NetGuardians

RiskTech 100 2018

Gartner 2015 Cool Vendor

Scoring API (SAPI)

Andrei Boca

May 2019

V1.4

swiss made software

Summary

- Introduction
- Type of controls
- Examples
- Main configuration

Scoring API - Introduction

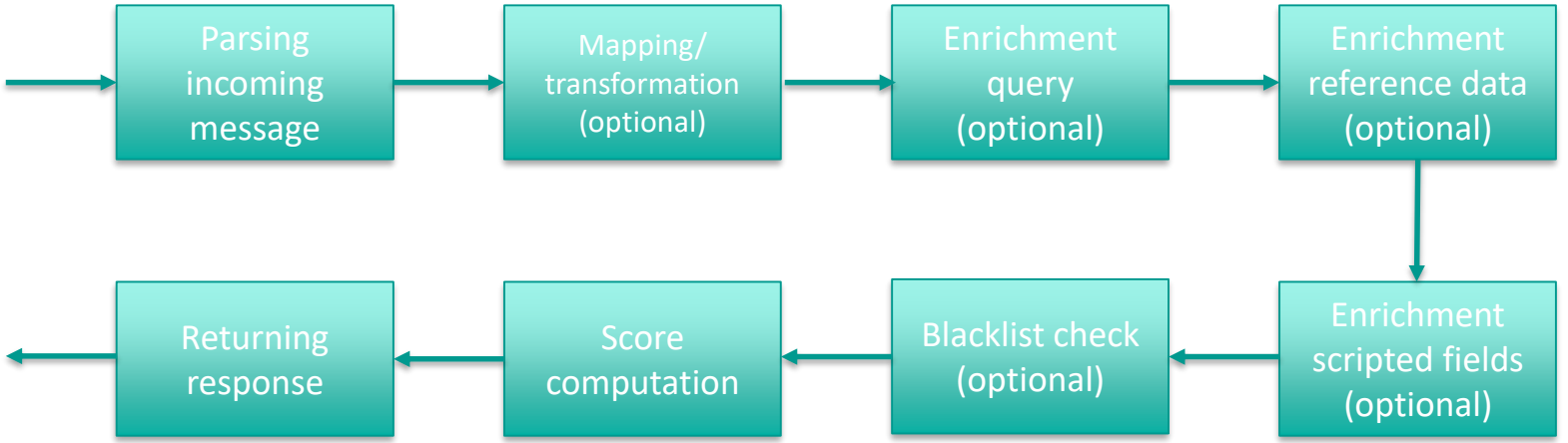
- A module which provides an API for external systems. It uses configured scoring models to score events (e.g. transactions) in a real-time fashion
- Independent service on NG|Screener server
- Configuration files:
  - log4j2.xml
  - ng-scoring-blacklist.conf
  - ng-scoring-jms.conf
  - ng-scoring-main.conf
  - ng-scoring-mapping.conf
  - ng-scoring-model.conf
  - ng-scoring-multitenancy.conf
  - ng-scoring-referencedata.conf
  - ng-scoring-rest.conf
  - ng-scoring-scriptedfields.conf

Scoring API positioning

- Choosing Scoring API for a project is a strategic decision. It has advantages but also limitations

Dimension	NG V7.2	V7.x + Scoring API
Response Time	< 2 minutes	<1s
Throughput	High	Limited
Distributed processing	Yes	No
Nb. Customers scaling	Yes	No (Limited)
Use cases	PBI + Profiling + ML	Simple PBI, Simple Profiling
Technology	Spark	In memory Java (a lot of RAM)
GUI	Yes	No
Maintainability	Easy	Complex

