CSC 8

John Ryan Zelling Analyst

Jan 2017

Contents

CSC 8.0

[1] "Critical Security Control #8: Malware Defenses"

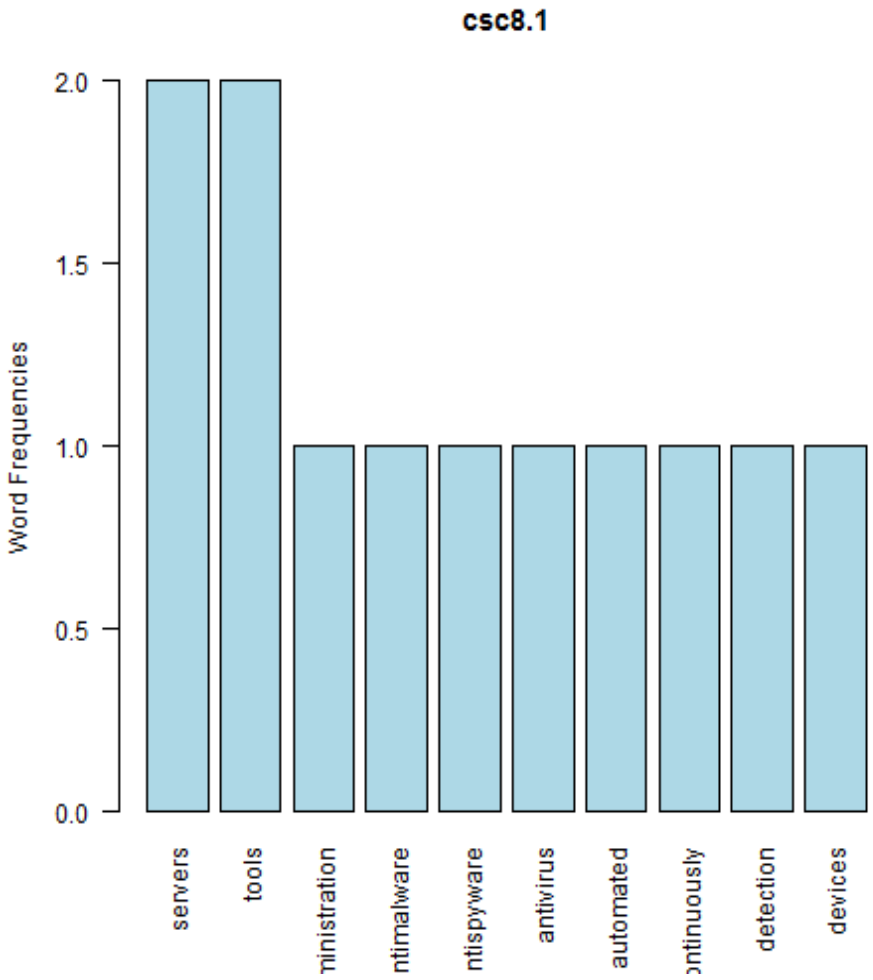
[1]

[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 8.1

[1] “servers + tools”

