CSC 9

John Ryan Zelling Analyst

Jan 2017

Contents

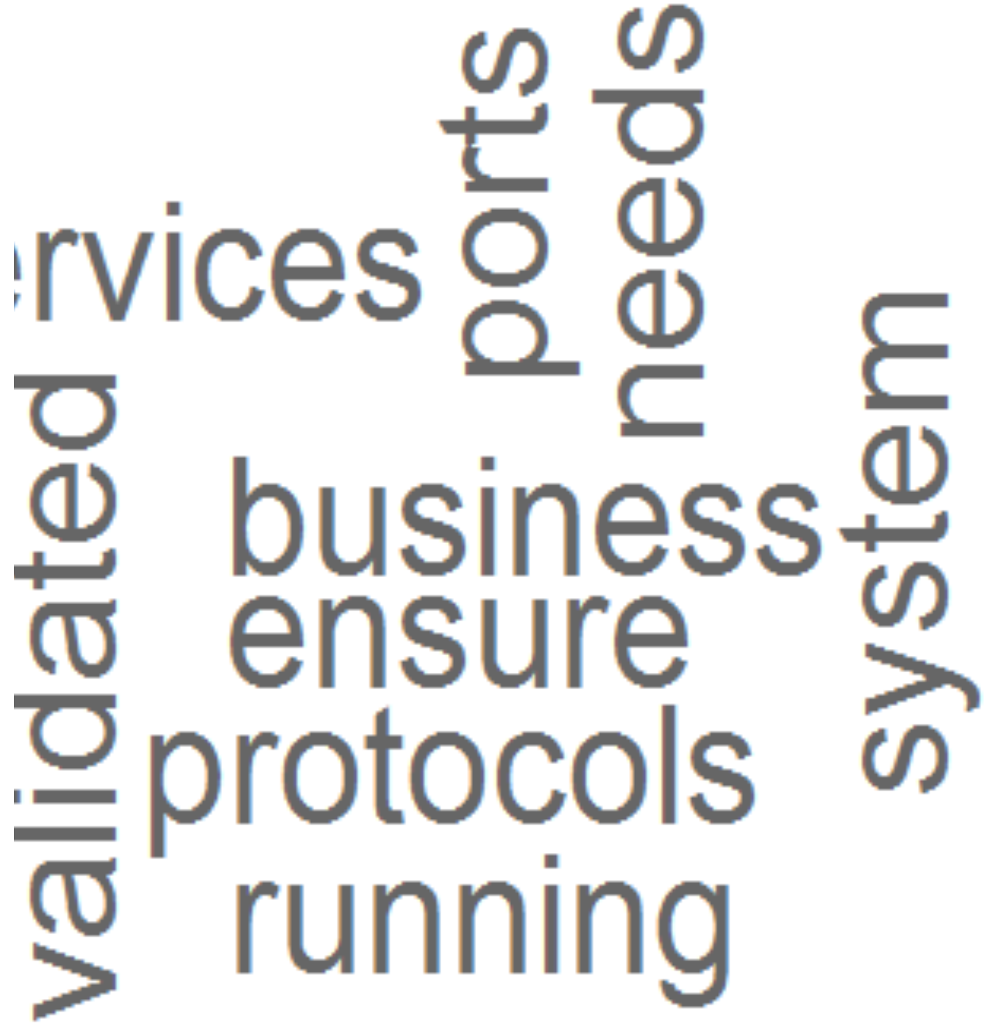
CSC 9.0

[1] “Critical Security Control #9: Limitation and Control of Network Ports”