Scoring API big picture

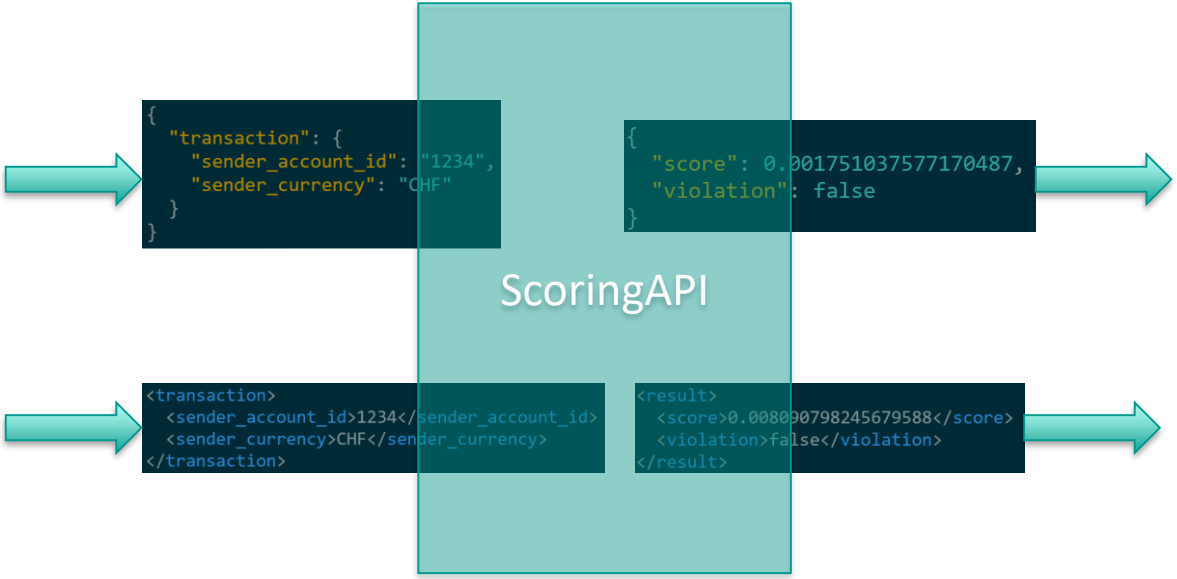


Terminology

- (Scoring) Model
  - defines all parameters which are used to compute risk score for individual event (such as financial transaction). Its definition is very similar to a profiling control's definition in NG|Screener
- Model chain
  - defines list of models involved in process of scoring. Final scoring decision is based on results from models computations
  - One model chain gives one answer: violation or no.
  - Scoring policies:
    - UNTIL_FIRST_VIOLATION - stops scoring on the first violation occurred. Default policy.
    - ANY_VIOLATION - violation only if at least one of models scores as violation
    - ALL_VIOLATIONS - violation only if ALL models scores as violation
    - SELECTED_MODEL - selects dynamically which model will score

Data format

- Incoming:
  - JSON
  - XML
  - SWIFT
- Outgoing
  - JSON
  - XML
  - Template available to create your own response



Endpoints (API)

- Supported endpoints:
  - JMS: IBM-JMS and Avaloq JMS-for-EMI – ng-scoring-jms.conf
  - REST: - ng-scoring-rest.conf
- Important configuration file:
  - /usr/local/ng-screener/scoring/tools/generate-scoring-systemd-env
    - Ability to switch endpoints (# ngScoring endpoints' switches). Example:
      - JAVA_OPTIONS="$JAVA_OPTIONS -DngScoring.endpoint.**rest**.enabled=**false** -DngScoring.endpoint.**jms**.enabled=**true**“
    - Configure memory of ScoringAPI (8GB configured for SAPI) - # memoy section
    - Other configuration (check Admin guide)

Publishing

- Specifies which transactions/events will be sent to ES
- ng-scoring-jms.conf
  - **ALL_TR_ALL_HITS** - sends all incoming transactions and all violation events - **FPS**
  - ONLY_TR_ALL_HITS - sends only suspicious transactions and all violation events
  - ALL_HITS - sends only violation events
  - NOTHING - sends nothing
  - Default value: NOTHING

Reference data & scripted fields

- Reference data possible: ng-scoring-referencedata.conf/ng-scoring-model.conf (check admin guide)
- Scripted fields possible: ng-scoring-scriptedfields.conf. Examples:

```
{
  field: "creation_trx_day_of_week"
  script: """
  ["Sontag","Montag","Dienstag","Mittwoch","Donnerstag","Freitag","Samstag"][new Date(event['@timestamp']).getDay()]
"""
},
```

```
  field: "amount_score"
  script: """
  function() {
    if (event['chf_amount']) {
      return event['chf_amount'] >= 5000 ? 1 : 0;
    } else {
      return null;
    }
  }()
  """
  type: INTEGER
},
```

```
  {
    field: "new_object_identifier",
    script: "'NC'",
    type: STRING
  }
]
```

