MICHIGAN STATE
UNIVERSITY

Alpha Presentation
Force Platform Ingestion Tool

The Capstone Experience

Team Rook

Roy Barnes
Matt Hammerly
Will McGee
Chiyu Song
Mark Velez

Department of Computer Science and Engineering
Michigan State University

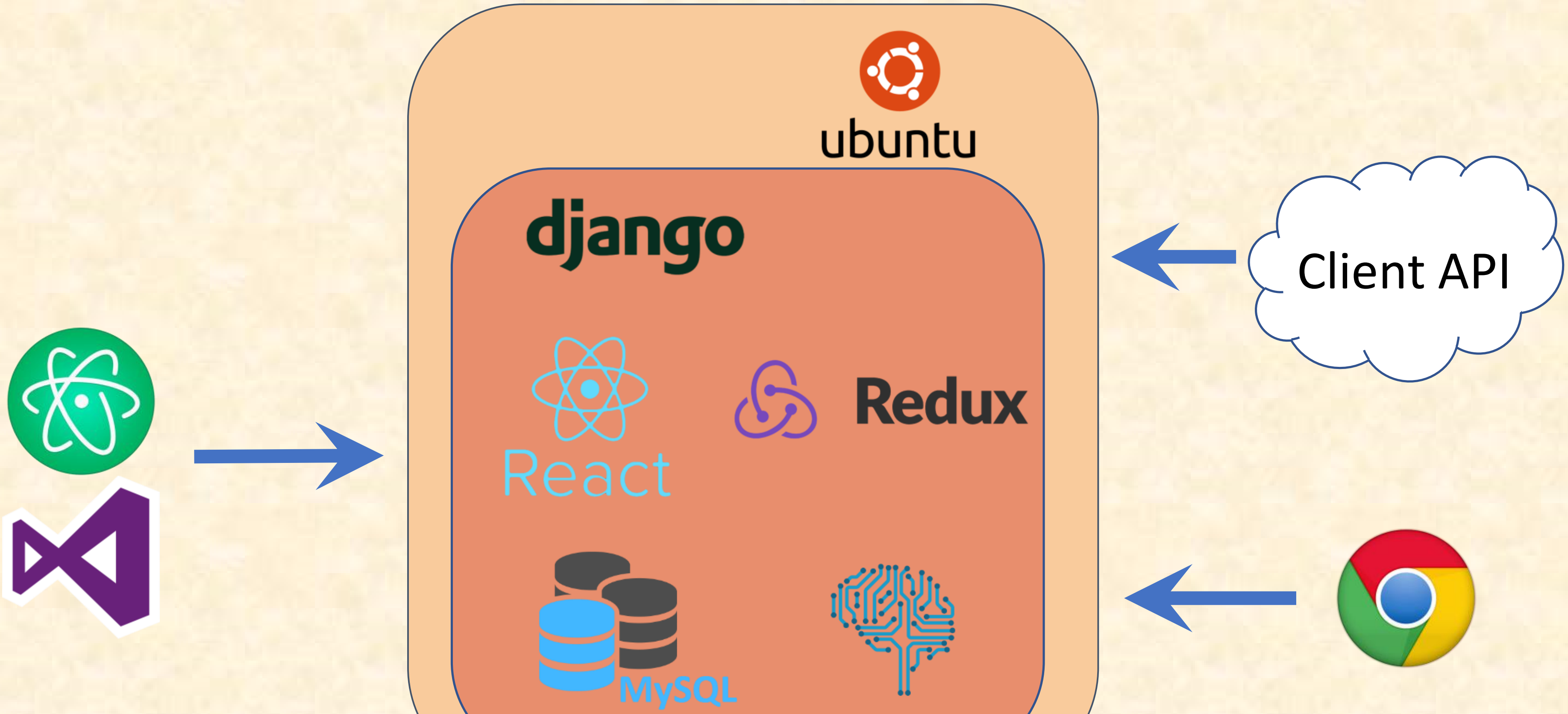
Spring 2017

From Students…
…to Professionals

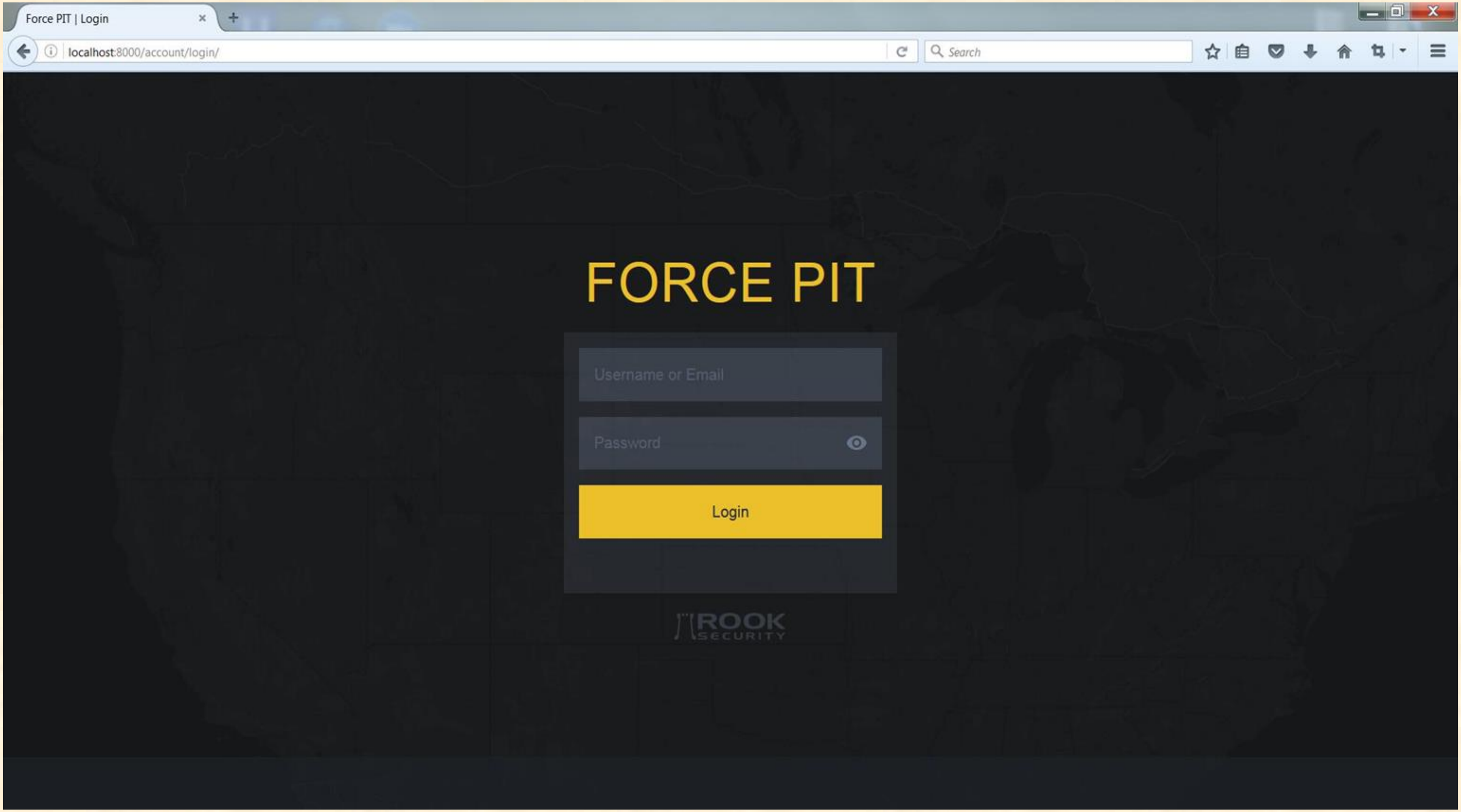
Project Overview

- Integration into Rook’s new Force platform
- Enhance analyst efficiency in daily work
- Provide an easy way to integrate new clients
- Machine learning to improve alert correlation

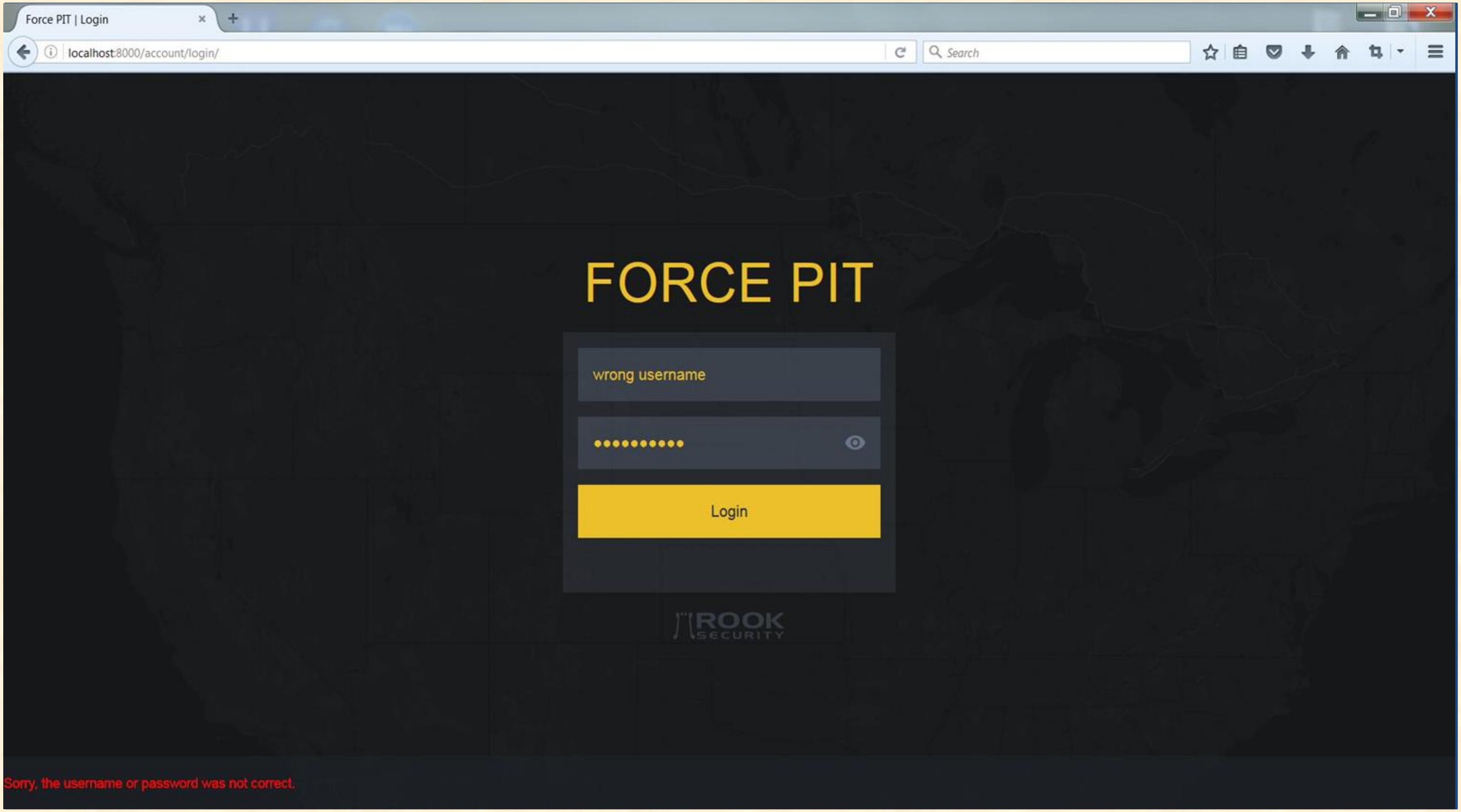
System Architecture



Login Page


Force PIT | Login
localhost:8000/account/login/
Search
FORCE PIT
Username or Email
Password
Login
ROOK
SECURITY

