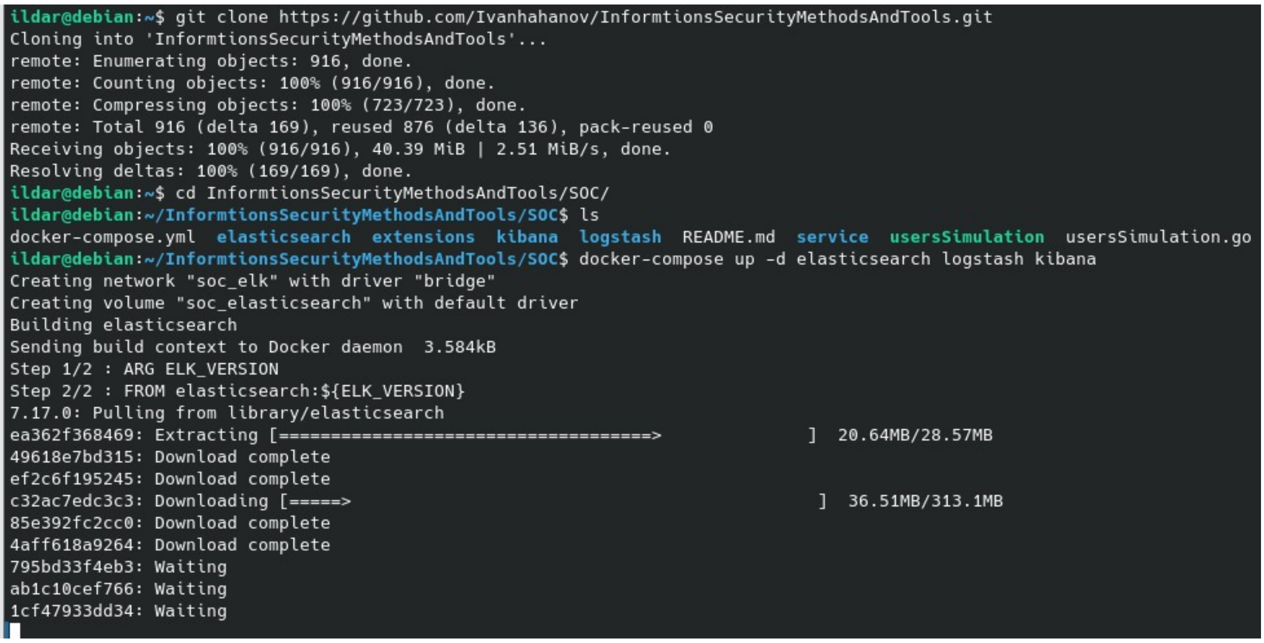
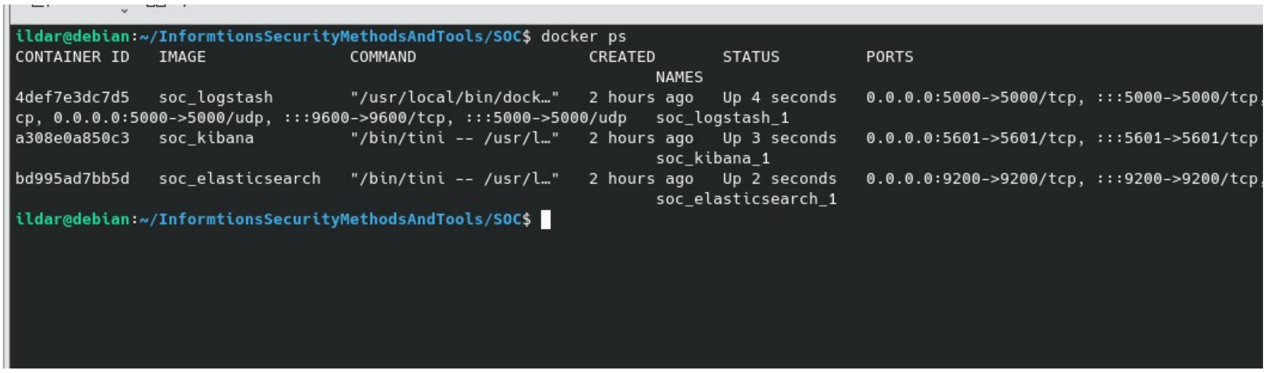
Логирование и визуализация с помощью elastic, logstash, kibana