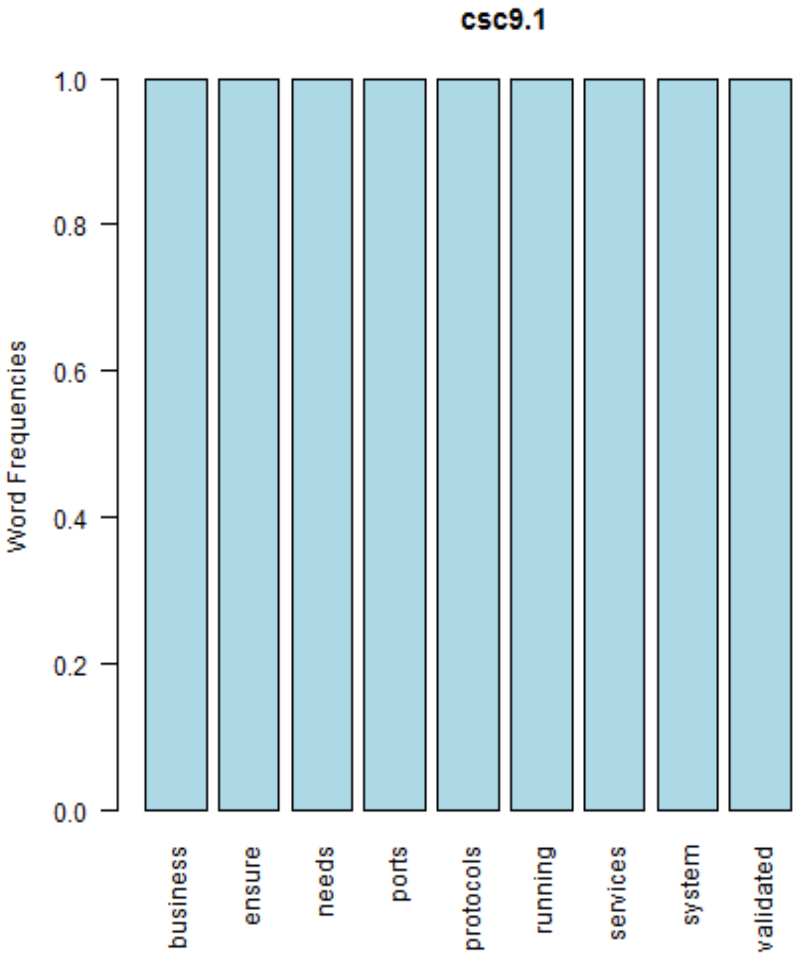
[1]

CSC 9.1

[1] "business + ensure"



