CSC 6

John Ryan Zelling Analyst

Jan 2017

Contents

CSC 6.0

[1] "Critical Security Control #6: Maintenance, Monitoring, and Analysis of Audit Logs"

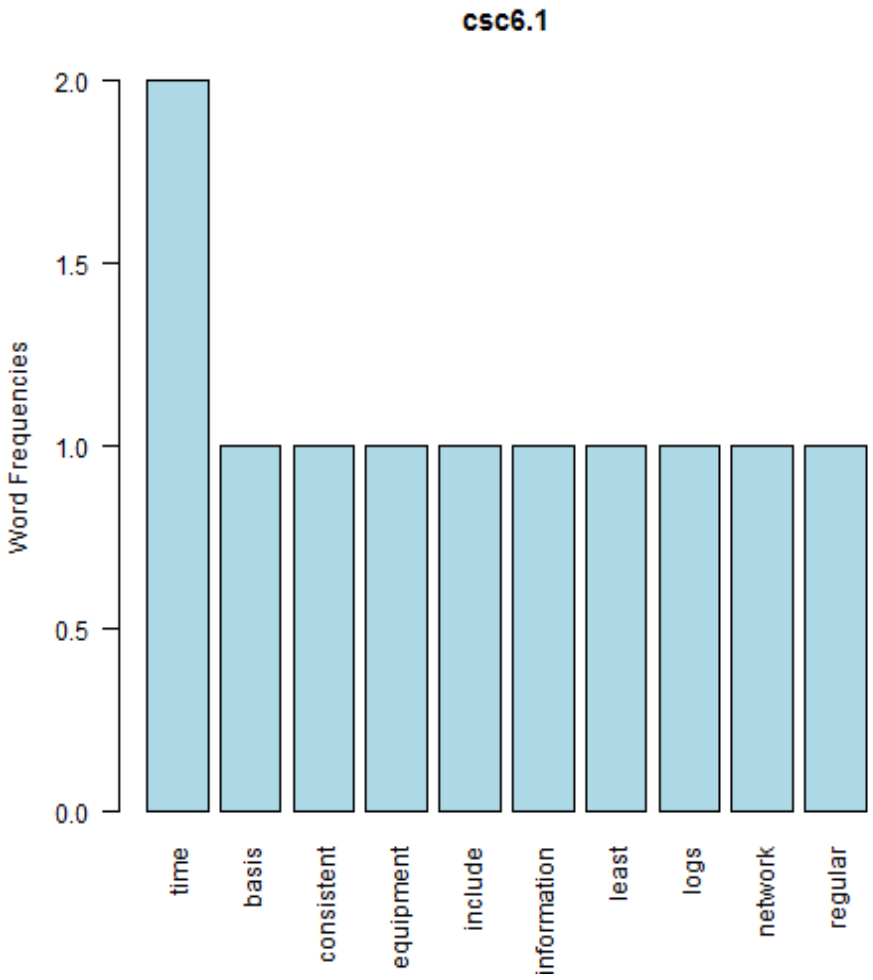
[1]

[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 6.1

[1] “time + basis”

