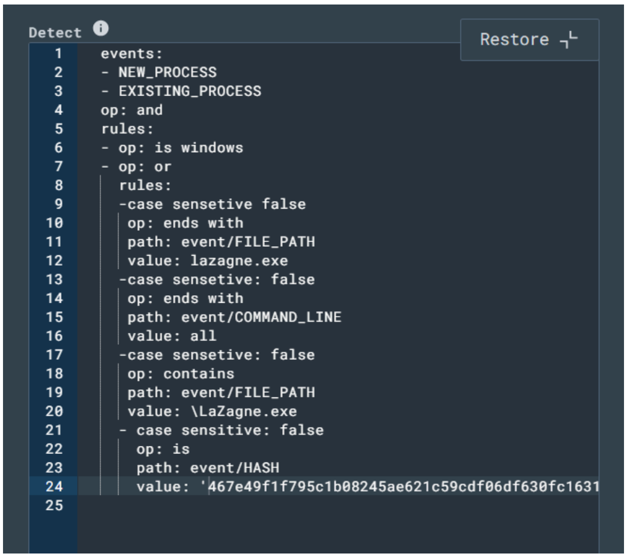
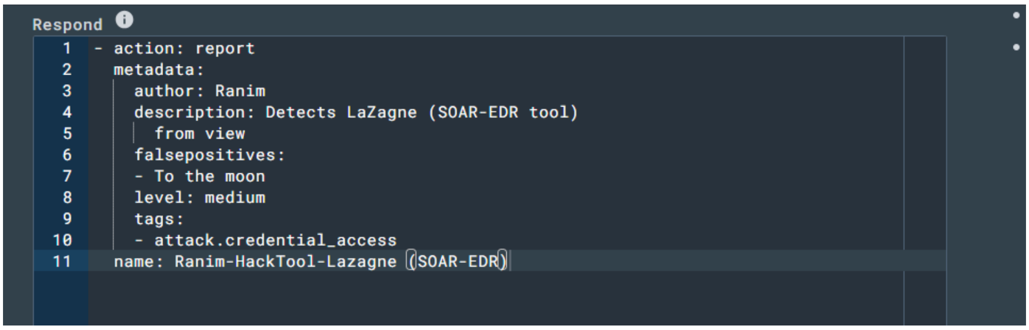
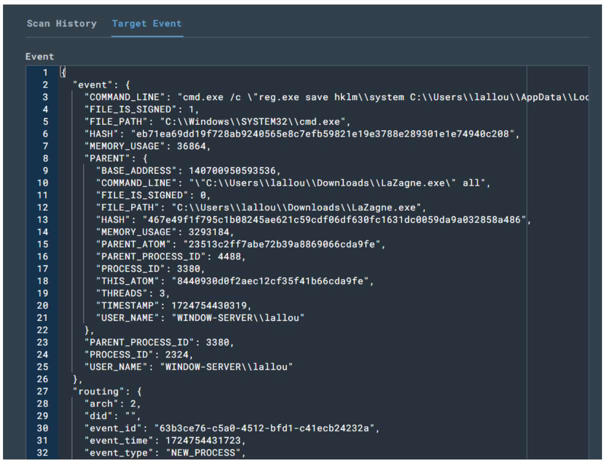


```
events:
- NEW_PROCESS
- EXISTING_PROCESS
op: and
rules:
- op: is windows
- op: or
  rules:
  -case sensetive false
   op: ends with
   path: event/FILE_PATH
   value: lazagne.exe
  -case sensetive: false
   op: ends with
   path: event/COMMAND_LINE
   value: all
  -case sensetive: false
   op: contains
   path: event/FILE_PATH
   value: \LaZagne.exe
  - case sensitive: false
    op: is
    path: event/HASH
    value: '467e49f1f795c1b08245ae621c59cdf06df630fc1631
```

