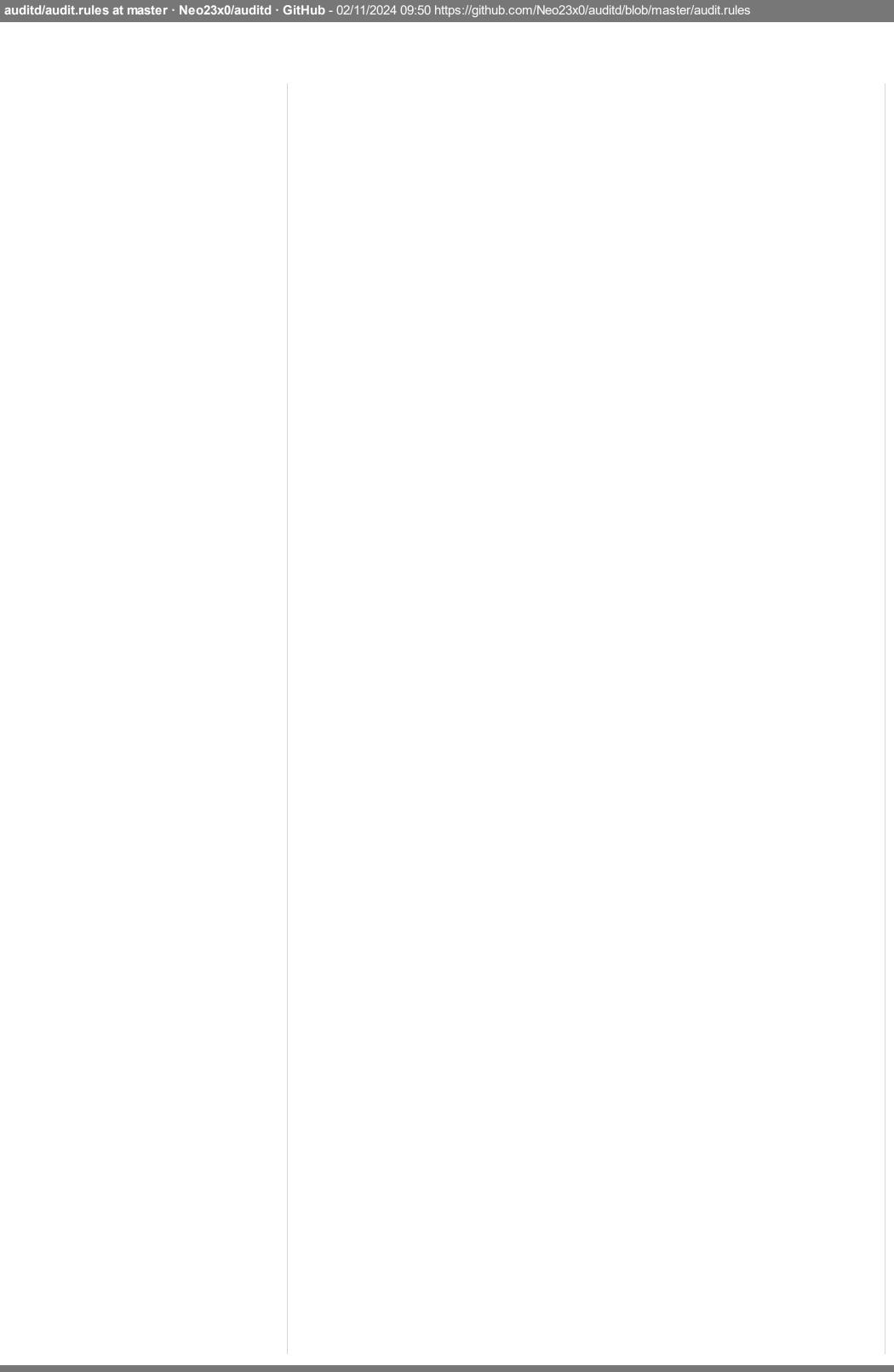