null device 1

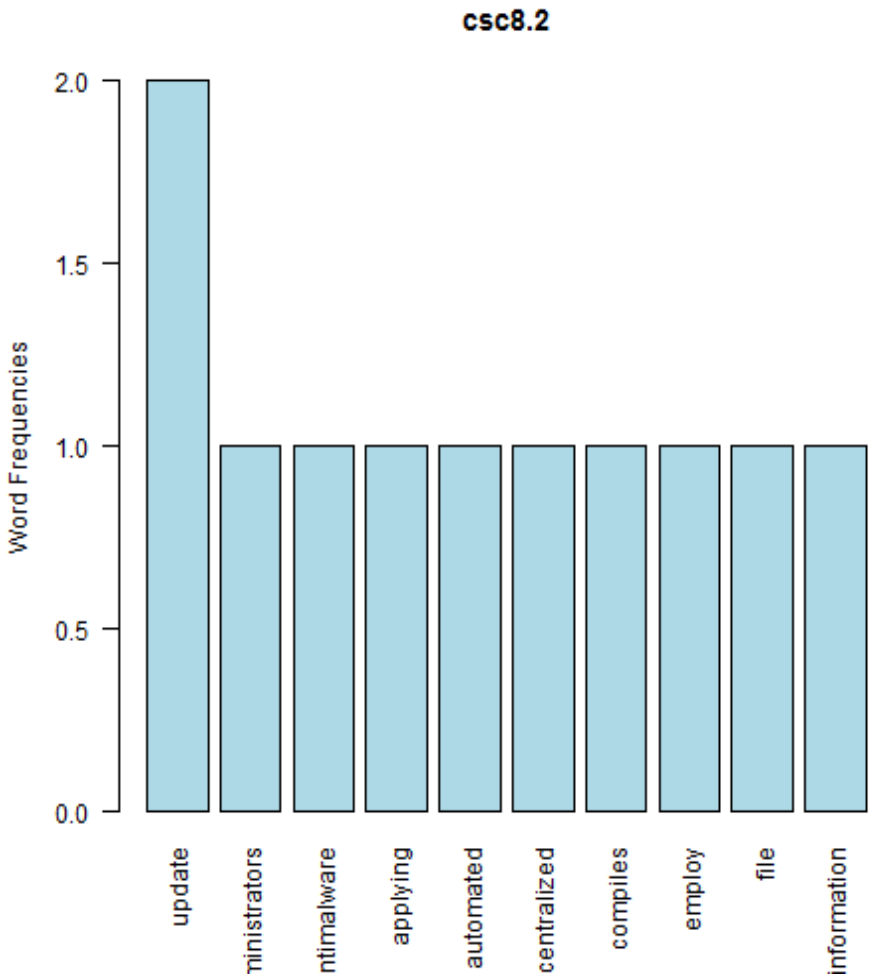


null device 1 [1] "Employ automated tools to continuously monitor workstations, servers, and mobile devices with anti-virus, anti-spyware, personal firewalls, and host-based IPS functionality. All malware detection events should be sent to enterprise anti-malware administration tools and event log servers."

CSC 8.2

[1] “update + administrators”