Controls

- Simple profiling controls (e.g. Unusual Transactions)
- Simple profiling controls and enrichment
- Enrichment:
  - JOIN_FIELDS – tries to find in ES a document which has the same value defined in joinFields
    - Missing Join fields:
      - Default: enrichment skipped
      - `failEnrichmentIfMissingJoinField: true` – scoring will fail (dafault :false case above)
      - `whenErrorOccurs: FAIL` – will throw a configured error – scoring will fail
  - QUERY_STRING result type: HITS
    - Will enrich the current fields in Scoring API with additional fields resulted from an ES query, that can be used for scoring. (Applicable when fields necessary for scoring not available in SAPI but available in ES)
  - QUERY_STRING result type: COUNT
    - One of the profiling variables (of the simple profiling control implemented in SAPI) is the COUNT result of an ES query
    - Example of an ES query returning a count: how many transactions between same sender and same receiver in the last 5 days
  - Check the result of enrichment in `enrichment_result` in csv audit files (`/data/scoringAudit`)

Controls

- Simple profiling control example: UT

```
 code: "Unusual-Transactions"
 violationThreshold: 0.3
 customProperties {"dashboard_id": "dashboard-control_5", "dashboard_host":"[redacted]"}
 profilingVariables: [

{ aggCode: tp_source_user                          ,weight:  2   ,scoringMethod:  STATISTICAL ,ignoreMissingValues: true     },
#{ aggCode: tp_creation_trx_day_of_week            ,weight:  1   ,scoringMethod:  STATISTICAL ,ignoreMissingValues: true     },
#{ aggCode: tp_creation_trx_part_of_day            ,weight:  1   ,scoringMethod:  STATISTICAL ,ignoreMissingValues: true     },
{ aggCode: tp_glob_beneficiary_account_id          ,weight:  7   ,scoringMethod:  LOGARITHMIC ,ignoreMissingValues: true     },
{ aggCode: tp_beneficiary_bank_country             ,weight:  9   ,scoringMethod:  STATISTICAL ,ignoreMissingValues: true     },
{ aggCode: tp_glob_beneficiary_bank_country        ,weight:  2   ,scoringMethod:  LOGARITHMIC ,ignoreMissingValues: true     },
{ aggCode: tp_channel                              ,weight:  8   ,scoringMethod:  STATISTICAL ,ignoreMissingValues: true     },
{ aggCode: tp_amount_in_chf                        ,weight:  8   ,scoringMethod:  STATISTICAL ,ignoreMissingValues: true     },
{ aggCode: tp_currency                             ,weight:  3   ,scoringMethod:  STATISTICAL ,ignoreMissingValues: true     },
{ aggCode: tp_glob_currency                        ,weight:  3   ,scoringMethod:  LOGARITHMIC ,ignoreMissingValues: true     },
{ aggCode: tp_sender_account_category              ,weight:  1   ,scoringMethod:  STATISTICAL ,ignoreMissingValues: true     },
{ aggCode: tp_beneficiary_account_id               ,weight:  5   ,scoringMethod:  STATISTICAL ,ignoreMissingValues: true     },
{ aggCode: tp_glob_stat_beneficiary_bank_country   ,weight:  6   ,scoringMethod:  STATISTICAL ,ignoreMissingValues: true     },
{ aggCode: tp_sender_account_id                    ,weight:  5   ,scoringMethod:  STATISTICAL ,ignoreMissingValues: true     },
{ aggCode: tp_payment_type                         ,weight:  2   ,scoringMethod:  STATISTICAL ,ignoreMissingValues: true     },
{ aggCode: tp_new_customer                         ,weight:  0   ,scoringMethod:  STATISTICAL ,ignoreMissingValues: false    }

]
},
```

