HackInBo Spring 2023 Edition

SCALABLE **MALWARE** ATTRIBUTION using **Malstream**

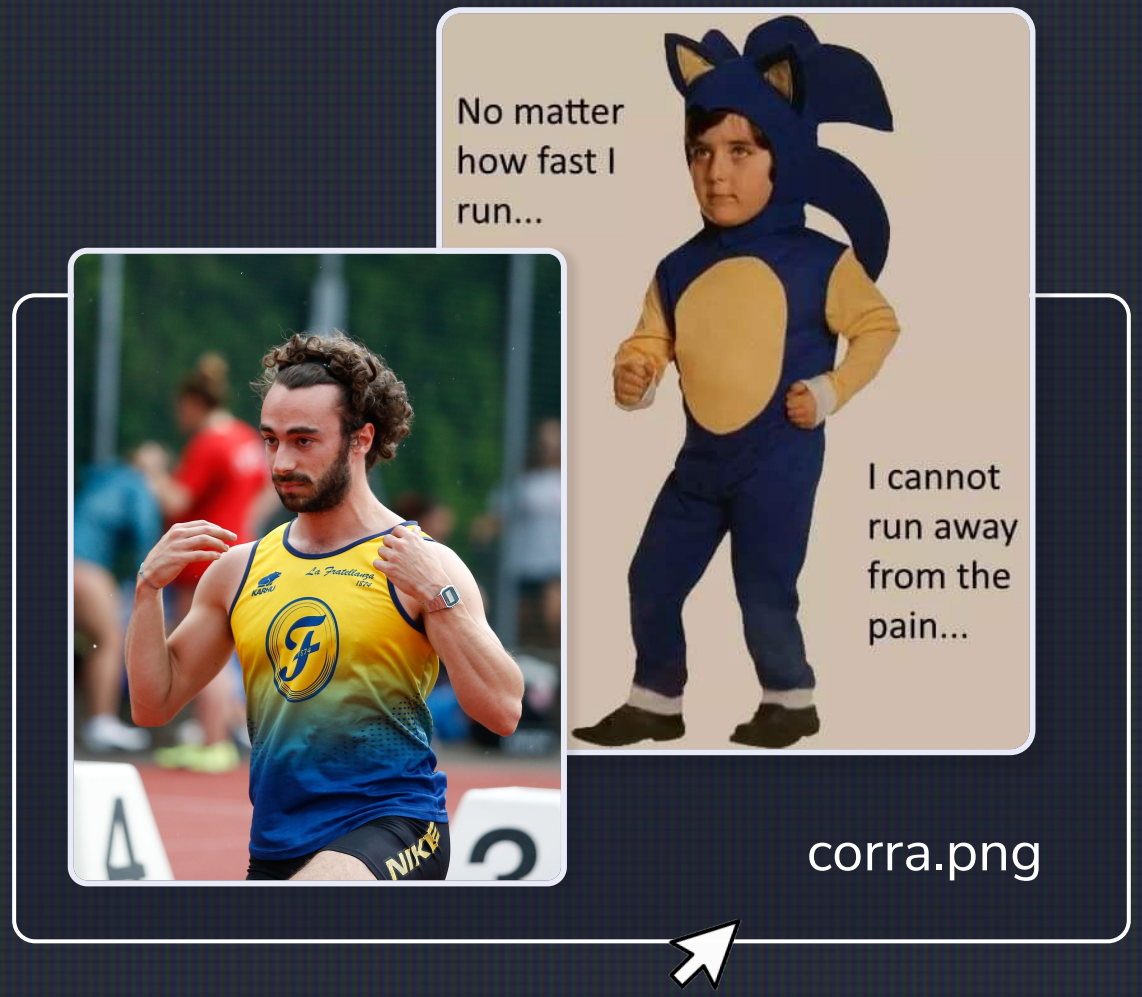
>_ **Matteo Corradini**

>_ Lead Cyber Threat Intelligence Engineer @ Cluster25

$ whoami

>_ **Lead Cyber Threat Intelligence Engineer** @ cluster25

>_ **Automatizzo** per pigrizia*, sportivo fuori dal lavoro



*non ditelo al mio capo

// agenda

>_ attribuzione

>_ malstream

>_ architettura

>_ scenario

>_ performance

>_ considerazioni

>_ bla bla bla bla bla

>_ bla bla bla bla bla

corratalk.mp4

// ATTRIBUZIONE

// intanto,
// serve davvero?

Attribuire un malware ad un **Threat Actor**

>_ **capire** il contesto geopolitico dell'attacco

Attribuire il sample ad una **malware family**

>_ **velocizzare** le attività di incident response

// le regole del gioco

// va bene le regole,ma…

malware.png

*“**Every day**,*
*the **AV-TEST** Institute*
*registers over **450,000***
new malware and PUA.”

// sistemi esistenti

>_ Strumenti **chiusi**, a **pagamento** e **poco personalizzabili**

>_ Soluzioni **on-prem** consentono una migliore gestione del **TLP**

>_ **Mancanza** di framework open-source all-in-one

INTEZER

ANY RUN
INTERACTIVE MALWARE HUNTING SERVICE

cuckoo

Triage

HYBRID ANALYSIS

VIRUSTOTAL

Cortex

JoeSecurity

spiderfoot

HACK IN BO
Spring ... Edition

// MALSTREAM

// features

>_ **Attribuzione automatica di sample**
grazie a regole YARA, Sigma e Suricata e servizi OSINT

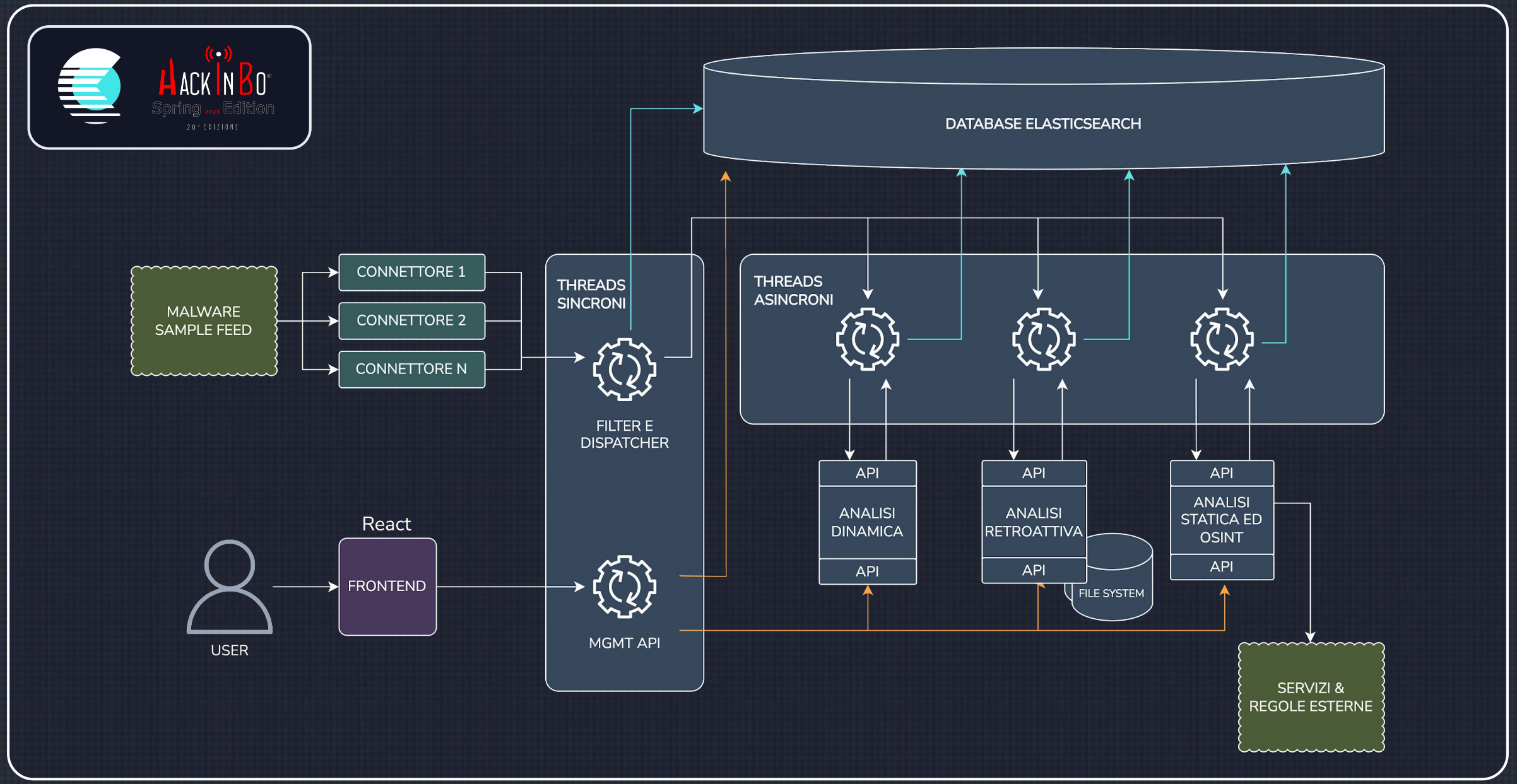
>_ **Analisi retroattive di nuove regole**
sui sample già analizzati per le regole YARA e Sigma