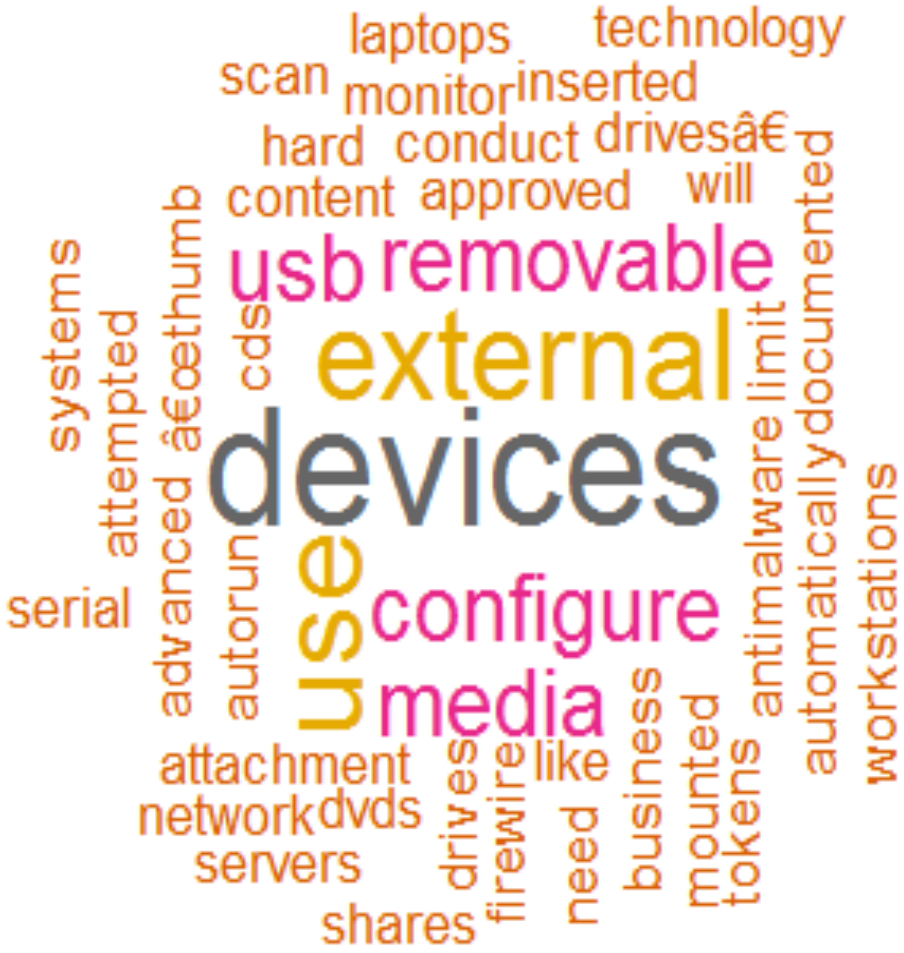
null device 1



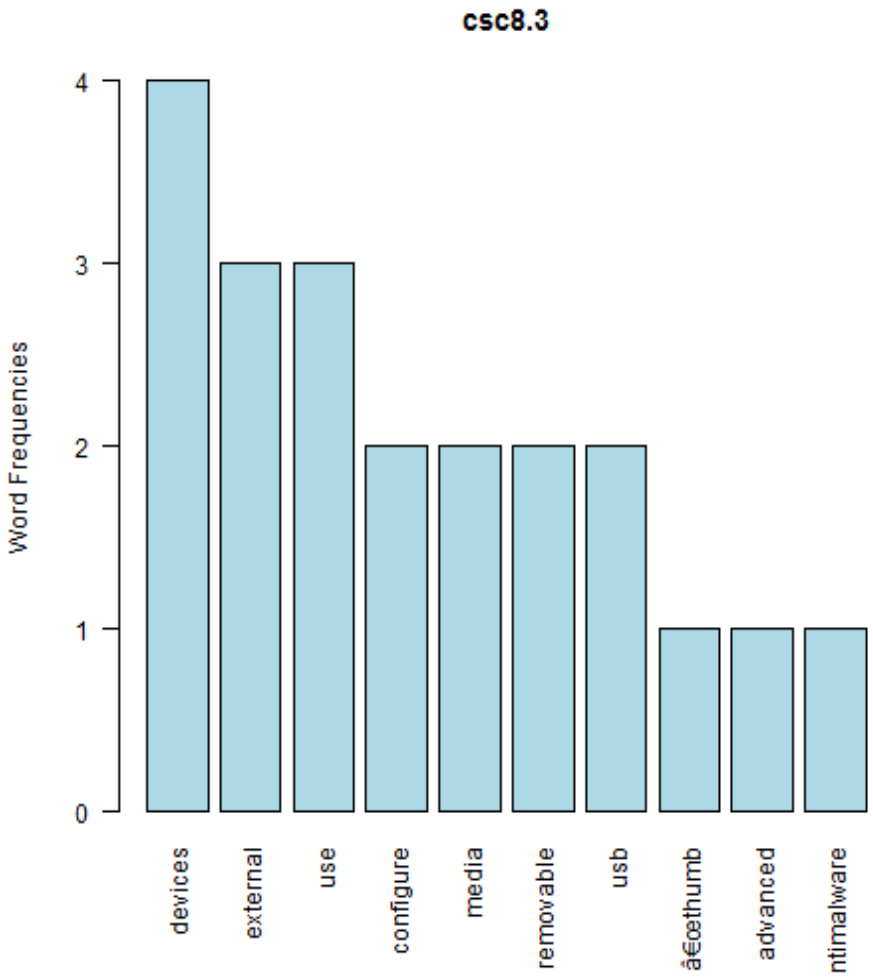
null device 1 [1] “Employ anti-malware software that offers a centralized infrastructure that compiles information on file reputations or have administrators manually push updates to all machines. After applying an update, automated systems should verify that each system has received its signature update.”