Login Page - Error Message

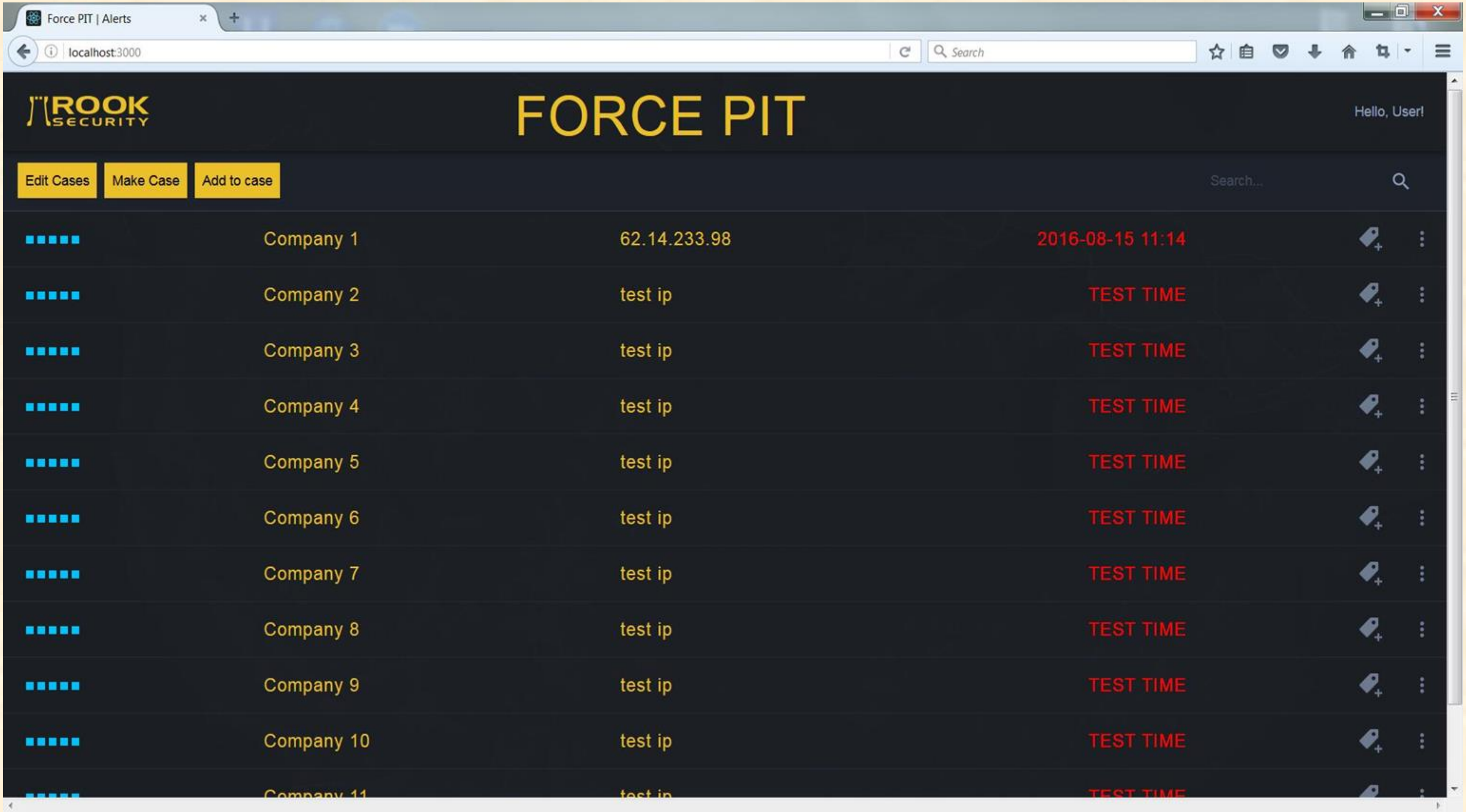


wrong username

●●●●●●●●●●●

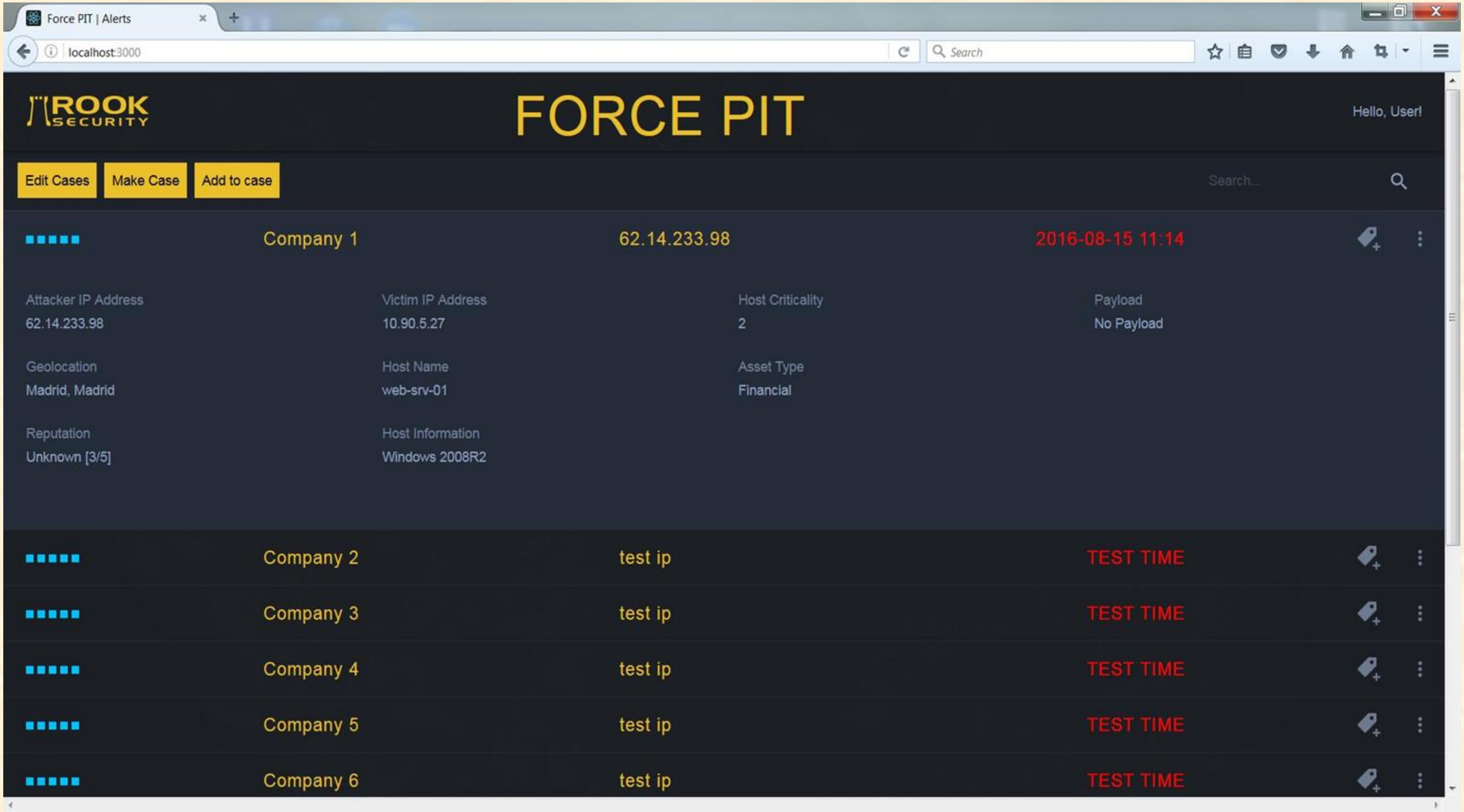
Sorry, the username or password was not correct.

Alerts Page



■■■■■	Company 1	62.14.233.98	2016-08-15 11:14
■■■■■	Company 2	test ip	TEST TIME
■■■■■	Company 3	test ip	TEST TIME
■■■■■	Company 4	test ip	TEST TIME
■■■■■	Company 5	test ip	TEST TIME
■■■■■	Company 6	test ip	TEST TIME
■■■■■	Company 7	test ip	TEST TIME
■■■■■	Company 8	test ip	TEST TIME
■■■■■	Company 9	test ip	TEST TIME
■■■■■	Company 10	test ip	TEST TIME
■■■■■	Company 11	test ip	TEST TIME

Alerts Page - Selected Alert



FORCE PIT

Hello, User!

