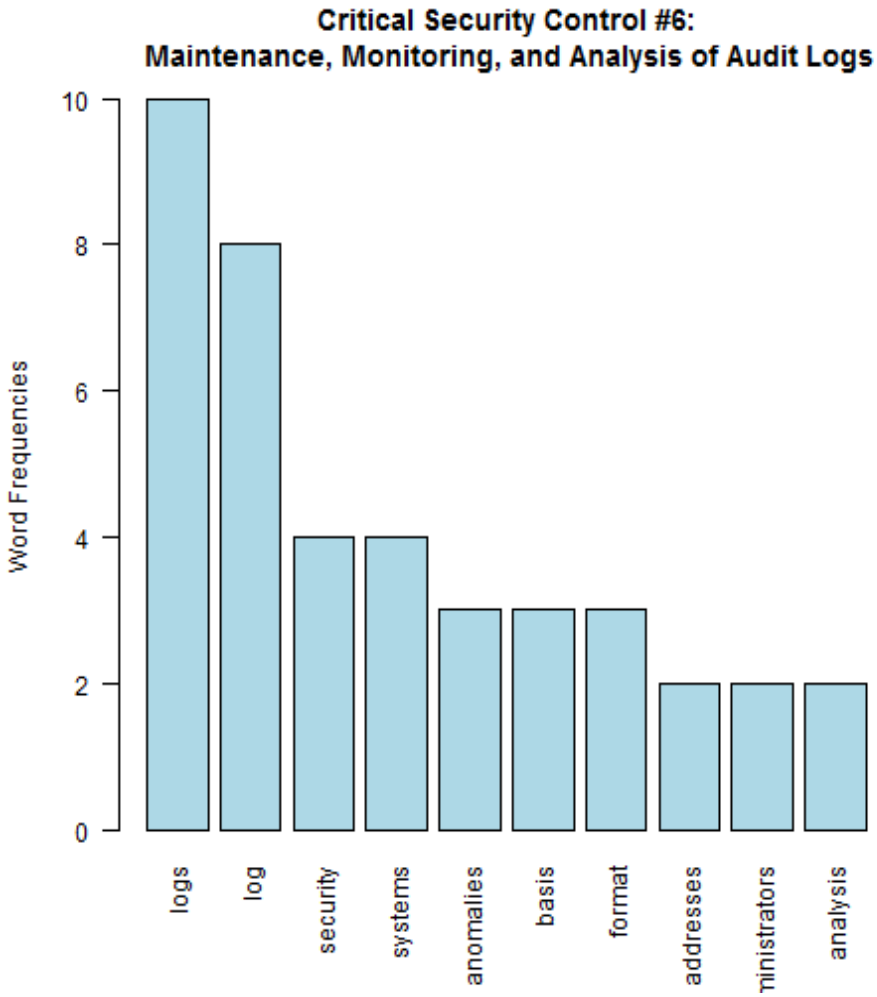


null device 1

CSC 6.x

[1] “logs + log”

null device 1

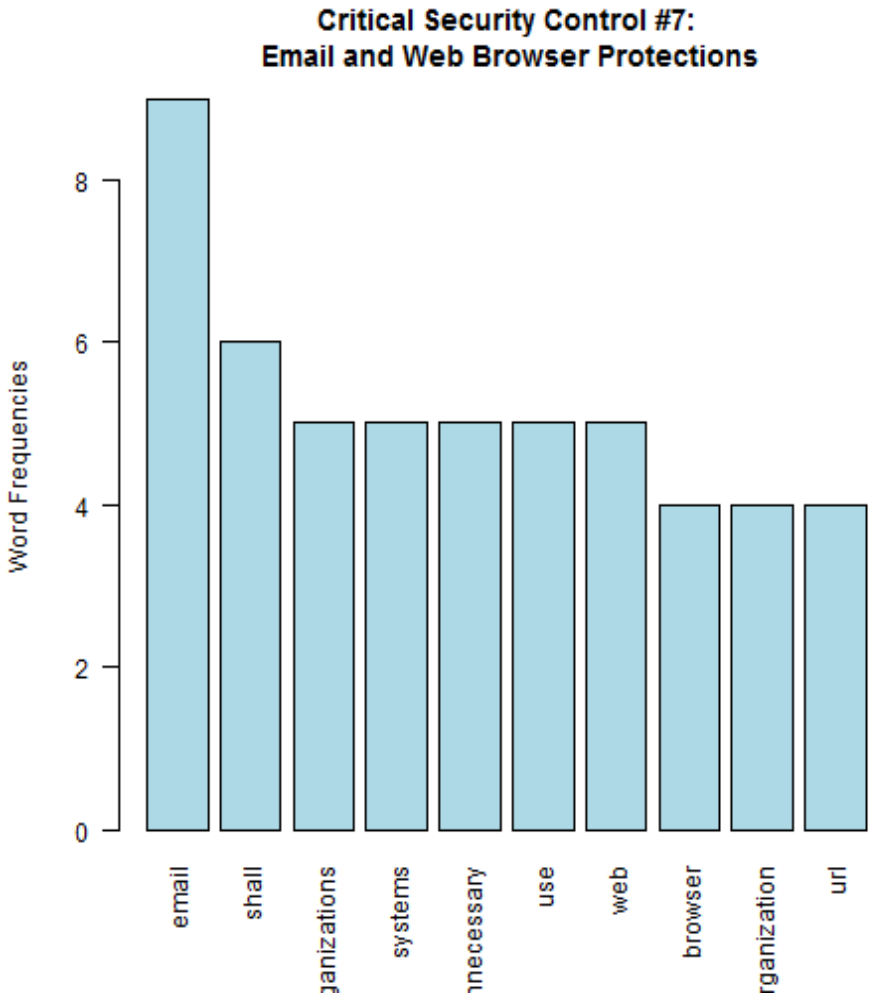


null device 1

CSC 7.x

[1] “email + shall”