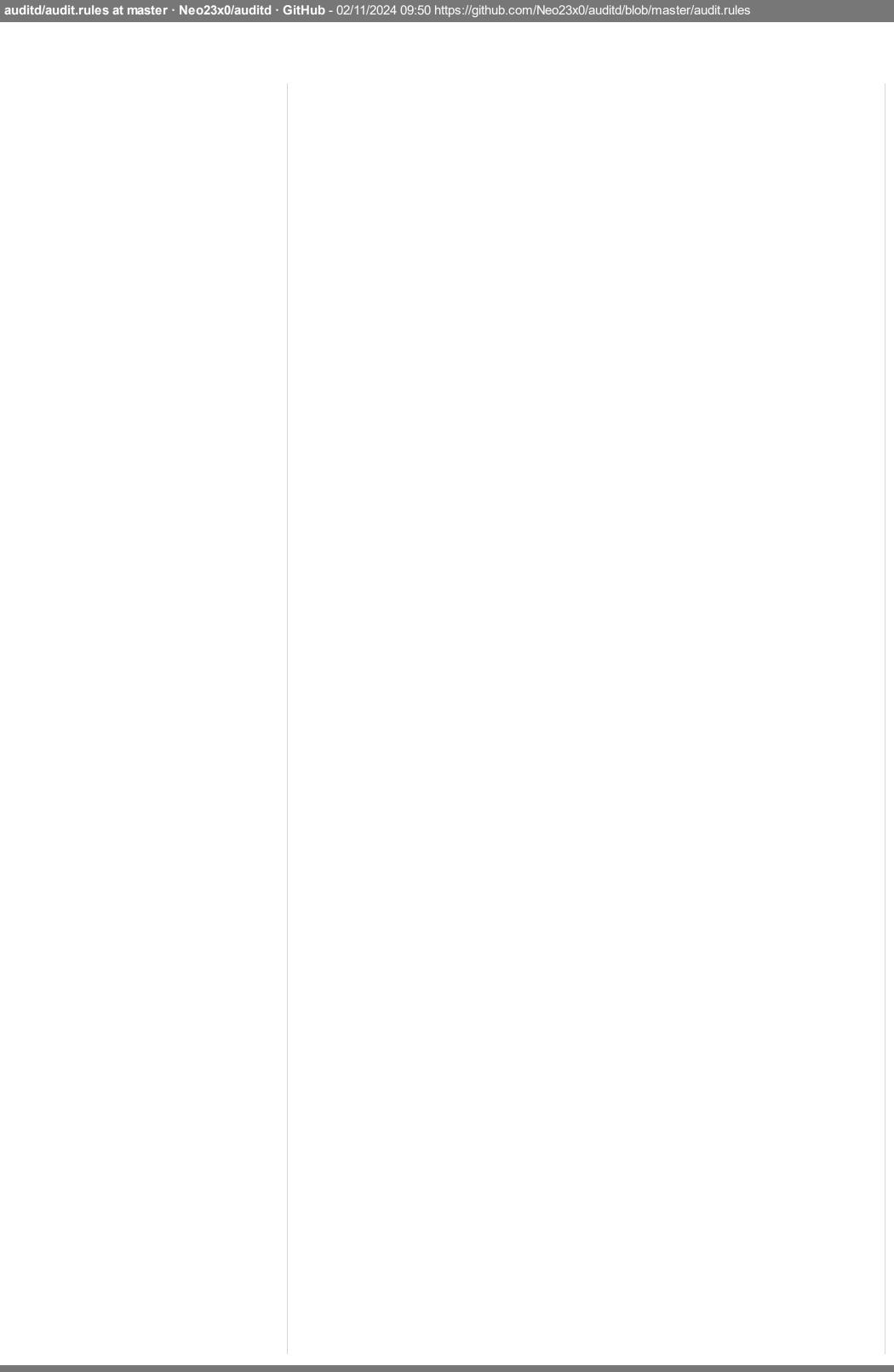
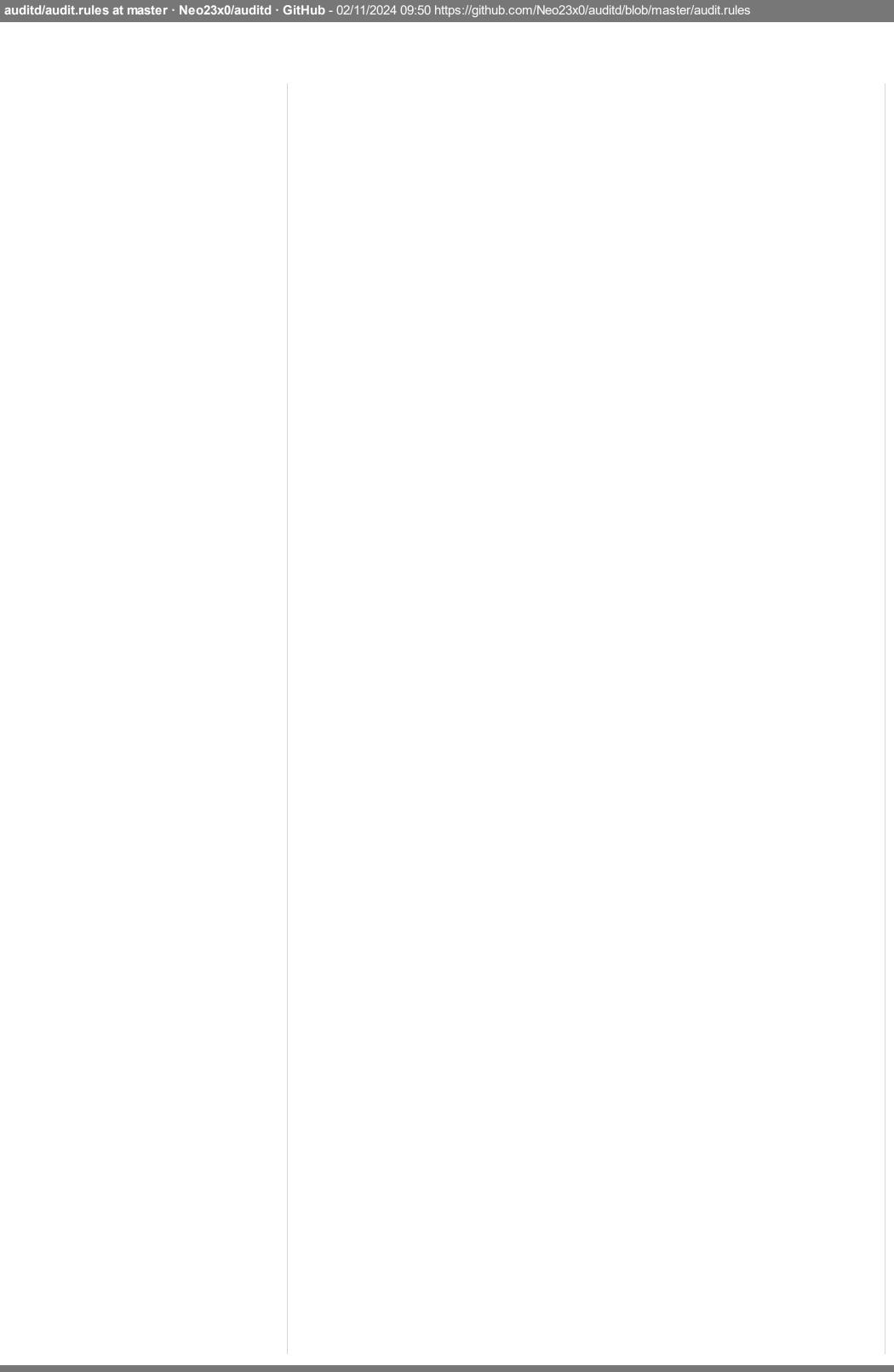


