```
# Invalid SSH Login Attempts
watchfor /(: [iI]nvalid [uU]ser )(.*)( from )(.*)$/
        threshold track_by=$4, type=limit, count=10, seconds=600
        mail=monitoring,subject=SSH dictionary attack

watchfor /(: [fF]ailed password for )(.*)( from )(.*)( port )(.*)$/
        threshold track_by=$4, type=limit, count=10, seconds=600
        mail=monitoring,subject=SSH brute force attempt

# Cisco config
watchfor /SYS-5-CONFIG_I: Configured from (.*) by (.*) on (.*) (\(.*\))$/
        mail=monitoring,subject=Router config by $2 from $4

# Denied AXFRs
watchfor /client ([0-9.:]+)\D\d+: zone transfer '(.*)\/.XFR\/IN' denied$/
        mail=monitoring,subject=Denied AXFR for zone '$2' from $1
        throttle threshold=3,delay=0:1:0,key=$1
        threshold track_by=$1, type=limit, count=10, seconds=600

# Portscan and/or sensitive port attempts
watchfor /SEC-6-IPACCESSLOGP: list \d+ (permitted|denied) (tcp|udp) ([a-fA-F0-
9.:]+)\((\d+)\) -> ([a-fA-F0-9.:]+)\((\d+)\), \d+ packet/
        mail=monitoring,subject=Attempt to connect to $2/$5:$6 from $3:$4
        threshold track_by=$3, type=limit, count=10, seconds=600
```