null device 1

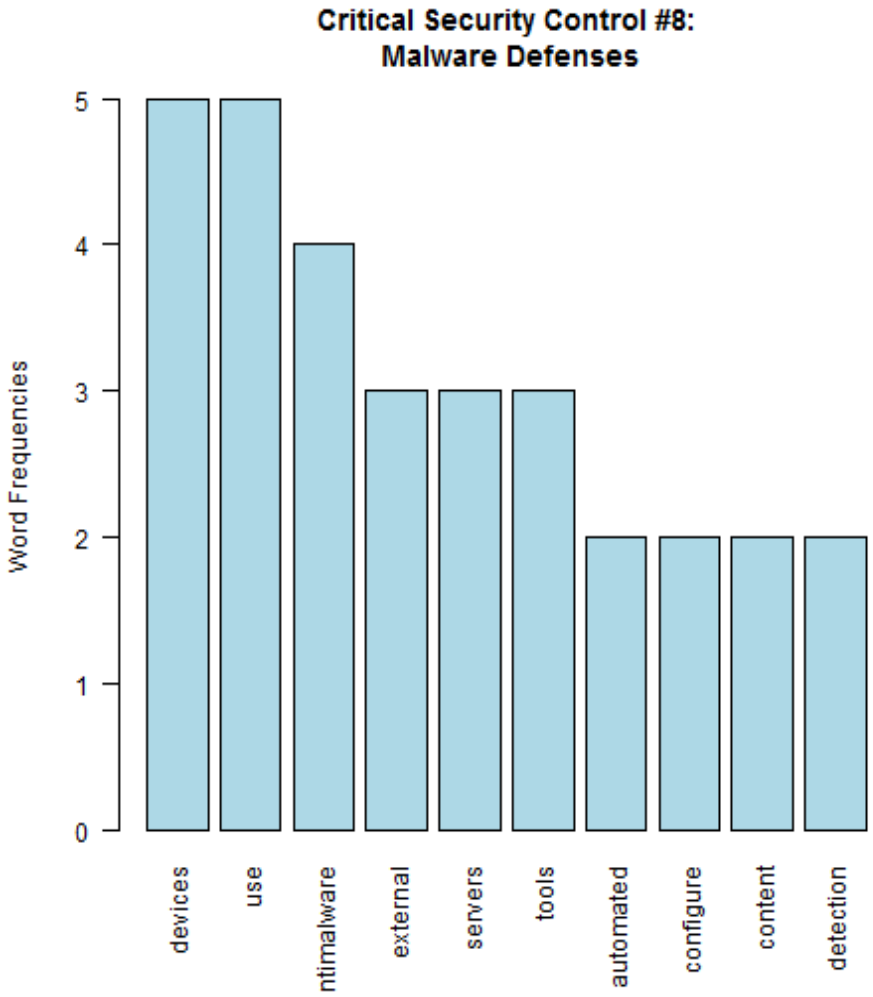


null device 1

CSC 8.x

[1] “devices + use”

null device 1

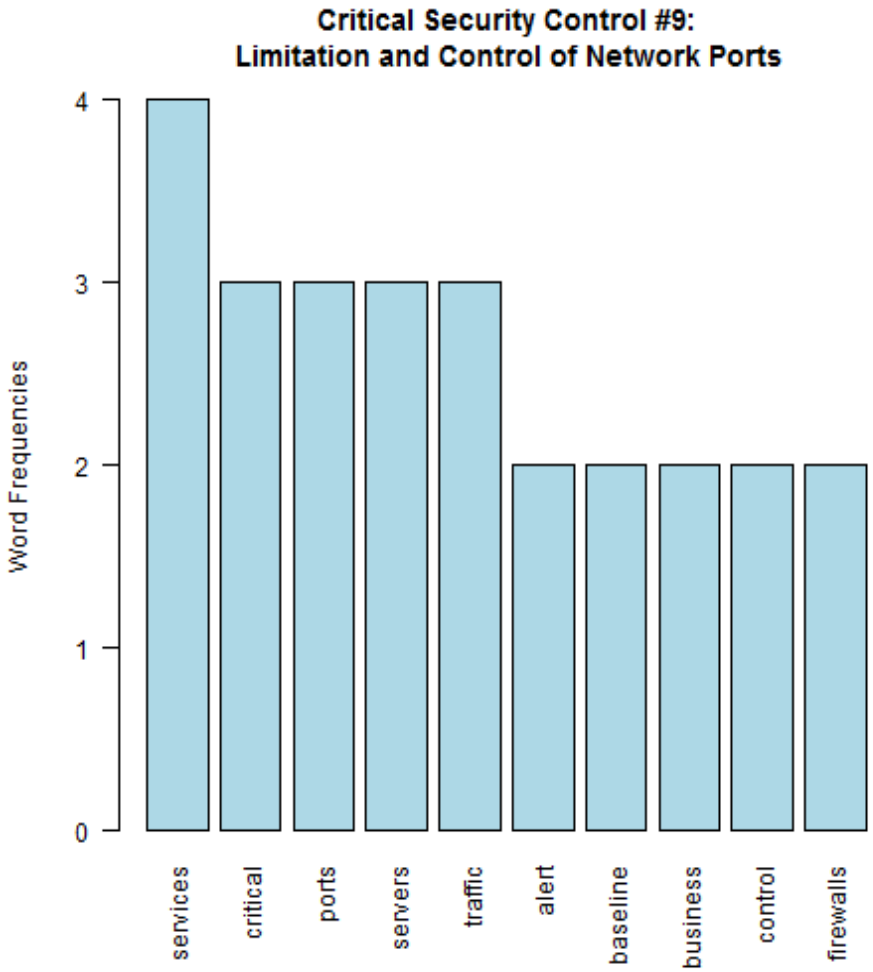


null device 1

CSC 9.x

[1] “services + critical”

null device 1

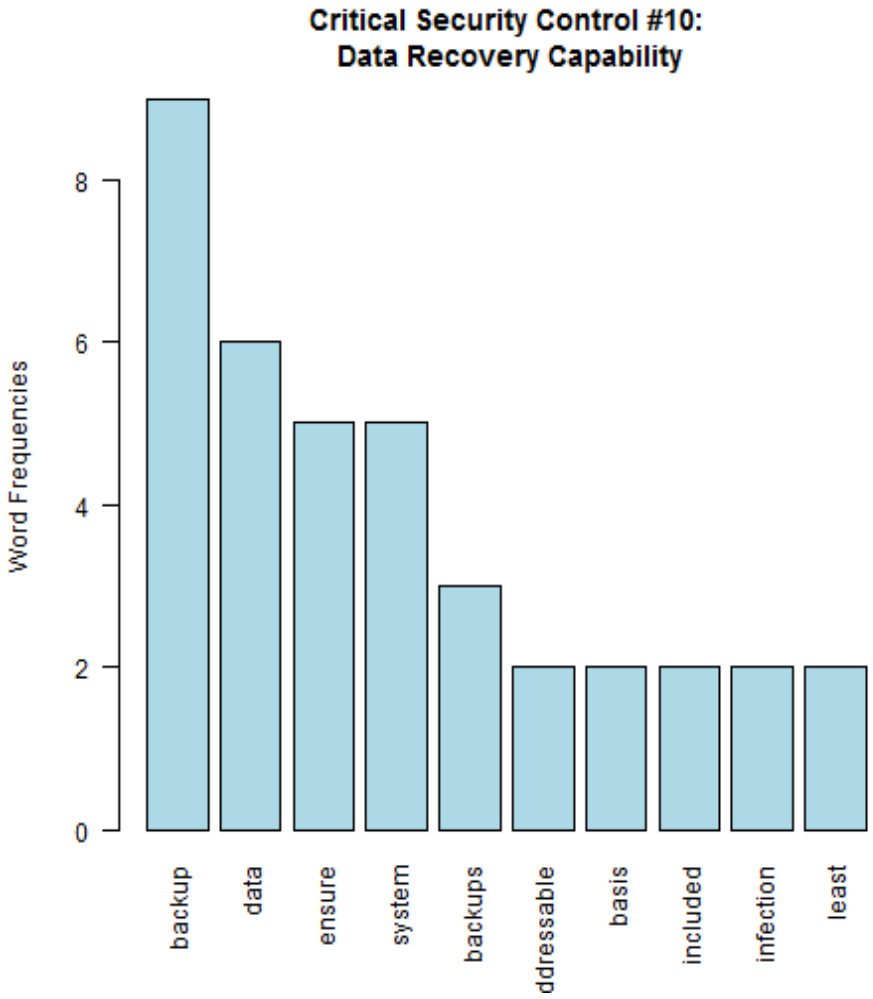


null device 1

CSC 10.x

[1] “backup + data”