■■■■■ Company 1 62.14.233.98 2016-08-15 11:14

Attacker IP Address
62.14.233.98

Victim IP Address
10.90.5.27

Host Criticality
2

Payload
No Payload

Geolocation
Madrid, Madrid

Host Name
web-srv-01

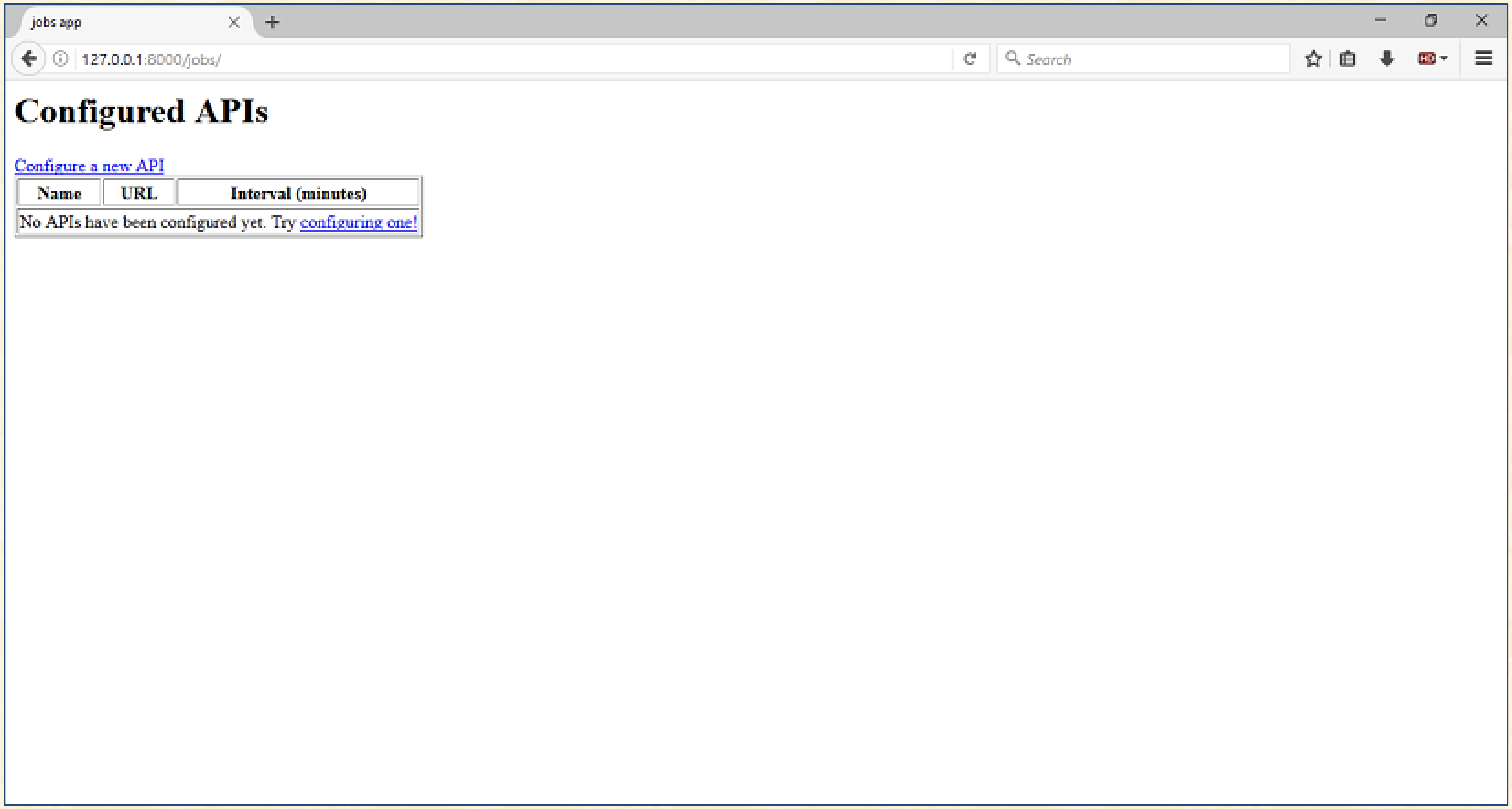
Asset Type
Financial

Reputation
Unknown [3/5]

Host Information
Windows 2008R2

■■■■■	Company 2	test ip	TEST TIME
■■■■■	Company 3	test ip	TEST TIME
■■■■■	Company 4	test ip	TEST TIME
■■■■■	Company 5	test ip	TEST TIME
■■■■■	Company 6	test ip	TEST TIME

Configuring an API

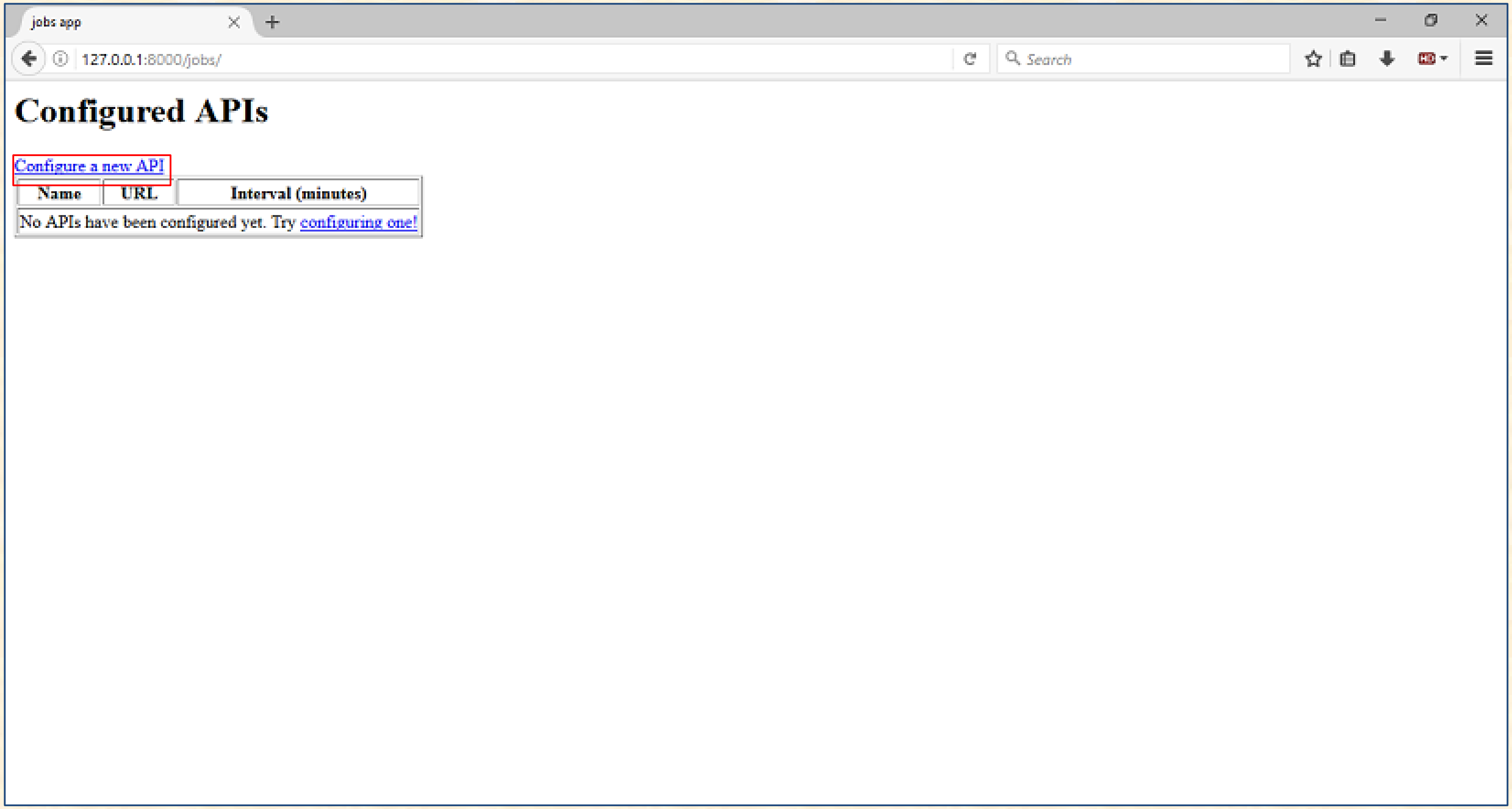


Configured APIs

Configure a new API

Name	URL	Interval (minutes)
No APIs have been configured yet. Try configuring one!		

Configuring an API

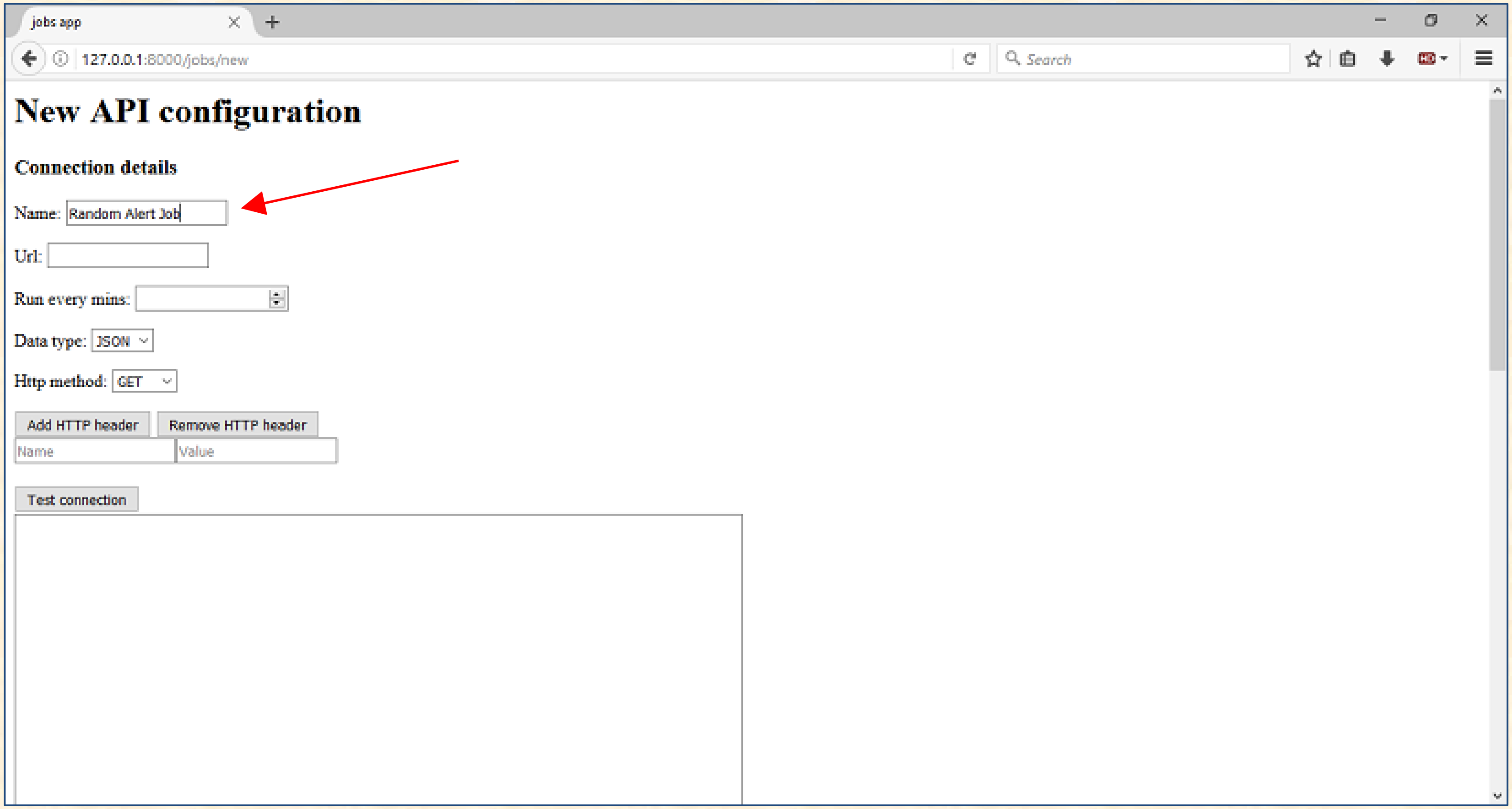


Configured APIs

Configure a new API

Name	URL	Interval (minutes)
No APIs have been configured yet. Try configuring one!		