null device 1

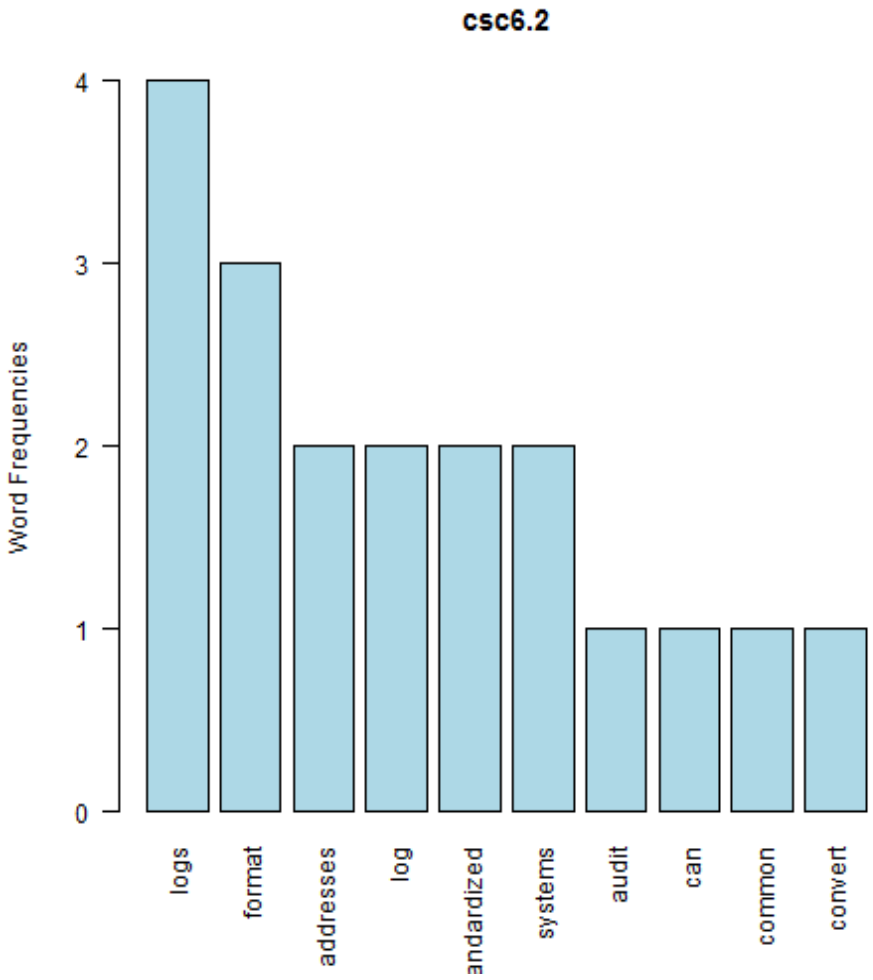


null device 1 [1] “Include at least two synchronized time sources from which all servers and network equipment retrieve time information on a regular basis so that timestamps in logs are consistent.”

CSC 6.2

[1] “logs + format”

null device 1



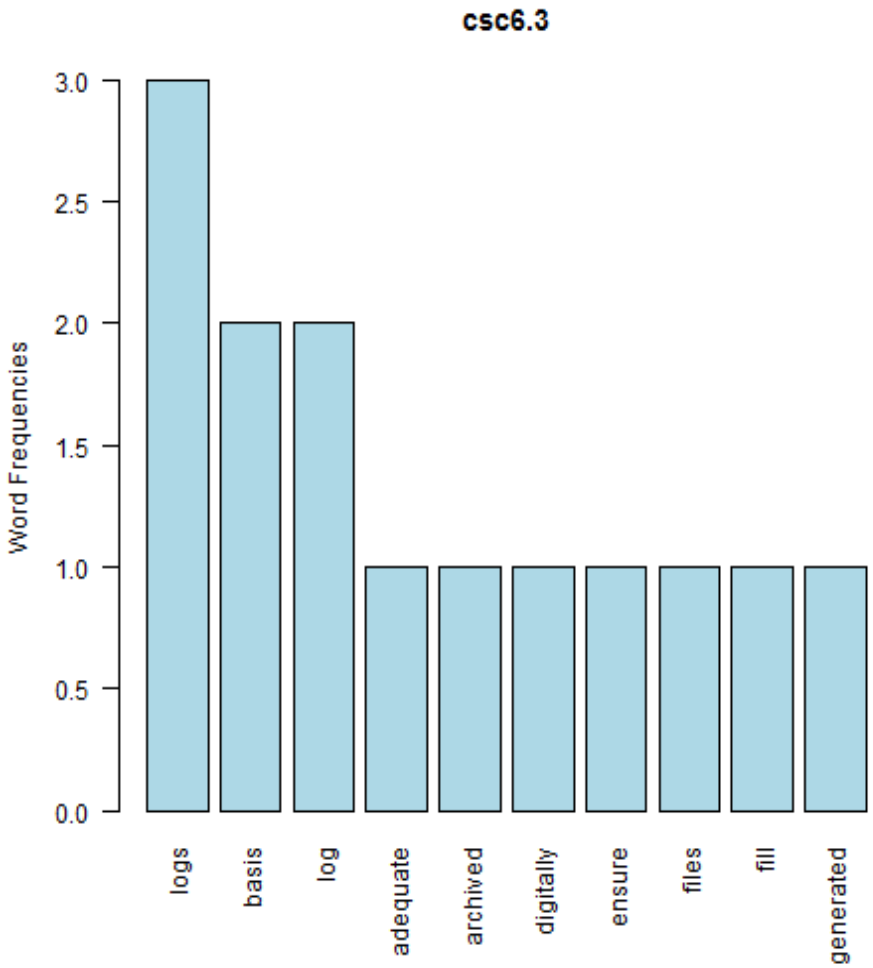
null device 1 [1] "Validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction. Systems should record logs in a standardized format such as syslog entries or those outlined by the Common Event Expression initiative. If systems cannot generate logs in a standardized format, log normalization tools can be deployed to convert logs into such a format."
2