null device 1

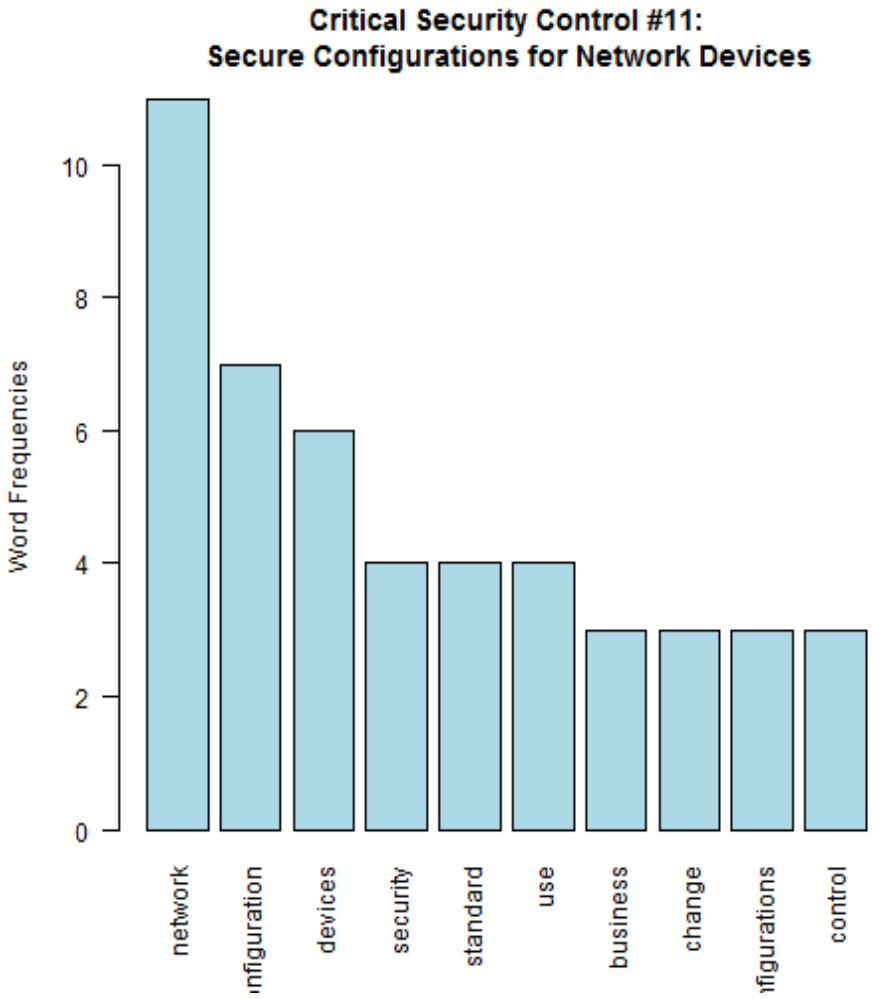


null device 1

CSC 11.x

[1] “network + configuration”

