```
# ignore errors
-i
# delete all rules
-D
# for busy systems
-b 8192
# capabilities, xattr, time change
-a always,exit -F arch=b32 -S capset -k pt_siem_api_caps
-a always,exit -F arch=b64 -S capset -k pt_siem_api_caps
-a always,exit -F arch=b32 -S setxattr,lsetxattr,fsetxattr -k pt_siem_api_xattr
-a always,exit -F arch=b64 -S setxattr,lsetxattr,fsetxattr -k pt_siem_api_xattr
-a always,exit -F arch=b32 -S settimeofday,adjtimex,clock_settime -k
pt_siem_api_time
-a always,exit -F arch=b64 -S adjtimex,settimeofday,clock_settime -k
pt_siem_api_time
# file monitoring
-a always,exit -S all -F path=/etc/shadow -F perm=r -F auid!=-1 -k
pt_siem_etc_read
-a always,exit -S all -F path=/etc/sudoers -F perm=r -F auid!=-1 -k
pt_siem_etc_read
-a always,exit -S all -F dir=/etc/sudoers.d -F perm=r -F auid!=-1 -k
pt_siem_etc_read
-a always,exit -S all -F path=/etc/passwd -F perm=r -F auid!=-1 -k
pt_siem_etc_read
-a always,exit -S all -F path=/etc/group -F perm=r -F auid!=-1 -k
pt_siem_etc_read
-a always,exit -S all -F path=/etc/security/opasswd -F perm=r -F auid!=-1 -k
pt_siem_etc_read
-a always,exit -S all -F dir=/var/log -F perm=rwa -F auid!=-1 -k
pt_siem_var_log_access
-w /etc -p wa -k pt_siem_etc_modify
-w /home -p rwa -k pt_siem_home_access
-w /root -p rwa -k pt_siem_home_access
-w /var/www -p rwa -k pt_siem_home_access
-w /var/spool/cron -p wa -k pt_siem_cron_modify
-w /var/spool/at -p wa -k pt_siem_cron_modify
-w /bin -p wa -k pt_siem_bin_modify
-w /usr/bin -p wa -k pt_siem_bin_modify
-w /sbin -p wa -k pt_siem_bin_modify
-w /usr/sbin -p wa -k pt_siem_bin_modify
-w /usr/local/bin -p wa -k pt_siem_bin_modify
-w /usr/local/sbin -p wa -k pt_siem_bin_modify
-w /usr/libexec -p wa -k pt_siem_bin_modify
-w /lib -p wa -k pt_siem_lib_modify
-w /lib64 -p wa -k pt_siem_lib_modify
-w /usr/lib -p wa -k pt_siem_lib_modify
-w /usr/lib64 -p wa -k pt_siem_lib_modify
-w /boot -p wa -k pt_siem_boot_modify
-w /var/www -p wa -k pt_siem_www_modify
# exclude bins
-a never,exit -F exe=/usr/bin/vmtoolsd
-a never,exit -F exe=/usr/sbin/haproxy
-a never,exit -F exe=/usr/sbin/cron
-a never,exit -F exe=/lib/systemd/systemd-timesyncd
```

```
-a never,exit -F exe=/lib/systemd/systemd-logind
-a never,exit -F exe=/usr/lib/systemd/systemd-timesyncd
-a never,exit -F exe=/usr/lib/systemd/systemd-logind
# network activities
-a always,exit -F arch=b32 -S socket -F a0=0x2 -k pt_siem_api_socket
-a always,exit -F arch=b64 -S socket -F a0=0x2 -k pt_siem_api_socket
-a always,exit -F arch=b32 -S socket -F a0=0xA -k pt_siem_api_socket
-a always,exit -F arch=b64 -S socket -F a0=0xA -k pt_siem_api_socket
-a always,exit -F arch=b32 -S socket -F a0=0x11 -k pt_siem_api_socket
-a always,exit -F arch=b64 -S socket -F a0=0x11 -k pt_siem_api_socket
-a always,exit -F arch=b32 -S connect -F a2=0x10 -k pt_siem_api_connect
-a always,exit -F arch=b64 -S connect -F a2=0x10 -k pt_siem_api_connect
-a always,exit -F arch=b32 -S connect -F a2=0x1C -k pt_siem_api_connect
-a always,exit -F arch=b64 -S connect -F a2=0x1C -k pt_siem_api_connect
-a always,exit -F arch=b32 -S accept4 -k pt_siem_api_accept
-a always,exit -F arch=b64 -S accept4 -k pt_siem_api_accept
-a always,exit -F arch=b64 -S accept -k pt_siem_api_accept
-a always,exit -F arch=b32 -S listen -k pt_siem_api_listen
-a always,exit -F arch=b64 -S listen -k pt_siem_api_listen
# execute
-a always,exit -F arch=b32 -S execve -F euid>0 -F euid<<UID_MIN> -F
key=pt_siem_execve_daemon
-a always,exit -F arch=b32 -S execveat -F euid>0 -F euid<<UID_MIN> -F
key=pt_siem_execve_daemon
-a always,exit -F arch=b64 -S execve -F euid>0 -F euid<<UID_MIN> -F
key=pt_siem_execve_daemon
-a always,exit -F arch=b64 -S execveat -F euid>0 -F euid<<UID_MIN> -F
key=pt_siem_execve_daemon
-a always,exit -F arch=b32 -S execve -k pt_siem_execve
-a always,exit -F arch=b32 -S execveat -k pt_siem_execve
-a always,exit -F arch=b64 -S execve -k pt_siem_execve
-a always,exit -F arch=b64 -S execveat -k pt_siem_execve
# kernel modules, process trace, special permissions
-a always,exit -F arch=b32 -S init_module,delete_module -F auid!=-1 -k
pt_siem_api_kernel_mods
-a always,exit -F arch=b32 -S finit_module -F auid!=-1 -k
pt_siem_api_kernel_mods
-a always,exit -F arch=b64 -S init_module,delete_module -F auid!=-1 -k
pt_siem_api_kernel_mods
-a always,exit -F arch=b64 -S finit_module -F auid!=-1 -k
pt_siem_api_kernel_mods
-a always,exit -F arch=b32 -S ptrace -k pt_siem_api_ptrace
-a always,exit -F arch=b64 -S ptrace -k pt_siem_api_ptrace
-a always,exit -F arch=b32 -S setuid,setgid,setreuid,setregid -k
pt_siem_api_setuid
-a always,exit -F arch=b64 -S setuid,setgid,setreuid,setregid -k
pt_siem_api_setuid
```