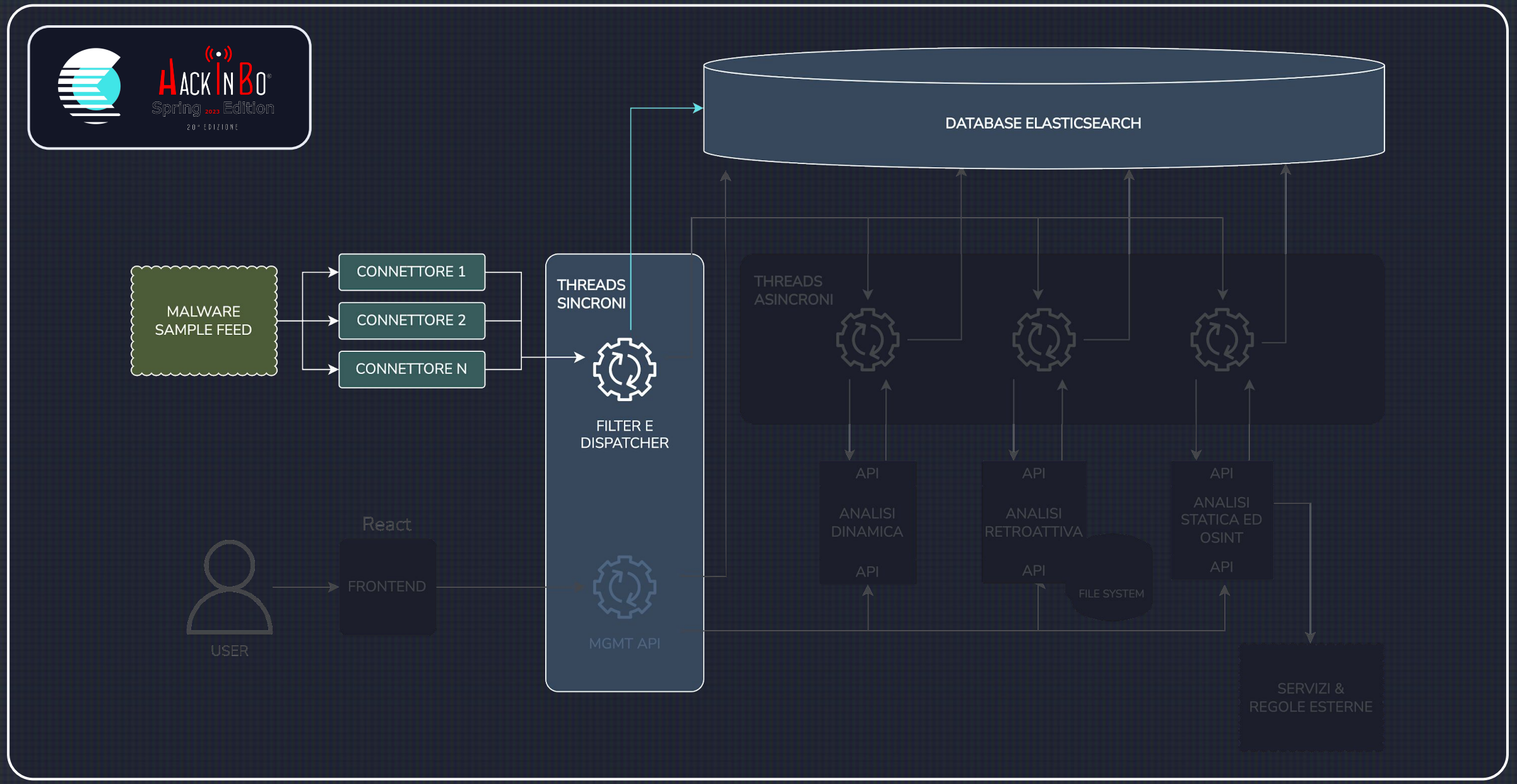
>_ **Sistema scalabile**
per far fronte ad un’ingente mole di sample

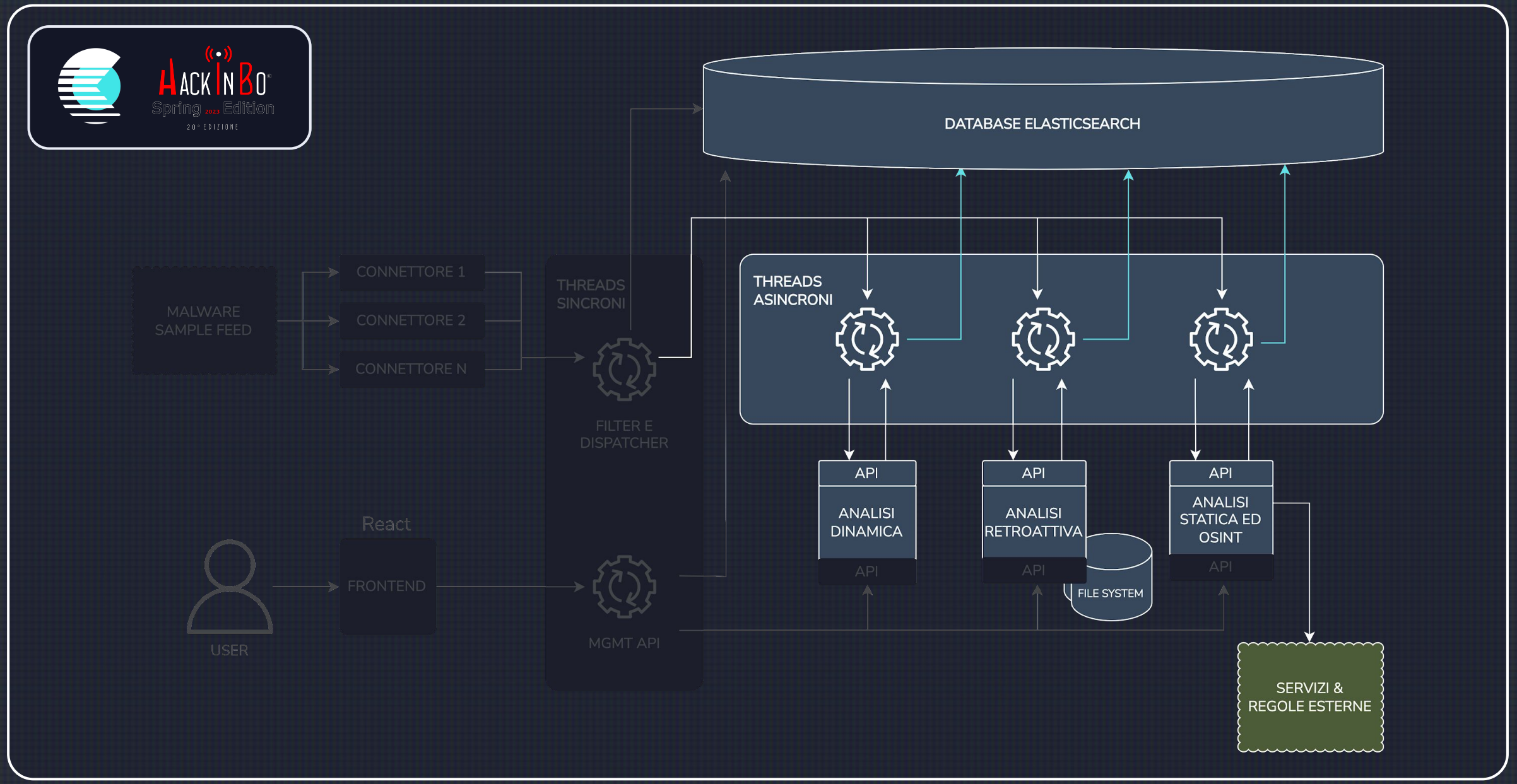
>_ **Consultabile da API e GUI**

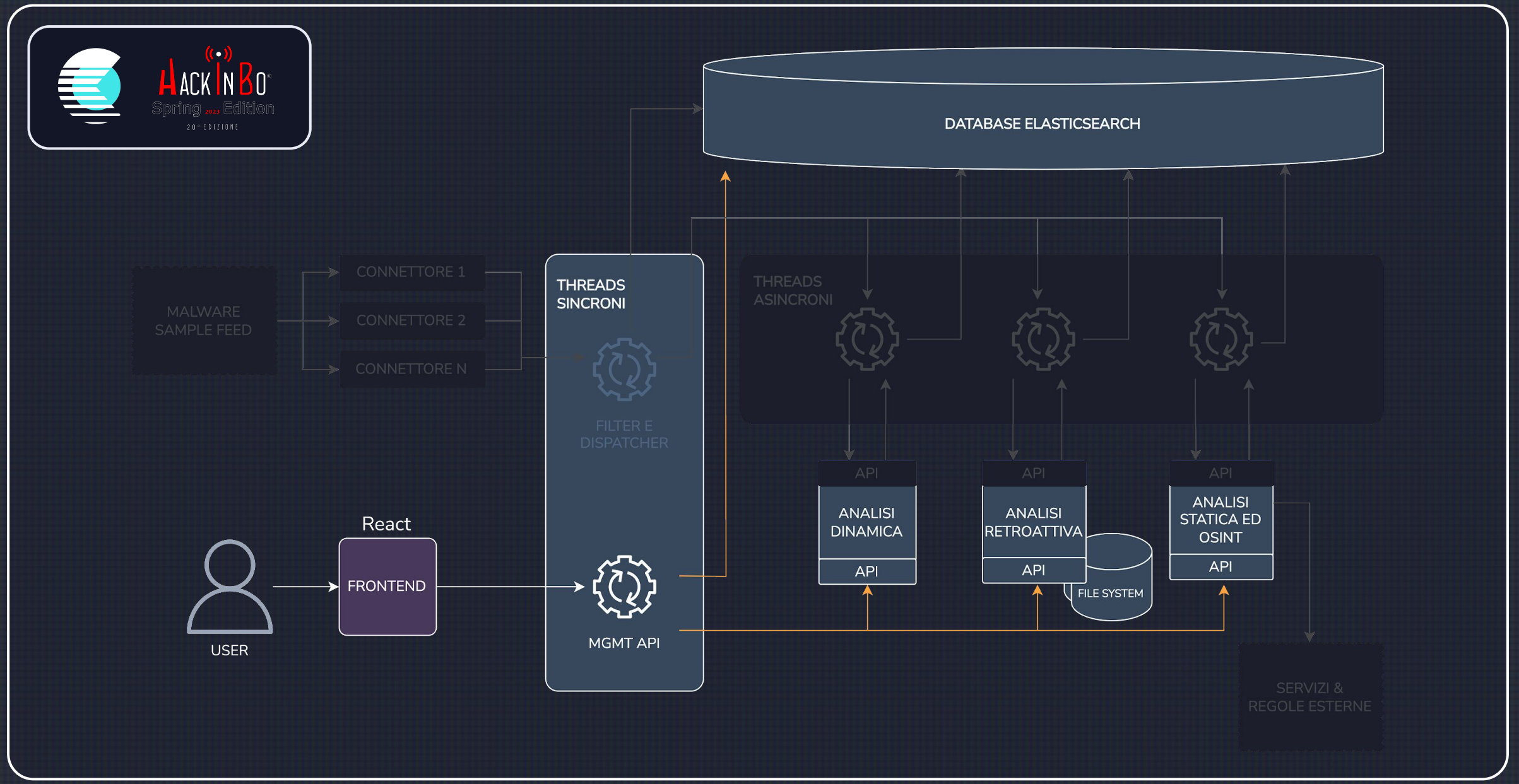
HACK IN BO
Spring ... Edition
2ª EDIZIONE