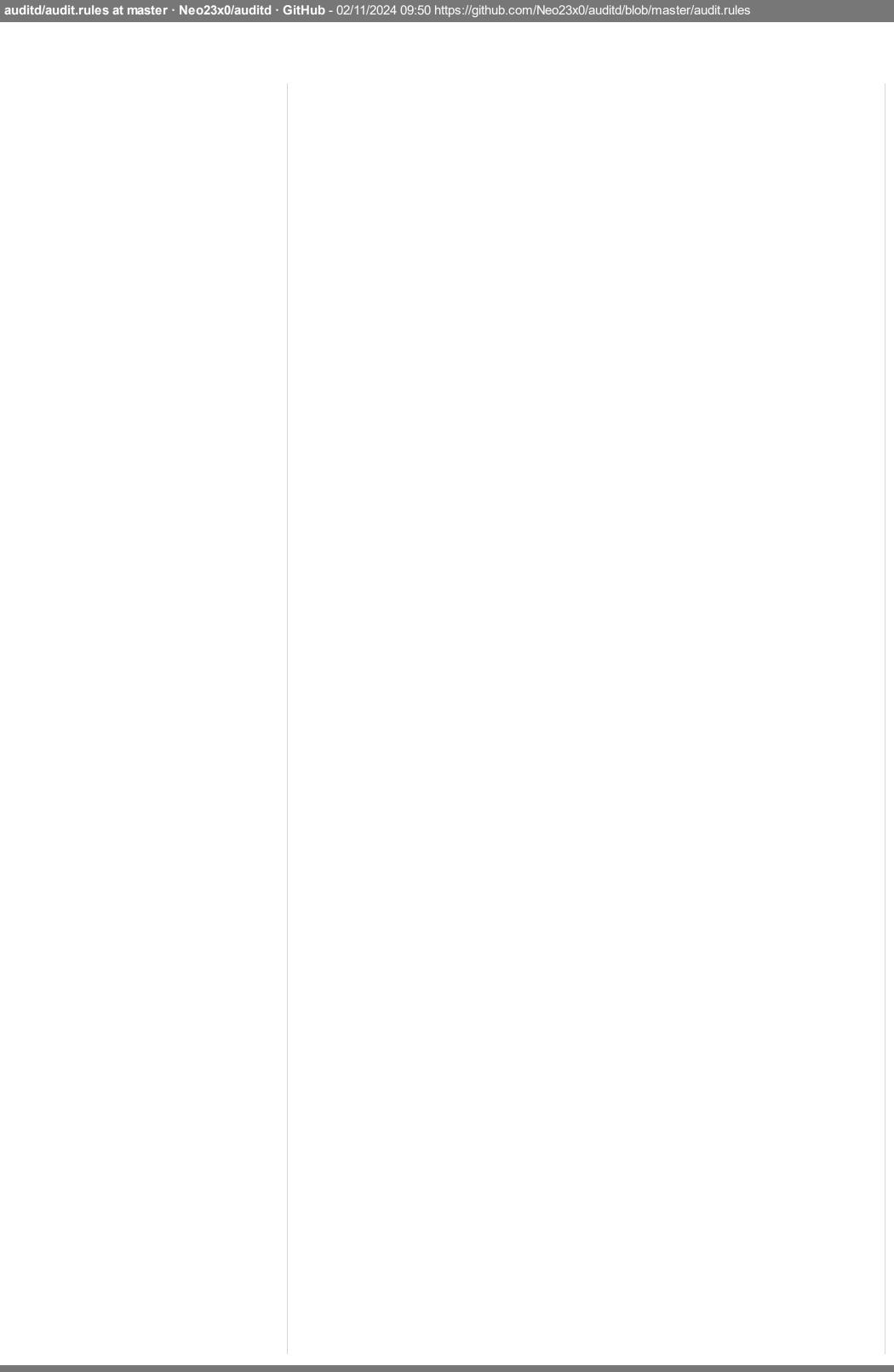
**J**/