Controls

- Simple profiling control, using artificial variable (scripted field) for filtering purpose (RD):

```
{
 code: "Risky-Destinations"
 violationThreshold: 0.5
 customProperties {"dashboard_id": "dashboard-control_6", "dashboard_host":"[redacted]"}
 profilingVariables: [

{ aggCode: tp_source_user                       ,weight:  7   ,scoringMethod:  STATISTICAL ,ignoreMissingValues: true     },
{ aggCode: tp_creation_trx_day_of_week          ,weight:  8   ,scoringMethod:  STATISTICAL ,ignoreMissingValues: true     },
{ aggCode: tp_glob_beneficiary_account_id       ,weight:  2   ,scoringMethod:  LOGARITHMIC ,ignoreMissingValues: true     },
{ aggCode: tp_beneficiary_bank_country          ,weight:  49  ,scoringMethod:  STATISTICAL ,ignoreMissingValues: true     },
{ aggCode: tp_glob_beneficiary_bank_country     ,weight:  3   ,scoringMethod:  LOGARITHMIC ,ignoreMissingValues: true     },
{ aggCode: tp_glob_stat_beneficiary_bank_country ,weight:  52  ,scoringMethod:  STATISTICAL ,ignoreMissingValues: true     },
{ aggCode: tp_sender_account_id                 ,weight:  2   ,scoringMethod:  STATISTICAL ,ignoreMissingValues: true     },
{ aggCode: tp_new_customer                      ,weight:  0   ,scoringMethod:  STATISTICAL ,ignoreMissingValues: false    }

]
 referenceDataRef: [
 ]
 artificialVariables: [
        {name: amount_rd_score            ,weight: 115, ignoreMissingValues: false }
        ]
},
```

Controls

- Simple profiling control, Enriched with QUERY STRING, result type: HITS (ET)

```
{
code: "Ebanking-Transactions"
violationThreshold: 0.2
customProperties {"dashboard_id": "dashboard-control_4", "dashboard_host":"[redacted]"}
profilingVariables: [
        { aggCode: et_ses_auth                      ,weight:  1.67  ,scoringMethod:  STATISTICAL ,ignoreMissingValues: true     },
        { aggCode: et_sess_browser                  ,weight:  5.7   ,scoringMethod:  STATISTICAL ,ignoreMissingValues: true     },
        { aggCode: et_sess_connection_country       ,weight:  2.7   ,scoringMethod:  STATISTICAL ,ignoreMissingValues: true     },
        { aggCode: et_sess_language                 ,weight:  6.85  ,scoringMethod:  STATISTICAL ,ignoreMissingValues: true     },
        { aggCode: et_sess_screen_resolution        ,weight:  5.75  ,scoringMethod:  STATISTICAL ,ignoreMissingValues: true     },
        { aggCode: et_channel                       ,weight:  2.74  ,scoringMethod:  STATISTICAL ,ignoreMissingValues: true     },
        { aggCode: et_payment_type                  ,weight:  2.24  ,scoringMethod:  STATISTICAL ,ignoreMissingValues: true     },
        { aggCode: et_beneficiary_account_id        ,weight:  2.26  ,scoringMethod:  STATISTICAL ,ignoreMissingValues: true     },
        { aggCode: et_glob_beneficiary_account_id   ,weight:  9.2   ,scoringMethod:  LOGARITHMIC ,ignoreMissingValues: true     },
        { aggCode: et_beneficiary_bank_country      ,weight:  0.13  ,scoringMethod:  STATISTICAL ,ignoreMissingValues: true     },
        { aggCode: et_beneficiary_bank              ,weight:  8.9   ,scoringMethod:  STATISTICAL ,ignoreMissingValues: true     },
        { aggCode: et_glob_beneficiary_bank         ,weight:  3.16  ,scoringMethod:  LOGARITHMIC ,ignoreMissingValues: true     },
        { aggCode: et_transaction_sender_amount     ,weight:  7.53  ,scoringMethod:  STATISTICAL ,ignoreMissingValues: true     },
        { aggCode: et_transaction_sender_currency   ,weight:  0.52  ,scoringMethod:  STATISTICAL ,ignoreMissingValues: true     },
        { aggCode: et_ord_exec_date_day_of_week     ,weight:  0.1   ,scoringMethod:  STATISTICAL ,ignoreMissingValues: true     },
        { aggCode: et_new_contract                  ,weight:  0.0   ,scoringMethod:  STATISTICAL ,ignoreMissingValues: false    }
]
transactionEnrichment {
        type: QUERY_STRING
        allowedSources: [{"hostName": "[redacted]","serviceName": "swisscomCrealogixEbanking"}]
        query.result.type = HITS
        query.value: """
                {"_source":{"includes":["*"],"excludes":["@timestamp","service","host","originallog"]},"size":1,"query":{"bool":{"must":
[{"term":{"_index":{"value":"ngc-default[redacted]avaloq-swisscomcrealogixebanking*"}}},{"term":{"external_reference":{"value":"${tx:external_referen
ce}"}}}]}}}"""
        failEnrichmentIfMissingJoinField: false
}
},
```