Клонирование репозитория, запуск контейнеров



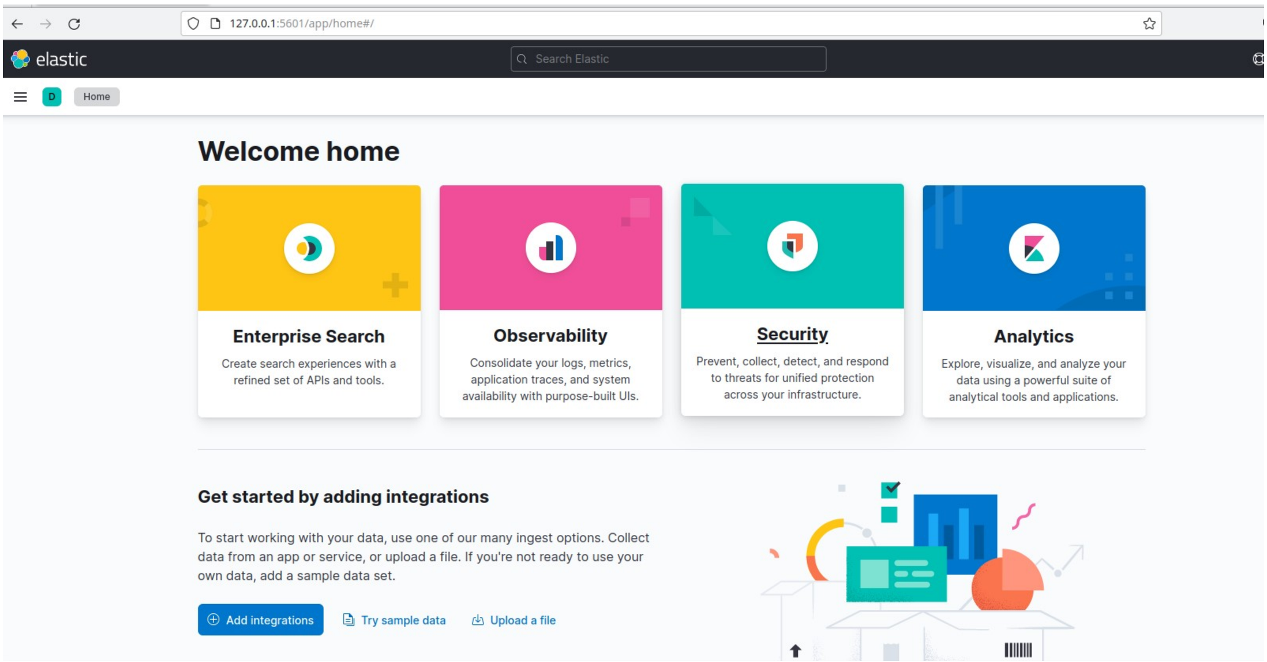
```
ildar@debian:~$ git clone https://github.com/Ivanhahanov/InformtionsSecurityMethodsAndTools.git
Cloning into 'InformtionsSecurityMethodsAndTools'...
remote: Enumerating objects: 916, done.
remote: Counting objects: 100% (916/916), done.
remote: Compressing objects: 100% (723/723), done.
remote: Total 916 (delta 169), reused 876 (delta 136), pack-reused 0
Receiving objects: 100% (916/916), 40.39 MiB | 2.51 MiB/s, done.
Resolving deltas: 100% (169/169), done.
ildar@debian:~$ cd InformtionsSecurityMethodsAndTools/SOC/
ildar@debian:~/InformtionsSecurityMethodsAndTools/SOC$ ls
docker-compose.yml  elasticsearch  extensions  kibana  logstash  README.md  service  usersSimulation  usersSimulation.go
ildar@debian:~/InformtionsSecurityMethodsAndTools/SOC$ docker-compose up -d elasticsearch logstash kibana
Creating network "soc_elk" with driver "bridge"
Creating volume "soc_elasticsearch" with default driver
Building elasticsearch
Sending build context to Docker daemon  3.584kB
Step 1/2 : ARG ELK_VERSION
Step 2/2 : FROM elasticsearch:${ELK_VERSION}
7.17.0: Pulling from library/elasticsearch
ea362f368469: Extracting [===================================>              ]  20.64MB/28.57MB
49618e7bd315: Download complete
ef2c6f195245: Download complete
c32ac7edc3c3: Downloading [=====>                                           ]  36.51MB/313.1MB
85e392fc2cc0: Download complete
4aff618a9264: Download complete
795bd33f4eb3: Waiting
ab1c10cef766: Waiting
1cf47933dd34: Waiting
```

