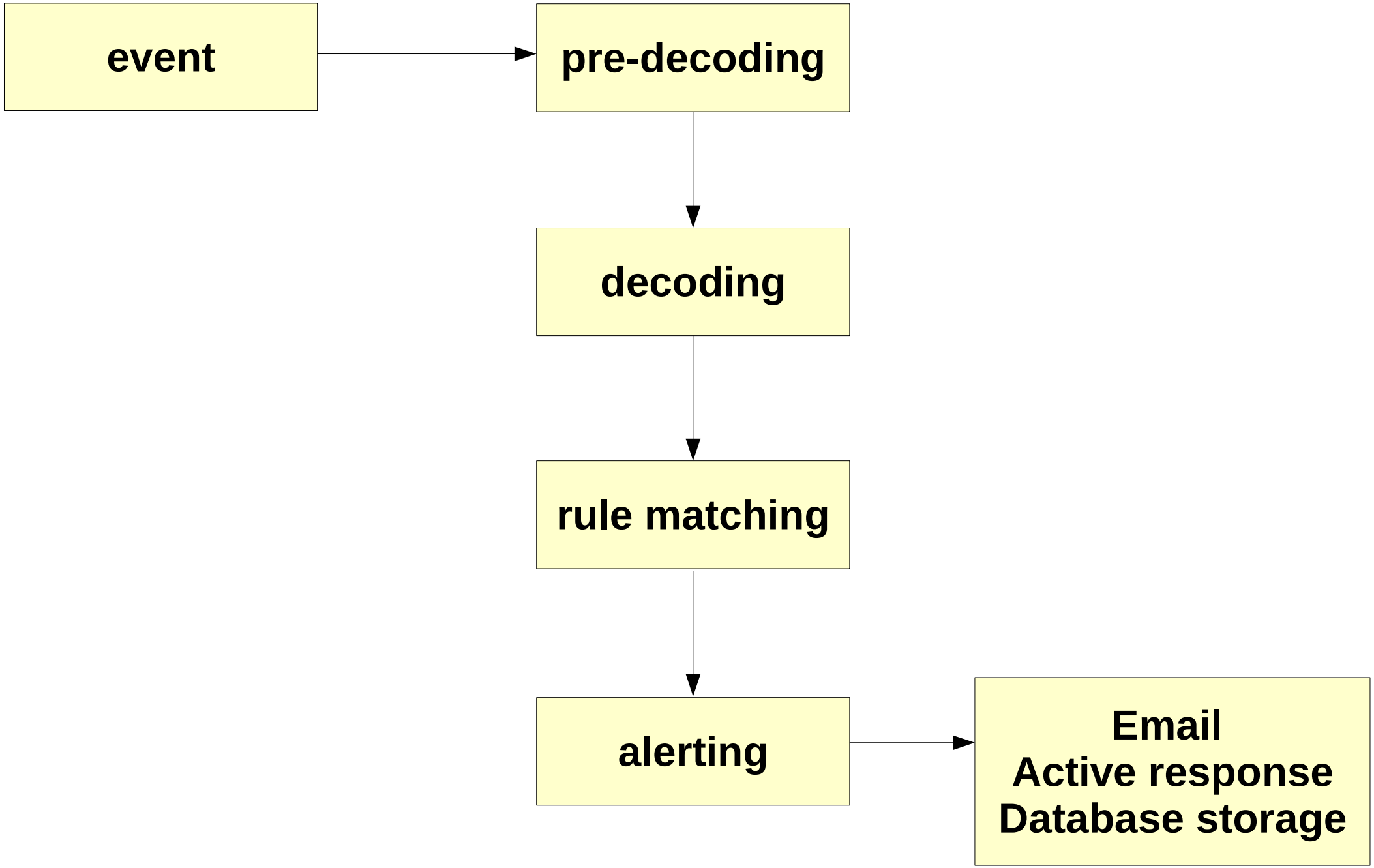

event
pre-decoding
decoding
rule matching
alerting
Email
Active response
Database storage

pre-decoding

Pre-decoded fields:

hostname
program_name
log
time/date

decoding

Decoders' options:

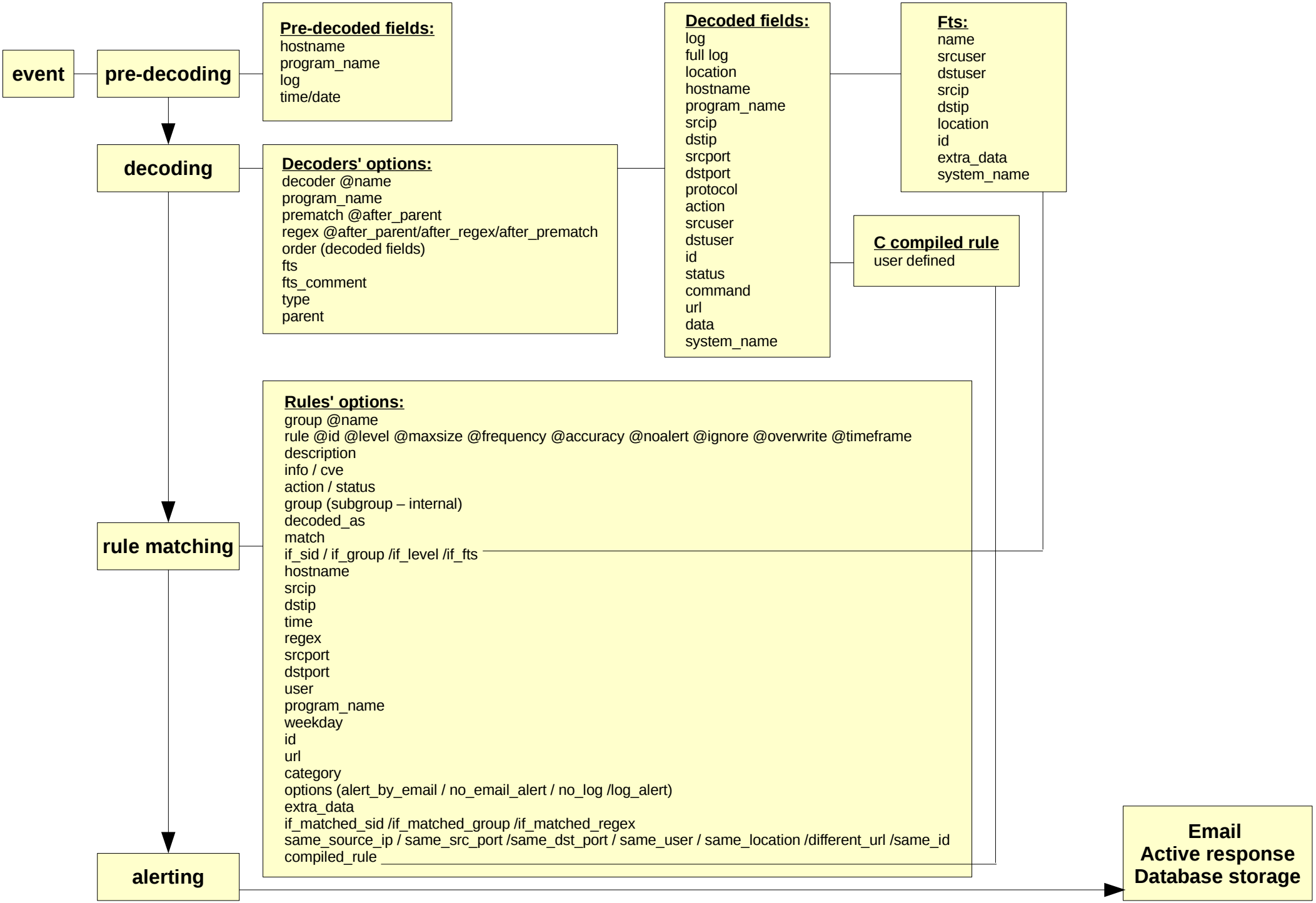
decoder @name
program_name
prematch @after_parent
regex @after_parent/after_regex/after_prematch
order (decoded fields)
fts
fts_comment
type
parent

Decoded fields:

log
full log
location
hostname
program_name
srcip
dstip
srcport
dstport
protocol
action
srcuser
dstuser
id
status
command
url
data
system_name

rule matching

Rules' options:
group @name
rule @id @level @maxsize @frequency @accuracy @noalert @ignore @overwrite @timeframe
description
info / cve
action / status
group (subgroup – internal)
decoded_as
match
if_sid / if_group /if_level /if_fts
hostname
srcip
dstip
time
regex
srcport
dstport
user
program_name
weekday
id
url
category
options (alert_by_email / no_email_alert / no_log /log_alert)
extra_data
if_matched_sid /if_matched_group /if_matched_regex
same_source_ip / same_src_port /same_dst_port / same_user / same_location /different_url /same_id
compiled_rule


event
pre-decoding
Pre-decoded fields:
hostname
program_name
log
time/date
decoding
Decoders' options:
decoder @name
program_name
prematch @after_parent
regex @after_parent/after_regex/after_prematch
order (decoded fields)
fts
fts_comment
type
parent
Decoded fields:
log
full log
location
hostname
program_name
srcip
dstip
srcport
dstport
protocol
action
srcuser
dstuser
id
status
command
url
data
system_name
Fts:
name
srcuser
dstuser
srcip
dstip
location
id
extra_data
system_name
C compiled rule
user defined
rule matching
Rules' options:
group @name
rule @id @level @maxsize @frequency @accuracy @noalert @ignore @overwrite @timeframe
description
info / cve
action / status
group (subgroup – internal)
decoded_as
match
if_sid / if_group /if_level /if_fts
hostname
srcip
dstip
time
regex
srcport
dstport
user
program_name
weekday
id
url
category
options (alert_by_email / no_email_alert / no_log /log_alert)
extra_data
if_matched_sid /if_matched_group /if_matched_regex
same_source_ip / same_src_port /same_dst_port / same_user / same_location /different_url /same_id
compiled_rule
alerting
Email
Active response
Database storage