[2]https://cee.mitre.org/about/faqs.html

CSC 6.3

[1] "logs + basis"

null device 1

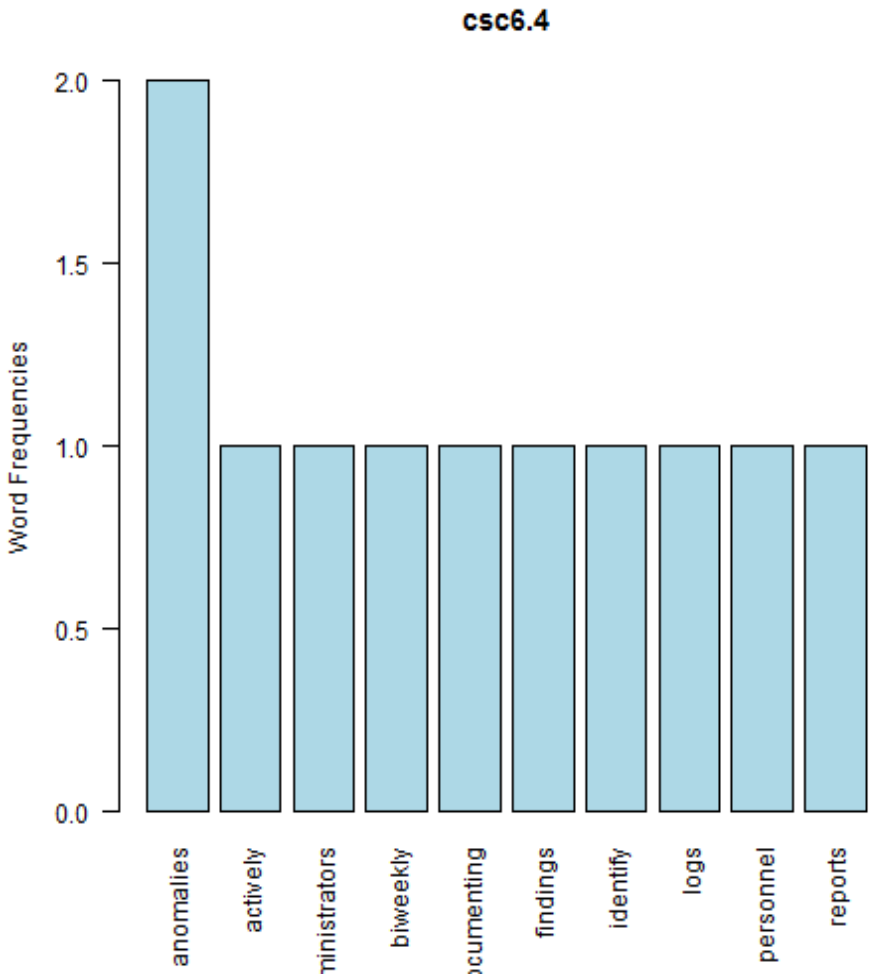


null device 1 [1] “Ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals. The logs must be archived and digitally signed on a periodic basis.”

CSC 6.4

[1] “anomalies + actively”