// ARCHITETTURA


HACK IN BO
Spring 2023 Edition
20ª EDIZIONE
DATABASE ELASTICSEARCH
MALWARE SAMPLE FEED
CONNETTORE 1
CONNETTORE 2
CONNETTORE N
THREADS SINCRONI
FILTER E DISPATCHER
MGMT API
THREADS ASINCRONI
API
ANALISI DINAMICA
API
API
ANALISI RETROATTIVA
API
FILE SYSTEM
API
ANALISI STATICA ED OSINT
API
React
FRONTEND
USER
SERVIZI & REGOLE ESTERNE


HACK IN BO
Spring 2023 Edition
20ª EDIZIONE
DATABASE ELASTICSEARCH
MALWARE SAMPLE FEED
CONNETTORE 1
CONNETTORE 2
CONNETTORE N
THREADS SINCRONI
FILTER E DISPATCHER
MGMT API
THREADS ASINCRONI
API
ANALISI DINAMICA
API
API
ANALISI RETROATTIVA
API
FILE SYSTEM
API
ANALISI STATICA ED OSINT
API
React
FRONTEND
USER
SERVIZI & REGOLE ESTERNE

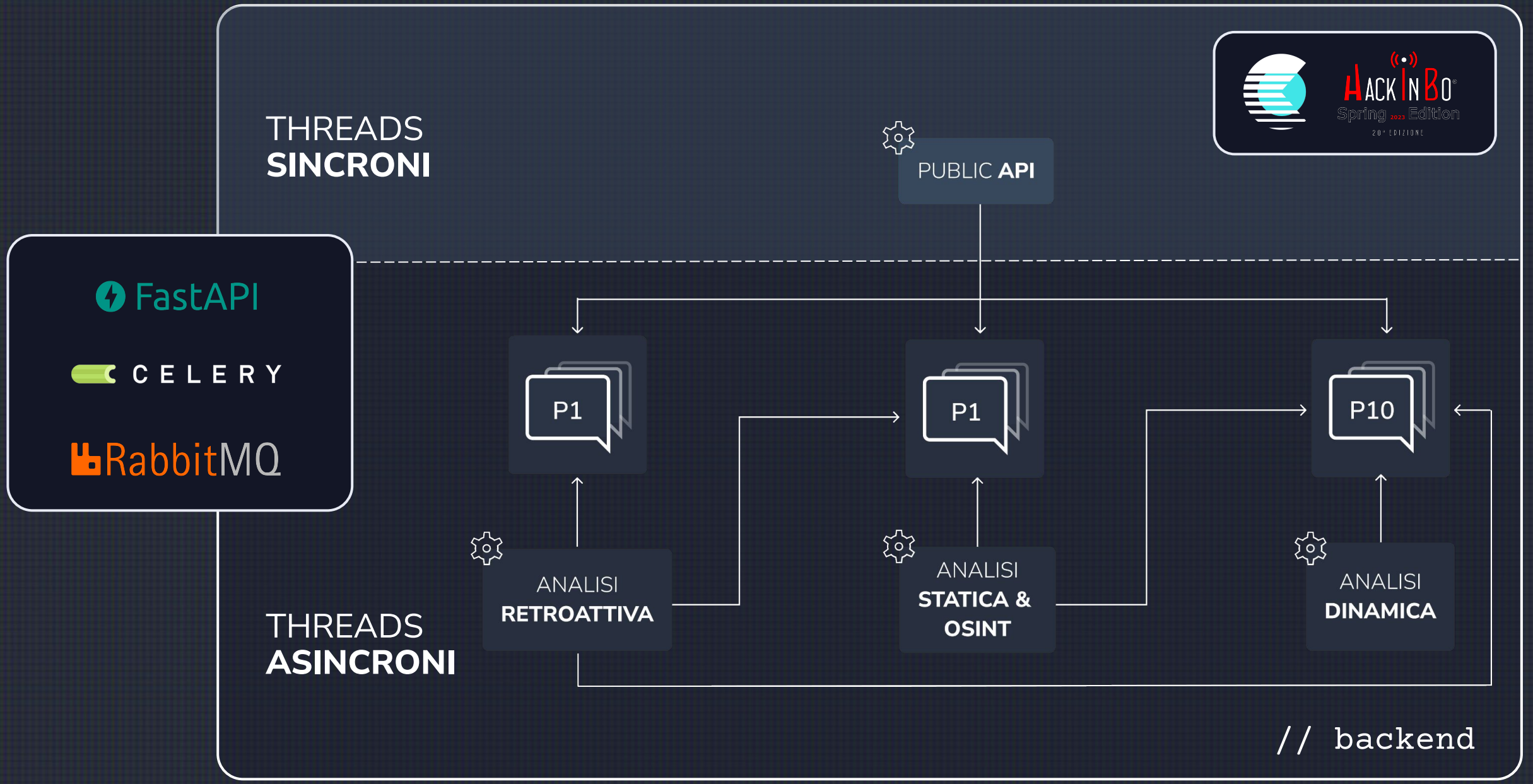

HACK IN BO
Spring 2023 Edition
20ª EDIZIONE
DATABASE ELASTICSEARCH
MALWARE SAMPLE FEED
CONNETTORE 1
CONNETTORE 2
CONNETTORE N
THREADS SINCRONI
FILTER E DISPATCHER
THREADS ASINCRONI
API
ANALISI DINAMICA
API
API
ANALISI RETROATTIVA
API
FILE SYSTEM
API
ANALISI STATICA ED OSINT
API
React
FRONTEND
USER
MGMT API
SERVIZI & REGOLE ESTERNE


HACK IN BO
Spring 2023 Edition
20ª EDIZIONE
DATABASE ELASTICSEARCH
MALWARE SAMPLE FEED
CONNETTORE 1
CONNETTORE 2
CONNETTORE N
THREADS SINCRONI
FILTER E DISPATCHER
MGMT API
THREADS ASINCRONI
API
ANALISI DINAMICA
API
API
ANALISI RETROATTIVA
API
FILE SYSTEM
API
ANALISI STATICA ED OSINT
API
React
FRONTEND
USER
SERVIZI & REGOLE ESTERNE

// connettori (kiss)

KISS

kiss.png


THREADS
SINCRONI
PUBLIC API
HackInBo
Spring 2023 Edition
20ª EDIZIONE
FastAPI
CELERY
RabbitMQ
P1
P1
P10
ANALISI
RETROATTIVA
ANALISI
STATICA &
OSINT
ANALISI
DINAMICA
THREADS
ASINCRONI
// backend

// analisi statica + OSINT
// IntelOWL

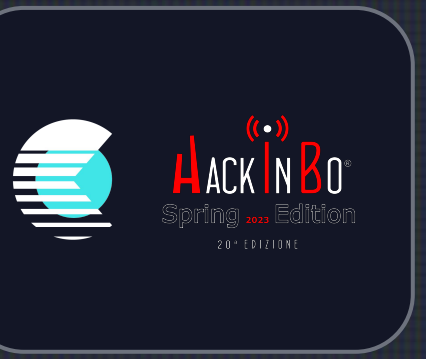
Aggiunta di un **analyzer YARA custom**

Creazione di **3 endpoint** per sincronizzare le regole:

- >_ POST /api/yara/upload
- >_ POST /api/yara/clean_up
- >_ DELETE /api/yara/{ id }

Configurazione degli **analyzer** per file ed hash

// analisi dinamica
// CAPEv2



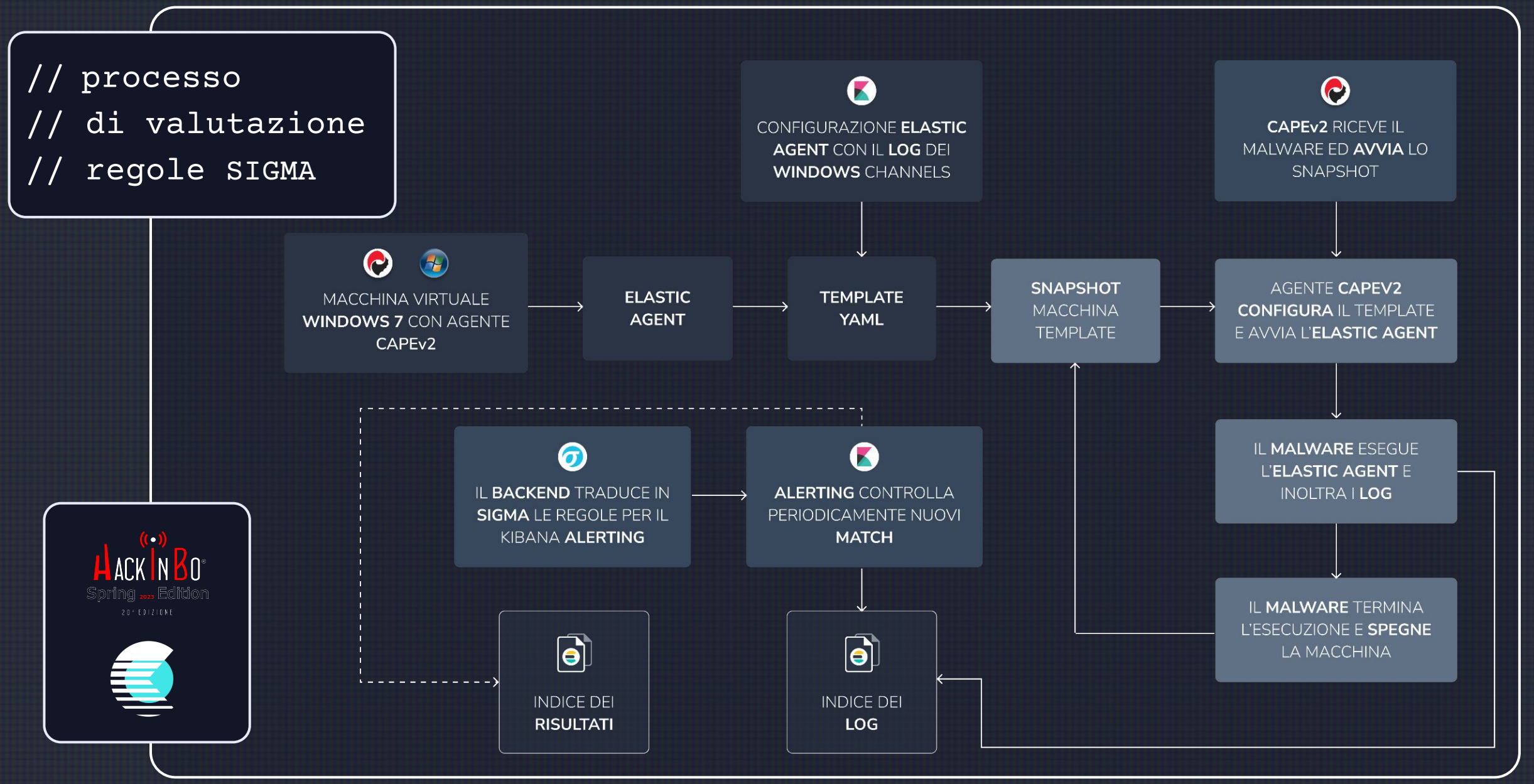
Creato il modulo di reporting per **Elasticsearch**
(PR #688 e #1212)