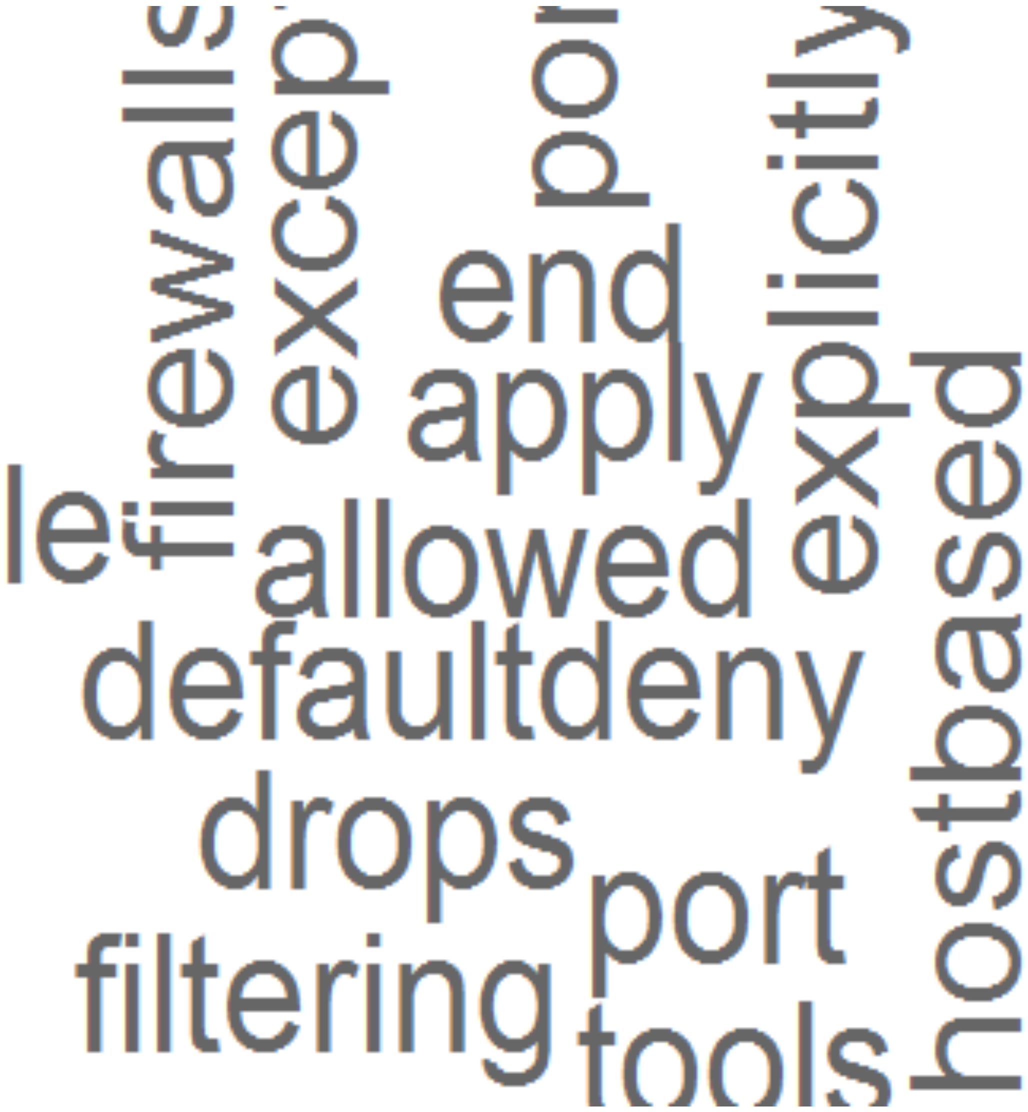
null device 1



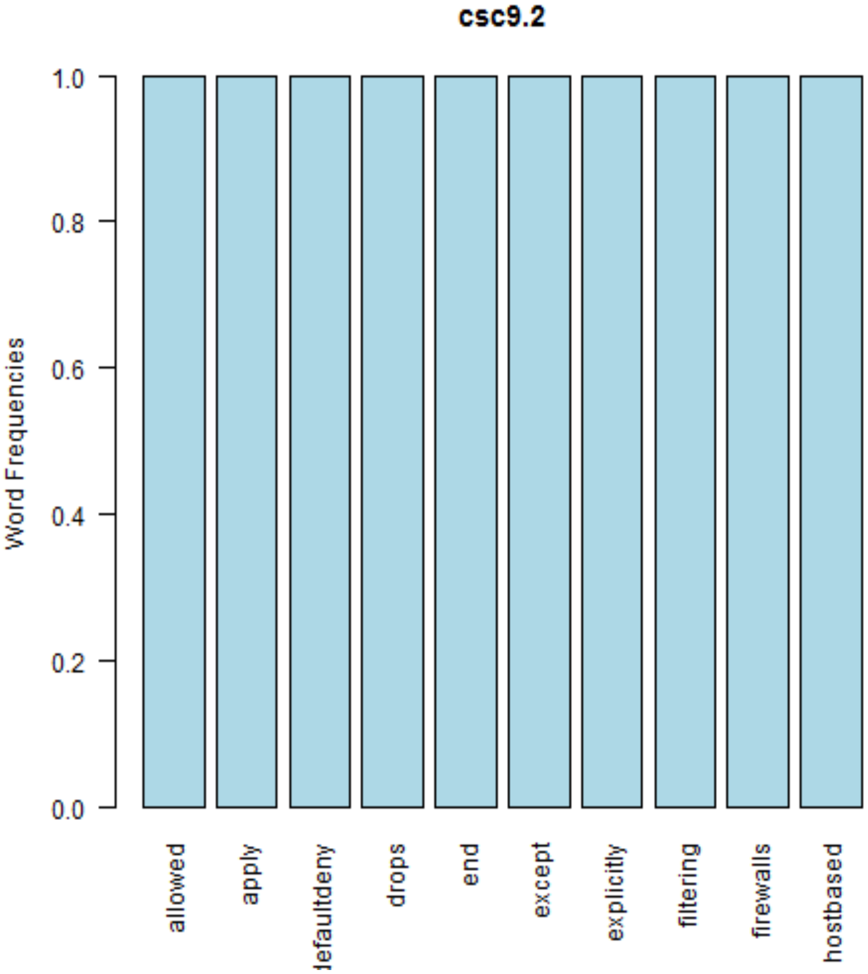
null device 1 [1] “Ensure that only ports, protocols, and services with validated business needs are running on each system.”

CSC 9.2

[1] “allowed + apply”



