FBK Pentest Lab

Создаём лабораторию для оптимизации системы внутреннего контроля в части ИБ

Who we are?

FBK | CS
cybersecurity

We are a subsidiary of the largest Russian audit and consulting FBK Grant Thornton and specializes in providing services in the field of practical information security.

Mikhail Firstov

Head of research group

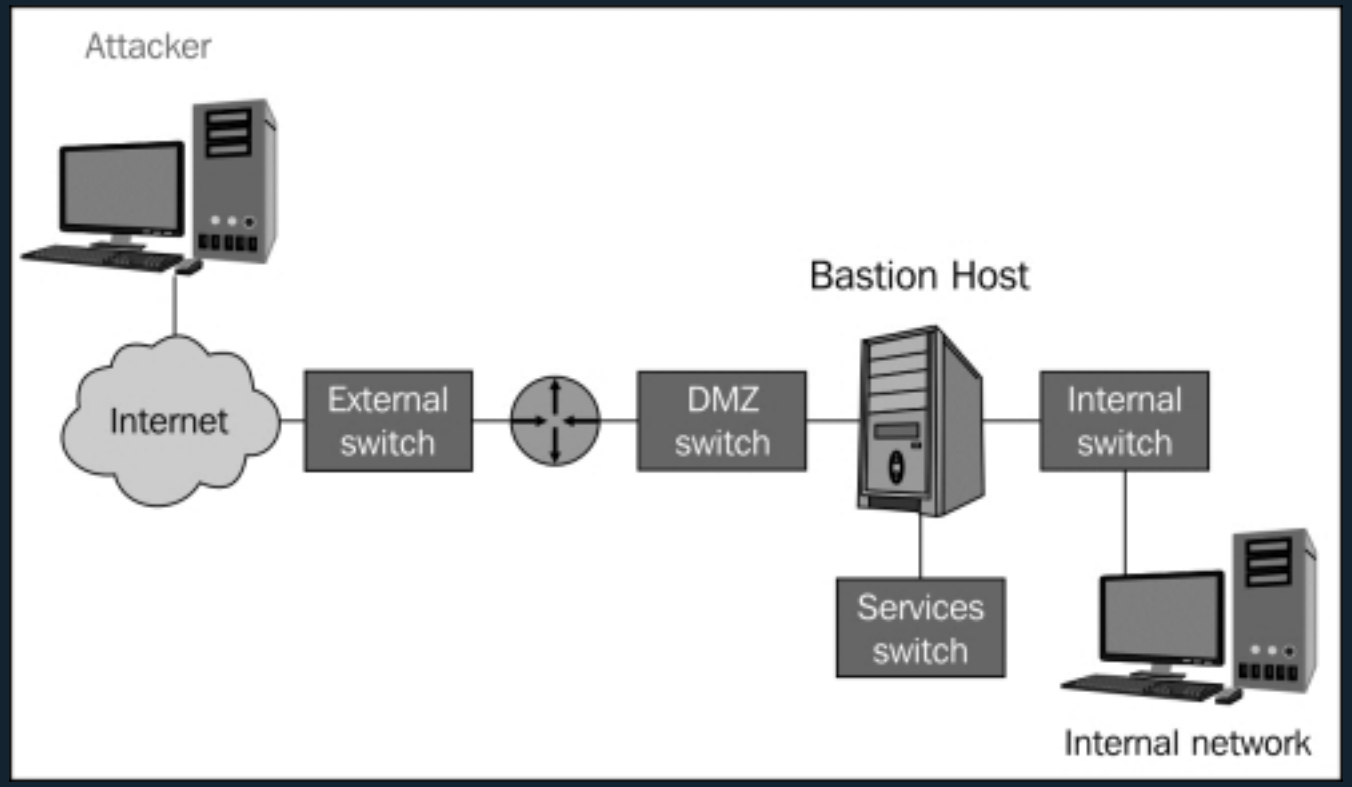
More than 10 years in hacking

What is penetration testing?

Black Hat
(real hacker)

White Hat
(pentester)

What is penetration testing lab?

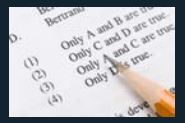


Simulate infrastructure of the real company

Why you need the lab?

Penetration testing team

How to test knowledge of job applicant?



Tests?

Come on, we are in the 21th century. It's non-practical and unrepresentative

Interview?

Yes, but how will the employee behave in a real project?

Make tasks?

Yes, but it's too labor-intensive. In addition, the write-ups may be leaked

Job applicant approved by HR specialist

Alternatives?

How to improve knowledge of your team?

Play CTF?