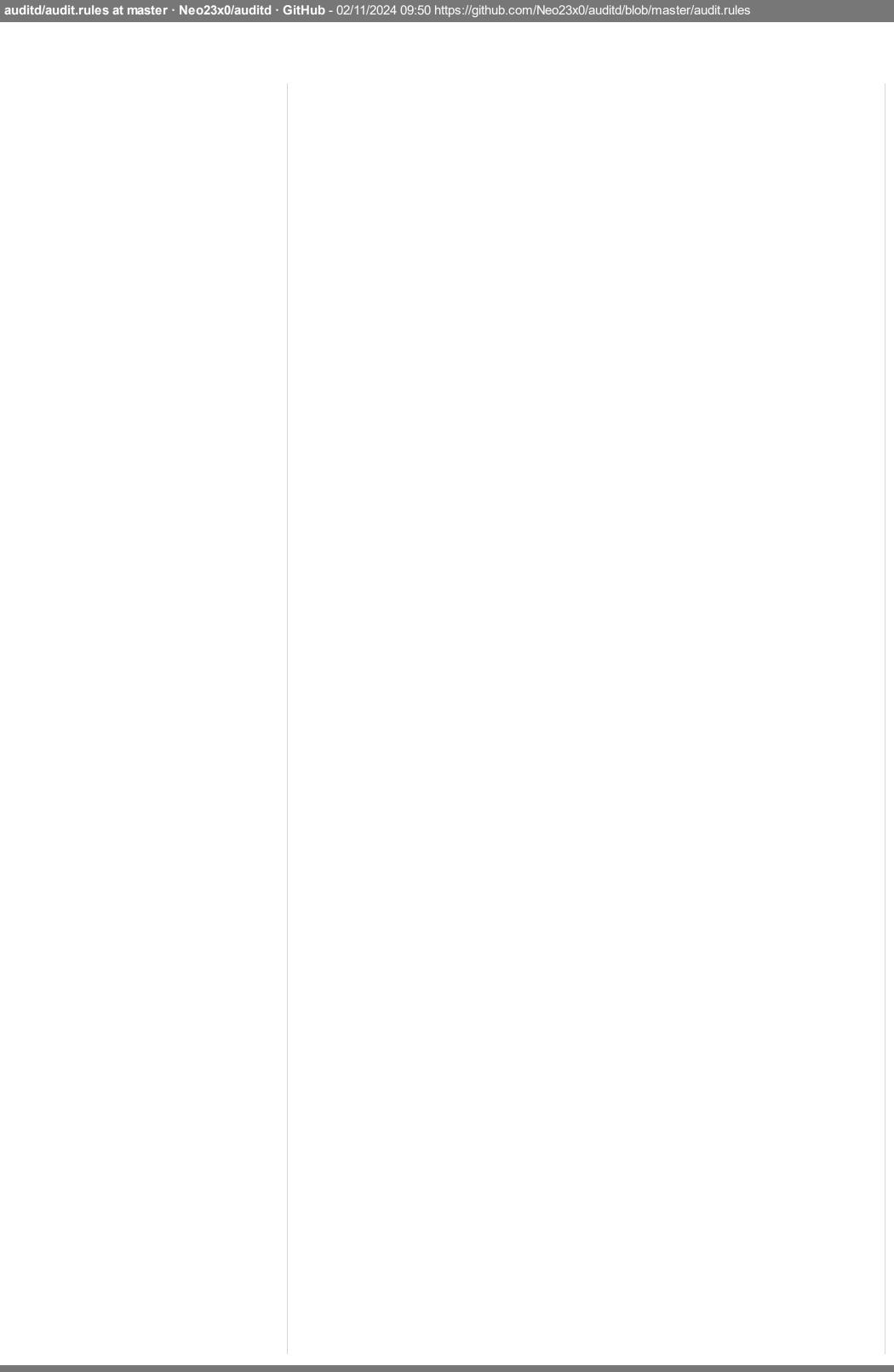
```
-m /erc/annish/ -h ma -k annishcomit
 58
        ## Monitor for use of audit management tools
 59
        -w /sbin/auditctl -p x -k audittools
 60
        -w /sbin/auditd -p x -k audittools
 61
        -w /usr/sbin/auditd -p x -k audittools
 62
        -w /usr/sbin/augenrules -p x -k audittools
 63
 64
        ## Access to all audit trails
 65
 66
        -a always, exit -F path=/usr/sbin/ausearch -F perm=x -k audittools
 67
        -a always, exit -F path=/usr/sbin/aureport -F perm=x -k audittools
 68
        -a always, exit -F path=/usr/sbin/aulast -F perm=x -k audittools
 69
        -a always,exit -F path=/usr/sbin/aulastlogin -F perm=x -k audittools
 70
        -a always, exit -F path=/usr/sbin/auvirt -F perm=x -k audittools
 71
 72
 73
 74
        ### We put these early because audit is a first match wins system.
 75
 76
 77
        ## Ignore current working directory records
        -a always, exclude -F msgtype=CWD
 78
 79
        ## Cron jobs fill the logs with stuff we normally don't want (works with SELinux)
 80
        -a never,user -F subj_type=crond_t
 81
        -a never,exit -F subj_type=crond_t
 82
 83
        ## This prevents chrony from overwhelming the logs
 84
        -a never, exit -F arch=b64 -S adjtimex -F auid=-1 -F uid=chrony -F subj_type=chronyd_t
 85
 86