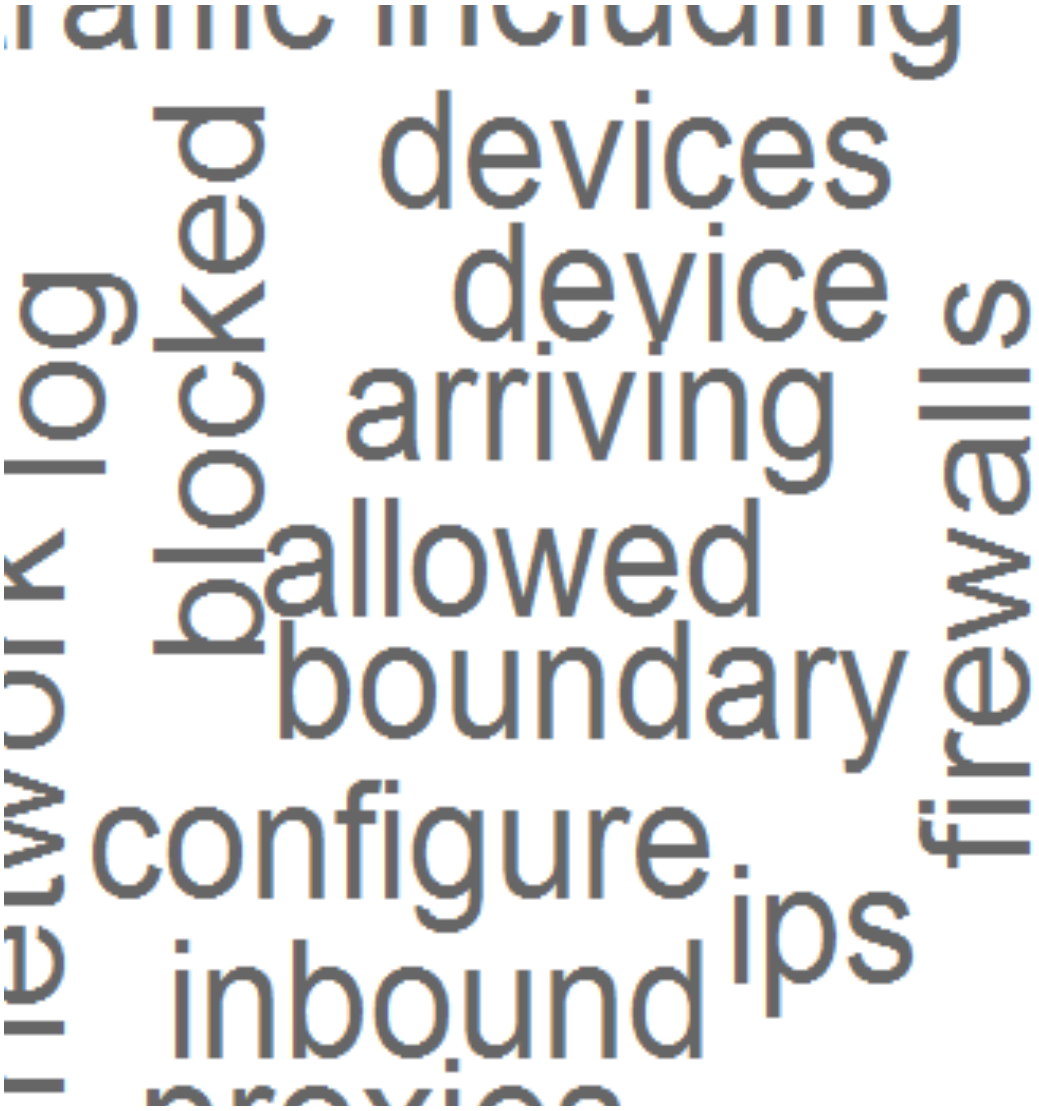
null device 1



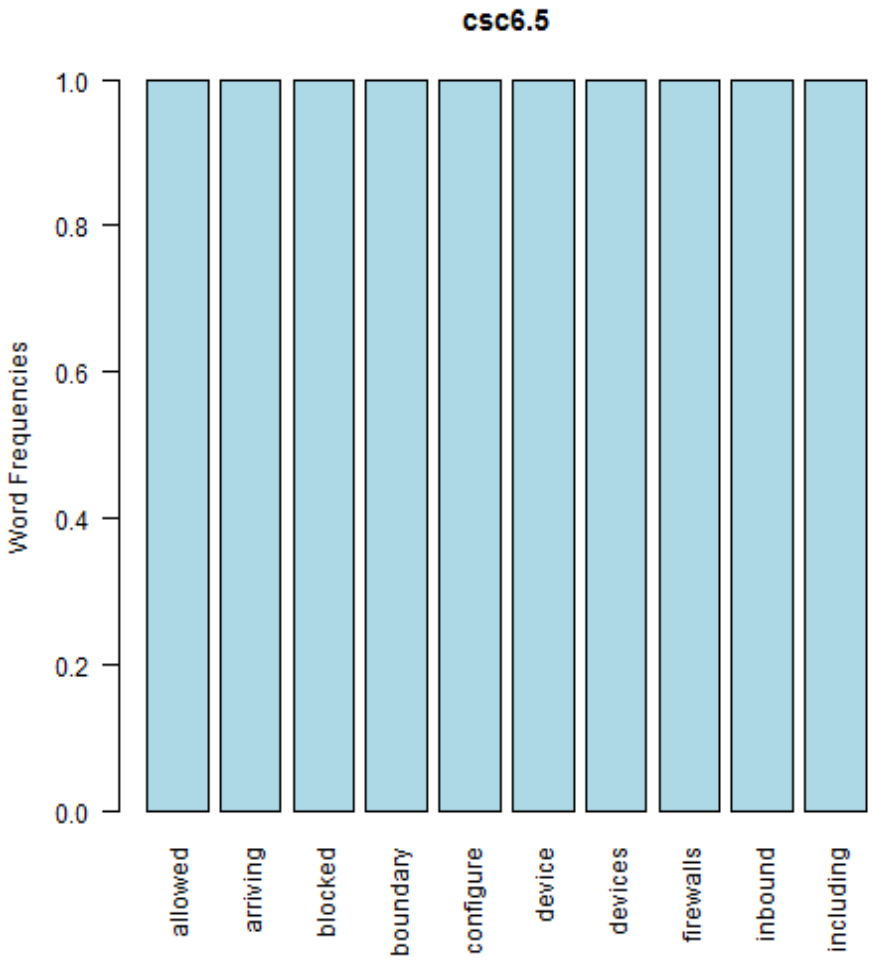
null device 1 [1] "Have security personnel and/or system administrators run biweekly reports that identify anomalies in logs. They should then actively review the anomalies, documenting their findings."