Unrealistic and there is no Active Directory vulnerabilities

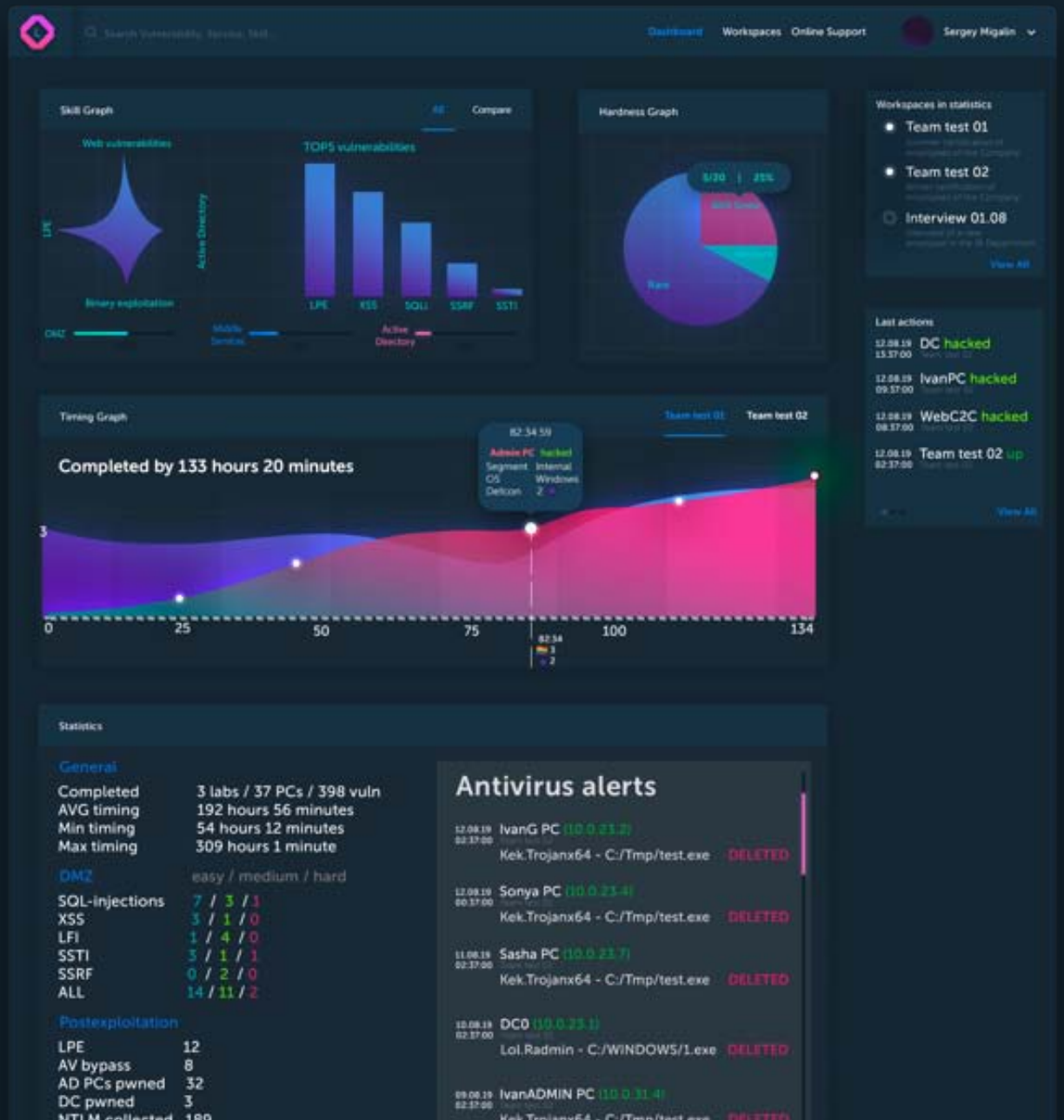
Hack The Box?

Monotony, unscaled, without detailed statistics on the skills

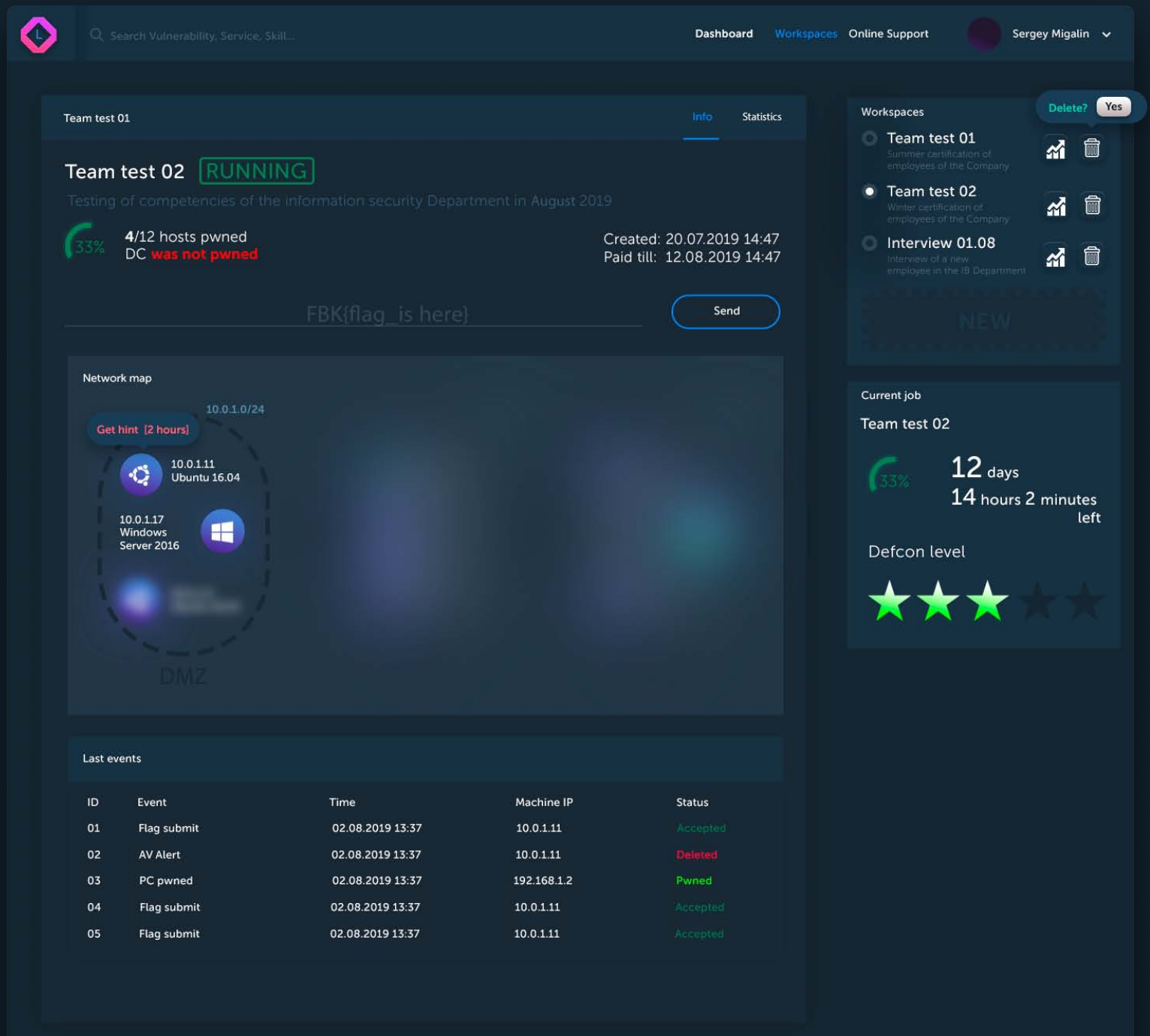
Pentest-it lab?