Controls

- Simple profiling control, Enriched with QUERY STRING, result type: COUNT (SD)

```
        code: "Sentinel-Days"
        violationThreshold: 0.94
        customProperties {"dashboard_id": "dashboard-control_7", "dashboard_host":'[redacted]}
        profilingVariables: [

       { aggCode: tp_beneficiary_account_id_30d         ,weight:  1    ,scoringMethod:  LOGARITHMIC ,ignoreMissingValues: false     },

        ]
        referenceDataRef: [
        ]
        artificialVariables: [
               {name: sentinel_days_score      ,weight: 1 },
               {name: amount_score             ,weight: 1, ignoreMissingValues: false }
               ]
        transactionEnrichment {
               type: QUERY_STRING
               allowedSources: [{"hostName": [redacted],"serviceName": "avaloqPillarsTrx"}]
               #whenErrorOccurs: FAIL
               query {
                result {
                       type: COUNT
                       fieldName = "sentinel_days_score"
                       maxValue = 1
               }
               whenMissingField: SKIP_ENRICHMENT
               value: """{"query":{"bool":{"must_not":[{"term":{"receiver_account_category":"ESR"}}],"must":[{"term":{"host":{"value":"[redacted]Aval
oq"}}},{"term":{"service":{"value":"avaloqPillarsTrx"}}},{"term":{"channel":{"value":"110"}}},{"term":{"payment_status":{"value":"90"}}},{"term"
:{"sender_account_id":{"value":"${tx:sender_account_id}"}}},{"term":{"receiver_account_id":{"value":"${tx:receiver_account_id}"}}},{"range":{"ch
f_amount":{"gte":0,"lt":${tx:chf_amount}}}},{"range":{"@timestamp":{"gte":"now-5d","lte":"now"}}}]}}"""
       }
       }
       },
```

Other Relevant config

- ng-scoring-main.conf
  - Aggregations refresh scheduling: aggregation.cache.refresh-schedule: "0 0 05 * * *“
  - Enable/disable csv audit publisher (score and partial scores of all transactions): /data/scoringAudit
- ng-scoring-mapping.conf
  - It defines simple translation from incoming key to desired one. Each line should contain one translation in the following format: "source key" : "target key“
- Blacklisting techniques (check admin guide)
  - ng-scoring-blacklist.conf
  - ng-scoring-model.conf
- ng-scoring-jms.conf
  - Error response template
  - URL response template
- Multitenancy:
  - ng-scoring-multitenancy.conf (Default – single tenant)

NG|Screener (in the picture with SAPI)

- Aggregation definition and recomputation
  - SAPI loads computed aggregations
- NG|Screener loads reference data in ES
- NG|Screener saves violations in ES
- SAPI communicates with ngStorage and ngSyslogNG

Scoring API minimum configuration

- At least 1 endpoint enabled
- Configured Endpoint
- Configured connection to NG|Storage
- Configured scoring model
  - Model with aggregations
  - Model with fixed score
  - Model with profile limits

Testing the scoring

1. Include partial scores in the response:

   ng-scoring-rest.conf

   1. In /usr/local/ng-screener/scoring/tools
   2. Edit generate-scoring-systemd-env
   3. Enable REST endpoint
   4. JAVA_OPTIONS="$JAVA_OPTIONS -DngScoring.endpoint.jms.enabled=true -DngScoring.endpoint.rest.enabled=true"
   5. restart scoring-API