Creazione di **6 endpoint** per sincronizzare le regole

>_ POST /api/yara/upload
>_ POST /api /yara/clean_up
>_ DELETE /api/yara/{ id }
>_ POST /api/suricata/upload
>_ POST /api/suricata/clean_up
>_ DELETE /api/suricata/{ id }

Aggiunto il reload delle regole **YARA**

Aggiunto un comando per ricaricare il ruleset di **Suricata**


// processo
// di valutazione
// regole SIGMA
HACK IN BO
Spring 2023 Edition
20ª EDIZIONE
MACCHINA VIRTUALE WINDOWS 7 CON AGENTE CAPEv2
ELASTIC AGENT
CONFIGURAZIONE ELASTIC AGENT CON IL LOG DEI WINDOWS CHANNELS
TEMPLATE YAML
SNAPSHOT MACCHINA TEMPLATE
CAPEv2 RICEVE IL MALWARE ED AVVIA LO SNAPSHOT
AGENTE CAPEV2 CONFIGURA IL TEMPLATE E AVVIA L'ELASTIC AGENT
IL MALWARE ESEGUE L'ELASTIC AGENT E INOLTRA I LOG
IL MALWARE TERMINA L'ESECUZIONE E SPEGNE LA MACCHINA
IL BACKEND TRADUCE IN SIGMA LE REGOLE PER IL KIBANA ALERTING
ALERTING CONTROLLA PERIODICAMENTE NUOVI MATCH
INDICE DEI RISULTATI
INDICE DEI LOG

// analisi retroattiva

YARA

CERT.PL>_

SIGMA

kibana

+

elasticsearch

// SCENARIO

// ogni mattina,
// un analista si sveglia
// e NON sa…

HACKINBO Spring 2023 Edition
20ª EDIZIONE

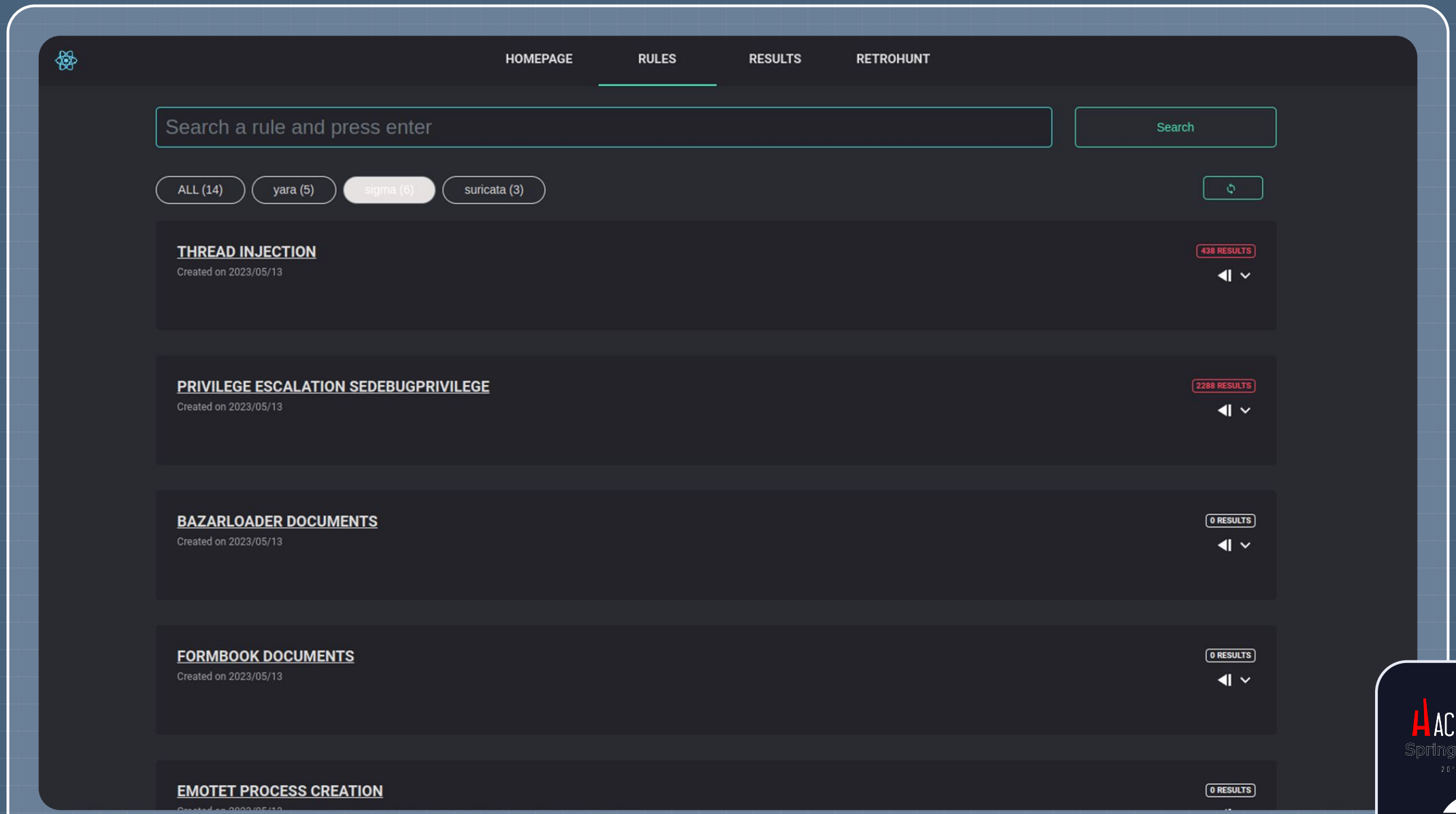
>_ L’analista deve scegliere il **malware** su cui lavorare

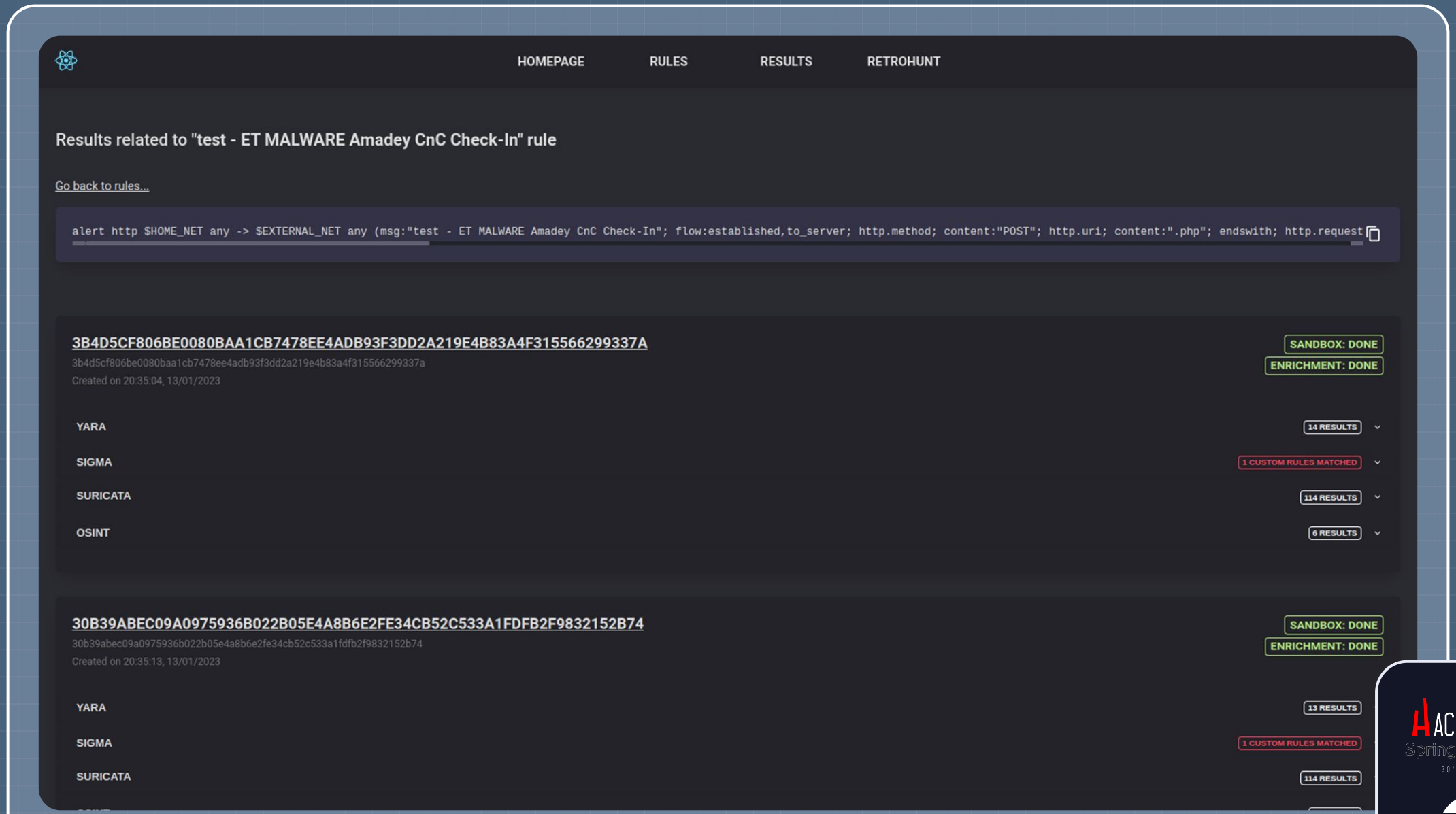
>_ Vuole concentrarsi su un sample **non ancora analizzato e attribuito**