The same: monotony, unscaled, without detailed statistics on the skills

FBK Pentest Lab

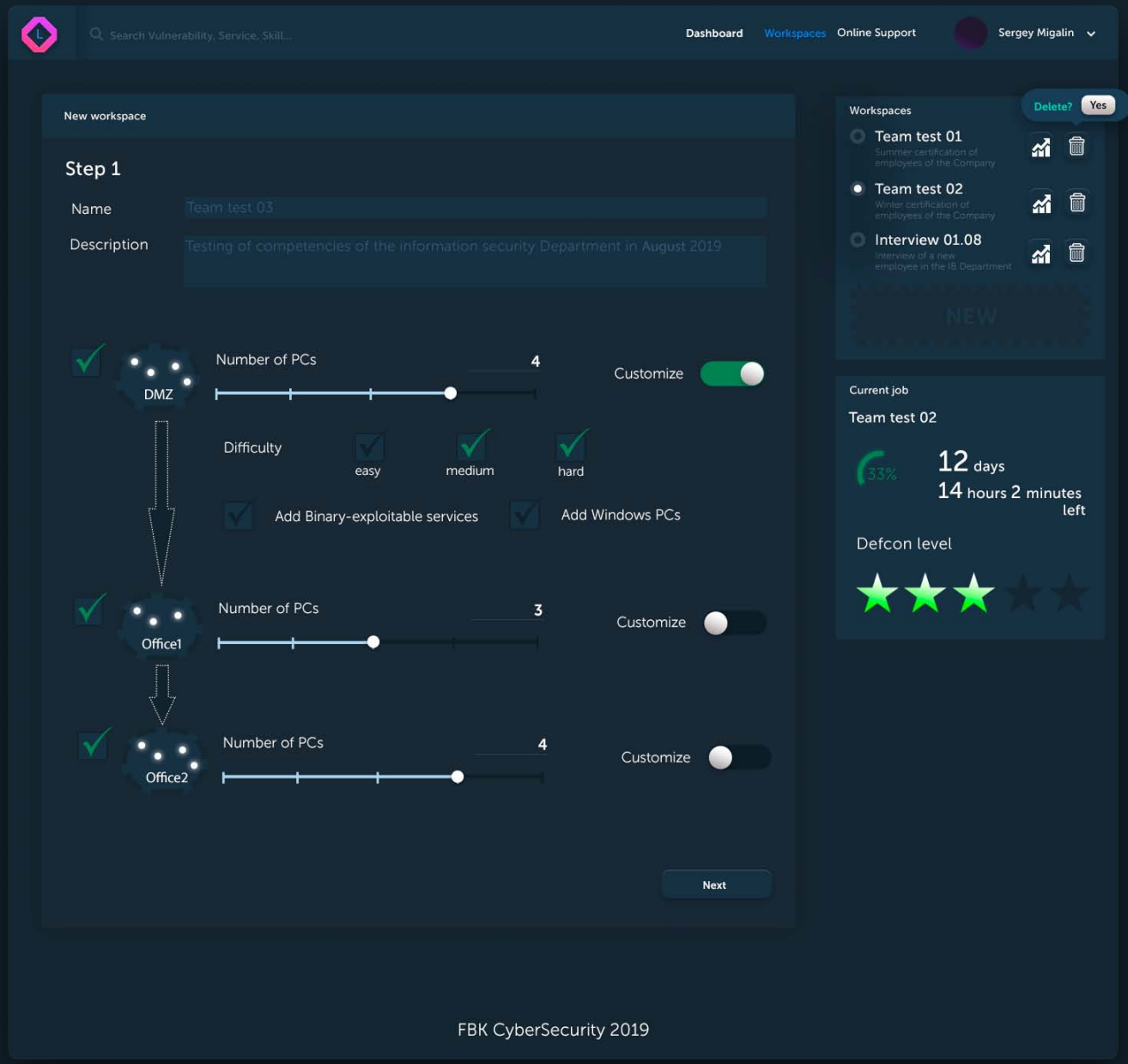


scalable → randomizable → great statistics features → supports any vulnerability


Search Vulnerability, Service, Skill...
Dashboard
Workspaces
Online Support
Sergey Migalin
Team test 01
Info
Statistics
Team test 02
RUNNING
Testing of competencies of the information security Department in August 2019
33%
4/12 hosts pwned
DC was not pwned
Created: 20.07.2019 14:47
Paid till: 12.08.2019 14:47
FBK{flag_is here}
Send
Network map
10.0.1.0/24
Get hint [2 hours]
10.0.1.11
Ubuntu 16.04
10.0.1.17
Windows
Server 2016
DMZ
Last events
ID Event Time Machine IP Status
01 Flag submit 02.08.2019 13:37 10.0.1.11 Accepted