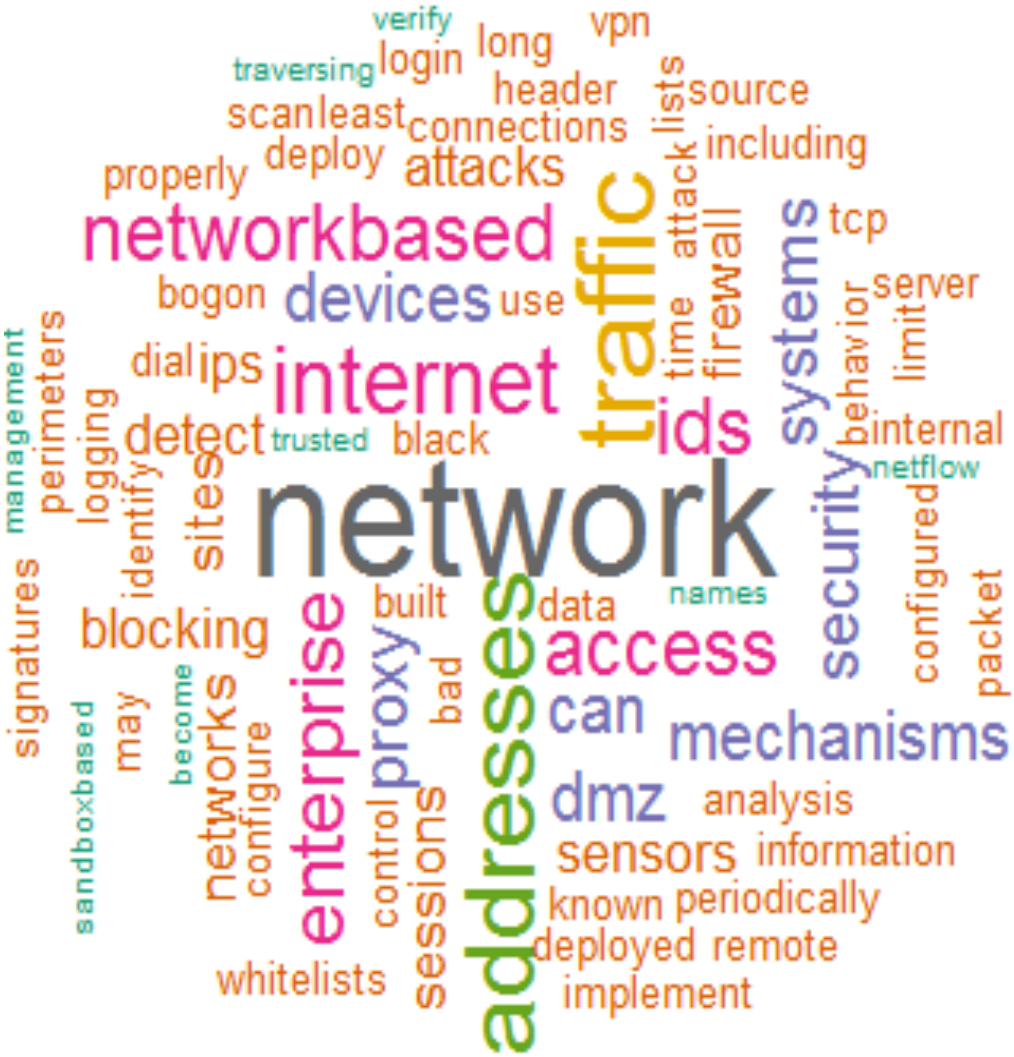
null device 1



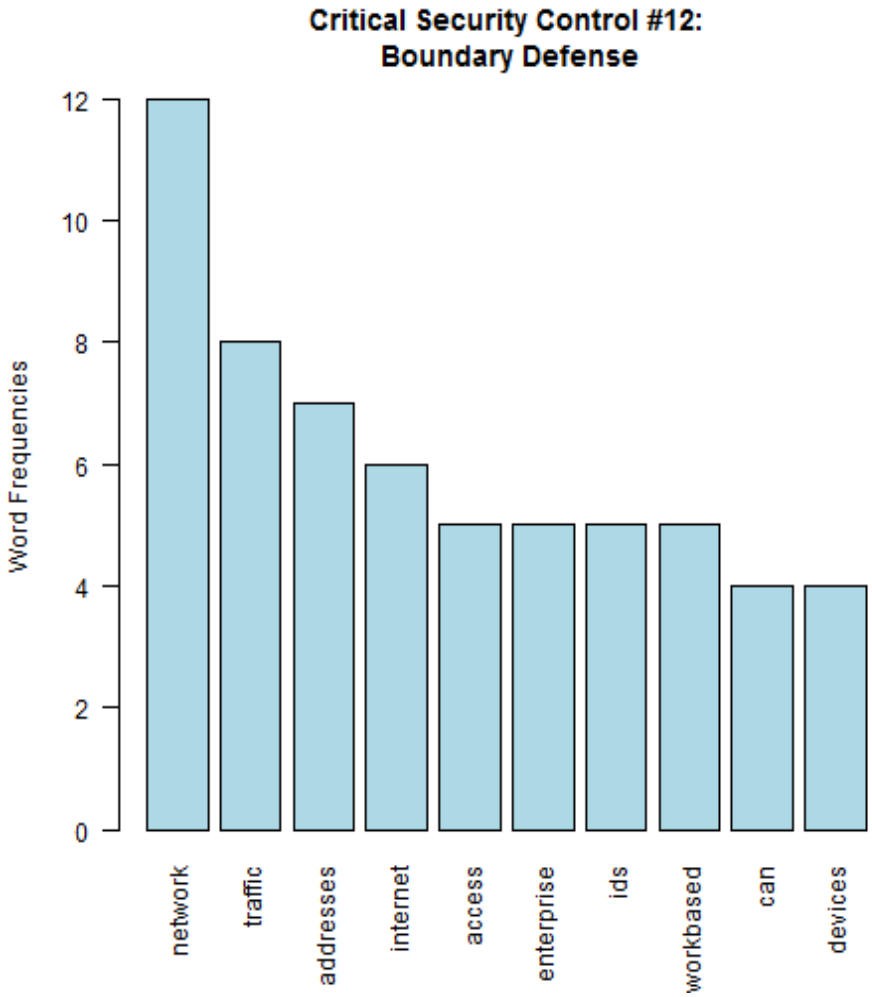
null device 1

CSC 12.x

[1] “network + traffic”



null device 1

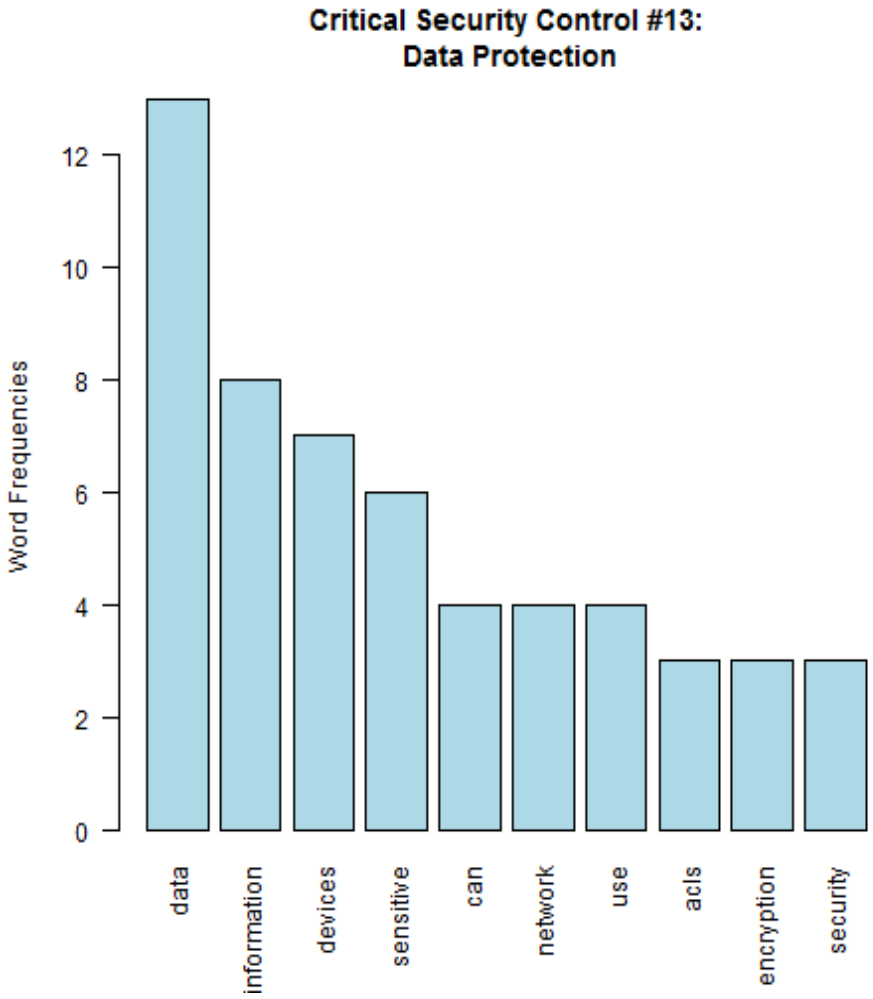


null device 1

CSC 13.x

[1] “data + information”