CSC 8.3

[1] “devices + external”



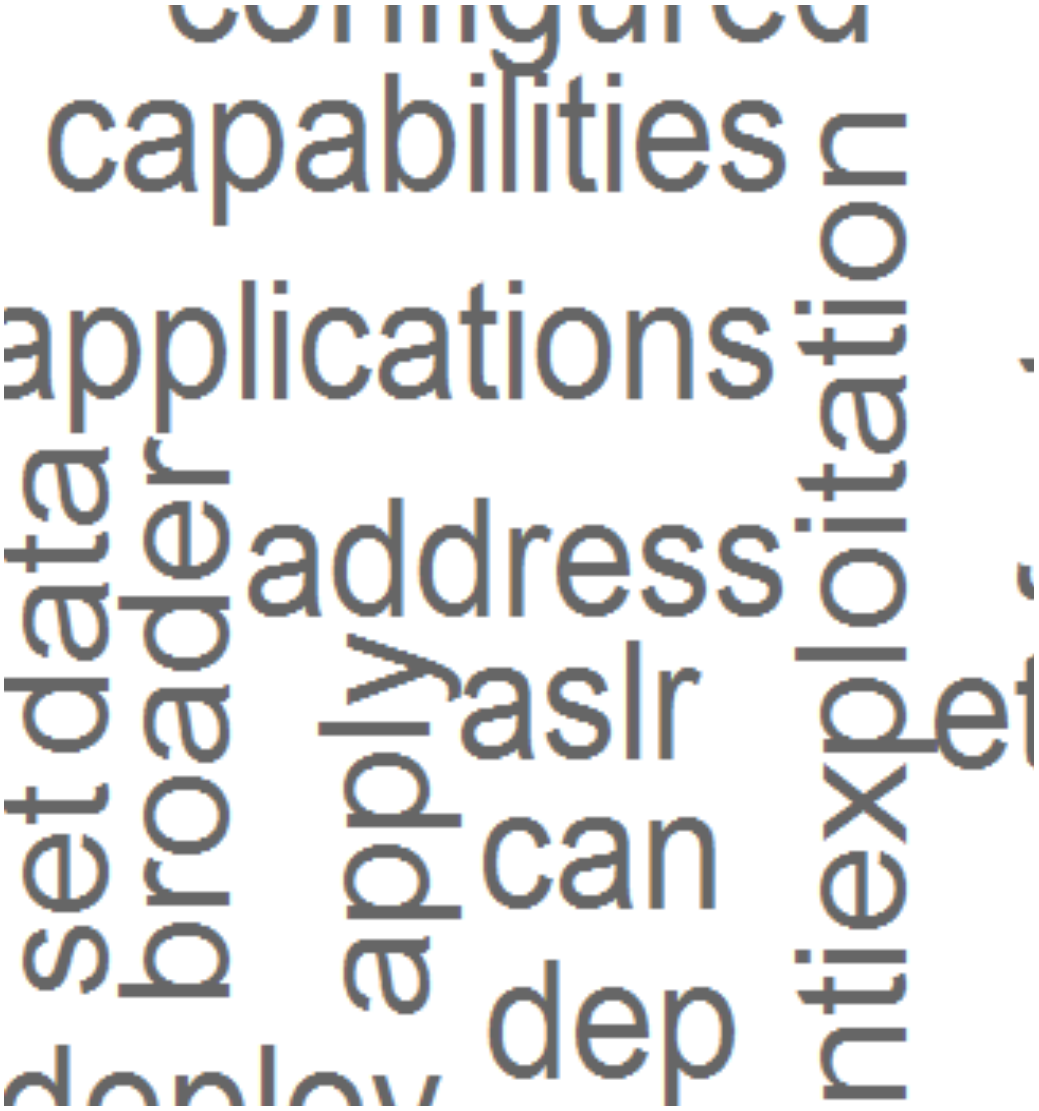
null device 1



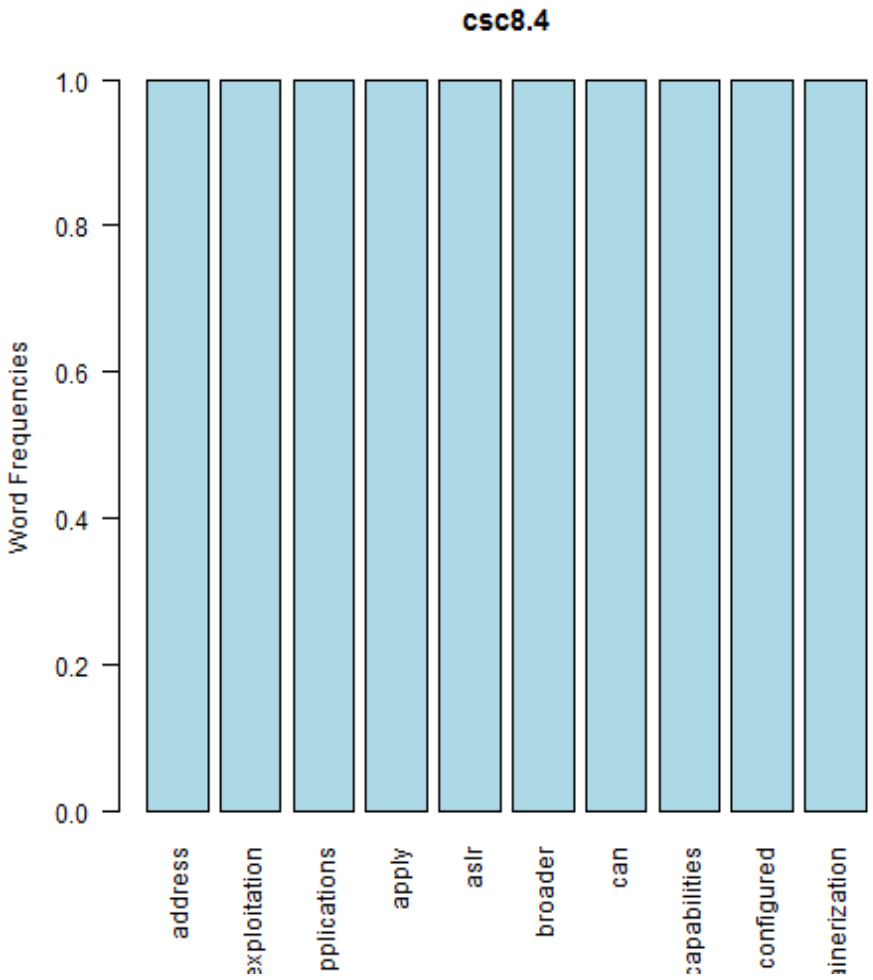
null device 1 [1] “Limit use of external devices to those with an approved, documented business need. Monitor for use and attempted use of external devices. Configure laptops, workstations, and servers so that they will not auto-run content from removable media, like USB tokens (i.e., â thumb drivesâ), USB hard drives, CDs/DVDs, FireWire devices, external serial advanced technology attachment devices, and mounted network shares. Configure systems so that they automatically conduct an anti-malware scan of removable media when inserted.”

CSC 8.4

[1] “address + antiexploitation”



null device 1



null device 1 [1] "Enable anti-exploitation features such as Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualization/containerization, etc. For increased protection, deploy capabilities such as Enhanced Mitigation Experience Toolkit (EMET) that can be configured to apply these protections to a broader set of applications and executables."