02 AV Alert 02.08.2019 13:37 10.0.1.11 Deleted
03 PC pwned 02.08.2019 13:37 192.168.1.2 Pwned
04 Flag submit 02.08.2019 13:37 10.0.1.11 Accepted
05 Flag submit 02.08.2019 13:37 10.0.1.11 Accepted
Workspaces
Delete? Yes
Team test 01
Summer certification of employees of the Company
Team test 02
Winter certification of employees of the Company
Interview 01.08
Interview of a new employee in the IB Department
NEW
Current job
Team test 02
33%
12 days
14 hours 2 minutes left
Defcon level

Workspace

Workspace | Creation



Every workspace is your **personal** unique penetration testing area

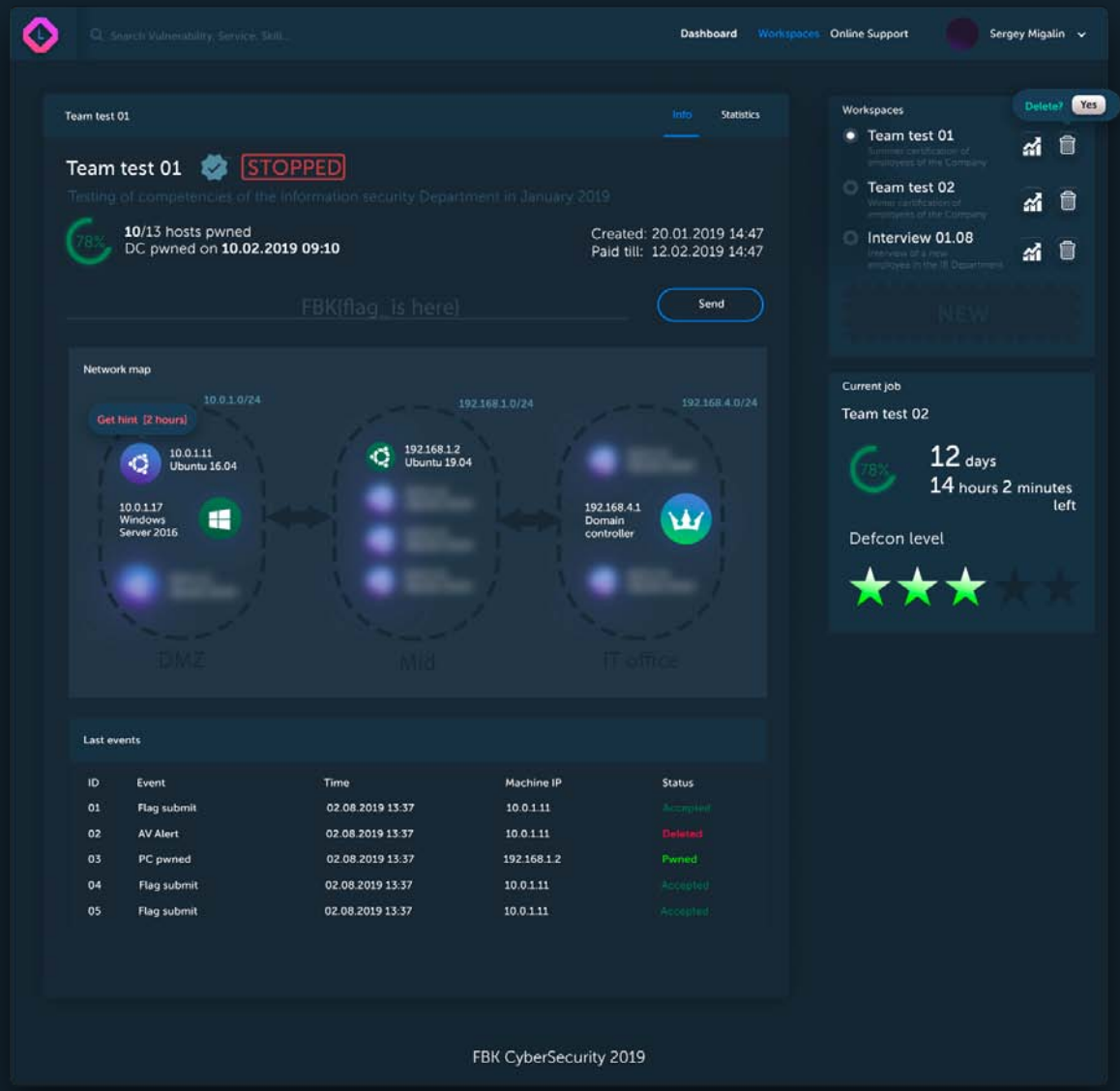
Workspace is **dedicated server** with various virtual machines