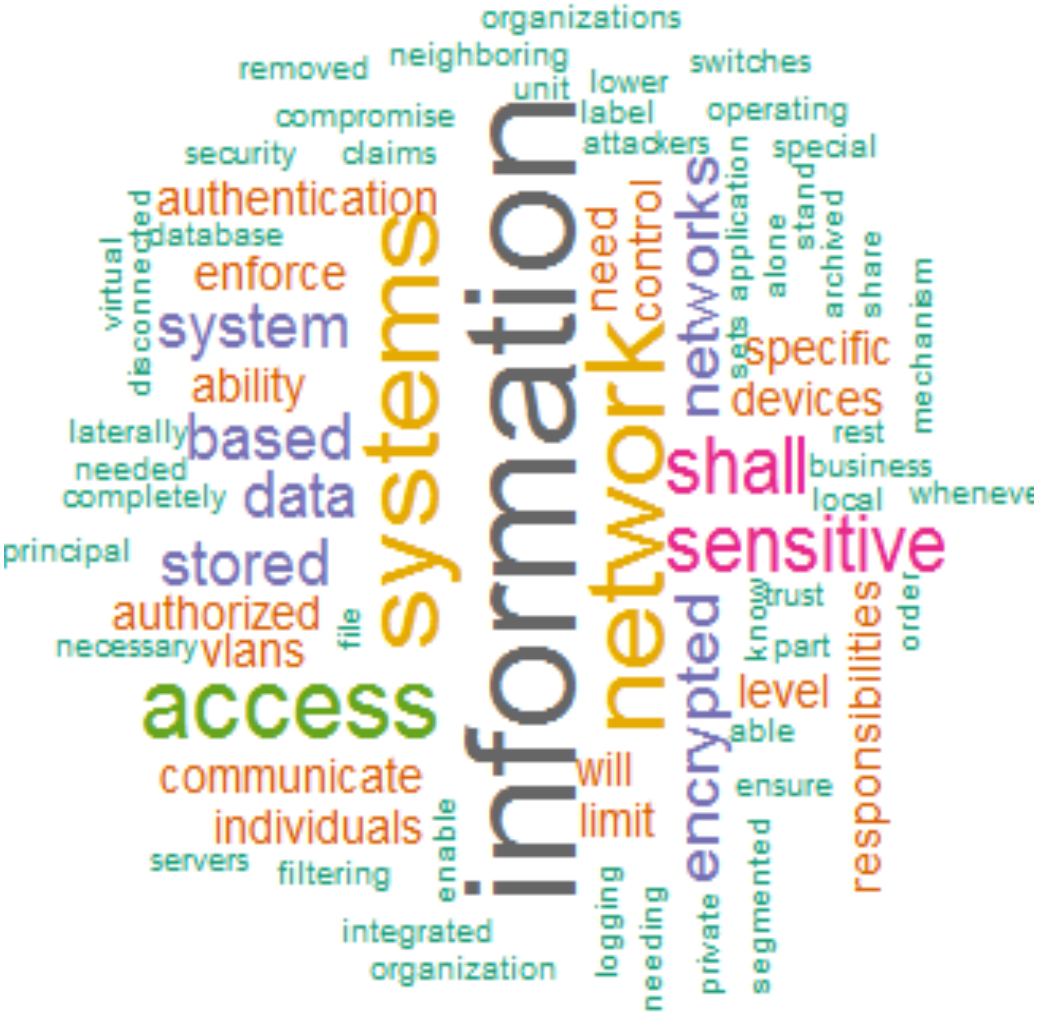
null device 1



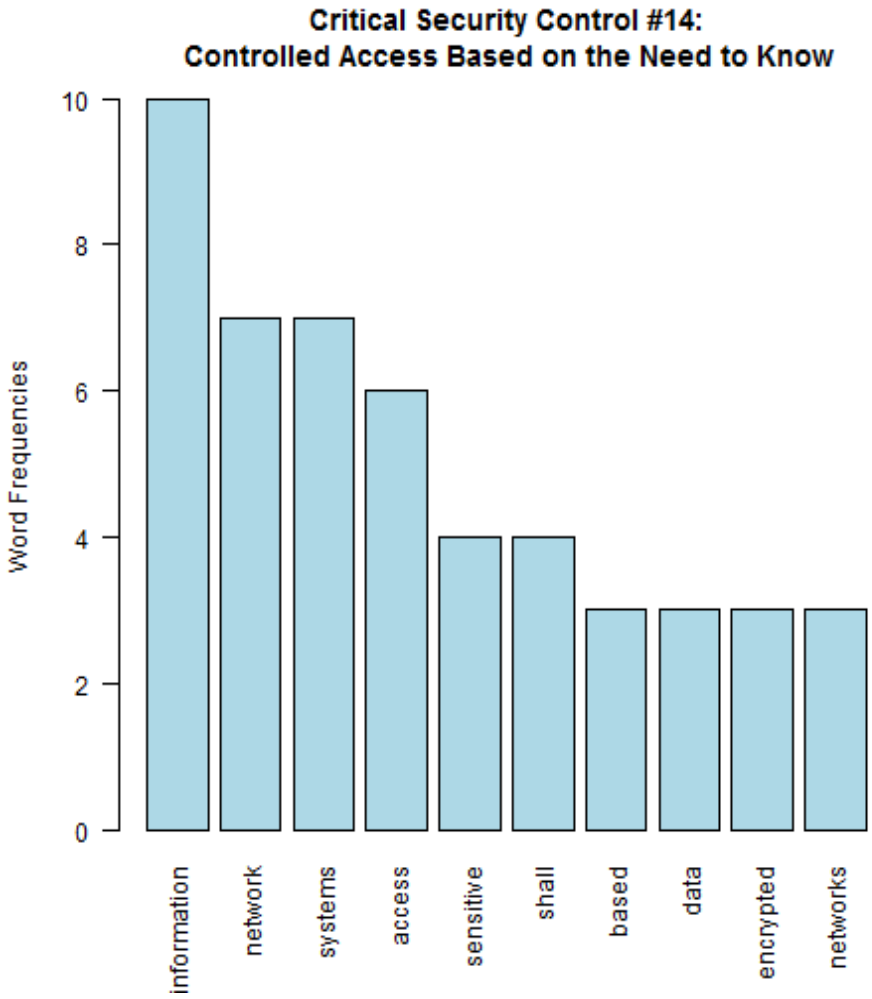
null device 1

CSC 14.x

[1] “information + network”