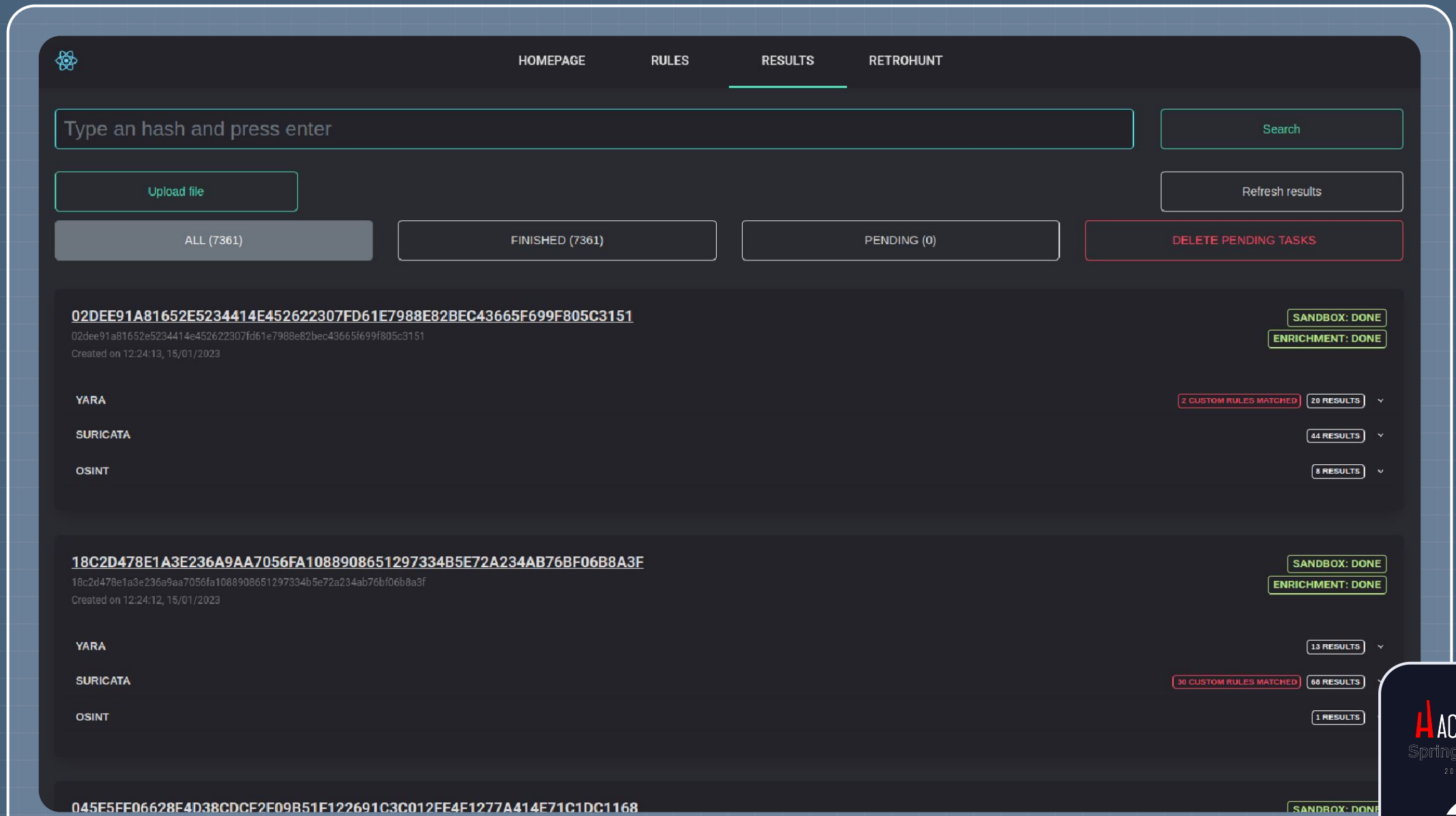
>_ Non può contare su un team I.R. o servizi di livehunt

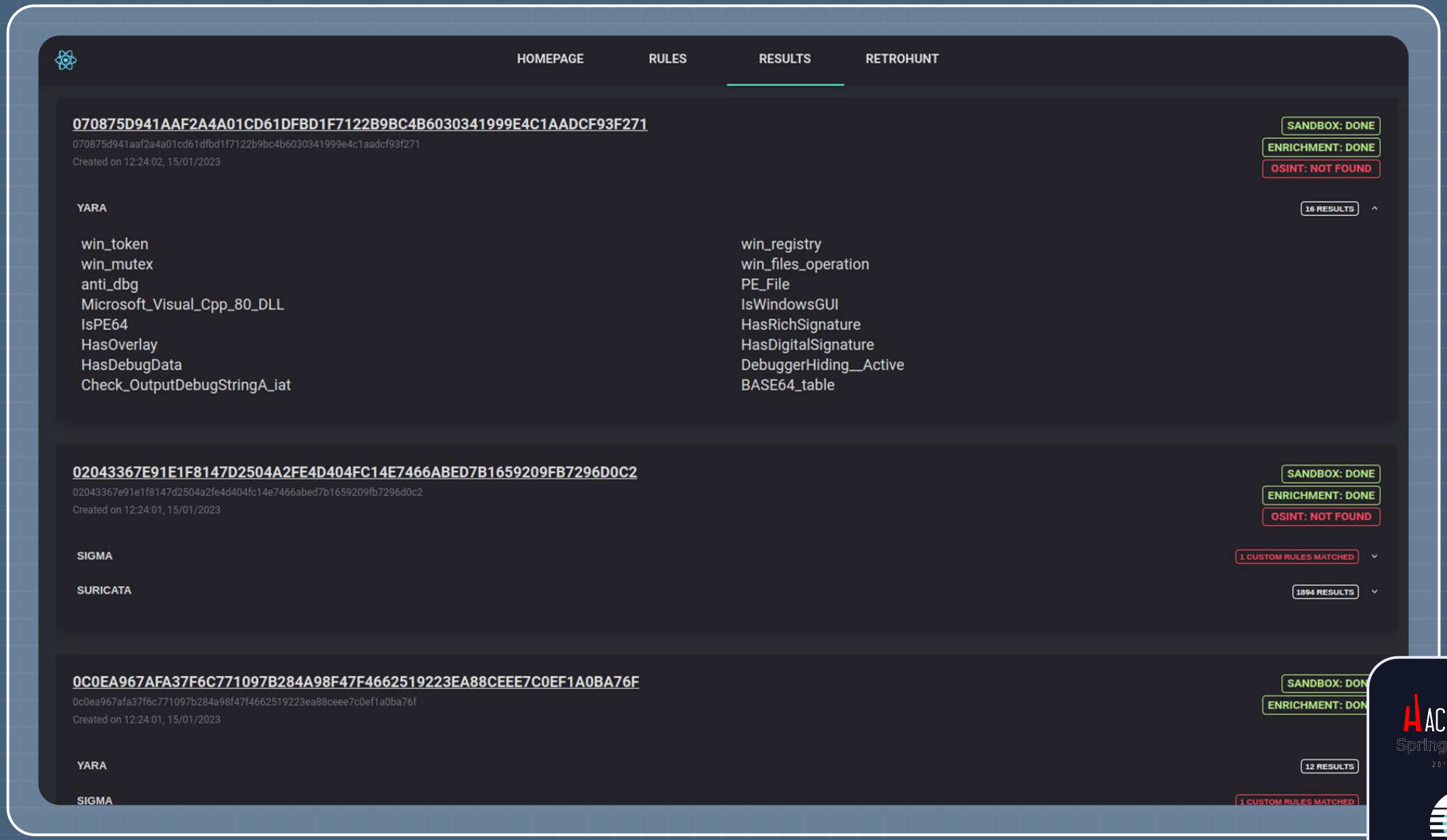
>_ Ha un sistema di antispam che ha collezionato centinaia di sample identificati come **Win.Trojan.Generic**

>_ Attraverso **Malstream**, sceglie il malware tra i **risultati delle regole** oppure tra **tutti i sample analizzati**


HOMEPAGE
RULES
RESULTS
RETROHUNT
Search a rule and press enter
Search
ALL (14)
yara (5)
sigma (6)
suricata (3)
THREAD INJECTION
Created on 2023/05/13
438 RESULTS
PRIVILEGE ESCALATION SEDEBUGPRIVILEGE
Created on 2023/05/13
2288 RESULTS
BAZARLOADER DOCUMENTS
Created on 2023/05/13
0 RESULTS
FORMBOOK DOCUMENTS
Created on 2023/05/13
0 RESULTS
EMOTET PROCESS CREATION
0 RESULTS


HOMEPAGE
RULES
RESULTS
RETROHUNT
Results related to "test - ET MALWARE Amadey CnC Check-In" rule
Go back to rules...
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"test - ET MALWARE Amadey CnC Check-In"; flow:established,to_server; http.method; content:"POST"; http.uri; content:".php"; endswith; http.request
3B4D5CF806BE0080BAA1CB7478EE4ADB93F3DD2A219E4B83A4F315566299337A
3b4d5cf806be0080baa1cb7478ee4adb93f3dd2a219e4b83a4f315566299337a
Created on 20:35:04, 13/01/2023
SANDBOX: DONE
ENRICHMENT: DONE
YARA
14 RESULTS
SIGMA
1 CUSTOM RULES MATCHED
SURICATA
114 RESULTS
OSINT
6 RESULTS
30B39ABEC09A0975936B022B05E4A8B6E2FE34CB52C533A1FDFB2F9832152B74
30b39abec09a0975936b022b05e4a8b6e2fe34cb52c533a1fdfb2f9832152b74
Created on 20:35:13, 13/01/2023
SANDBOX: DONE
ENRICHMENT: DONE
YARA
13 RESULTS
SIGMA
1 CUSTOM RULES MATCHED
SURICATA
114 RESULTS