Проверка состояния контейнеров



```
ildar@debian:~/InformtionsSecurityMethodsAndTools/SOC$ docker ps
CONTAINER ID   IMAGE                COMMAND                  CREATED       STATUS          PORTS
                                                                 NAMES
4def7e3dc7d5   soc_logstash         "/usr/local/bin/dock…"   2 hours ago   Up 4 seconds    0.0.0.0:5000->5000/tcp, :::5000->5000/tcp,
cp, 0.0.0.0:5000->5000/udp, :::9600->9600/tcp, :::5000->5000/udp   soc_logstash_1
a308e0a850c3   soc_kibana           "/bin/tini -- /usr/l…"   2 hours ago   Up 3 seconds    0.0.0.0:5601->5601/tcp, :::5601->5601/tcp
                                                                 soc_kibana_1
bd995ad7bb5d   soc_elasticsearch    "/bin/tini -- /usr/l…"   2 hours ago   Up 2 seconds    0.0.0.0:9200->9200/tcp, :::9200->9200/tcp,
                                                                 soc_elasticsearch_1
ildar@debian:~/InformtionsSecurityMethodsAndTools/SOC$
```

Успешный вход в elastic



Welcome home

Enterprise Search
Create search experiences with a refined set of APIs and tools.

Observability
Consolidate your logs, metrics, application traces, and system availability with purpose-built UIs.

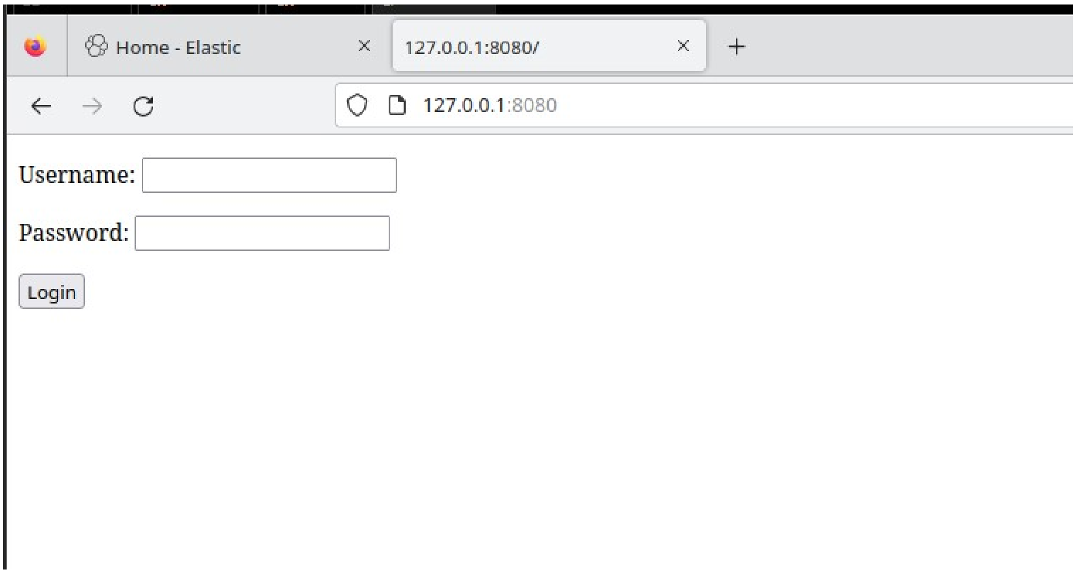
Security
Prevent, collect, detect, and respond to threats for unified protection across your infrastructure.