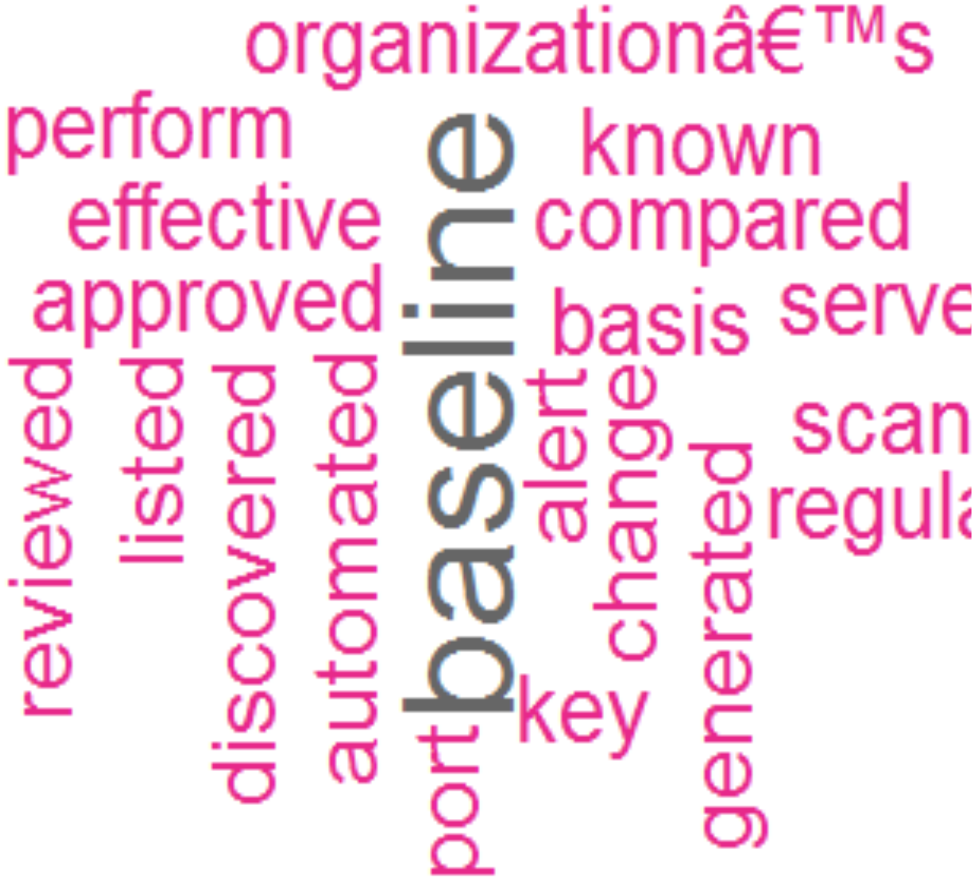
null device 1



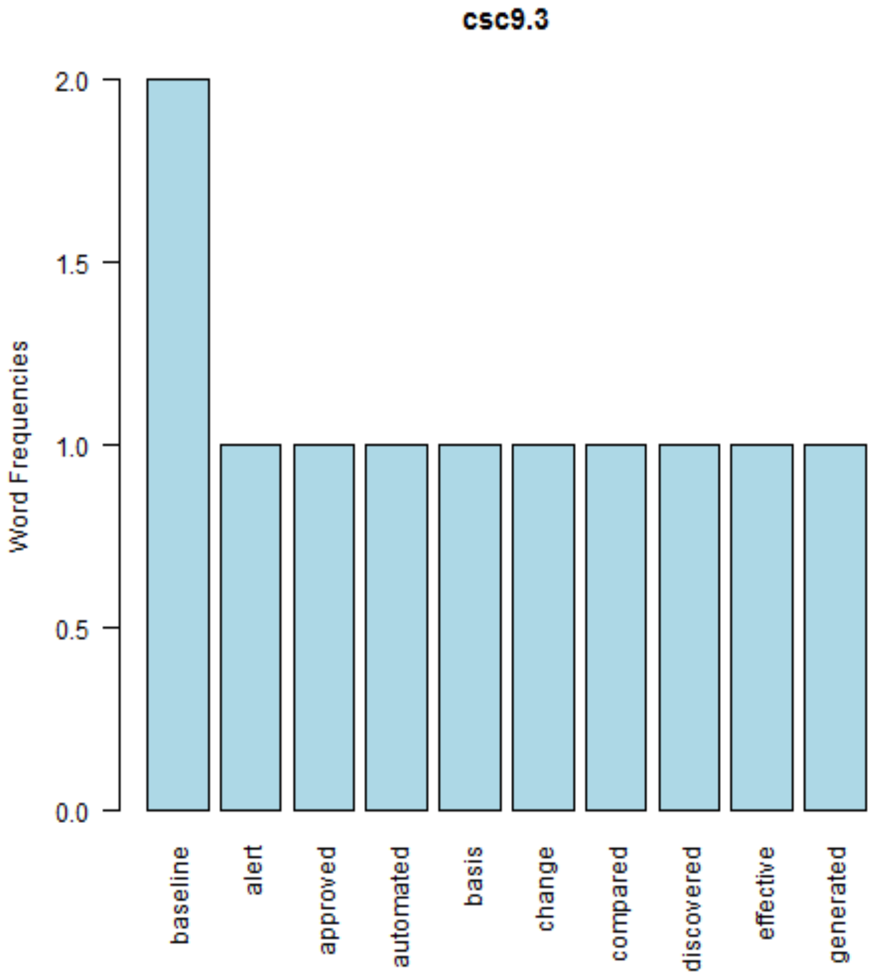
null device 1 [1] “Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.”