HOMEPAGE
RULES
RESULTS
RETROHUNT
Type an hash and press enter
Search
Upload file
Refresh results
ALL (7361)
FINISHED (7361)
PENDING (0)
DELETE PENDING TASKS
02DEE91A81652E5234414E452622307FD61E7988E82BEC43665F699F805C3151
02dee91a81652e5234414e452622307fd61e7988e82bec43665f699f805c3151
Created on 12:24:13, 15/01/2023
SANDBOX: DONE
ENRICHMENT: DONE
YARA
2 CUSTOM RULES MATCHED
20 RESULTS
SURICATA
44 RESULTS
OSINT
8 RESULTS
18C2D478E1A3E236A9AA7056FA1088908651297334B5E72A234AB76BF06B8A3F
18c2d478e1a3e236a9aa7056fa1088908651297334b5e72a234ab76bf06b8a3f
Created on 12:24:12, 15/01/2023
SANDBOX: DONE
ENRICHMENT: DONE
YARA
13 RESULTS
SURICATA
30 CUSTOM RULES MATCHED
68 RESULTS
OSINT
1 RESULTS
045E5FF06628E4D38CDCF2E09B51F122691C3C012FE4F1277A414E71C1DC1168
SANDBOX: DONE


HOMEPAGE
RULES
RESULTS
RETROHUNT
070875D941AAF2A4A01CD61DFBD1F7122B9BC4B6030341999E4C1AADCF93F271
070875d941aaf2a4a01cd61dfbd1f7122b9bc4b6030341999e4c1aadcf93f271
Created on 12:24:02, 15/01/2023
SANDBOX: DONE
ENRICHMENT: DONE
OSINT: NOT FOUND
YARA
16 RESULTS
win_token
win_mutex
anti_dbg
Microsoft_Visual_Cpp_80_DLL
IsPE64
HasOverlay
HasDebugData
Check_OutputDebugStringA_iat
win_registry
win_files_operation
PE_File
IsWindowsGUI
HasRichSignature
HasDigitalSignature
DebuggerHiding__Active
BASE64_table
02043367E91E1F8147D2504A2FE4D404FC14E7466ABED7B1659209FB7296D0C2
02043367e91e1f8147d2504a2fe4d404fc14e7466abed7b1659209fb7296d0c2
Created on 12:24:01, 15/01/2023
SANDBOX: DONE
ENRICHMENT: DONE
OSINT: NOT FOUND
SIGMA
1 CUSTOM RULES MATCHED
SURICATA
1894 RESULTS
0C0EA967AFA37F6C771097B284A98F47F4662519223EA88CEEE7C0EF1A0BA76F
0c0ea967afa37f6c771097b284a98f47f4662519223ea88ceee7c0ef1a0ba76f
Created on 12:24:01, 15/01/2023
SANDBOX: DON
ENRICHMENT: DON
YARA
12 RESULTS
SIGMA
1 CUSTOM RULES MATCHED
HACK IN BO
Spring 2023 Edition
20ª EDIZIONE

// rimboccarsi le maniche

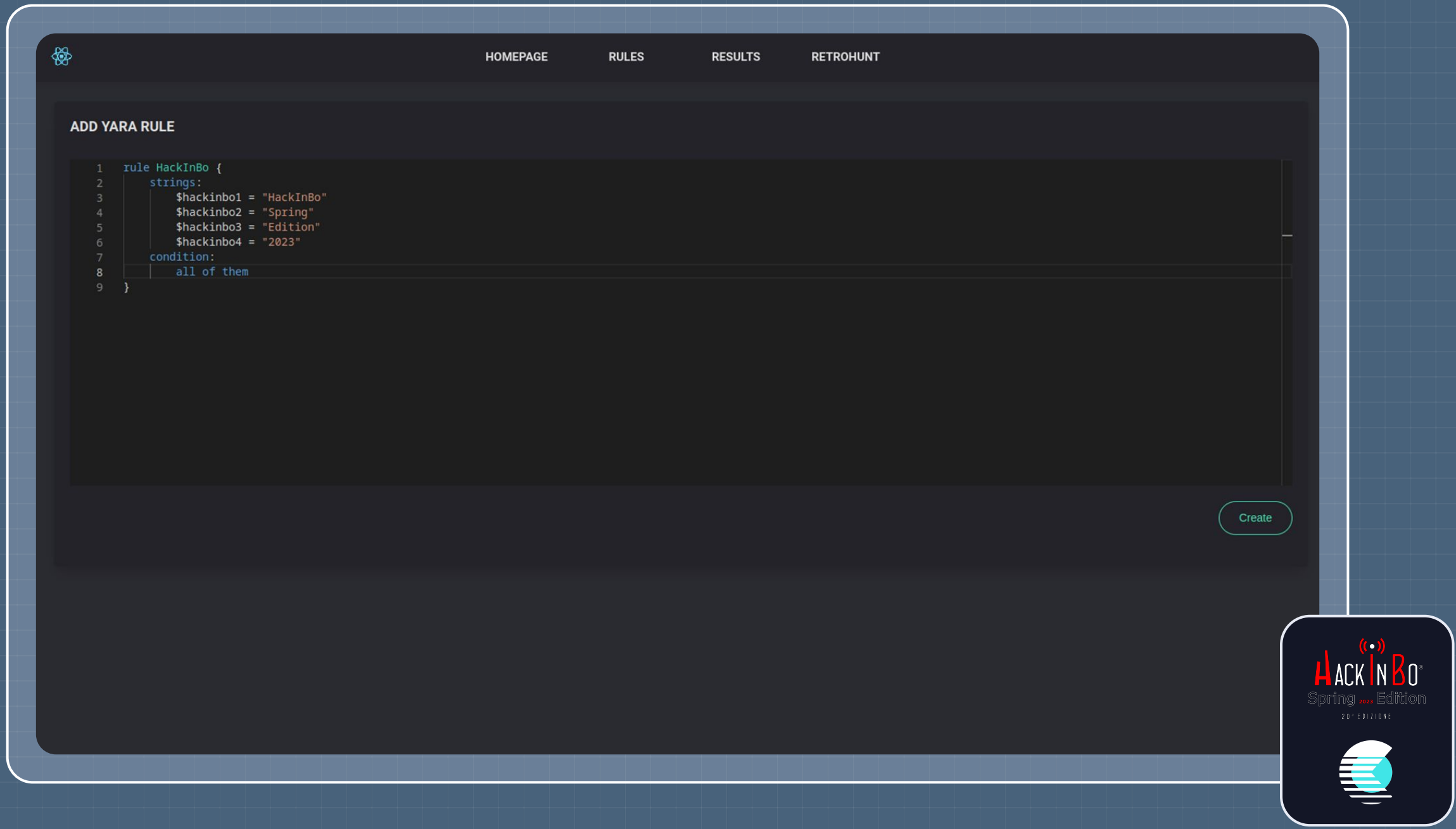
>_ L’analista analizza e reversa il malware e crea tre regole:

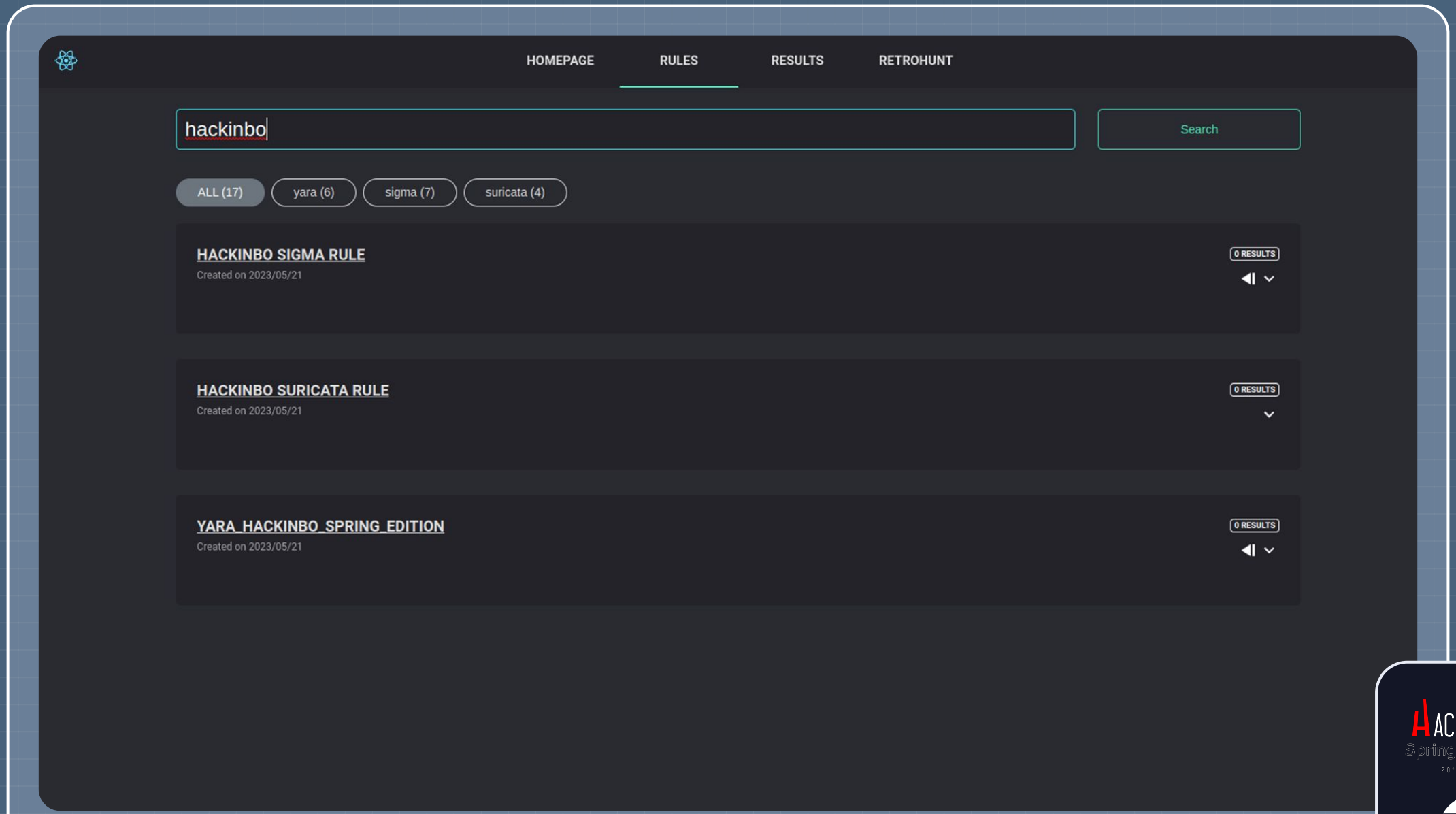
YARA, Sigma e Suricata

>_ Inserisce le regole dentro **Malstream**

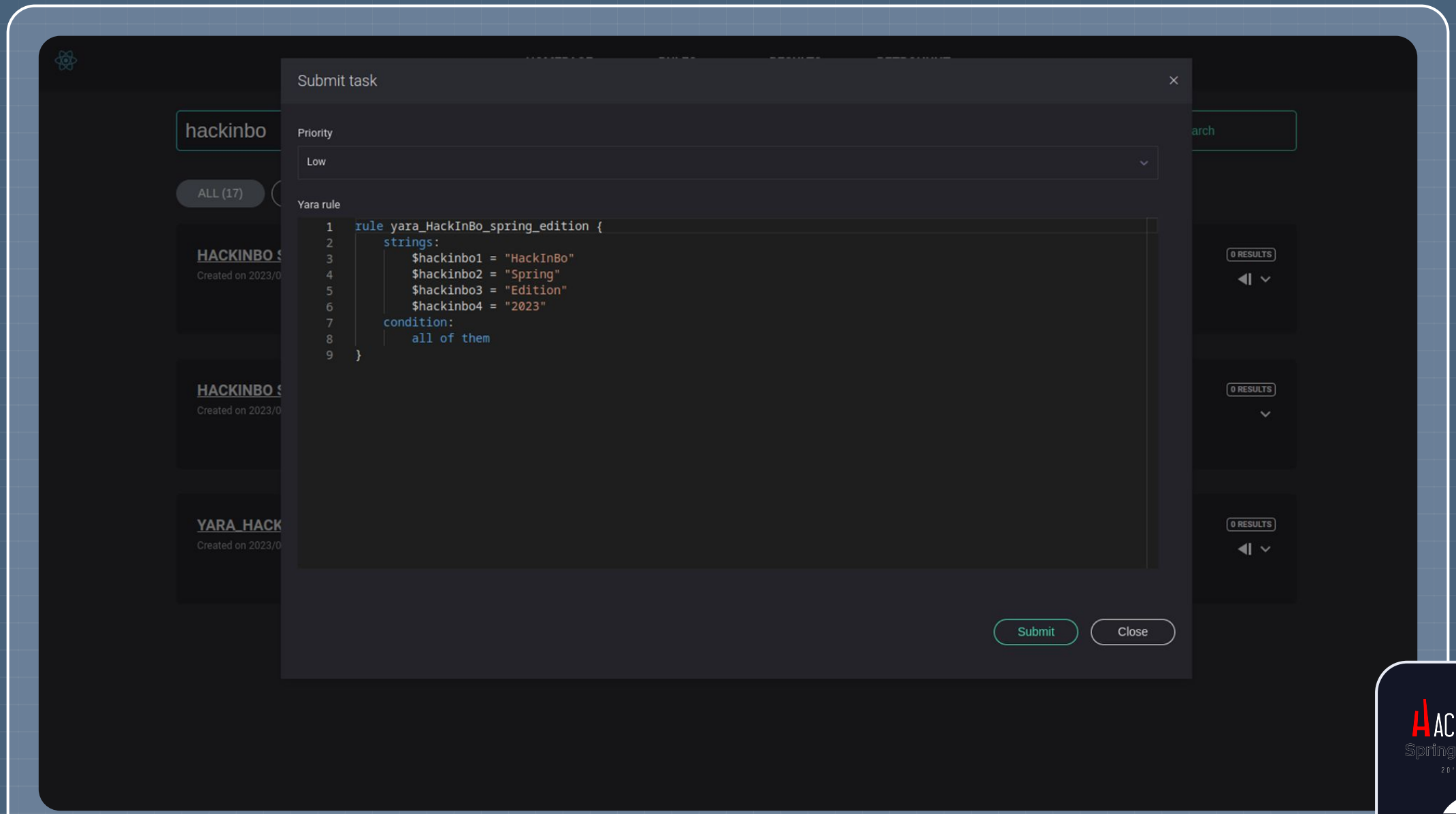
>_ Avvia **analisi retroattive** sul dataset raccolto

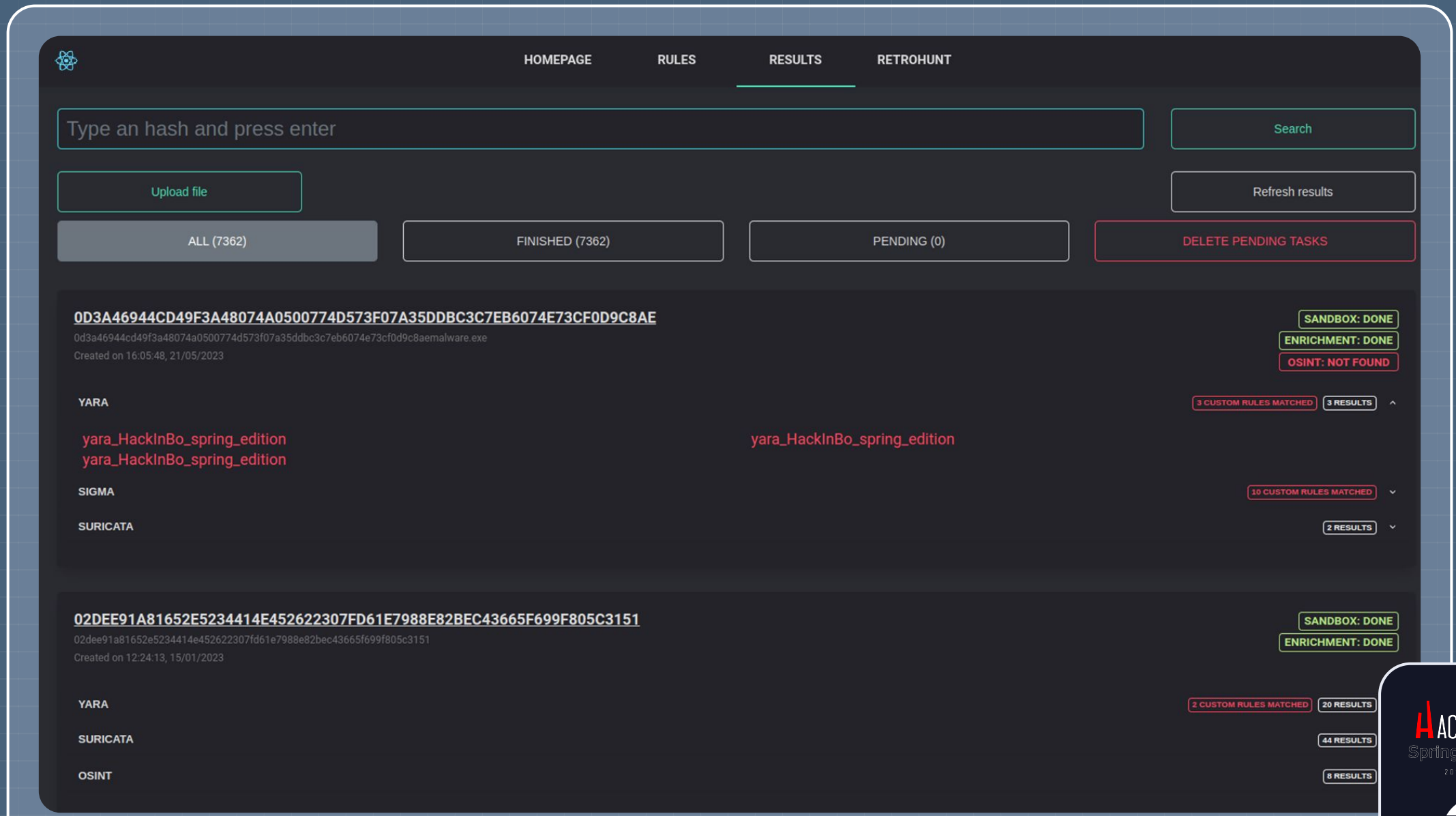
>_ **Monitora nuovi match** sull’interfaccia delle regole
per cercare FP o malware correlati