null device 1

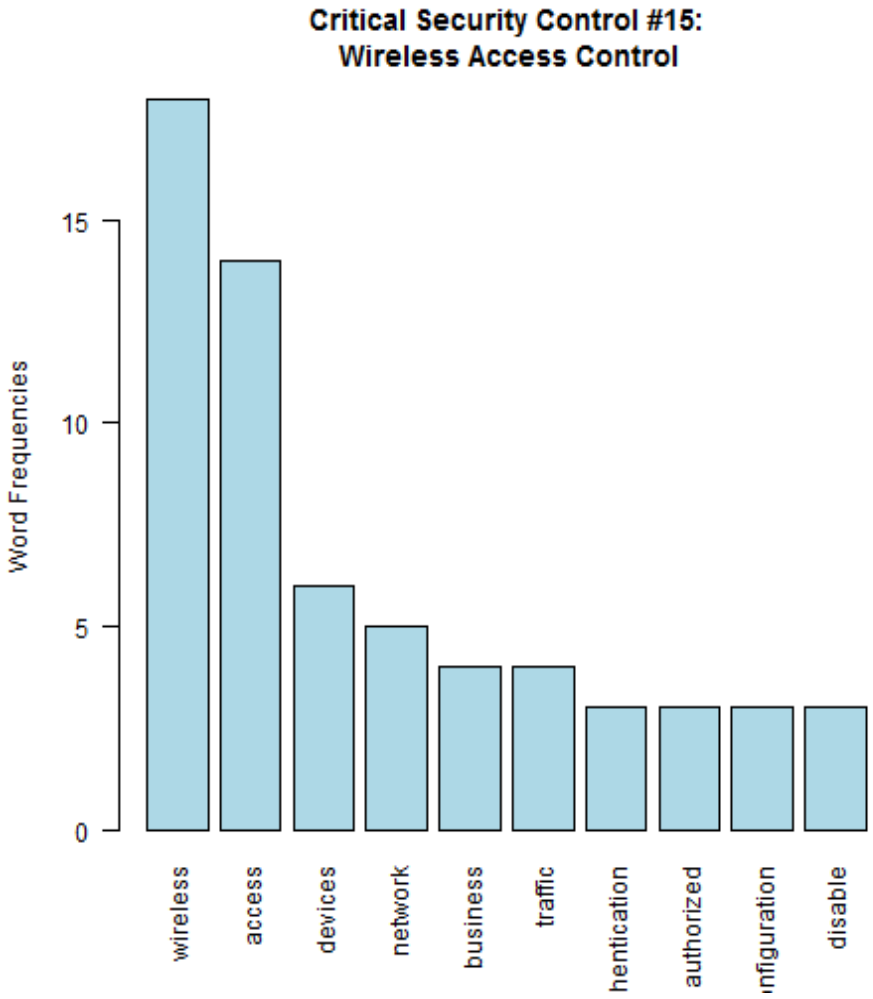


null device 1

CSC 15.x

[1] “wireless + access”