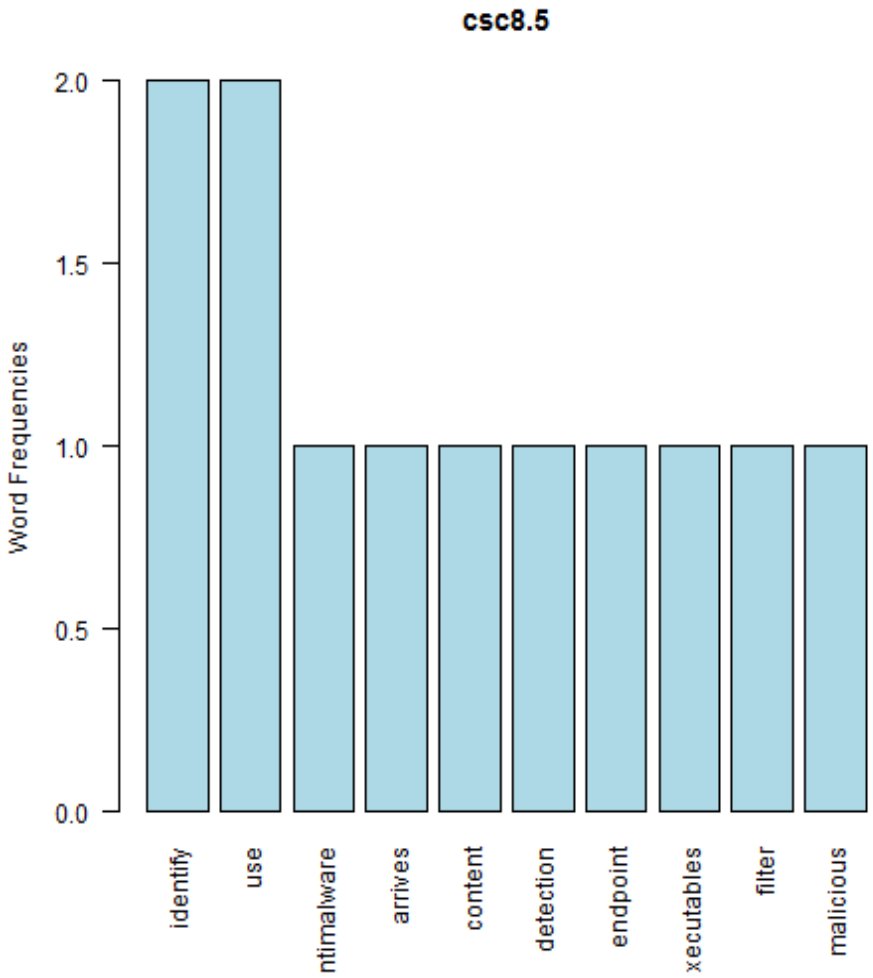
[2]

[2] https://support.microsoft.com/en-us/kb/2458544

CSC 8.5

[1] “identify + use”