Every VM is unique and uses on **different technologies**

Random mix of vulnerable VMs and AD configuration per each lab

Easy to customize and set difficulty level

Workspace | Interface



User-friendly and **easy-to-use** interface

78%

10/13 hosts pwned
DC pwned on **10.02.2019 09:10**

Created: 20.01.2019 14:47
Paid till: 12.02.2019 14:47

FBK{flag_is here}

Send

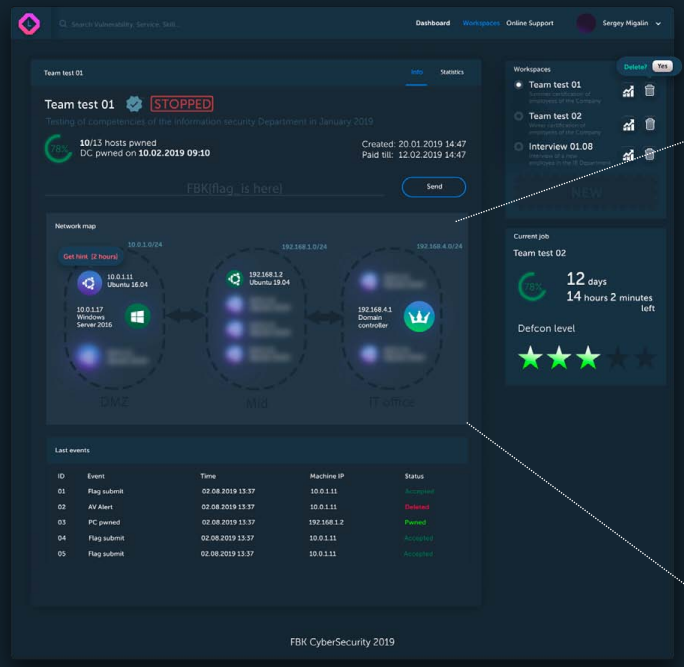
Only **one** field to input **all** flags

Last events

ID	Event	Time	Machine IP	Status
01	Flag submit	02.08.2019 13:37	10.0.1.11	Accepted
02	AV Alert	02.08.2019 13:37	10.0.1.11	Deleted
03	PC pwned	02.08.2019 13:37	192.168.1.2	Pwned
04	Flag submit	02.08.2019 13:37	10.0.1.11	Accepted
05	Flag submit	02.08.2019 13:37	10.0.1.11	Accepted

The **story** of your invasion

Workspace | Network map



Watch the attack in real time

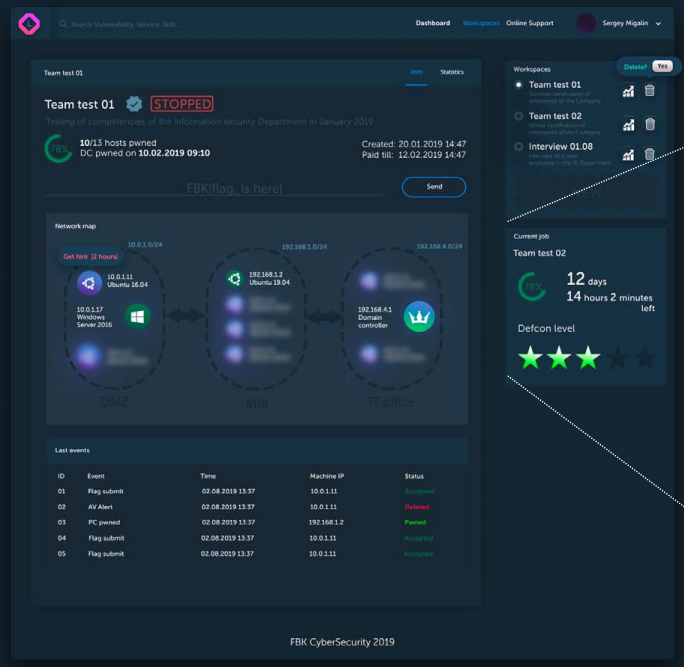
The network map allows you to track how far you have progressed