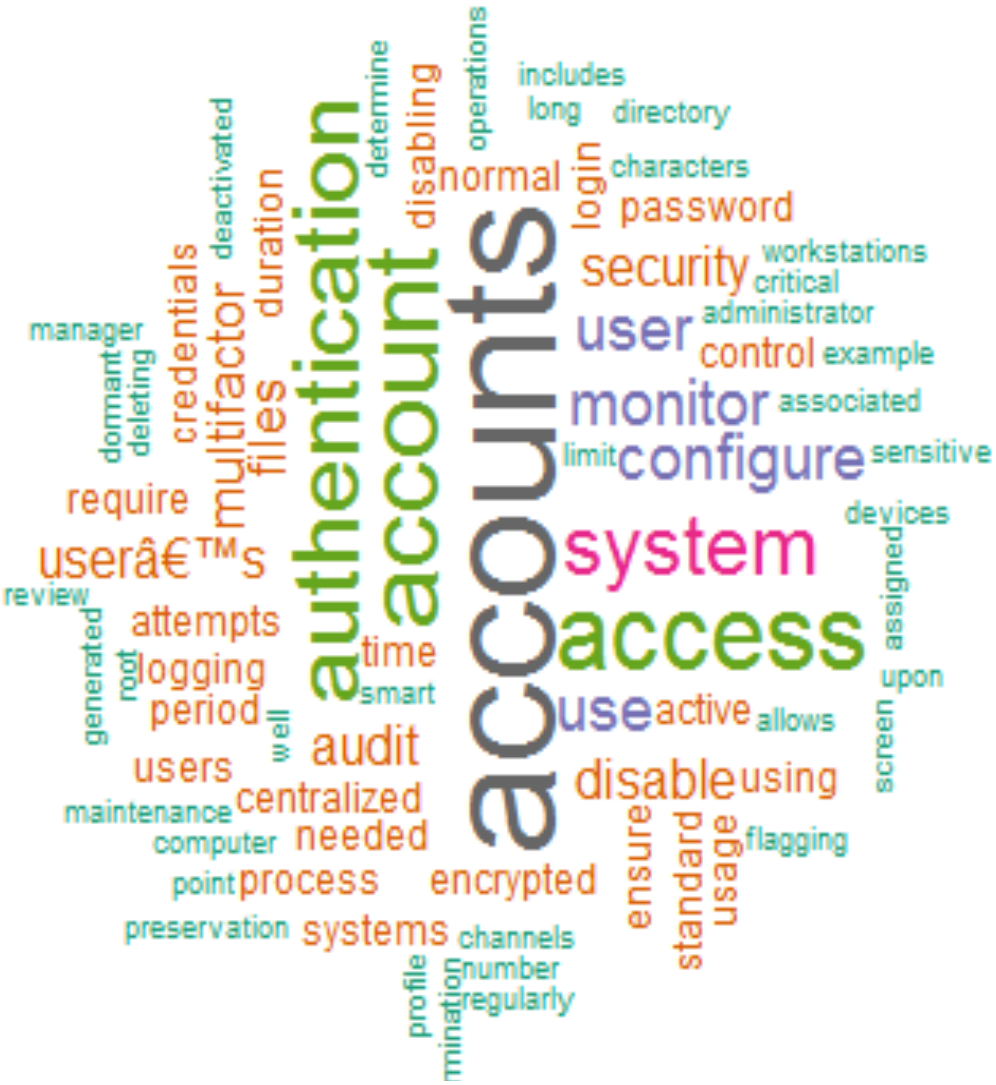
null device 1



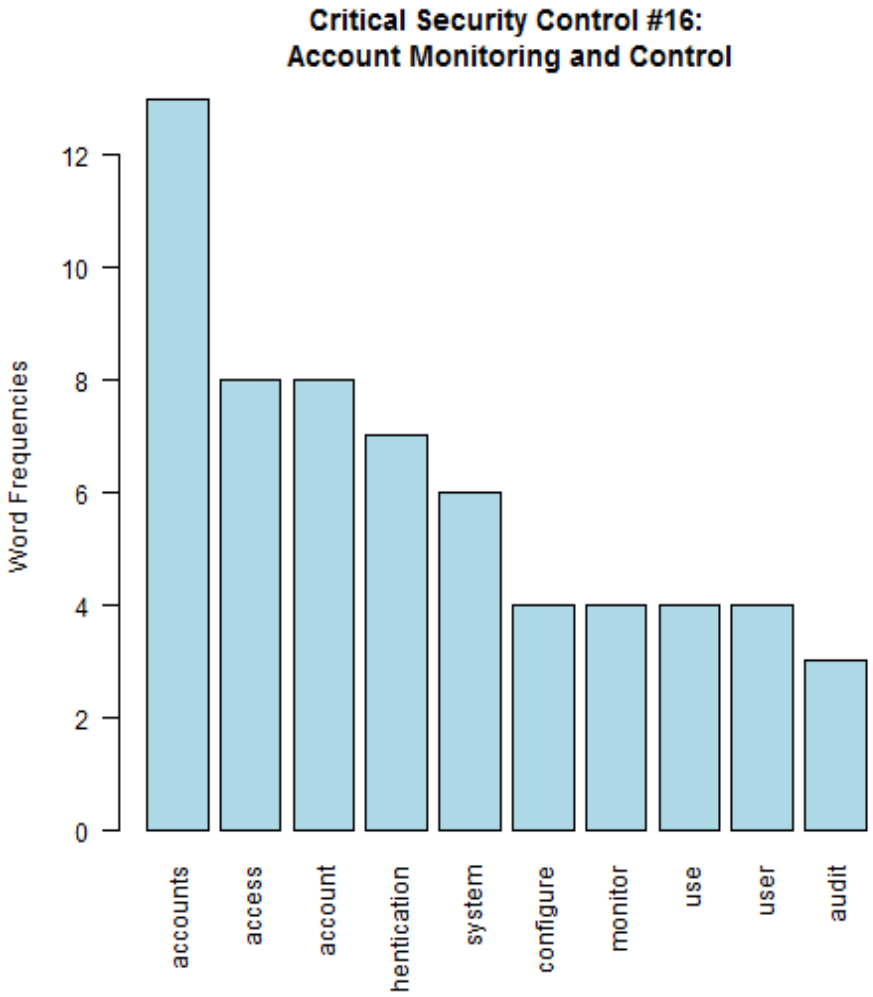
null device 1

CSC 16.x

[1] “accounts + access”



null device 1

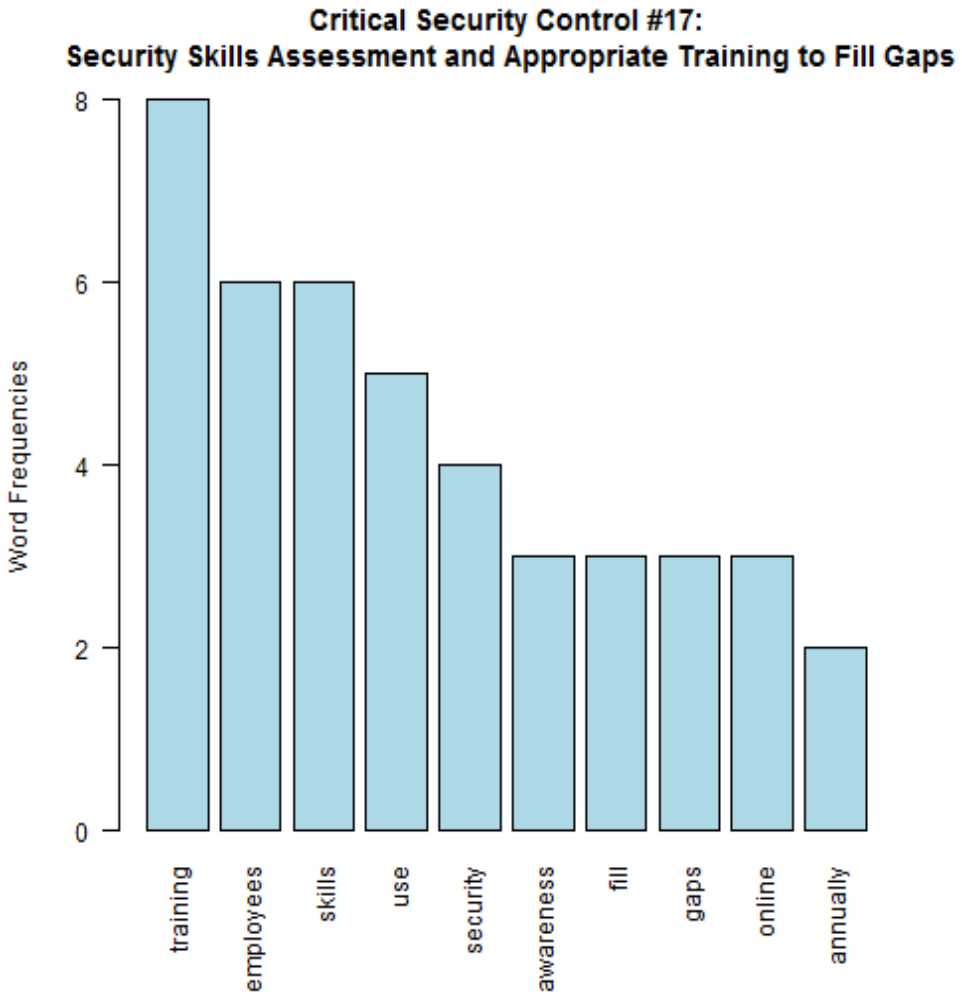


null device 1

CSC 17.x

[1] “training + employees”

null device 1

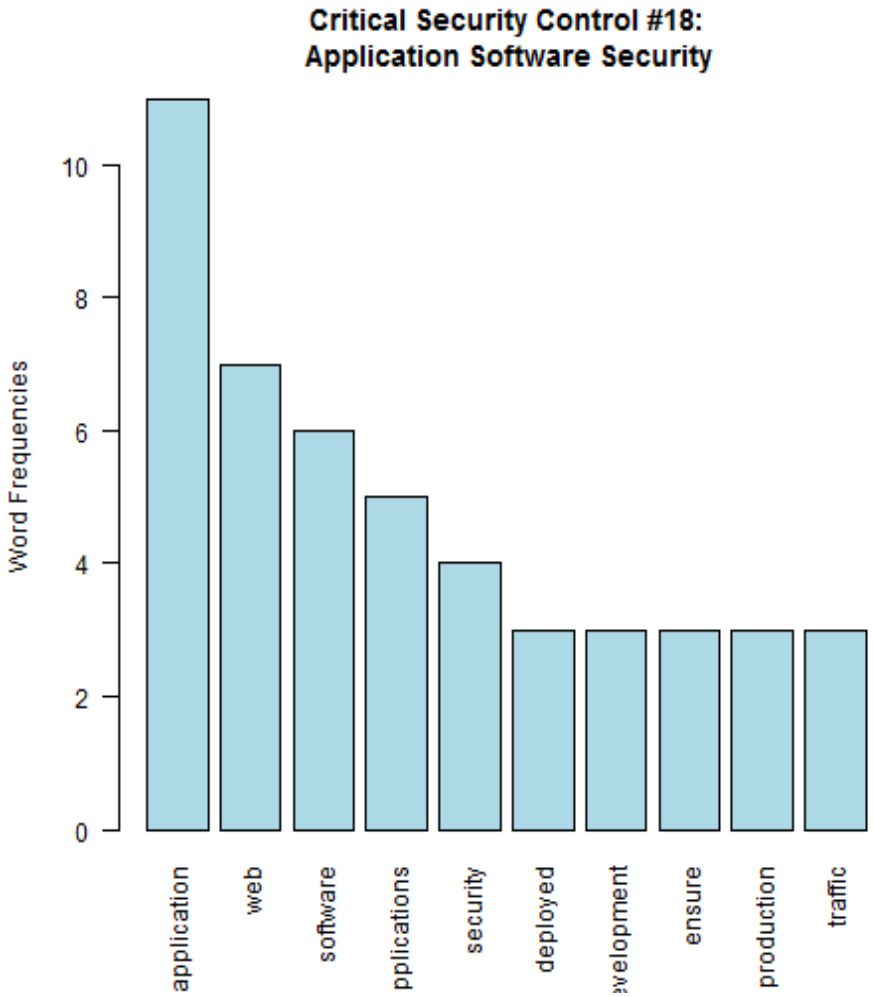


null device 1

CSC 18.x

[1] “application + web”