Configuring an API



New API configuration

Connection details

Name: Random Alert Job

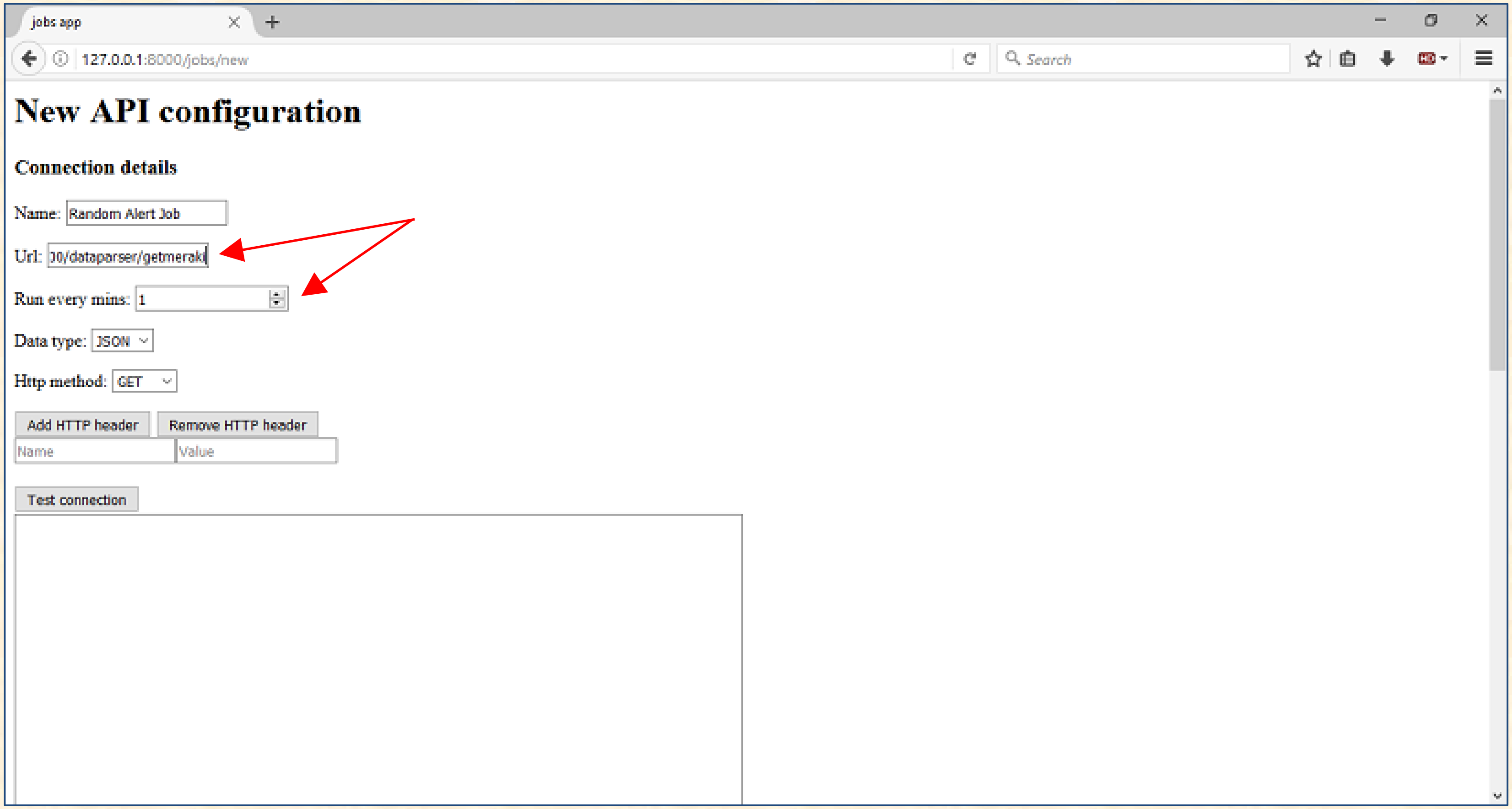
Url:

Run every mins:

Data type: JSON

Http method: GET

Configuring an API



New API configuration

Connection details

Name: Random Alert Job

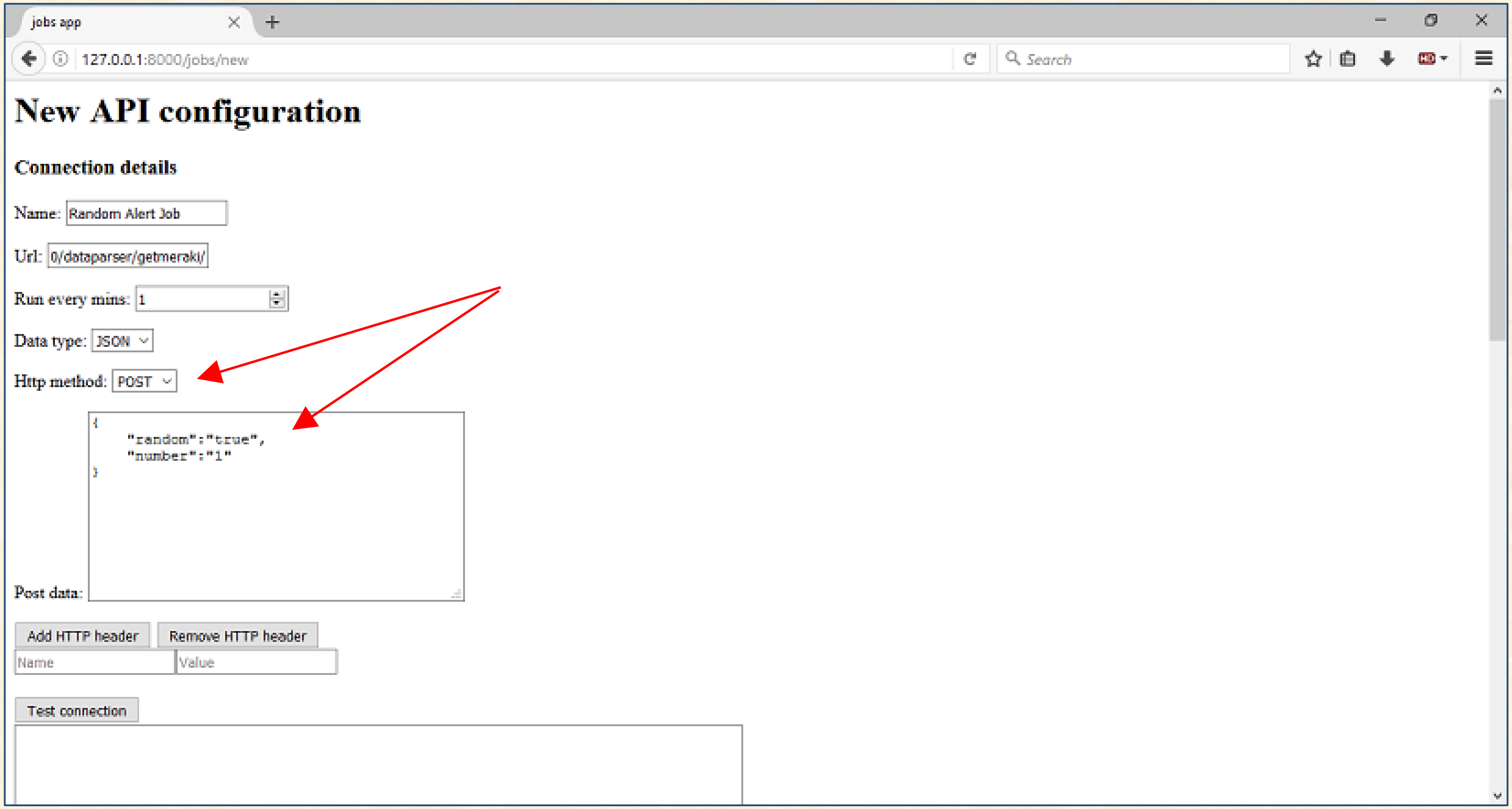
Url: 0/dataparser/getmeraki

Run every mins: 1

Data type: JSON

Http method: GET

Configuring an API



New API configuration

Connection details

Name: Random Alert Job

Url: 0/dataparser/getmeraki/

Run every mins: 1

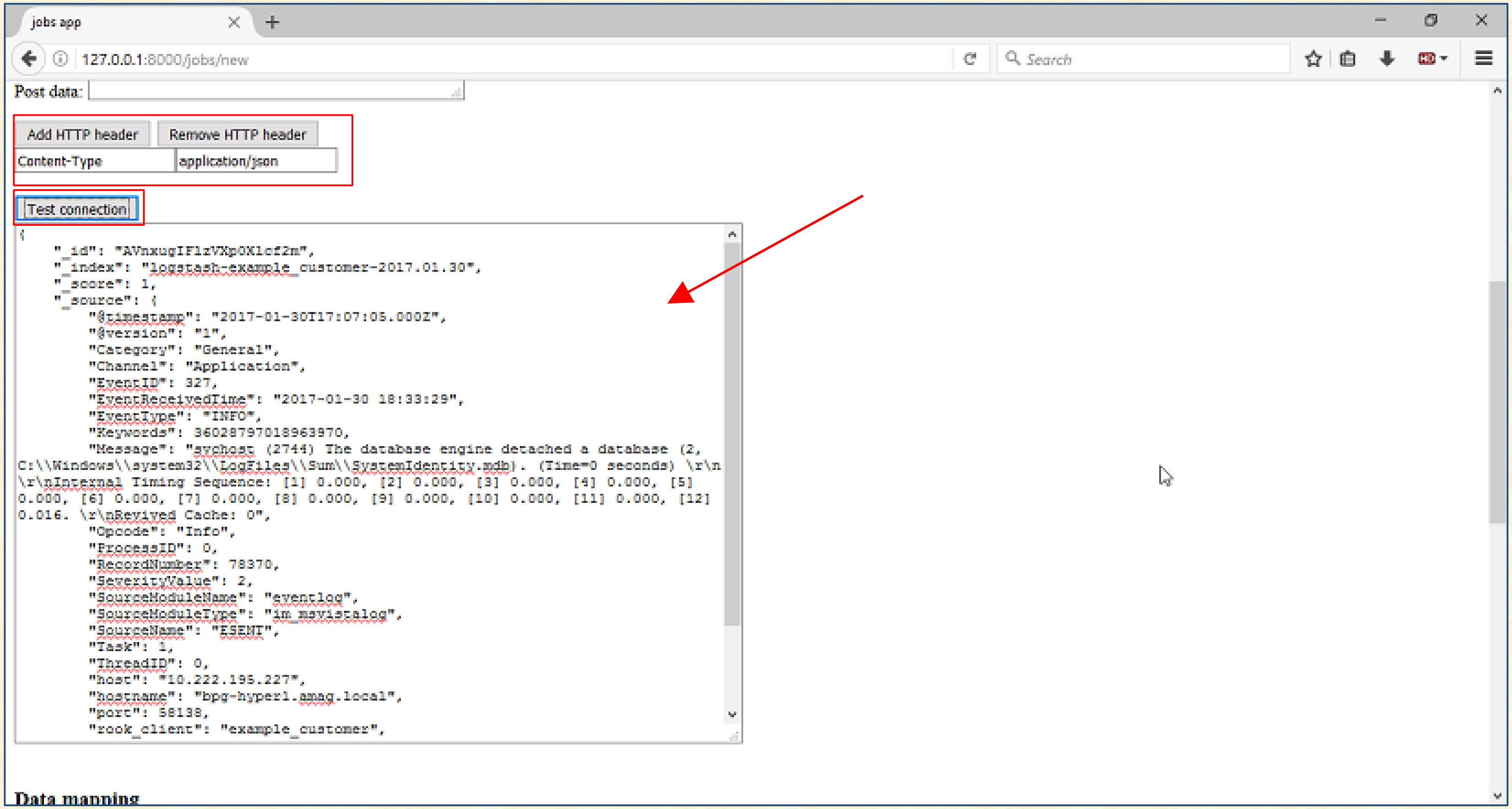
Data type: JSON

Http method: POST

Post data:

```
{
    "random":"true",
    "number":"1"
}
```

Configuring an API



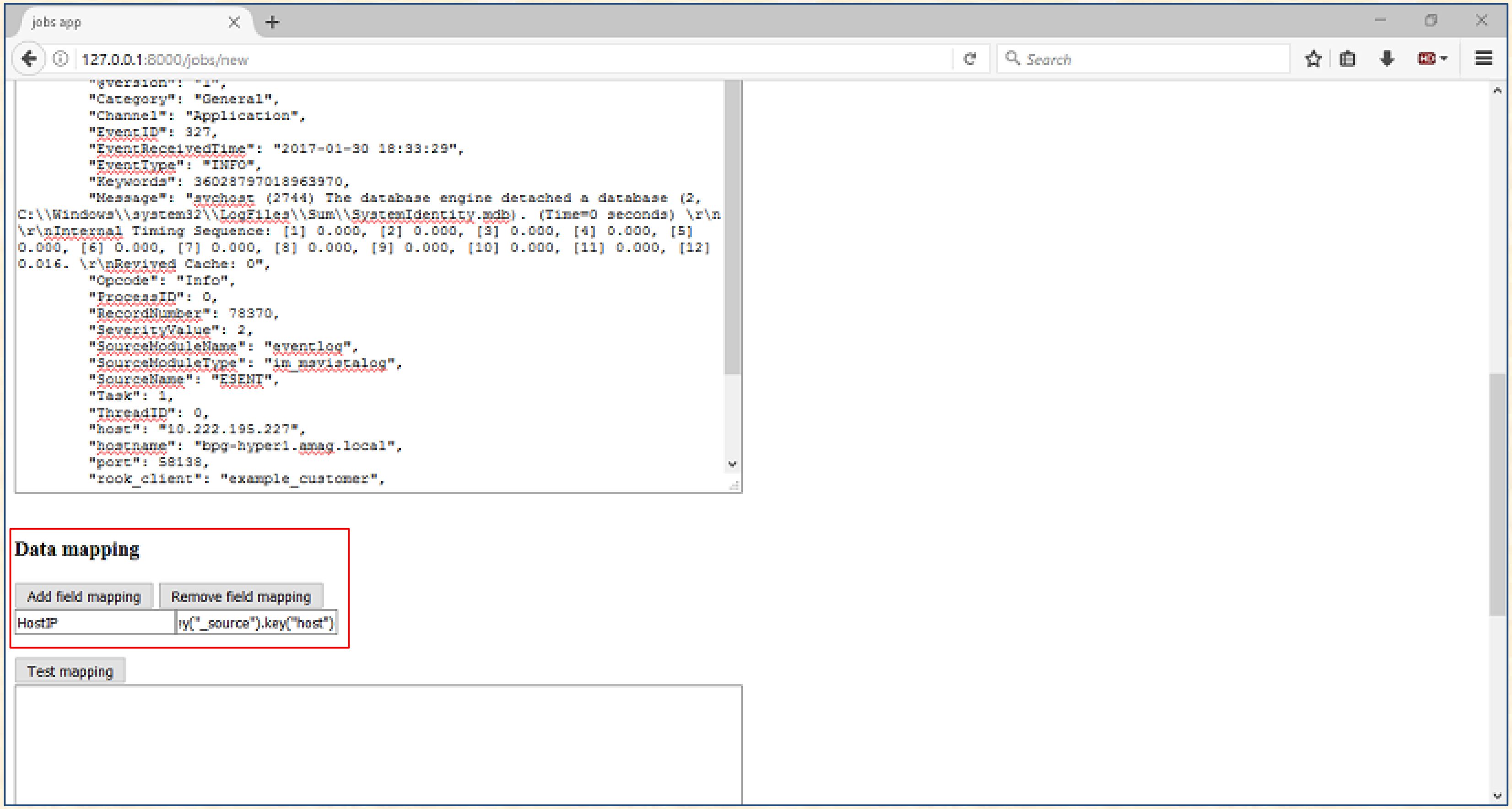
Post data:

Content-Type: application/json

```
{
    "_id": "AVnxugIFlzVXp0Xlcf2m",
    "_index": "logstash-example_customer-2017.01.30",
    "_score": 1,
    "_source": {
        "@timestamp": "2017-01-30T17:07:05.000Z",
        "@version": "1",
        "Category": "General",
        "Channel": "Application",
        "EventID": 327,
        "EventReceivedTime": "2017-01-30 18:33:29",
        "EventType": "INFO",
        "Keywords": 36028797018963970,
        "Message": "svchost (2744) The database engine detached a database (2,
C:\\Windows\\system32\\LogFiles\\Sum\\SystemIdentity.mdb). (Time=0 seconds) \r\n
\r\nInternal Timing Sequence: [1] 0.000, [2] 0.000, [3] 0.000, [4] 0.000, [5]
0.000, [6] 0.000, [7] 0.000, [8] 0.000, [9] 0.000, [10] 0.000, [11] 0.000, [12]
0.016. \r\nRevived Cache: 0",
        "Opcode": "Info",
        "ProcessID": 0,
        "RecordNumber": 78370,
        "SeverityValue": 2,
        "SourceModuleName": "eventlog",
        "SourceModuleType": "im_msvistalog",
        "SourceName": "ESENT",
        "Task": 1,
        "ThreadID": 0,
        "host": "10.222.195.227",
        "hostname": "bpg-hyper1.amag.local",
        "port": 58138,
        "rook_client": "example_customer",
```

Data mapping

Configuring an API

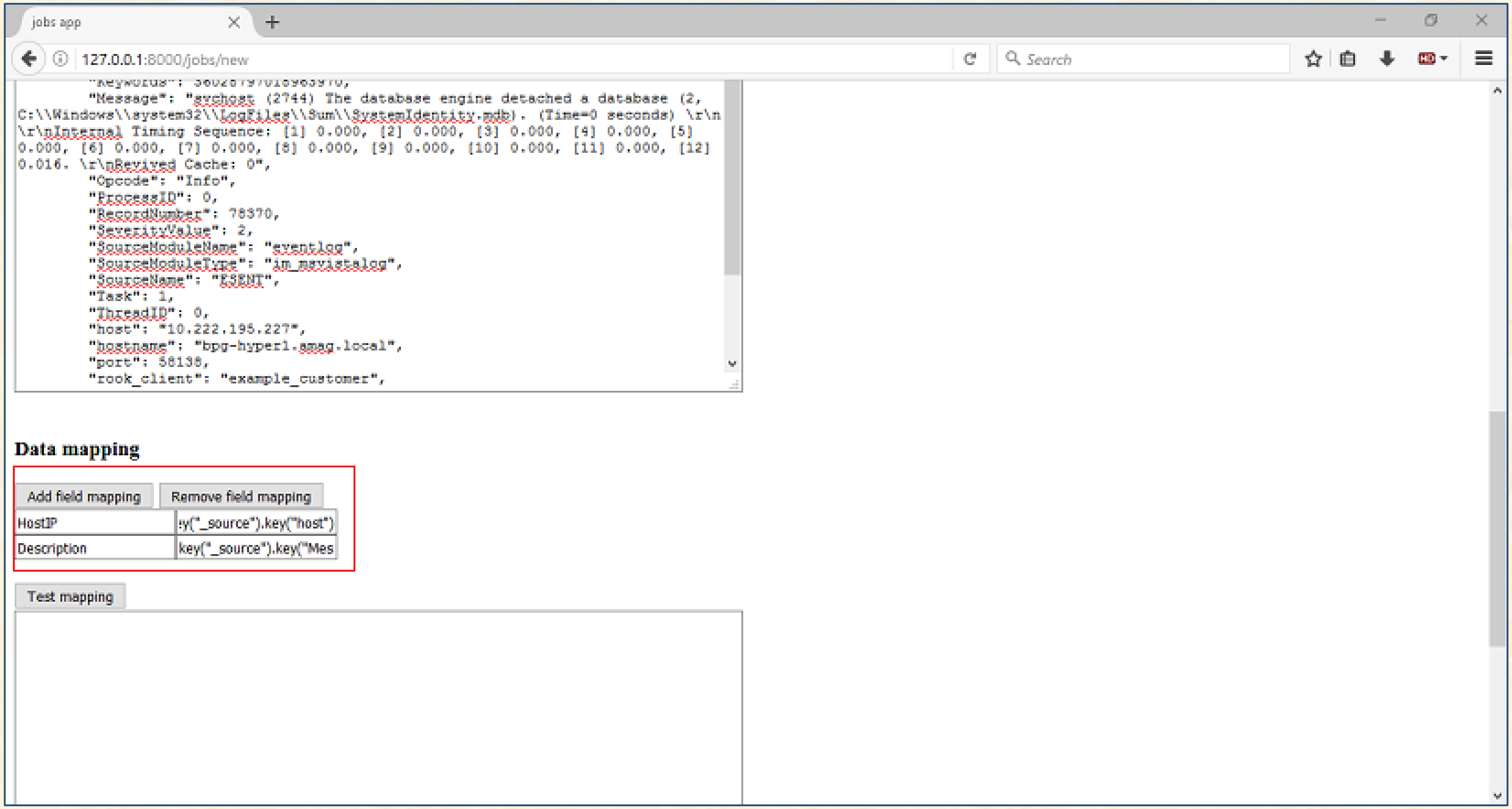


```
        "@version": "1",
        "Category": "General",
        "Channel": "Application",
        "EventID": 327,
        "EventReceivedTime": "2017-01-30 18:33:29",
        "EventType": "INFO",
        "Keywords": 36028797018963970,
        "Message": "svchost (2744) The database engine detached a database (2,
C:\\Windows\\system32\\LogFiles\\Sum\\SystemIdentity.mdb). (Time=0 seconds) \r\n
\r\nInternal Timing Sequence: [1] 0.000, [2] 0.000, [3] 0.000, [4] 0.000, [5]
0.000, [6] 0.000, [7] 0.000, [8] 0.000, [9] 0.000, [10] 0.000, [11] 0.000, [12]
0.016. \r\nRevived Cache: 0",
        "Opcode": "Info",
        "ProcessID": 0,
        "RecordNumber": 78370,
        "SeverityValue": 2,
        "SourceModuleName": "eventlog",
        "SourceModuleType": "im_msvistalog",
        "SourceName": "ESENT",
        "Task": 1,
        "ThreadID": 0,
        "host": "10.222.195.227",
        "hostname": "bpg-hyper1.amag.local",
        "port": 58138,
        "rook_client": "example_customer",
```

Data mapping

HostIP | ry("_source").key("host")