        ## This is not very interesting and wastes a lot of space if the server is public facin
 87
        -a always,exclude -F msgtype=CRYPTO_KEY_USER
 88
 89
 90
        ## Open VM Tools
 91
        -a exit, never -F arch=b64 -S all -F exe=/usr/bin/vmtoolsd
 92
        ## High Volume Event Filter (especially on Linux Workstations)
 93
        -a never, exit -F arch=b32 -F dir=/dev/shm/ -F key=sharedmemaccess
 94
        -a never, exit -F arch=b64 -F dir=/dev/shm/ -F key=sharedmemaccess
 95
 96
        -a never, exit -F arch=b32 -F dir=/var/lock/lvm/ -F key=locklvm
 97
        -a never, exit -F arch=b64 -F dir=/var/lock/lvm/ -F key=locklvm
 98
 99
        ## Filebeat
100
        ### https://www.elastic.co/guide/en/beats/filebeat/current/directory-layout.html
101
102
        -a never,exit -F arch=b32 -F path=/opt/filebeat -F perm=wa -F key=filebeat
103
        -a never,exit -F arch=b64 -F path=/opt/filebeat -F perm=wa -F key=filebeat
104
105
        -a always,exit -F arch=b32 -F dir=/etc/filebeat/ -F perm=wa -F key=filebeat
106
        -a always,exit -F arch=b64 -F dir=/etc/filebeat/ -F perm=wa -F key=filebeat
107
108
        -a always,exit -F arch=b32 -F dir=/usr/share/filebeat/ -F perm=wa -F key=filebeat
109
        -a always,exit -F arch=b64 -F dir=/usr/share/filebeat/ -F perm=wa -F key=filebeat
110
111
        -a always,exit -F arch=b64 -F dir=/usr/share/filebeat/bin/ -F perm=x -F key=filebeat
112