Analytics
Explore, visualize, and analyze your data using a powerful suite of analytical tools and applications.

Get started by adding integrations

To start working with your data, use one of our many ingest options. Collect data from an app or service, or upload a file. If you're not ready to use your own data, add a sample data set.

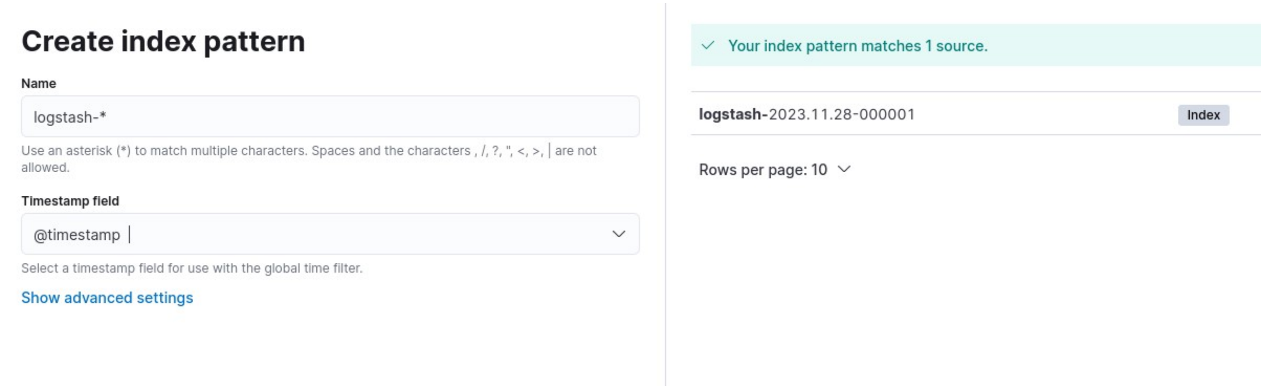
Проверка работоспособности формы ввода логина/пароля



Username:

Password:

Создание индекса с помощью маски logstash-*



Create index pattern

Name

logstash-*

Use an asterisk (*) to match multiple characters. Spaces and the characters , /, ?, ", <, >, | are not allowed.