Configuring an API

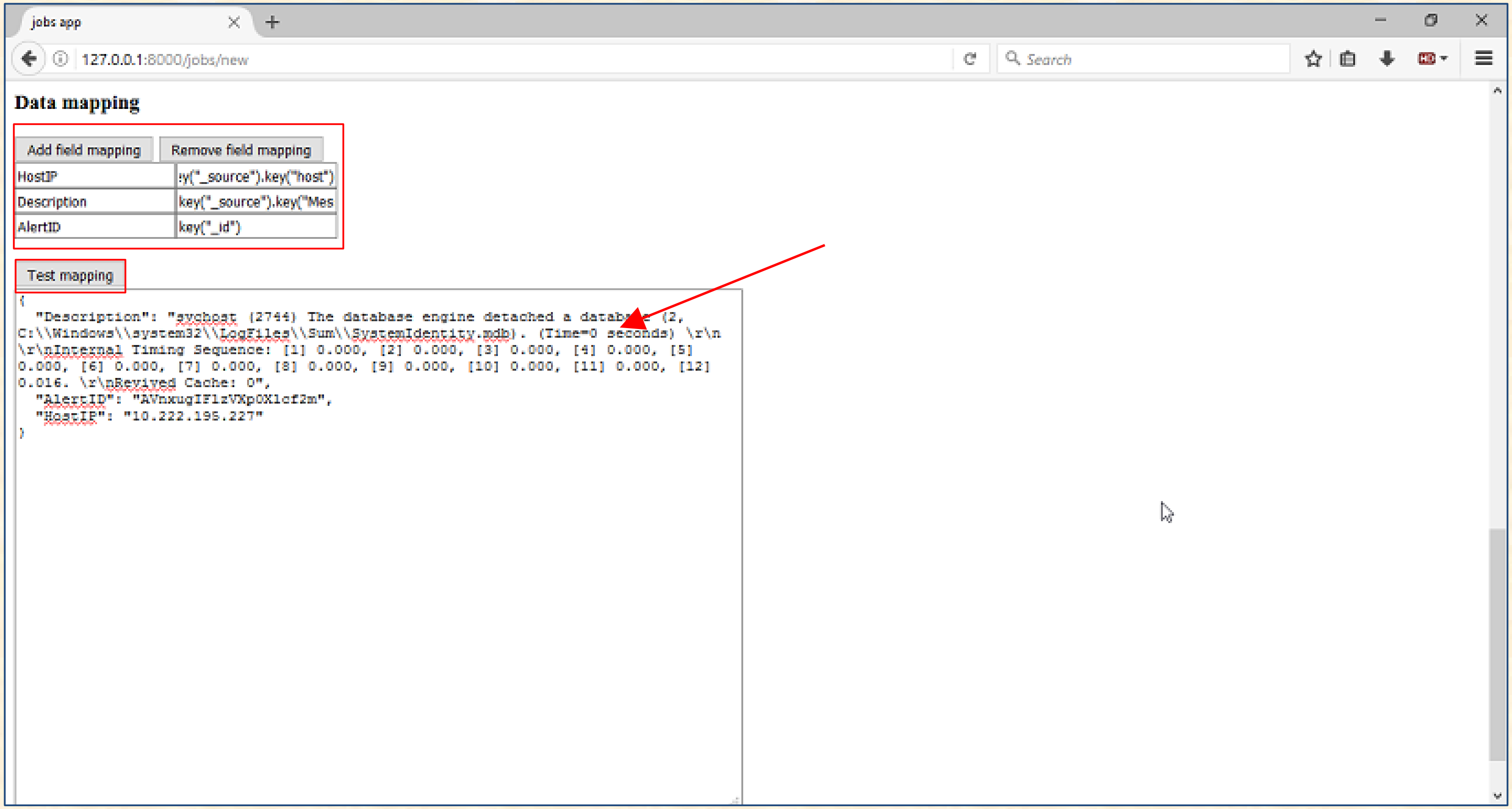


```
        "Keywords": 36028797018963970,
        "Message": "svchost (2744) The database engine detached a database (2,
C:\\Windows\\system32\\LogFiles\\Sum\\SystemIdentity.mdb). (Time=0 seconds) \r\n
\r\nInternal Timing Sequence: [1] 0.000, [2] 0.000, [3] 0.000, [4] 0.000, [5]
0.000, [6] 0.000, [7] 0.000, [8] 0.000, [9] 0.000, [10] 0.000, [11] 0.000, [12]
0.016. \r\nRevived Cache: 0",
        "Opcode": "Info",
        "ProcessID": 0,
        "RecordNumber": 78370,
        "SeverityValue": 2,
        "SourceModuleName": "eventlog",
        "SourceModuleType": "im_msvistalog",
        "SourceName": "ESENT",
        "Task": 1,
        "ThreadID": 0,
        "host": "10.222.195.227",
        "hostname": "bpg-hyper1.amag.local",
        "port": 58138,
        "rook_client": "example_customer",
```

Data mapping

HostIP	:y("_source").key("host")
Description	key("_source").key("Mes

Configuring an API

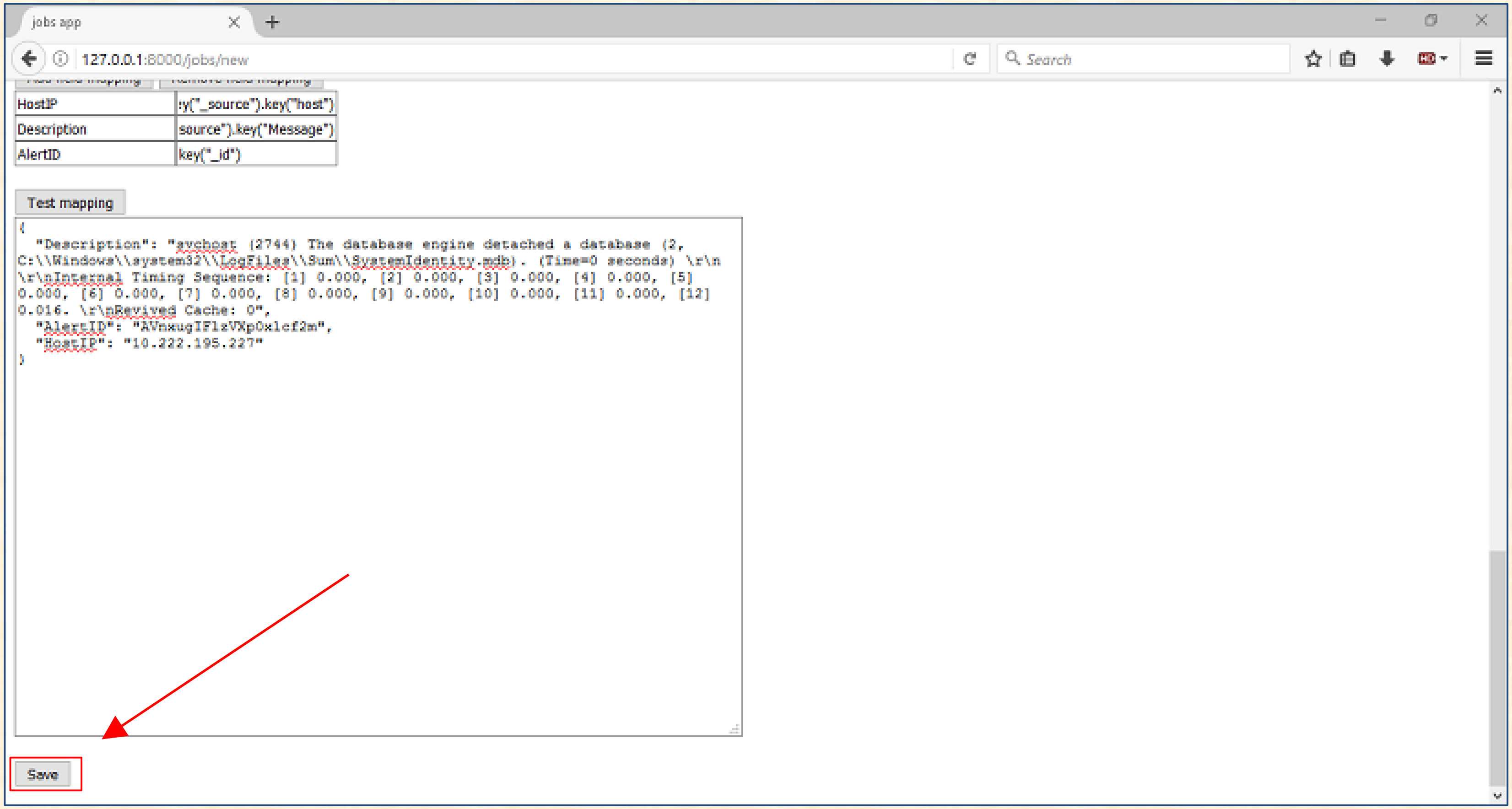


Data mapping

HostIP	:y("_source").key("host")
Description	key("_source").key("Mes
AlertID	key("_id")

```
{
  "Description": "svchost (2744) The database engine detached a database (2,
C:\\Windows\\system32\\LogFiles\\Sum\\SystemIdentity.mdb). (Time=0 seconds) \r\n
\r\nInternal Timing Sequence: [1] 0.000, [2] 0.000, [3] 0.000, [4] 0.000, [5]
0.000, [6] 0.000, [7] 0.000, [8] 0.000, [9] 0.000, [10] 0.000, [11] 0.000, [12]
0.016. \r\nRevived Cache: 0",
  "AlertID": "AVnxugIFlzVXp0Xlcf2m",
  "HostIP": "10.222.195.227"
}
```