        -a always,exit -F arch=b32 -F dir=/usr/share/filebeat/bin/ -F perm=x -F key=filebeat
113
114
115
        #### https://www.elastic.co/guide/en/beats/filebeat/7.17/directory-layout.html
116
        -a always,exit -F arch=b32 -F path=/usr/local/var/homebrew/linked/filebeat-full -F perm
117
        -a always,exit -F arch=b64 -F path=/usr/local/var/homebrew/linked/filebeat-full -F perm
118
```

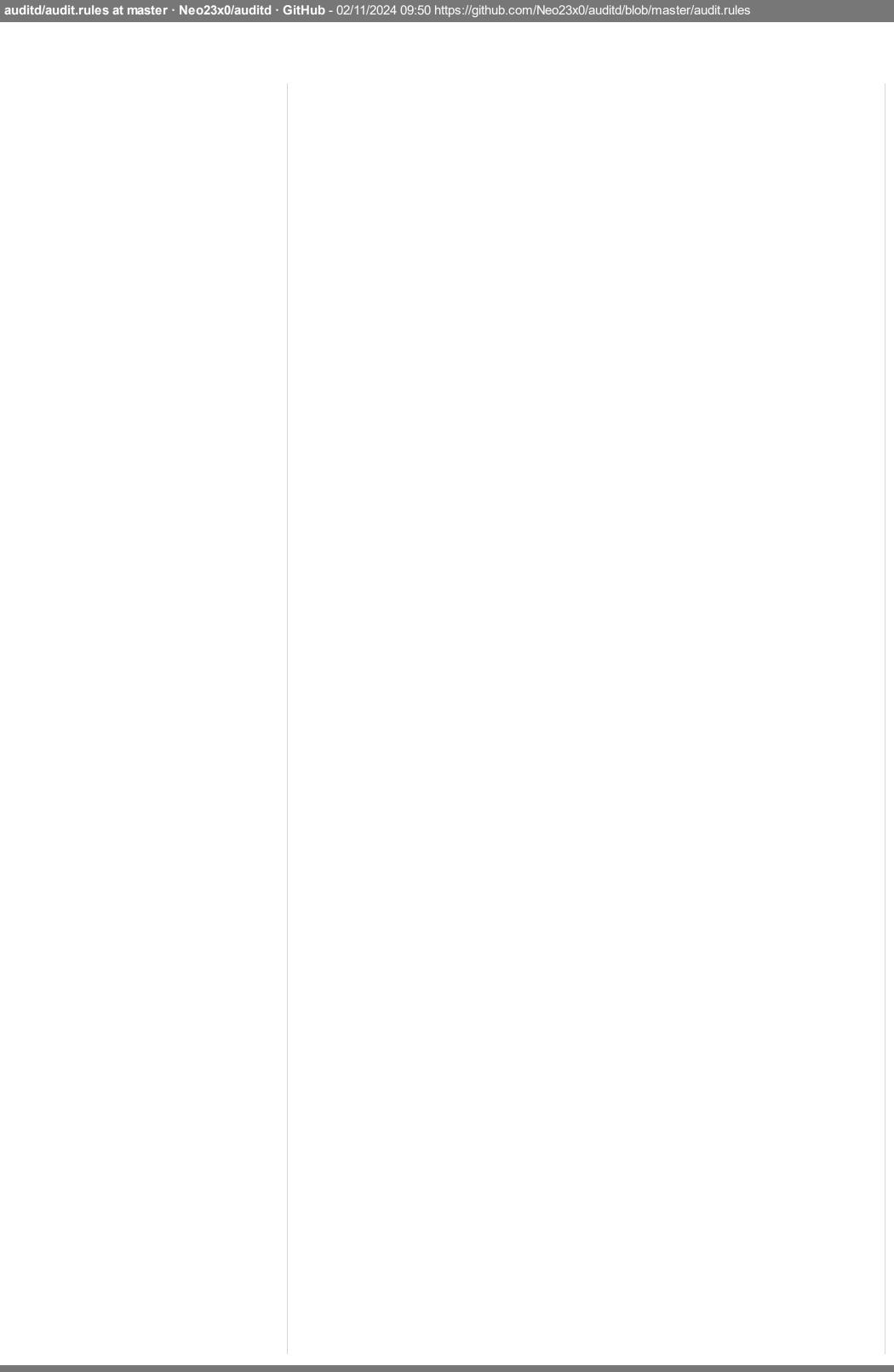


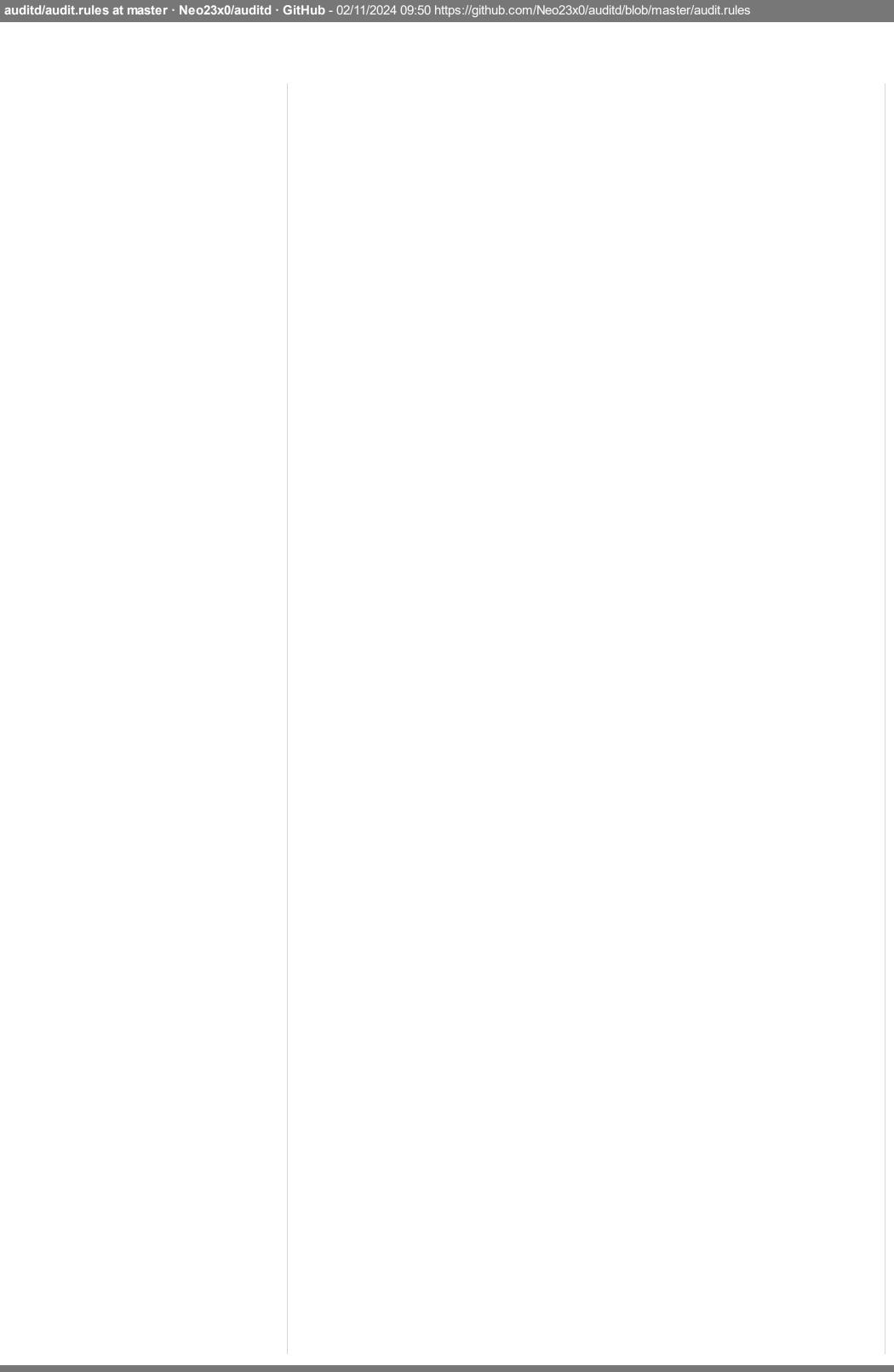


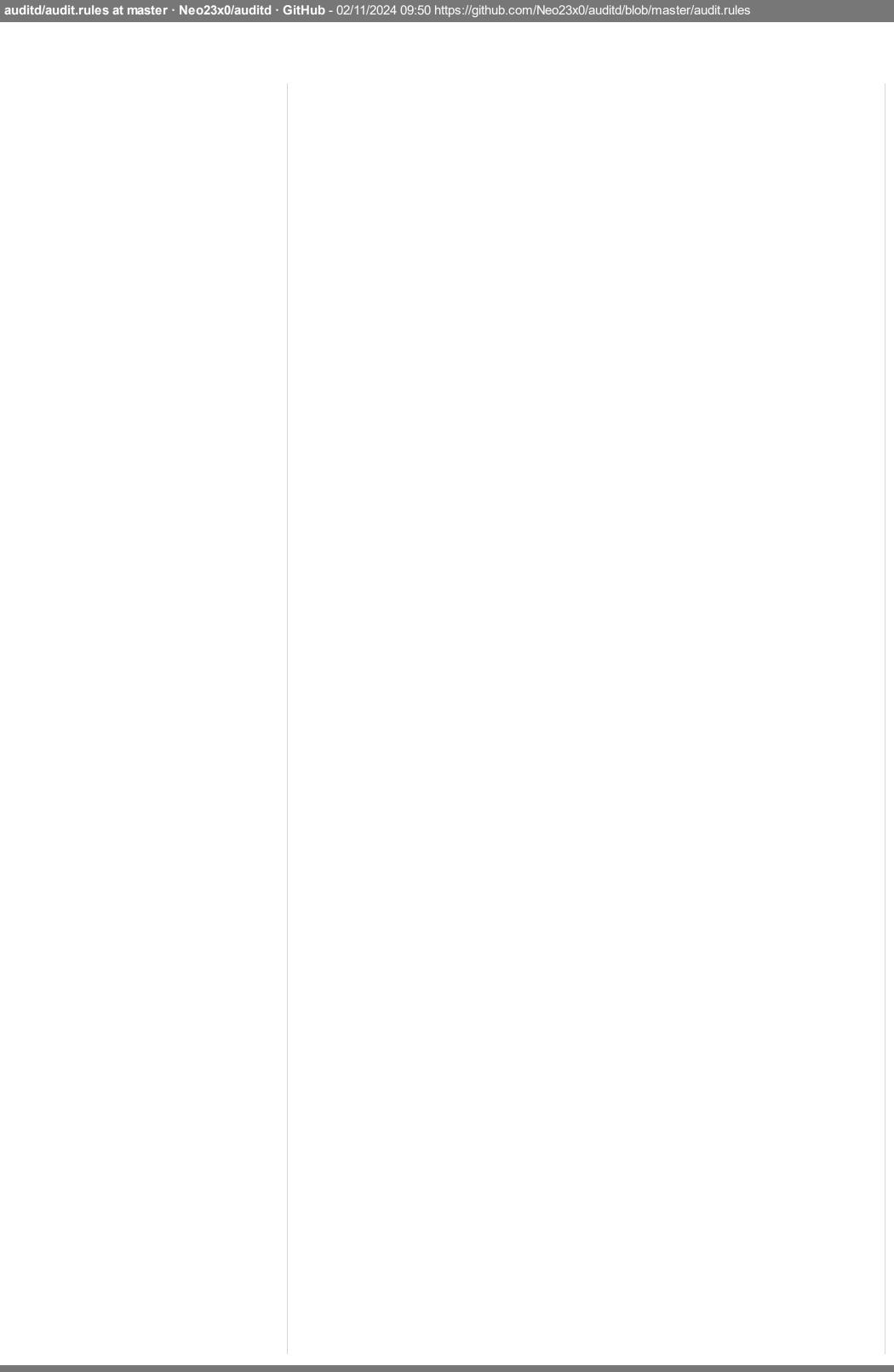












```
745
        # ipc system call
        # /usr/include/linux/ipc.h
746
747
        ## msgctl
748
        #-a always,exit -S ipc -F a0=14 -k Inter-Process_Communication
749
750
        #-a always,exit -S ipc -F a0=13 -k Inter-Process_Communication
751
        ## Use these lines on x86_64, ia64 instead
752
        -a always, exit -F arch=b64 -S msgctl -k Inter-Process_Communication
753
        -a always, exit -F arch=b64 -S msgget -k Inter-Process_Communication
754
755
        ## semctl
756
        #-a always, exit -S ipc -F a0=3 -k Inter-Process Communication
757
758
        #-a always, exit -S ipc -F a0=2 -k Inter-Process_Communication
759
760
        #-a always,exit -S ipc -F a0=1 -k Inter-Process_Communication
761
        ## semtimedop
762
        #-a always,exit -S ipc -F a0=4 -k Inter-Process_Communication
763
        ## Use these lines on x86_64, ia64 instead