null device 1

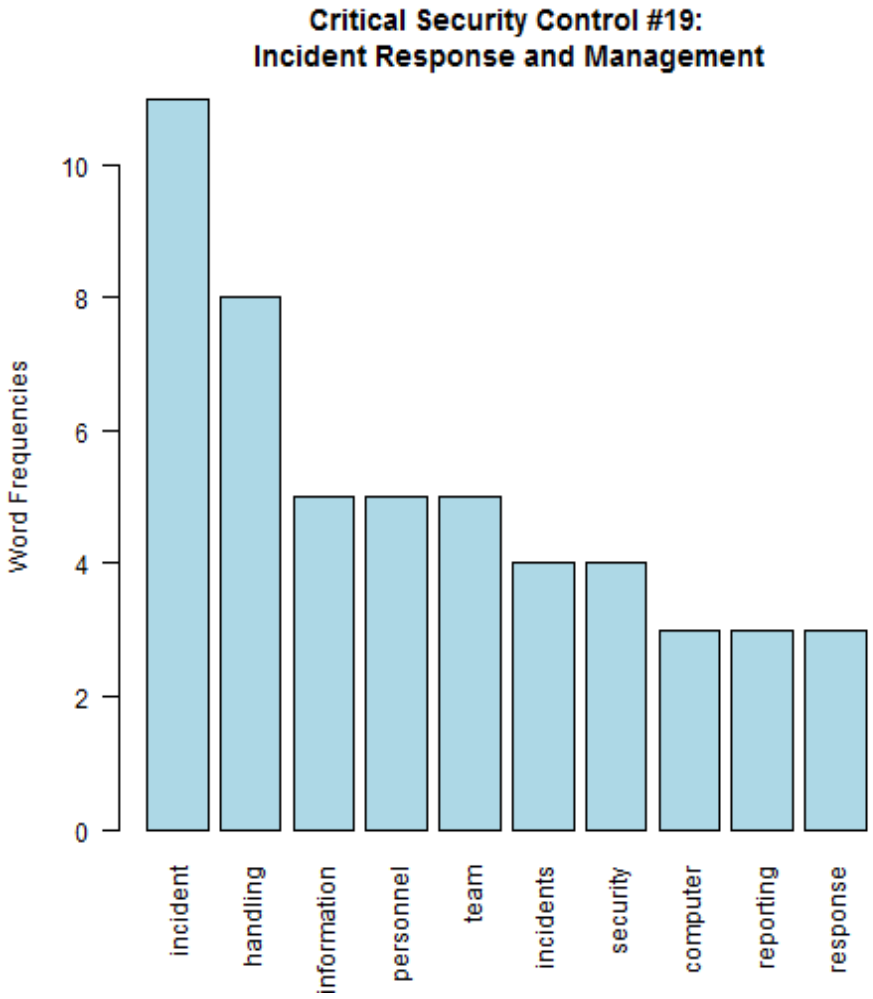


null device 1

CSC 19.x

[1] “incident + handling”

null device 1

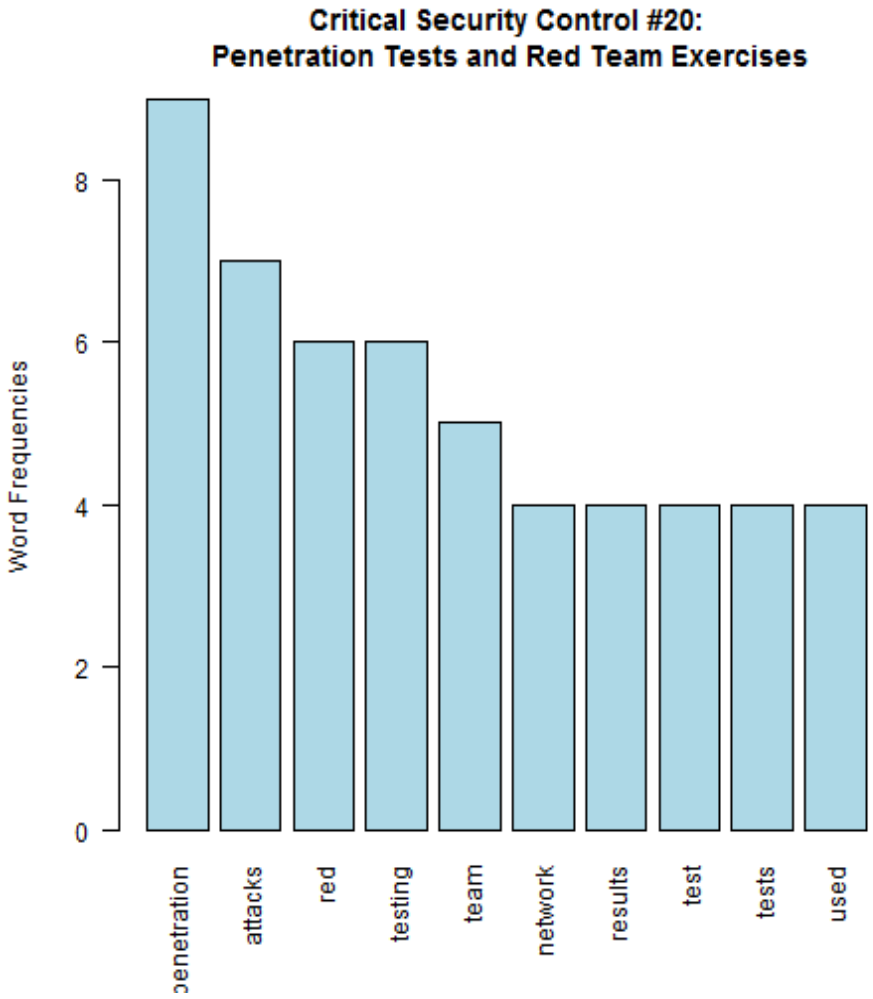


null device 1

CSC 20.x

[1] “penetration + attacks”

null device 1



null device 1