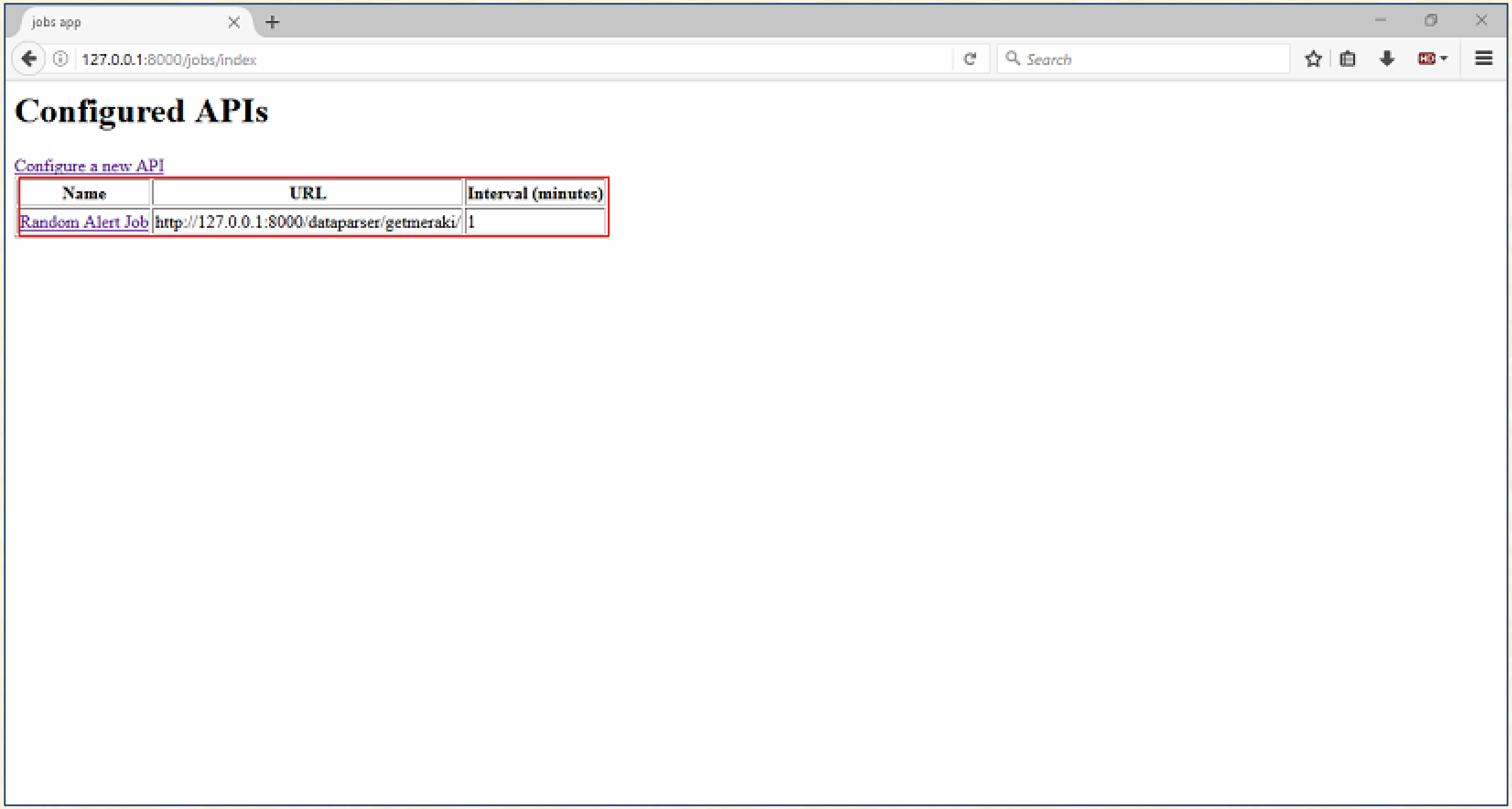
Configuring an API



HostIP	:y("_source").key("host")
Description	source").key("Message")
AlertID	key("_id")

```
{
  "Description": "svchost (2744) The database engine detached a database (2,
C:\\Windows\\system32\\LogFiles\\Sum\\SystemIdentity.mdb). (Time=0 seconds) \r\n
\r\nInternal Timing Sequence: [1] 0.000, [2] 0.000, [3] 0.000, [4] 0.000, [5]
0.000, [6] 0.000, [7] 0.000, [8] 0.000, [9] 0.000, [10] 0.000, [11] 0.000, [12]
0.016. \r\nRevived Cache: 0",
  "AlertID": "AVnxugIFlzVXp0xlcf2m",
  "HostIP": "10.222.195.227"
}
```

Configuring an API

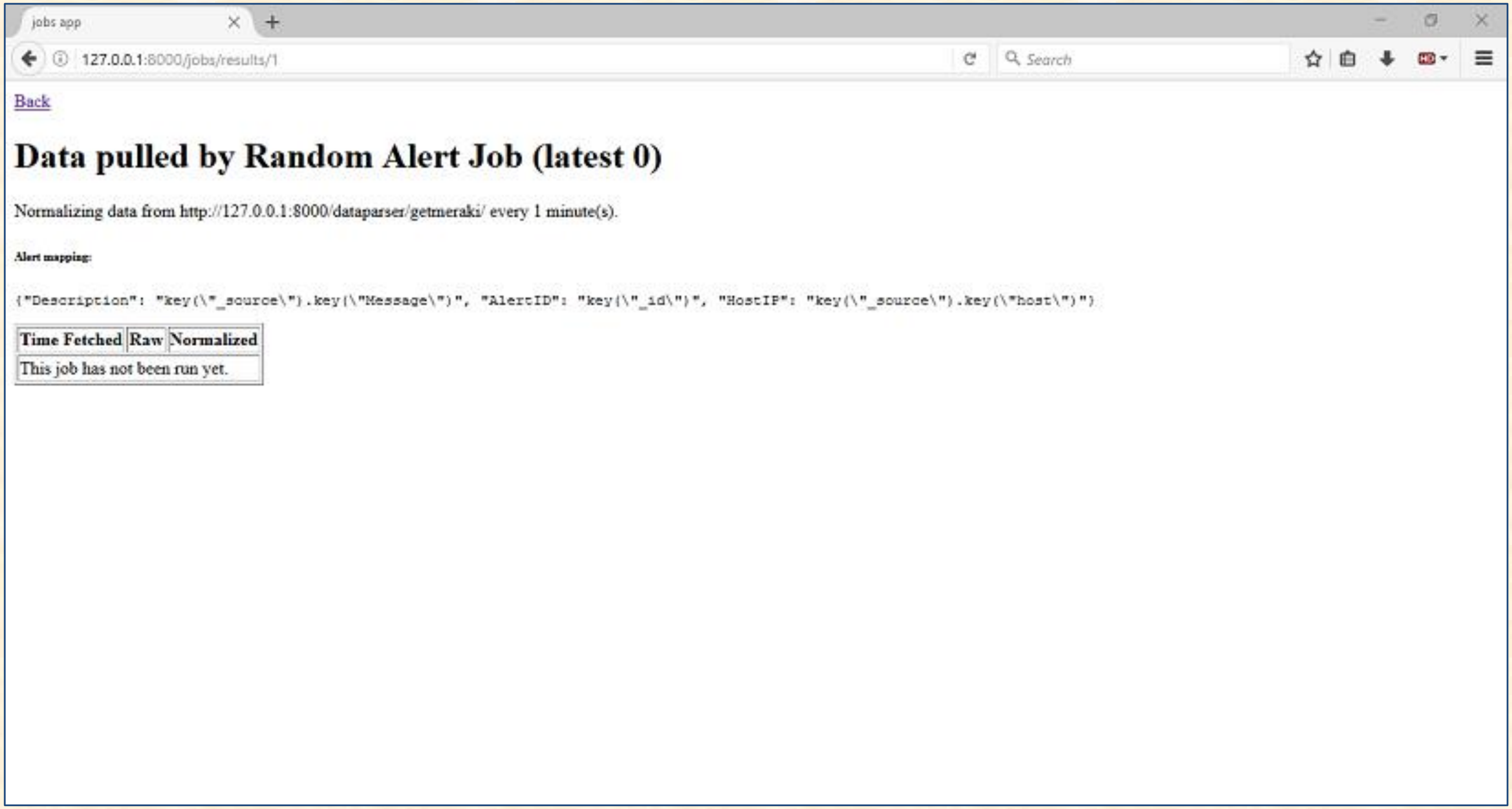


Configured APIs

Configure a new API

Name	URL	Interval (minutes)
Random Alert Job	http://127.0.0.1:8000/dataparser/getmeraki/	1

Configuring an API



Back

Data pulled by Random Alert Job (latest 0)

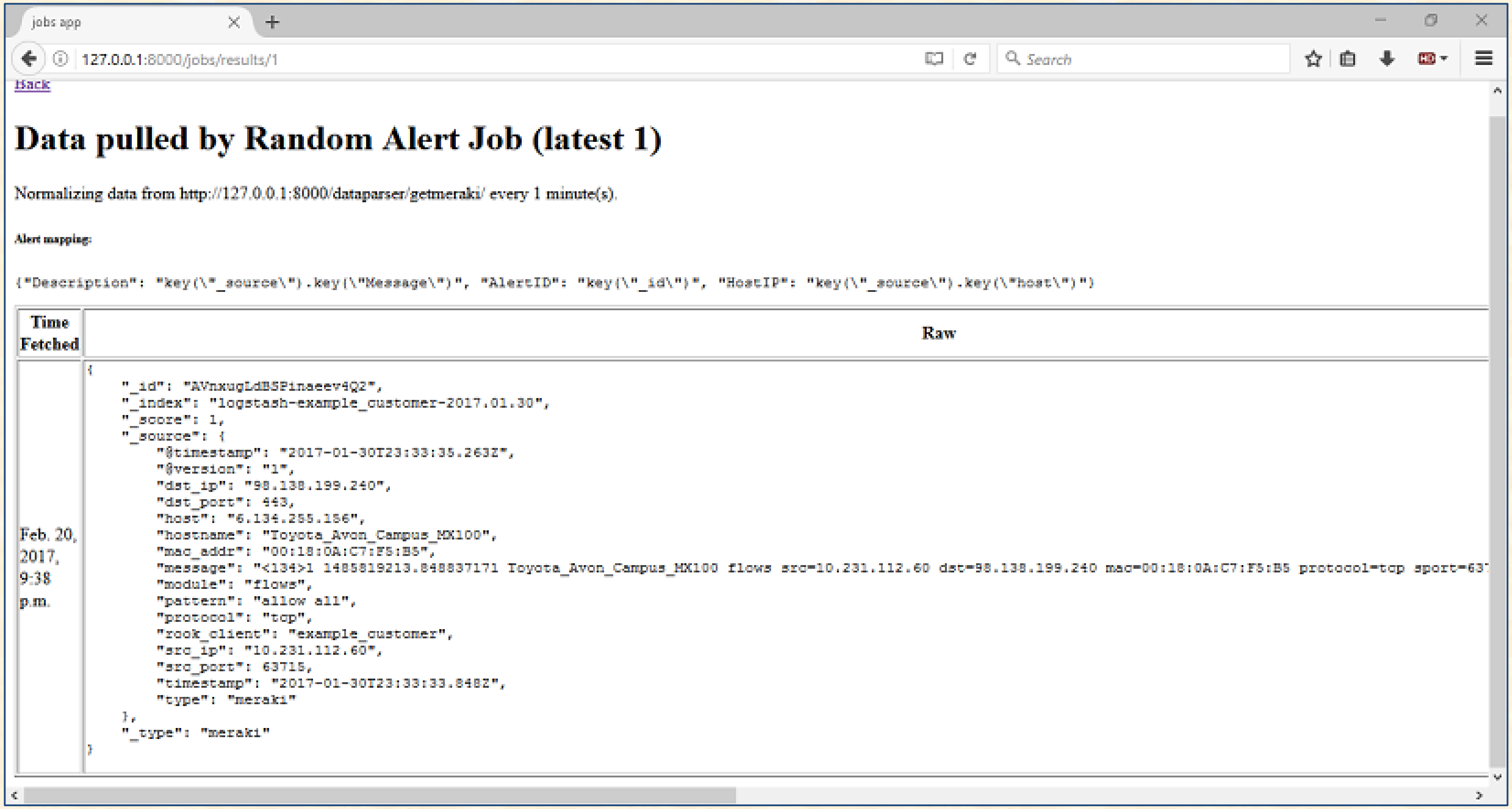
Normalizing data from http://127.0.0.1:8000/dataparser/getmeraki/ every 1 minute(s).

Alert mapping:

```
{"Description": "key(\"_source\").key(\"Message\")", "AlertID": "key(\"_id\")", "HostIP": "key(\"_source\").key(\"host\")"}
```

Time Fetched	Raw	Normalized
This job has not been run yet.		