Hosts appear only if you find them

Segments open if you pwn PC

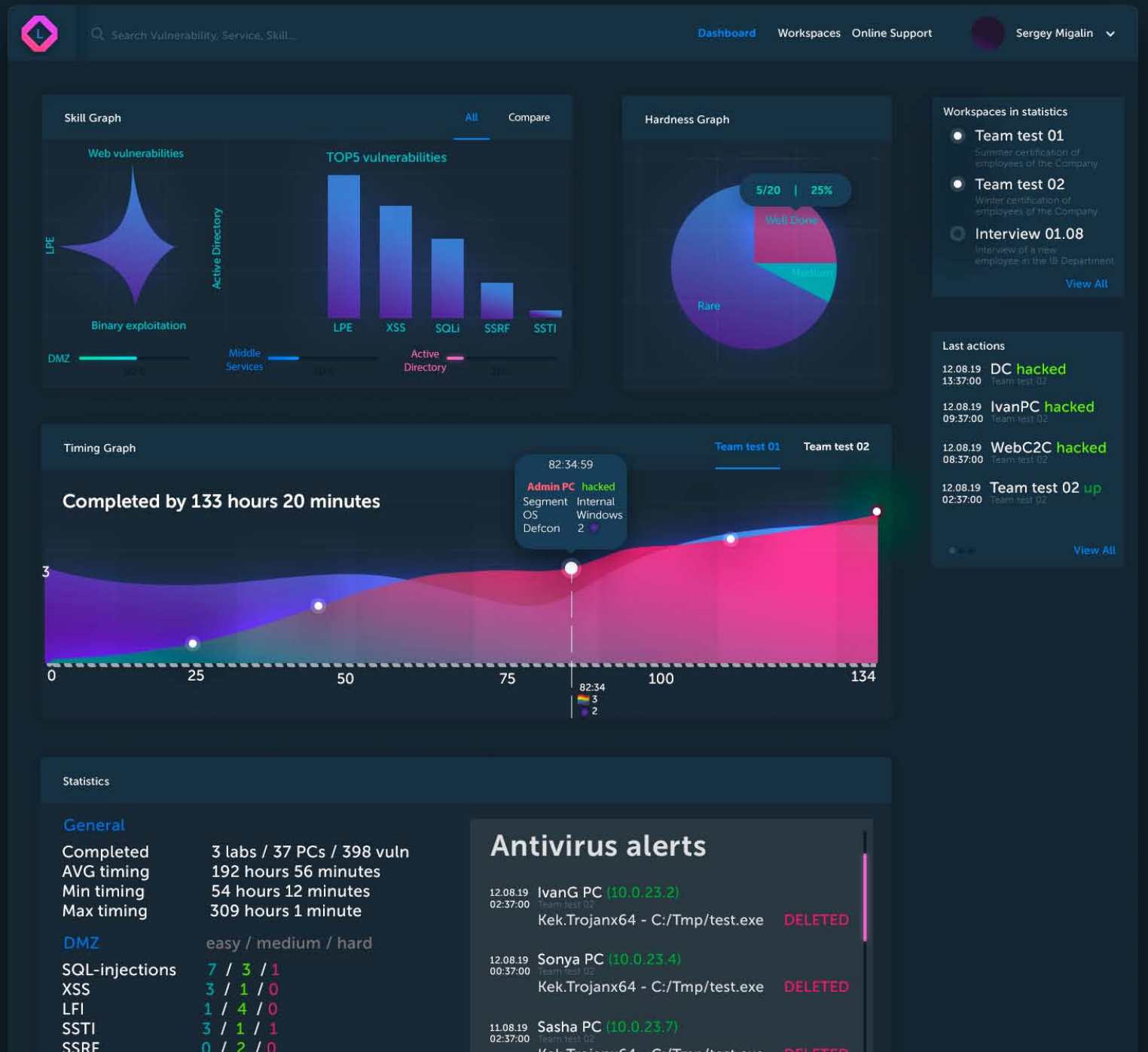
Make green every PC to 100% progress

Workspace | Defcon level



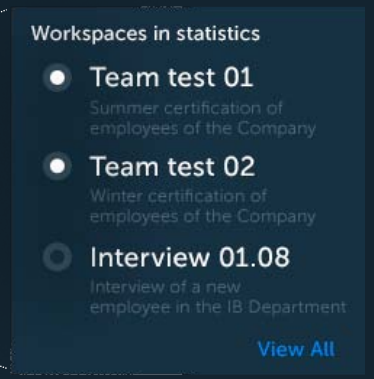
See how “silent” you are

It shows how "noisy" you are in the network and determines how standard are of your actions

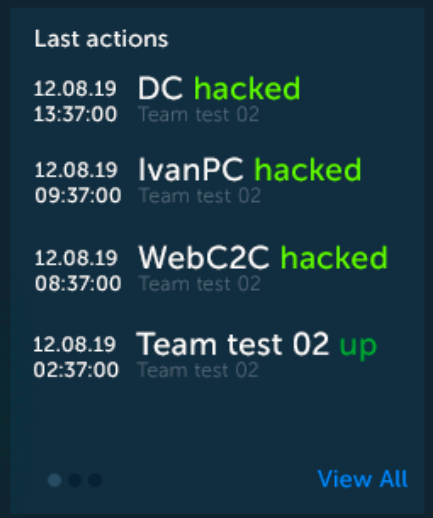

Search Vulnerability, Service, Skill...
Dashboard
Workspaces
Online Support
Sergey Migalin
Skill Graph
All
Compare
Web vulnerabilities
LPE
Active Directory
Binary exploitation
TOP5 vulnerabilities
LPE
XSS
SQLi
SSRF
SSTI
DMZ
Middle Services
Active Directory
Hardness Graph
5/20 | 25%
Well Done
Medium
Rare
Workspaces in statistics
Team test 01
Summer certification of employees of the Company
Team test 02
Winter certification of employees of the Company
Interview 01.08
Interview of a new employee in the IB Department
View All
Last actions
12.08.19 13:37:00 DC hacked
12.08.19 09:37:00 IvanPC hacked
12.08.19 08:37:00 WebC2C hacked
12.08.19 02:37:00 Team test 02 up
View All
Timing Graph
Team test 01
Team test 02
Completed by 133 hours 20 minutes
82:34:59
Admin PC hacked
Segment Internal
OS Windows
Defcon 2
3
0
25
50
75
100
134
82:34
3
2
Statistics
General
Completed 3 labs / 37 PCs / 398 vuln
AVG timing 192 hours 56 minutes
Min timing 54 hours 12 minutes
Max timing 309 hours 1 minute
DMZ easy / medium / hard
SQL-injections 7 / 3 / 1
XSS 3 / 1 / 0
LFI 1 / 4 / 0
SSTI 3 / 1 / 1
SSRF 0 / 2 / 0
Antivirus alerts
12.08.19 02:37:00 IvanG PC (10.0.23.2)
Kek.Trojanx64 - C:/Tmp/test.exe DELETED
12.08.19 00:37:00 Sonya PC (10.0.23.4)
Kek.Trojanx64 - C:/Tmp/test.exe DELETED
11.08.19 02:37:00 Sasha PC (10.0.23.7)