CSC 6.5

[1] “allowed + arriving”



null device 1

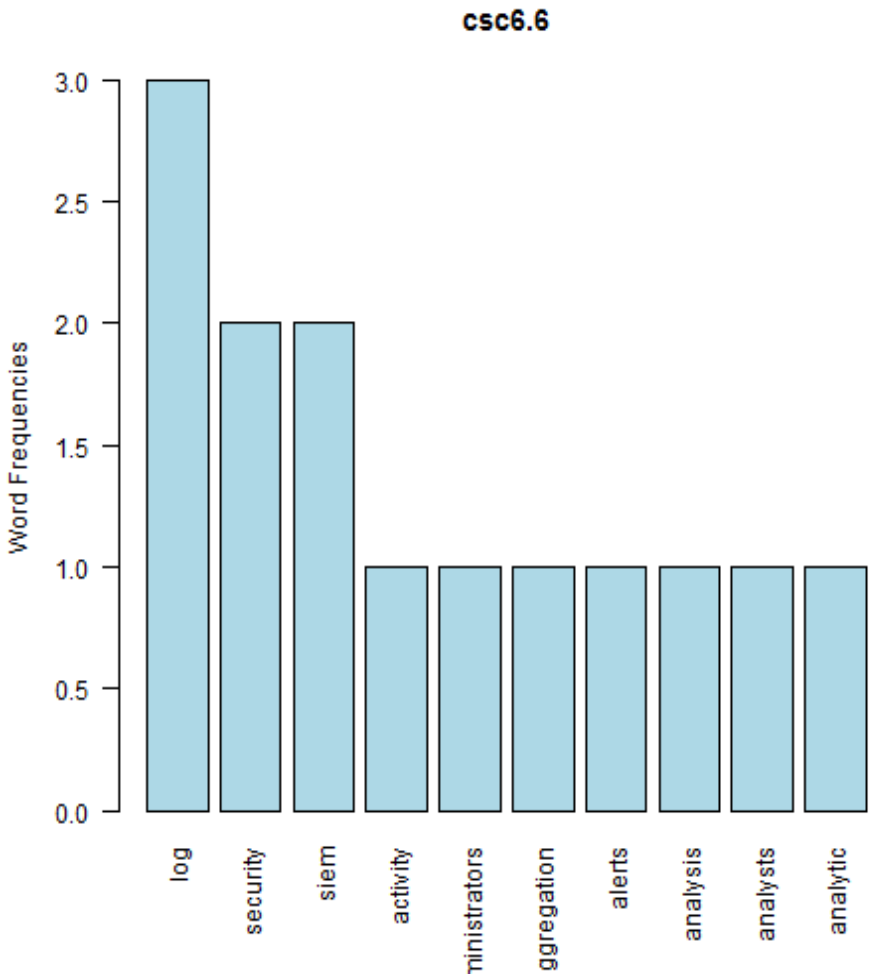


null device 1 [1] “Configure network boundary devices, including firewalls, network-based IPS, and inbound and outbound proxies, to verbosely log all traffic (both allowed and blocked) arriving at the device.”

CSC 6.6

[1] "log + security"

null device 1



null device 1 [1] “Deploy a SIEM (Security Information and Event Management) or log analytic tools for log aggregation and consolidation from multiple machines and for log correlation and analysis. Using the SIEM tool, system administrators and security personnel should devise profiles of common events from given systems so that they can tune detection to focus on unusual activity, avoid false positives, more rapidly identify anomalies, and prevent overwhelming analysts with insignificant alerts.”