CSC 9.3

[1] “baseline + alert”



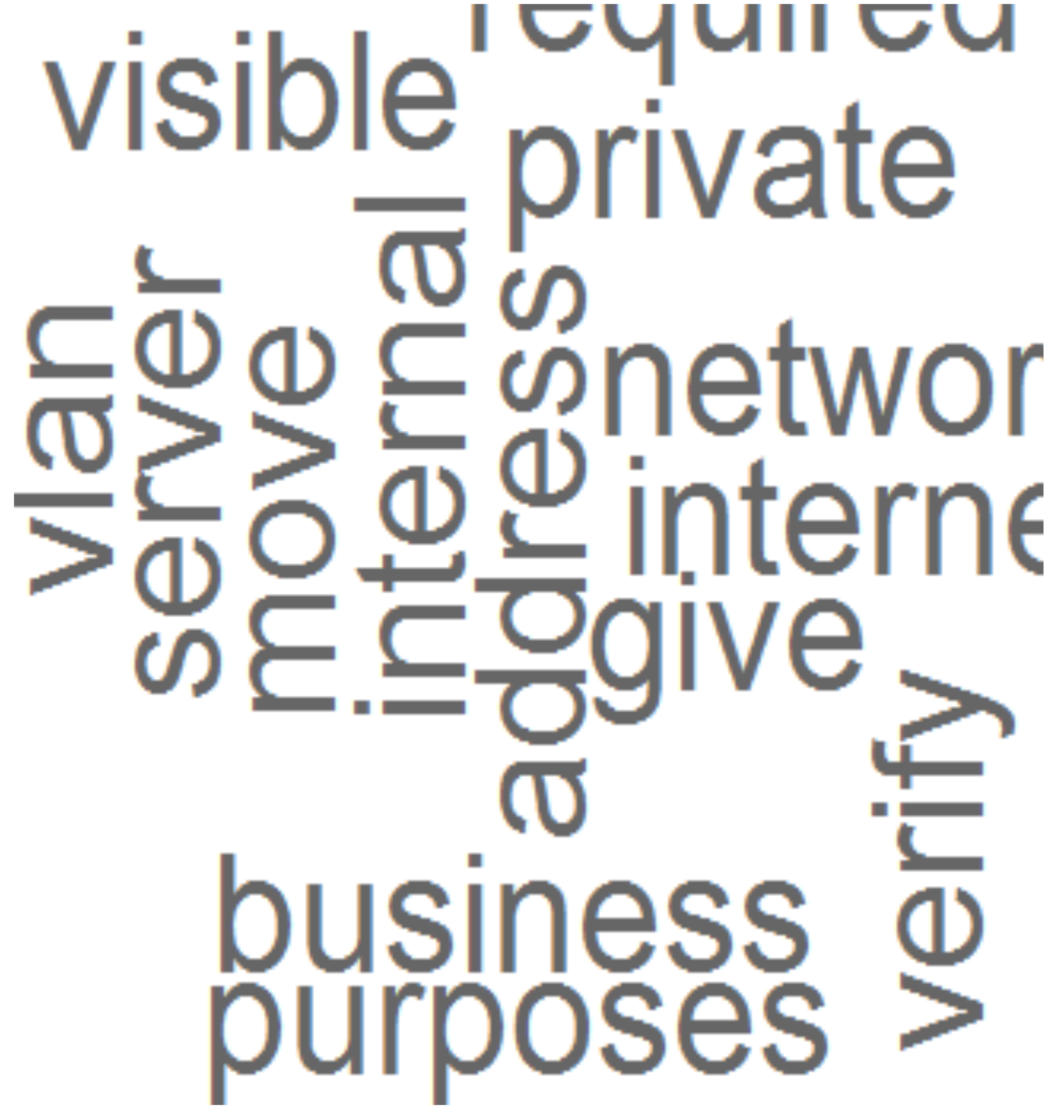
null device 1



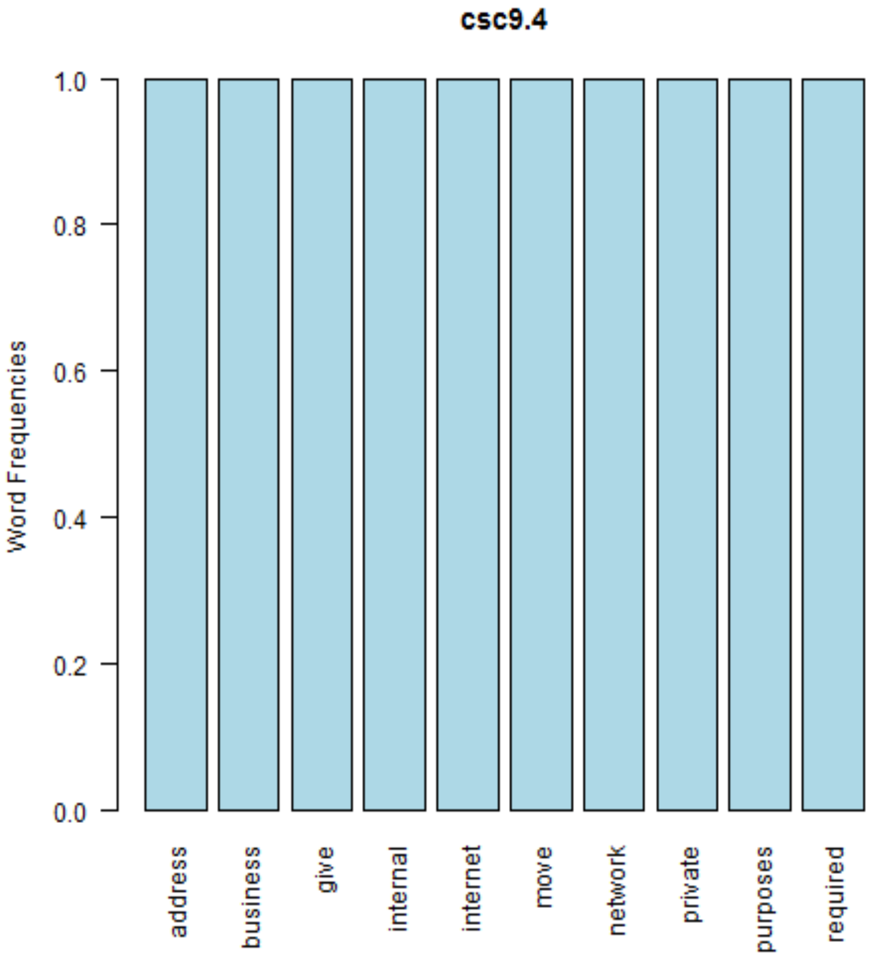
null device 1 [1] “Perform automated port scans on a regular basis against all key servers and compared to a known effective baseline. If a change that is not listed on the organizationâ s approved baseline is discovered, an alert should be generated and reviewed.”

CSC 9.4

[1] “address + business”