Statistics

Statistics

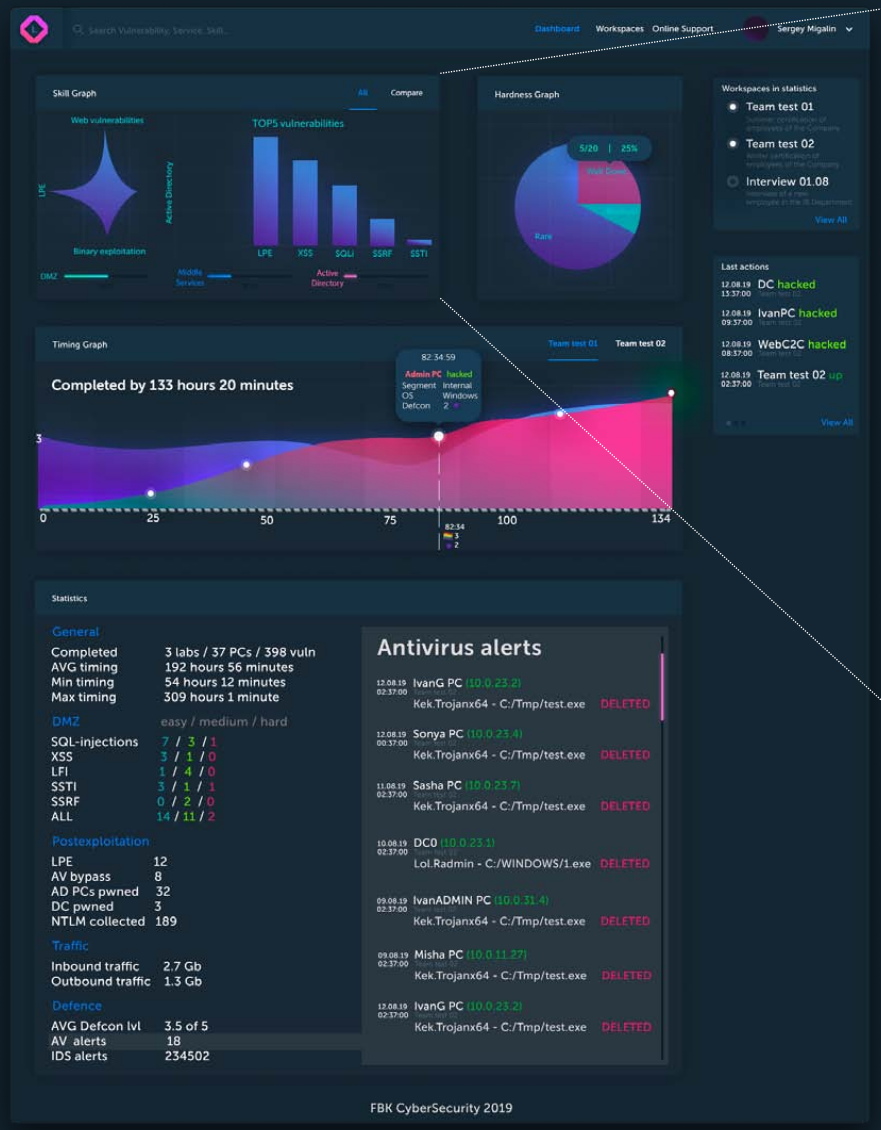


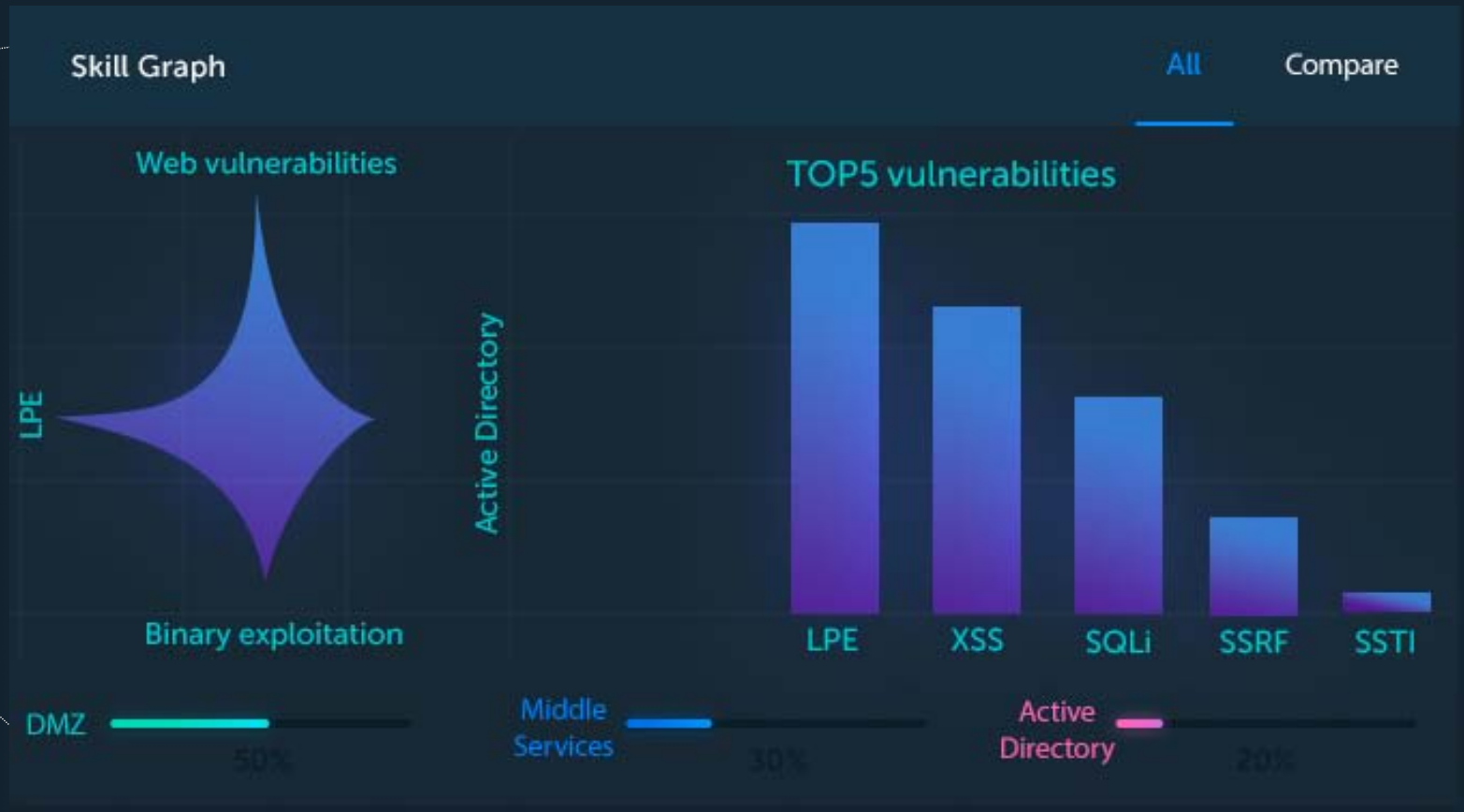
Choose workspaces which