2. Send a curl request (xml/JSON) →
3. Check response and partial scores

```
curl --request POST \
 --url http://localhost:8880/models/SM-SD-NC-RD-UT-ET/scoreTransaction \
 --header 'accept: application/xml' \
 --header 'content-type: application/xml' \
 --data '<transaction>
 <business_reference>770077996</business_reference>
 <payment_type>10020</payment_type>
… all the fields involved in the profiling model to be tested …
 <channel>eBanking</channel>
 <chf_amount>1175</chf_amount>
 <sender_account_id>0244.4488.2001</sender_account_id>
 <receiver_account_id>CH41 0076 1016 0944 0138 9</receiver_account_id>
 <receiver_account_category>IBAN</receiver_account_category>
 <receiver_bank_id>1</receiver_bank_id>
 <receiver_bank_type>BP</receiver_bank_type>
 <receiver_bank_country>CH</receiver_bank_country>
 <payment_status>3</payment_status>
 </transaction>'
```

Thank you!

NetGuardians

+41 24 425 97 60

info@netguardians.ch

www.netguardians.ch

Linkedin.com/company/netguardians

Facebook.com/NetGuardians

@netguardians

https://www.youtube.com/netguardians

First name / Last name

+41 78 641 00 85

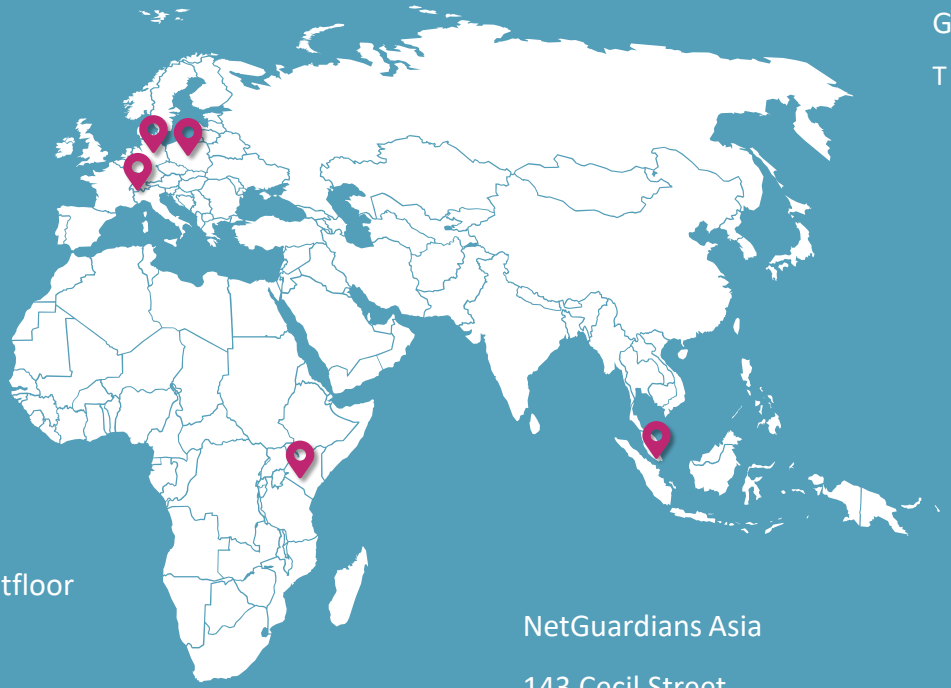
boca@netguardians.ch

Contact us

NetGuardians Headquarters

Y-Parc, Av. des Sciences 13
1400 Yverdon-les-Bains
Switzerland

T +41 24 425 97 60



NetGuardians Germany

Rhein-Main Gebiet
Germany

T +49 172 3799003

NetGuardians
Eastern Europe

WeWork
Krucza 50, 00-025
Warsaw, Poland

NetGuardians Africa

The Mirage, Tower 2, Pentfloor
Waiyaki Way, Westlands
00101 Nairobi, Kenya

T +254 797735 050

NetGuardians Asia

143 Cecil Street
#09-01 GB Building
069542 Singapore

T +65 6224 0987