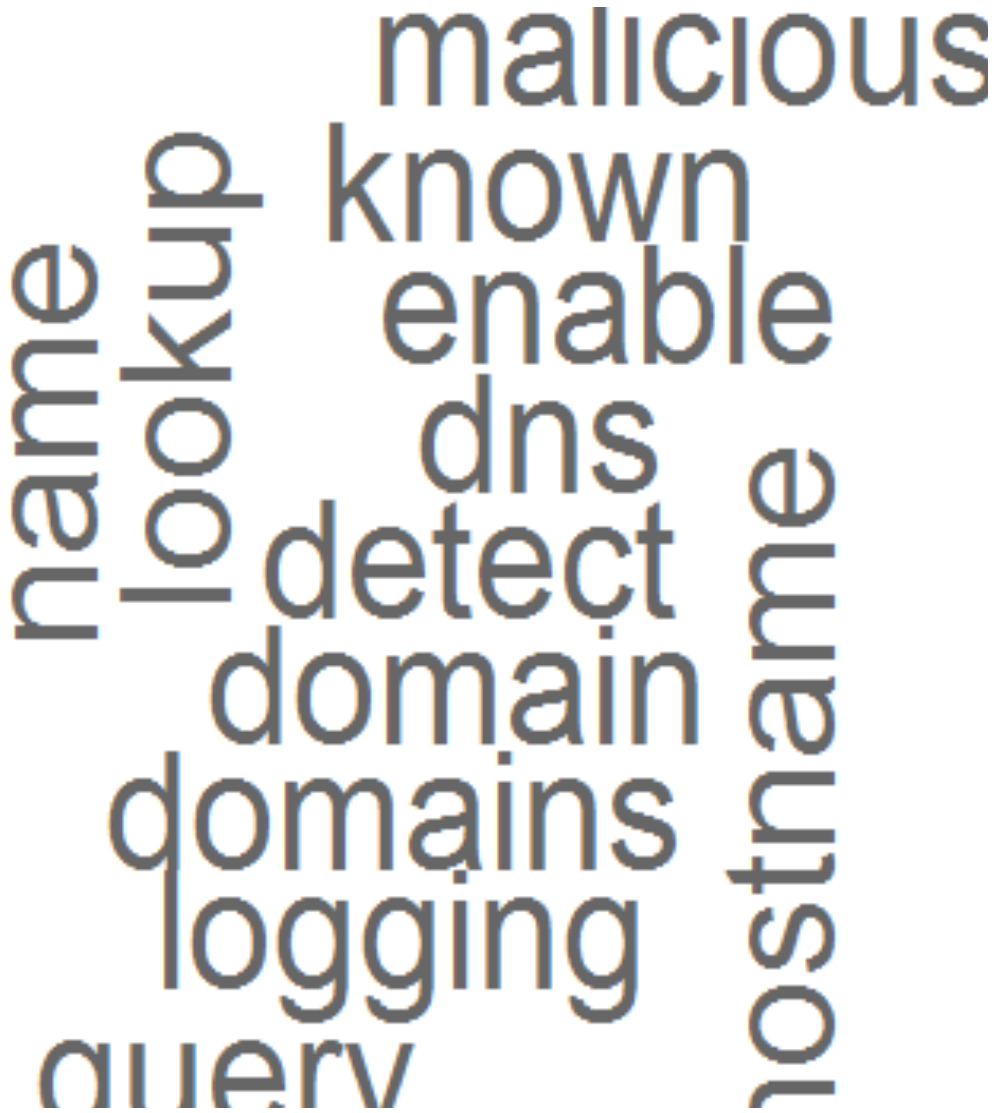
null device 1



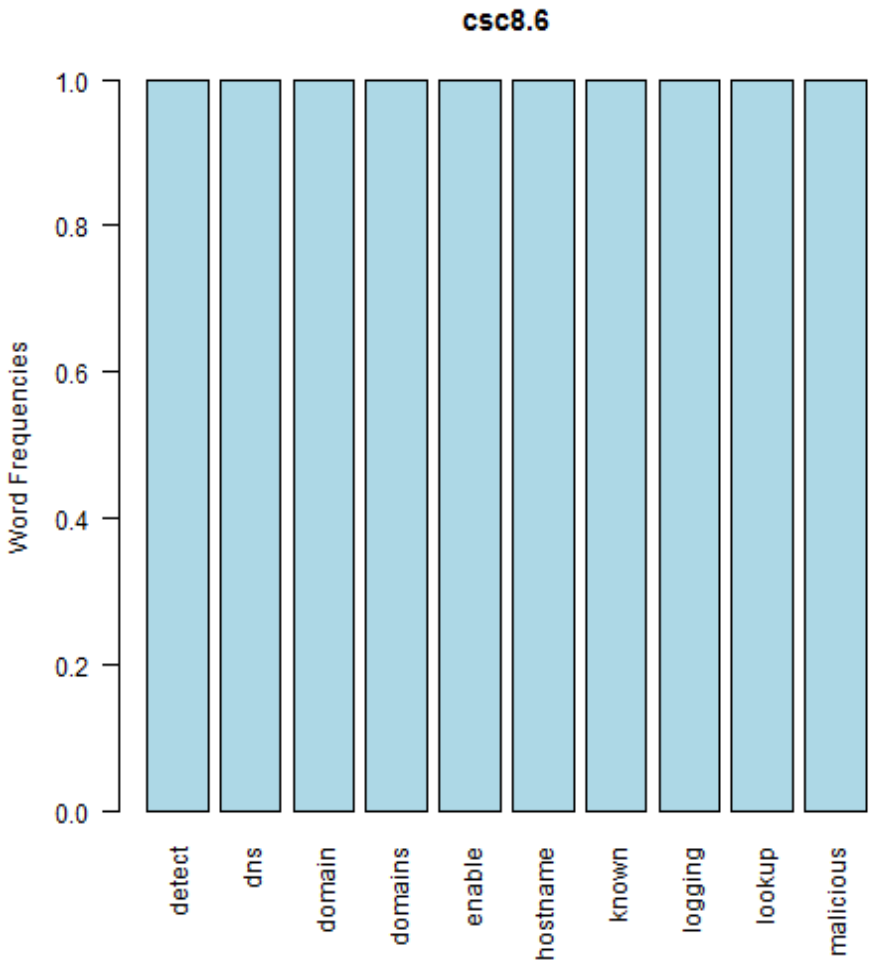
null device 1 [1] “Use network-based anti-malware tools to identify executables in all network traffic and use techniques other than signature-based detection to identify and filter out malicious content before it arrives at the endpoint.”

CSC 8.6

[1] “detect + dns”



null device 1



null device 1 [1] “Enable domain name system (DNS) query logging to detect hostname lookup for known malicious C2 domains.”