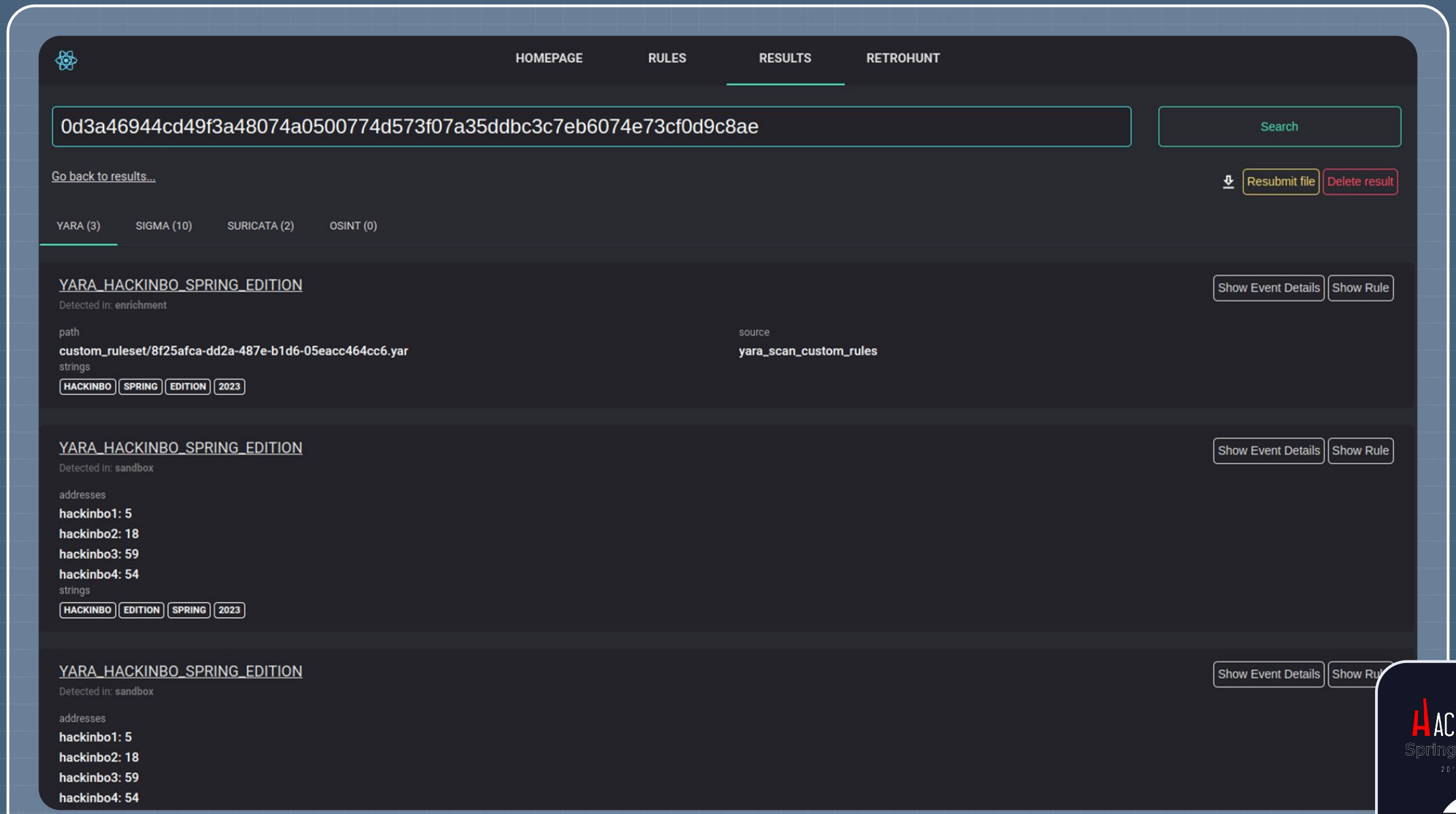

HOMEPAGE
RULES
RESULTS
RETROHUNT
ADD YARA RULE
rule HackInBo {
strings:
$hackinbo1 = "HackInBo"
$hackinbo2 = "Spring"
$hackinbo3 = "Edition"
$hackinbo4 = "2023"
condition:
all of them
}
Create


HOMEPAGE
RULES
RESULTS
RETROHUNT
hackinbo
Search
ALL (17)
yara (6)
sigma (7)
suricata (4)
HACKINBO SIGMA RULE
Created on 2023/05/21
0 RESULTS
HACKINBO SURICATA RULE
Created on 2023/05/21
0 RESULTS
YARA_HACKINBO_SPRING_EDITION
Created on 2023/05/21
0 RESULTS


HACKINBO
Spring 2023 Edition
20° EDIZIONE


Submit task
Priority
Low
Yara rule
rule yara_HackInBo_spring_edition {
strings:
$hackinbo1 = "HackInBo"
$hackinbo2 = "Spring"
$hackinbo3 = "Edition"
$hackinbo4 = "2023"
condition:
all of them
}
Submit
Close
hackinbo
ALL (17)
0 RESULTS

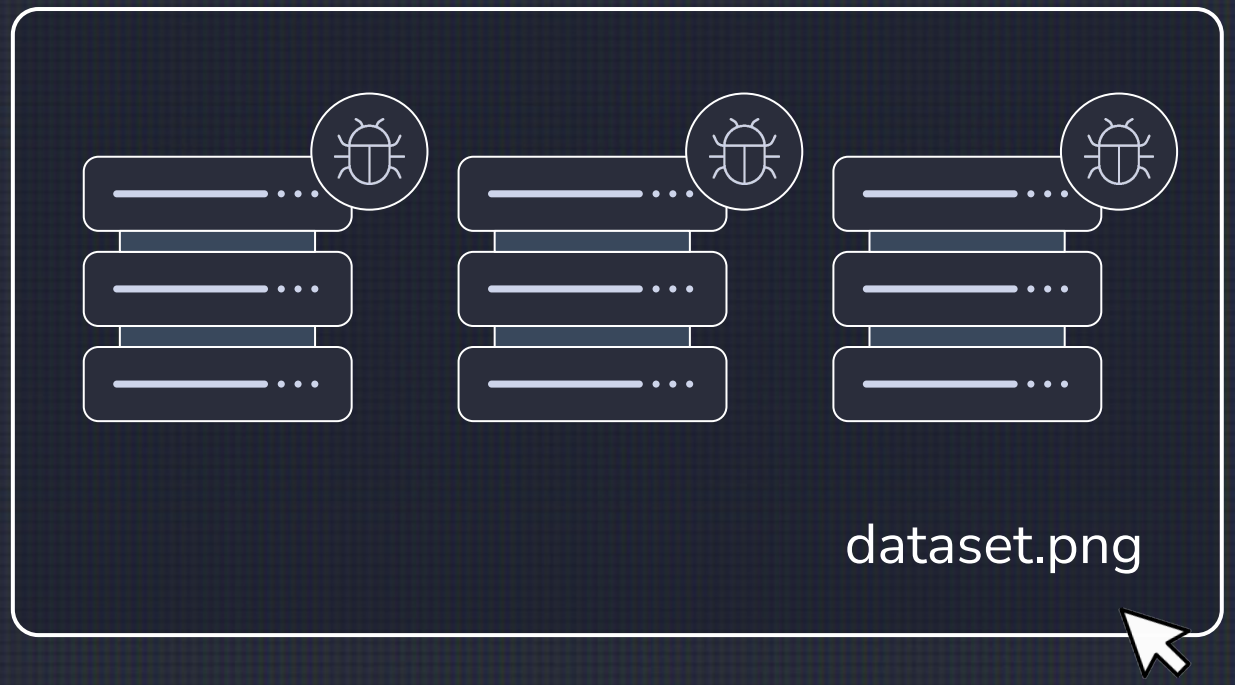

HOMEPAGE
RULES
RESULTS
RETROHUNT
Type an hash and press enter
Search
Upload file
Refresh results
ALL (7362)
FINISHED (7362)
PENDING (0)
DELETE PENDING TASKS
0D3A46944CD49F3A48074A0500774D573F07A35DDBC3C7EB6074E73CF0D9C8AE
0d3a46944cd49f3a48074a0500774d573f07a35ddbc3c7eb6074e73cf0d9c8aemalware.exe
Created on 16:05:48, 21/05/2023
SANDBOX: DONE
ENRICHMENT: DONE
OSINT: NOT FOUND
YARA
3 CUSTOM RULES MATCHED
3 RESULTS
yara_HackInBo_spring_edition
yara_HackInBo_spring_edition
yara_HackInBo_spring_edition
SIGMA
10 CUSTOM RULES MATCHED
SURICATA
2 RESULTS
02DEE91A81652E5234414E452622307FD61E7988E82BEC43665F699F805C3151
02dee91a81652e5234414e452622307fd61e7988e82bec43665f699f805c3151
Created on 12:24:13, 15/01/2023
SANDBOX: DONE
ENRICHMENT: DONE
YARA
2 CUSTOM RULES MATCHED
20 RESULTS
SURICATA
44 RESULTS
OSINT
8 RESULTS


HOMEPAGE
RULES
RESULTS
RETROHUNT
0d3a46944cd49f3a48074a0500774d573f07a35ddbc3c7eb6074e73cf0d9c8ae
Search
Go back to results...
Resubmit file
Delete result
YARA (3)
SIGMA (10)
SURICATA (2)
OSINT (0)
YARA_HACKINBO_SPRING_EDITION
Detected in: enrichment
Show Event Details
Show Rule
path
custom_ruleset/8f25afca-dd2a-487e-b1d6-05eacc464cc6.yar
source
yara_scan_custom_rules
strings
HACKINBO
SPRING
EDITION
2023
YARA_HACKINBO_SPRING_EDITION
Detected in: sandbox
Show Event Details
Show Rule
addresses
hackinbo1: 5
hackinbo2: 18
hackinbo3: 59
hackinbo4: 54
strings
HACKINBO
EDITION
SPRING
2023
YARA_HACKINBO_SPRING_EDITION
Detected in: sandbox
Show Event Details
addresses
hackinbo1: 5
hackinbo2: 18
hackinbo3: 59
hackinbo4: 54

// scenario bonus
// annotated dataset

>_ Possibile creare un **dataset annotato** in cui le label sono le attribuzioni ottenute dalle regole

>_ Il dataset può essere utilizzato per scopi di ML/AI



HACK IN BO
Spring .... Edition
2° EDIZIONE

// PERFORMANCE

// deploy

>_ **Host analisi dinamica su GCP** :
8 CPU e 32GB RAM

>_ **Elastic Cloud** :
2 nodi, 2.5 vCPU e 8GB RAM

>_ **Host analisti statica e retroattiva** :
16TB, 16 CPU e 32GB RAM

>_ **Host backend e frontend** :
4 CPU e 8GB RAM

// deploy

HOST ANALISI DINAMICA

- CAPEv2
  - MACCHINA VIRTUALE WIN7 ITA
  - MACCHINA VIRTUALE WIN7 ENG

ELASTICSEARCH CLOUD

- ELASTICSEARCH NODE
- ELASTICSEARCH NODE
- KIBANA NODE

HOST ANALISI STATICA & RETROATTIVA

- MQUERY
- INTELOWL

MALWARE FEED

- MALWARE BAZAAR
- TRIAGE

HOST BACKEND, FRONTEND & CONNETTORI

- BACKEND
- FRONTEND
- FILE STREAM CONNECTORS

// prestazioni
// 1000 sample

	Rate (sample/minuto)	Tempo di esecuzione
Ingestion	312.5	192s
Analisi Statica & OSINT	9.56	104m
Analisi Dinamica	0.61	27h 2VM / **13h 4VM**

// CONSIDERAZIONI

// considerazioni

>_ **Framework open-source e scalabile**

>_ **Automatizza l'attribuzione**
secondo regole YARA, Sigma e Suricata ed OSINT

>_ **Permette l'analisi retroattiva**
su regole YARA e Sigma

>_ **Consente agli analisti**
di concentrarsi su sample rilevanti risparmiando tempo

// tutto molto bello
// (spero)
// ma dove si trova?

>_ Presto **disponibile su:**

https://github.com/CorraMatte/malstream

Per un’anteprima, contattatemi in privato

>_ **Repository** dei servizi terzi disponibili:

https://github.com/CorraMatte/IntelOwl

https://github.com/CorraMatte/mquery

https://github.com/CorraMatte/CAPEv2

corra.matteo@gmail.com

@komra__

.../in/matteo-corradini

CorraMatte