Timestamp field

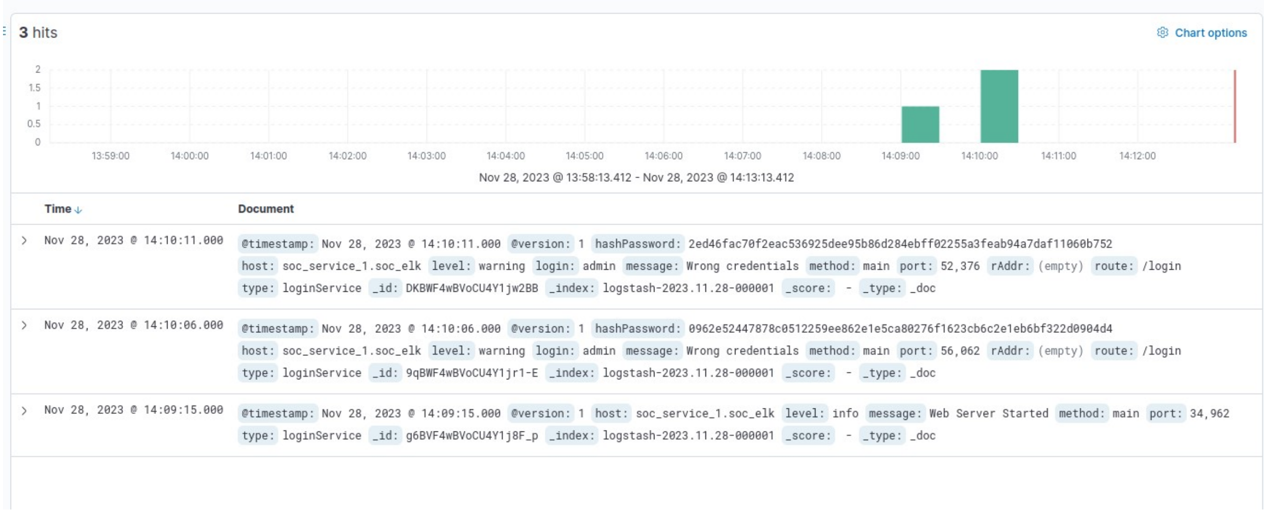
@timestamp

Select a timestamp field for use with the global time filter.

Your index pattern matches 1 source.

logstash-2023.11.28-000001

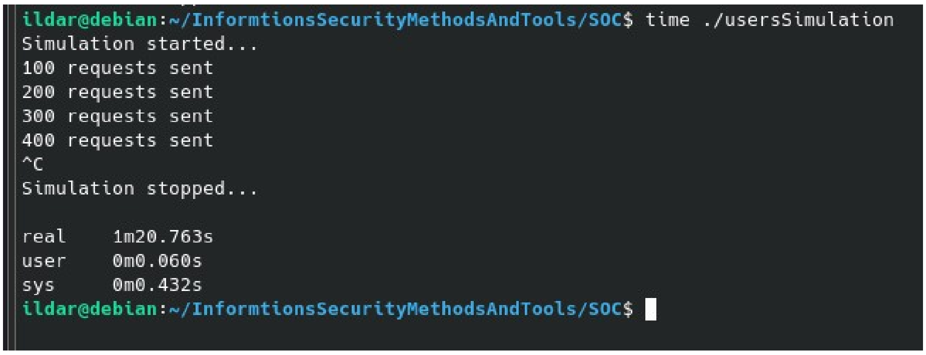
Активность в логах по паттерну



Nov 28, 2023 @ 13:58:13.412 - Nov 28, 2023 @ 14:13:13.412

Time ↓	Document
Nov 28, 2023 @ 14:10:11.000	@timestamp: Nov 28, 2023 @ 14:10:11.000 @version: 1 hashPassword: 2ed46fac70f2eac536925dee95b86d284ebff02255a3feab94a7daf11060b752 host: soc_service_1.soc_elk level: warning login: admin message: Wrong credentials method: main port: 52,376 rAddr: (empty) route: /login type: loginService _id: DKBWF4wBVoCU4Y1jw2BB _index: logstash-2023.11.28-000001 _score: - _type: _doc
Nov 28, 2023 @ 14:10:06.000	@timestamp: Nov 28, 2023 @ 14:10:06.000 @version: 1 hashPassword: 0962e52447878c0512259ee862e1e5ca80276f1623cb6c2e1eb6bf322d0904d4 host: soc_service_1.soc_elk level: warning login: admin message: Wrong credentials method: main port: 56,062 rAddr: (empty) route: /login type: loginService _id: 9qBWF4wBVoCU4Y1jr1-E _index: logstash-2023.11.28-000001 _score: - _type: _doc
Nov 28, 2023 @ 14:09:15.000	@timestamp: Nov 28, 2023 @ 14:09:15.000 @version: 1 host: soc_service_1.soc_elk level: info message: Web Server Started method: main port: 34,962 type: loginService _id: g6BVF4wBVoCU4Y1j8F_p _index: logstash-2023.11.28-000001 _score: - _type: _doc