764
        -a always, exit -F arch=b64 -S semctl -k Inter-Process_Communication
765
        -a always, exit -F arch=b64 -S semget -k Inter-Process_Communication
766
        -a always, exit -F arch=b64 -S semop -k Inter-Process_Communication
767
        -a always, exit -F arch=b64 -S semtimedop -k Inter-Process_Communication
768
769
        ## shmctl
770
        #-a always,exit -S ipc -F a0=24 -k Inter-Process_Communication
771
772
        #-a always, exit -S ipc -F a0=23 -k Inter-Process_Communication
773
        ## Use these lines on x86_64, ia64 instead
774
        -a always, exit -F arch=b64 -S shmctl -k Inter-Process_Communication
775
        -a always, exit -F arch=b64 -S shmget -k Inter-Process_Communication
776
777
        # High Volume Events -----
778
779
        ## Disable these rules if they create too many events in your environment
780
781
        ## Common Shells
782
        -w /bin/bash -p x -k susp_shell
783
        -w /bin/dash -p x -k susp_shell
784
        -w /bin/busybox -p x -k susp_shell
785
        -w /bin/zsh -p x -k susp_shell
786
        -w /bin/sh -p x -k susp_shell
787
        -w /bin/ksh -p x -k susp shell
788
789
        ## Root command executions
790
        -a always,exit -F arch=b64 -F euid=0 -F auid>=1000 -F auid!=-1 -S execve -k rootcmd
791
792
        ## File Deletion Events by User
793