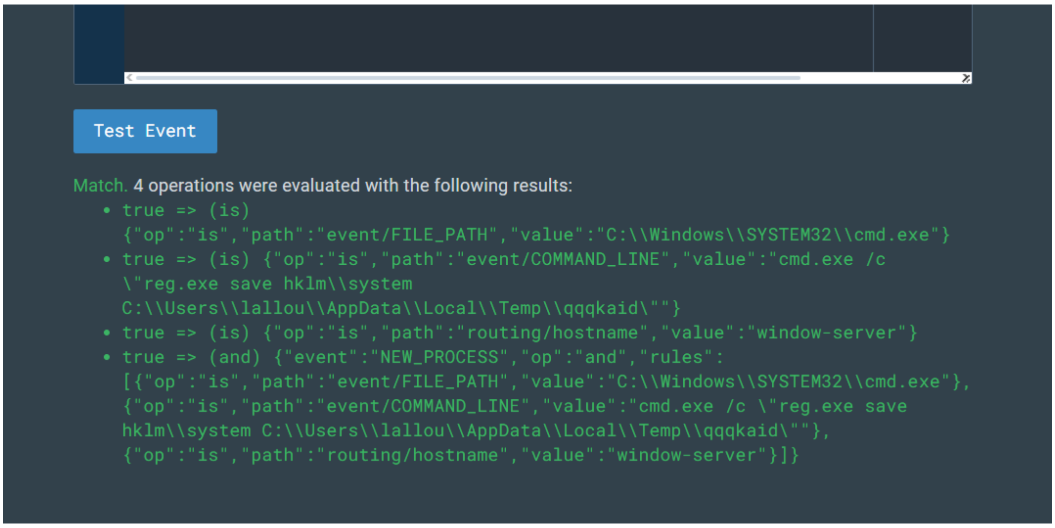


```
- action: report
  metadata:
    author: Ranim
    description: Detects LaZagne (SOAR-EDR tool)
      from view
    falsepositives:
    - To the moon
    level: medium
    tags:
    - attack.credential_access
  name: Ranim-HackTool-Lazagne (SOAR-EDR)
```

Simulating the rule



```
{
  "event": {
    "COMMAND_LINE": "cmd.exe /c \"reg.exe save hklm\\system C:\\Users\\lallou\\AppData\\Loc
    "FILE_IS_SIGNED": 1,
    "FILE_PATH": "C:\\Windows\\SYSTEM32\\cmd.exe",
    "HASH": "eb71ea69dd19f728ab9240565e8c7efb59821e19e3788e289301e1e74940c208",
    "MEMORY_USAGE": 36864,
    "PARENT": {
      "BASE_ADDRESS": 140700950593536,
      "COMMAND_LINE": "\"C:\\Users\\lallou\\Downloads\\LaZagne.exe\" all",
      "FILE_IS_SIGNED": 0,
      "FILE_PATH": "C:\\Users\\lallou\\Downloads\\LaZagne.exe",
      "HASH": "467e49f1f795c1b08245ae621c59cdf06df630fc1631dc0059da9a032858a486",
      "MEMORY_USAGE": 3293184,
      "PARENT_ATOM": "23513c2ff7abe72b39a8869066cda9fe",
      "PARENT_PROCESS_ID": 4488,
      "PROCESS_ID": 3380,
      "THIS_ATOM": "8440930d0f2aec12cf35f41b66cda9fe",
      "THREADS": 3,
      "TIMESTAMP": 1724754430319,
      "USER_NAME": "WINDOW-SERVER\\lallou"
    },
    "PARENT_PROCESS_ID": 3380,
    "PROCESS_ID": 2324,
    "USER_NAME": "WINDOW-SERVER\\lallou"
  },
  "routing": {
    "arch": 2,
    "did": "",
    "event_id": "63b3ce76-c5a0-4512-bfd1-c41ecb24232a",
    "event_time": 1724754431723,
    "event_type": "NEW_PROCESS",
```



Match. 4 operations were evaluated with the following results:

- true => (is) {"op":"is","path":"event/FILE_PATH","value":"C:\\Windows\\SYSTEM32\\cmd.exe"}
- true => (is) {"op":"is","path":"event/COMMAND_LINE","value":"cmd.exe /c \"reg.exe save hklm\\system C:\\Users\\lallou\\AppData\\Local\\Temp\\qqqkaid\""}
- true => (is) {"op":"is","path":"routing/hostname","value":"window-server"}
- true => (and) {"event":"NEW_PROCESS","op":"and","rules":[{"op":"is","path":"event/FILE_PATH","value":"C:\\Windows\\SYSTEM32\\cmd.exe"},{"op":"is","path":"event/COMMAND_LINE","value":"cmd.exe /c \"reg.exe save hklm\\system C:\\Users\\lallou\\AppData\\Local\\Temp\\qqqkaid\""},{"op":"is","path":"routing/hostname","value":"window-server"}]}