Configuring an API



Data pulled by Random Alert Job (latest 1)

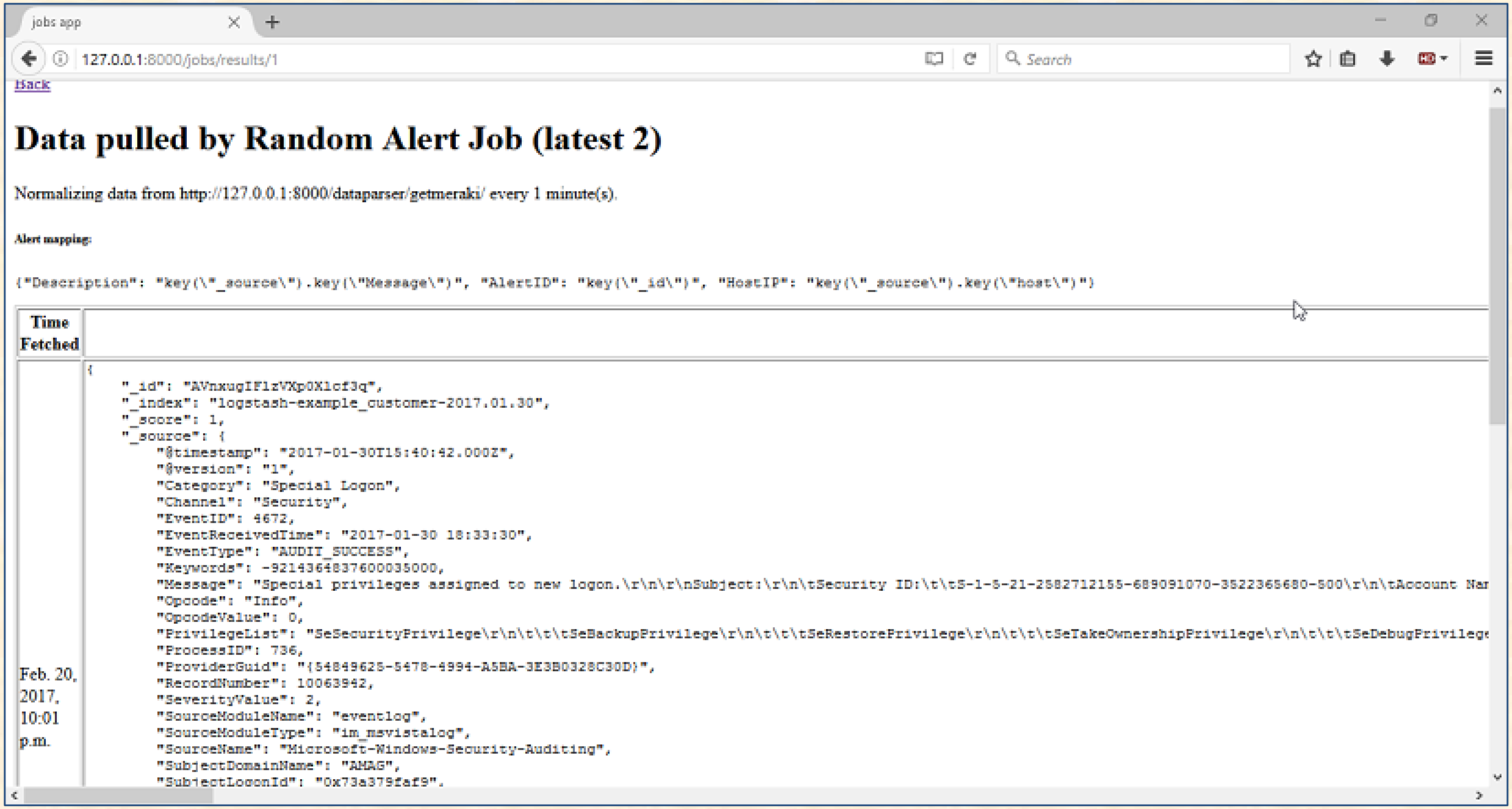
Normalizing data from http://127.0.0.1:8000/dataparser/getmeraki/ every 1 minute(s).

Alert mapping:

```
{"Description": "key(\"_source\").key(\"Message\")", "AlertID": "key(\"_id\")", "HostIP": "key(\"_source\").key(\"host\")"}
```

<table>
<tr><th>Time Fetched</th><th>Raw</th></tr>
<tr><td>Feb. 20, 2017, 9:38 p.m.</td><td><pre>
{
    "_id": "AVnxugLdBSPinaeev4Q2",
    "_index": "logstash-example_customer-2017.01.30",
    "_score": 1,
    "_source": {
        "@timestamp": "2017-01-30T23:33:35.263Z",
        "@version": "1",
        "dst_ip": "98.138.199.240",
        "dst_port": 443,
        "host": "6.134.255.156",
        "hostname": "Toyota_Avon_Campus_MX100",
        "mac_addr": "00:18:0A:C7:F5:B5",
        "message": "<134>1 1485819213.848837171 Toyota_Avon_Campus_MX100 flows src=10.231.112.60 dst=98.138.199.240 mac=00:18:0A:C7:F5:B5 protocol=tcp sport=63
        "module": "flows",
        "pattern": "allow all",
        "protocol": "tcp",
        "rook_client": "example_customer",
        "src_ip": "10.231.112.60",
        "src_port": 63715,
        "timestamp": "2017-01-30T23:33:33.848Z",
        "type": "meraki"
    },
    "_type": "meraki"
}
</pre></td></tr>
</table>

Configuring an API



Back

Data pulled by Random Alert Job (latest 2)

Normalizing data from http://127.0.0.1:8000/dataparser/getmeraki/ every 1 minute(s).

Alert mapping:

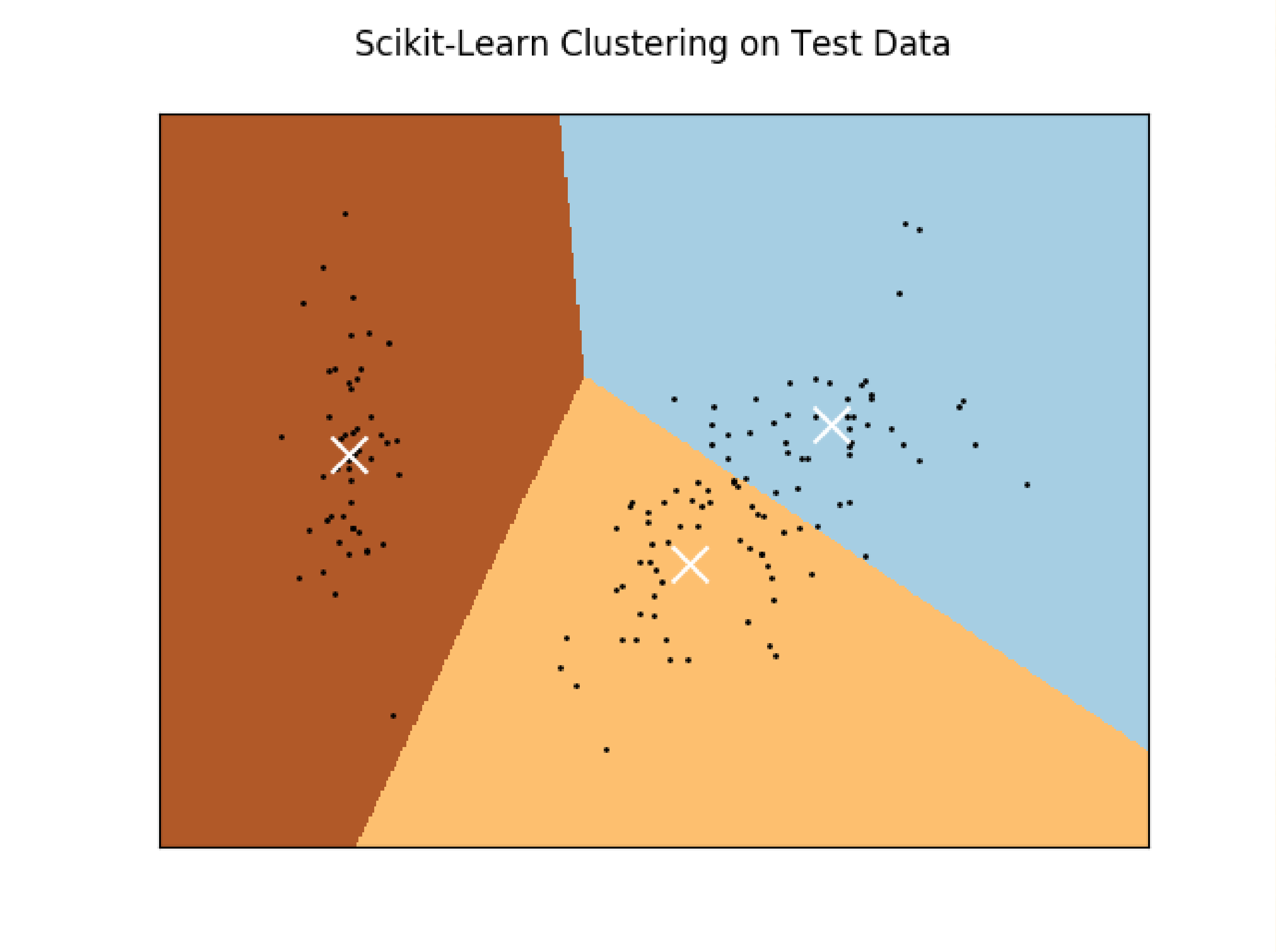
```
{"Description": "key(\"_source\").key(\"Message\")", "AlertID": "key(\"_id\")", "HostIP": "key(\"_source\").key(\"host\")"}
```

Time Fetched

Feb. 20, 2017, 10:01 p.m.

```
{
    "_id": "AVnxugIFlzVXp0Xlcf3q",
    "_index": "logstash-example_customer-2017.01.30",
    "_score": 1,
    "_source": {
        "@timestamp": "2017-01-30T15:40:42.000Z",
        "@version": "1",
        "Category": "Special Logon",
        "Channel": "Security",
        "EventID": 4672,
        "EventReceivedTime": "2017-01-30 18:33:30",
        "EventType": "AUDIT_SUCCESS",
        "Keywords": -9214364837600035000,
        "Message": "Special privileges assigned to new logon.\r\n\r\nSubject:\r\n\tSecurity ID:\t\tS-1-5-21-2582712155-689091070-3522365680-500\r\n\tAccount Nar
        "Opcode": "Info",
        "OpcodeValue": 0,
        "PrivilegeList": "SeSecurityPrivilege\r\n\t\t\tSeBackupPrivilege\r\n\t\t\tSeRestorePrivilege\r\n\t\t\tSeTakeOwnershipPrivilege\r\n\t\t\tSeDebugPrivilege
        "ProcessID": 736,
        "ProviderGuid": "{54849625-5478-4994-A5BA-3E3B0328C30D}",
        "RecordNumber": 10063942,
        "SeverityValue": 2,
        "SourceModuleName": "eventlog",
        "SourceModuleType": "im_msvistalog",
        "SourceName": "Microsoft-Windows-Security-Auditing",
        "SubjectDomainName": "AMAG",
        "SubjectLogonId": "0x73a379faf9",
```

ML Clustering into Cases



What’s left to do?

- Make UI design cohesive, get Rook feedback
- Use Django “Channels” library to update React/Redux UI in real time
- Finish ML, append to data normalization flow
- Build out support for as many APIs as we can

Questions?

? ? ? ?

? ?

? ? ?