        -a always,exit -F arch=b64 -S rmdir -S unlink -S unlinkat -S rename -S renameat -F auid
794
795
        ## File Access
796
        ### Unauthorized Access (unsuccessful)
797
        -a always,exit -F arch=b64 -S creat -S open -S openat -S open_by_handle_at -S truncate
798
        -a always,exit -F arch=b64 -S creat -S open -S openat -S open_by_handle_at -S truncate
799
800
        ### Unsuccessful Creation
801
        -a always,exit -F arch=b64 -S mkdir,creat,link,symlink,mknod,mknodat,linkat,symlinkat -
802
         a always avit E anch-h64 C mydin link symlink mydinat E avit- EDEDM k fila spaatia
opo
```

```
-a always,exic -r anchebo4 -s mkuin,iiik,symiink,mkuinac -r exic--crchh -k lite_cheacid
CUO
804
805
       ### Unsuccessful Modification
806
       -a always,exit -F arch=b64 -S rename -S renameat -S truncate -S chmod -S setxattr -S ls
807
       -a always,exit -F arch=b64 -S rename -S renameat -S truncate -S chmod -S setxattr -S ls
808
809
       ## 32bit API Exploitation
810
       ### If you are on a 64 bit platform, everything _should_ be running
811
       ### in 64 bit mode. This rule will detect any use of the 32 bit syscalls
812
       \#\#\# because this might be a sign of someone exploiting a hole in the 32
813
       ### bit API.
814
       -a always, exit -F arch=b32 -S all -k 32bit_api
815
816
       # Make The Configuration Immutable ------
817
818
       ##-e 2
```