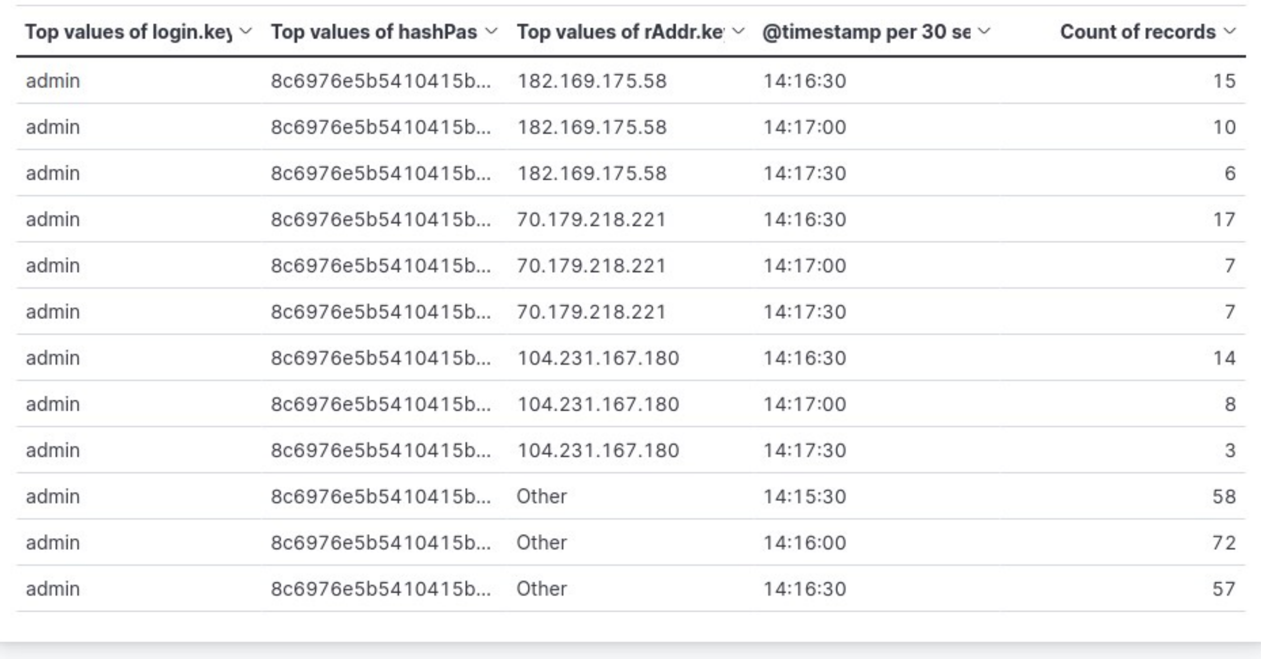
Запуск симуляции активности, продолжительность 1м20с



```
ildar@debian:~/InformtionsSecurityMethodsAndTools/SOC$ time ./usersSimulation
Simulation started...
100 requests sent
200 requests sent
300 requests sent
400 requests sent
^C
Simulation stopped...

real	1m20.763s
user	0m0.060s
sys	0m0.432s
ildar@debian:~/InformtionsSecurityMethodsAndTools/SOC$ 
```

Средства визуализации логов



Top values of login.key ⌄	Top values of hashPas ⌄	Top values of rAddr.ke ⌄	@timestamp per 30 se ⌄	Count of records ⌄
admin	8c6976e5b5410415b...	182.169.175.58	14:16:30	15
admin	8c6976e5b5410415b...	182.169.175.58	14:17:00	10
admin	8c6976e5b5410415b...	182.169.175.58	14:17:30	6
admin	8c6976e5b5410415b...	70.179.218.221	14:16:30	17
admin	8c6976e5b5410415b...	70.179.218.221	14:17:00	7
admin	8c6976e5b5410415b...	70.179.218.221	14:17:30	7
admin	8c6976e5b5410415b...	104.231.167.180	14:16:30	14
admin	8c6976e5b5410415b...	104.231.167.180	14:17:00	8
admin	8c6976e5b5410415b...	104.231.167.180	14:17:30	3
admin	8c6976e5b5410415b...	Other	14:15:30	58
admin	8c6976e5b5410415b...	Other	14:16:00	72
admin	8c6976e5b5410415b...	Other	14:16:30	57