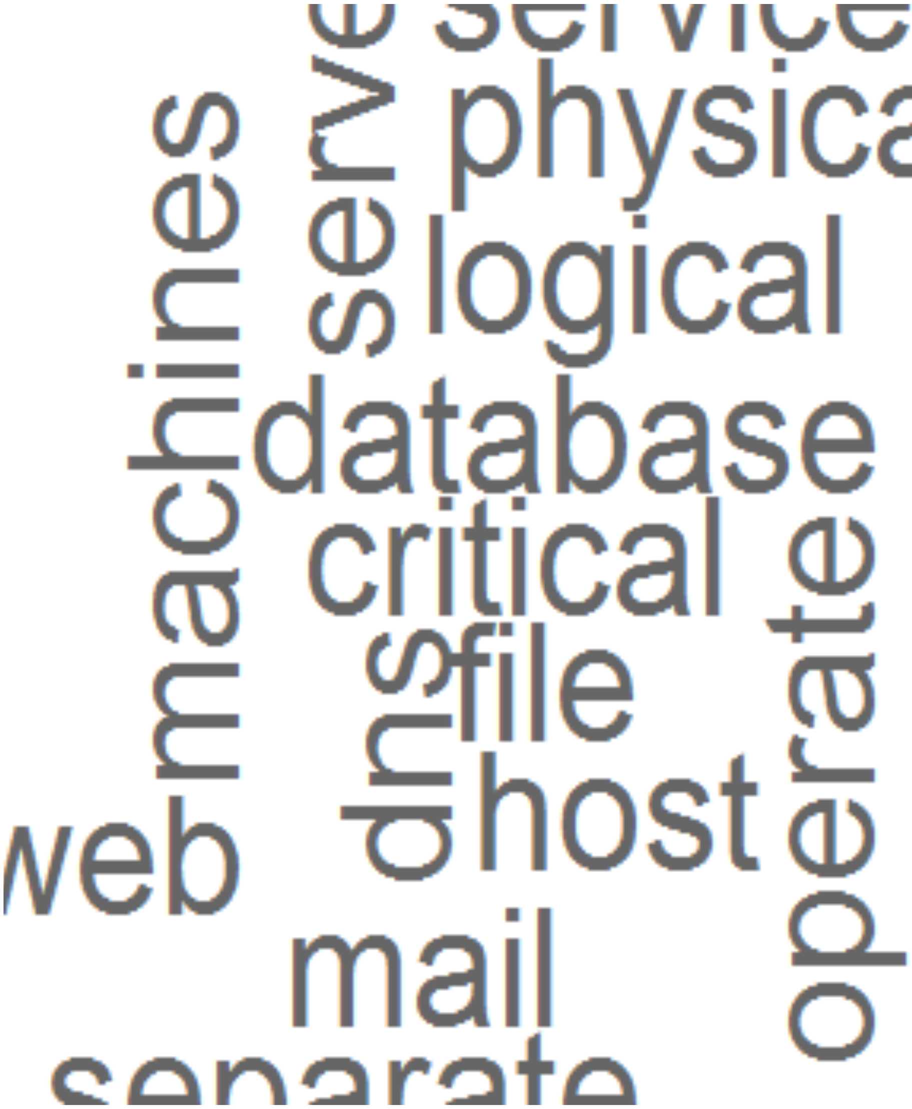
null device 1



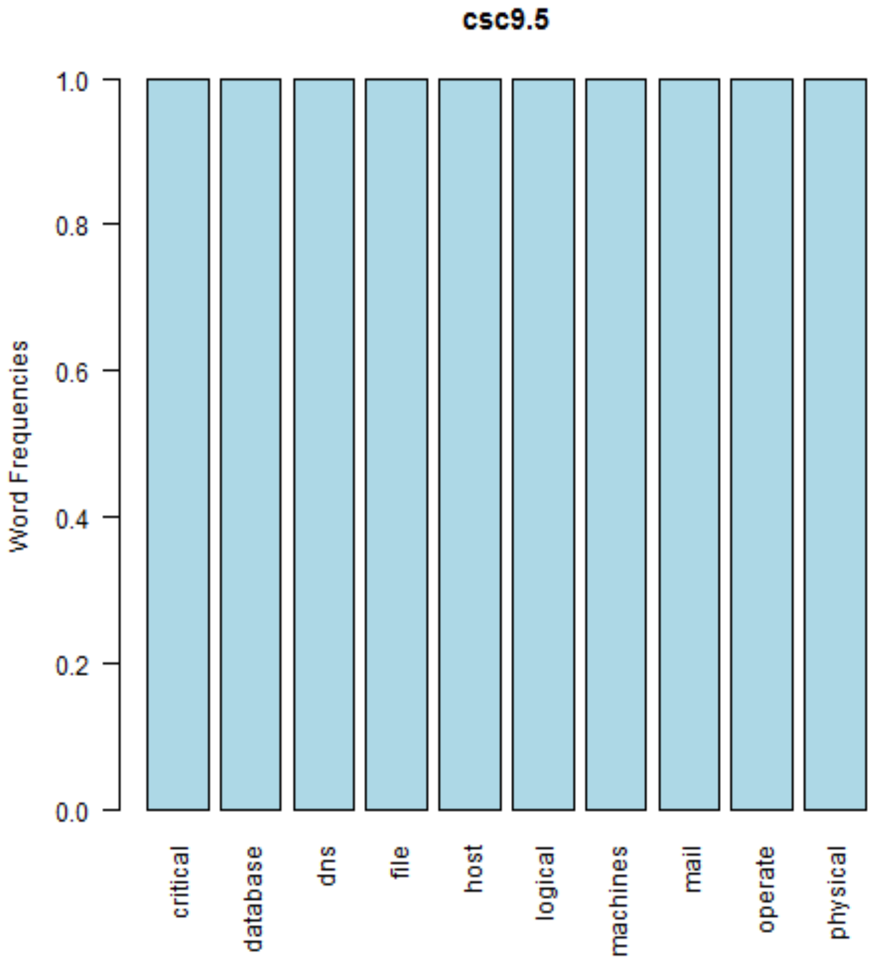
null device 1 [1] “Verify any server that is visible from the Internet or an untrusted network, and if it is not required for business purposes, move it to an internal VLAN and give it a private address.”

CSC 9.5

[1] "critical + database"



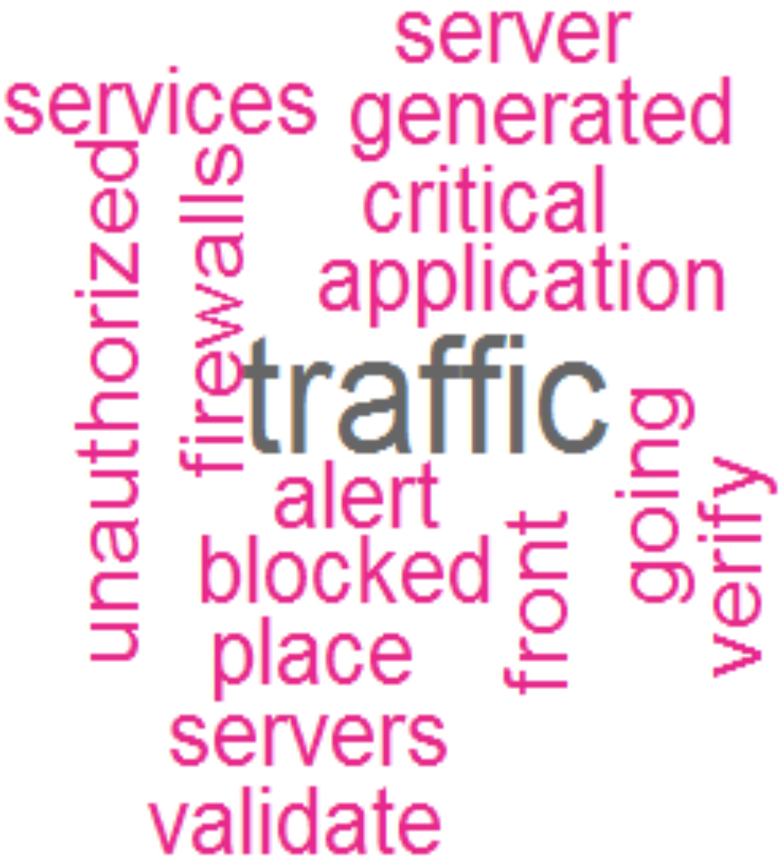
null device 1



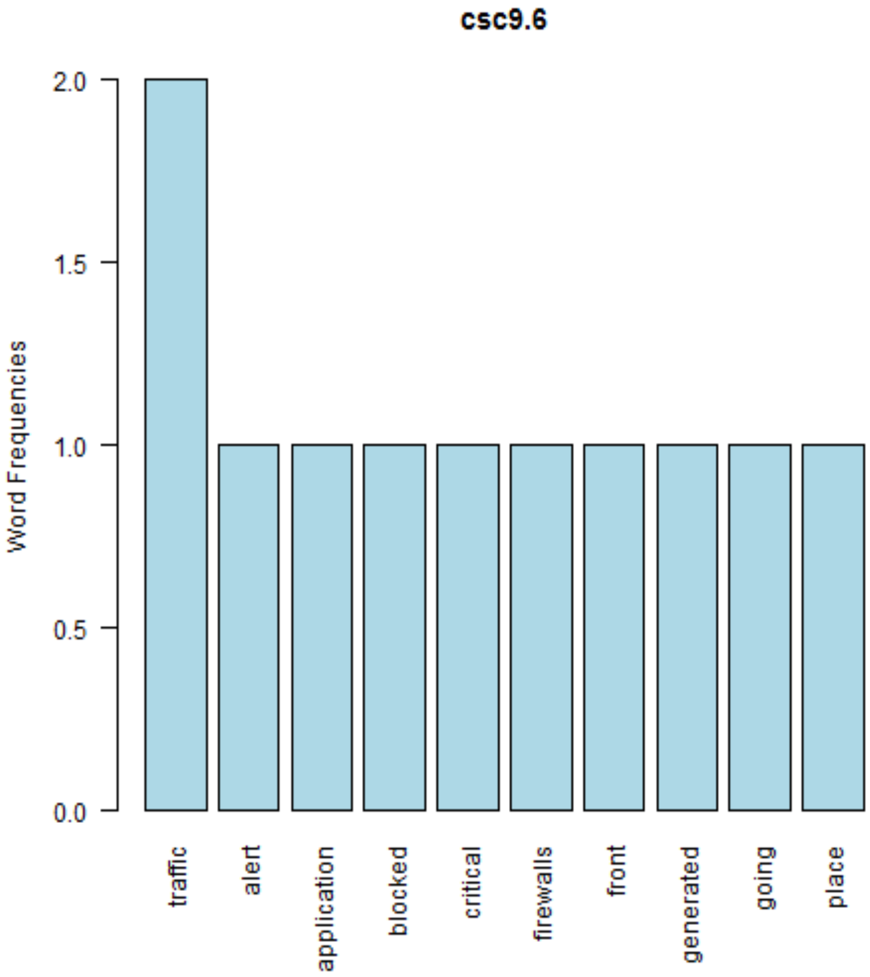
null device 1 [1] “Operate critical services on separate physical or logical host machines, such as DNS, file, mail, web, and database servers.”

CSC 9.6

```
[1] “traffic + alert”
```



```
null device 1
```



null device 1 [1] “Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized services or traffic should be blocked and an alert generated.”