statistic you want to compare with



Track your last actions in real time

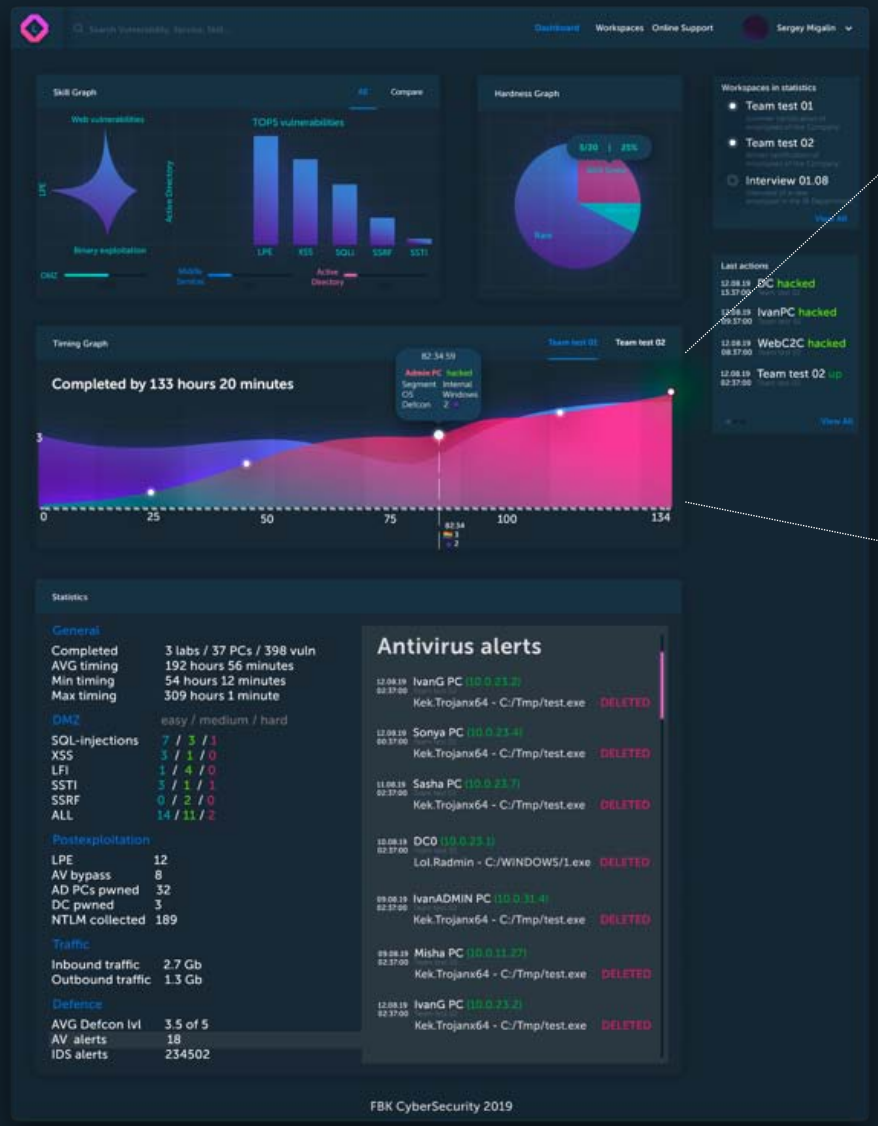
Statistics

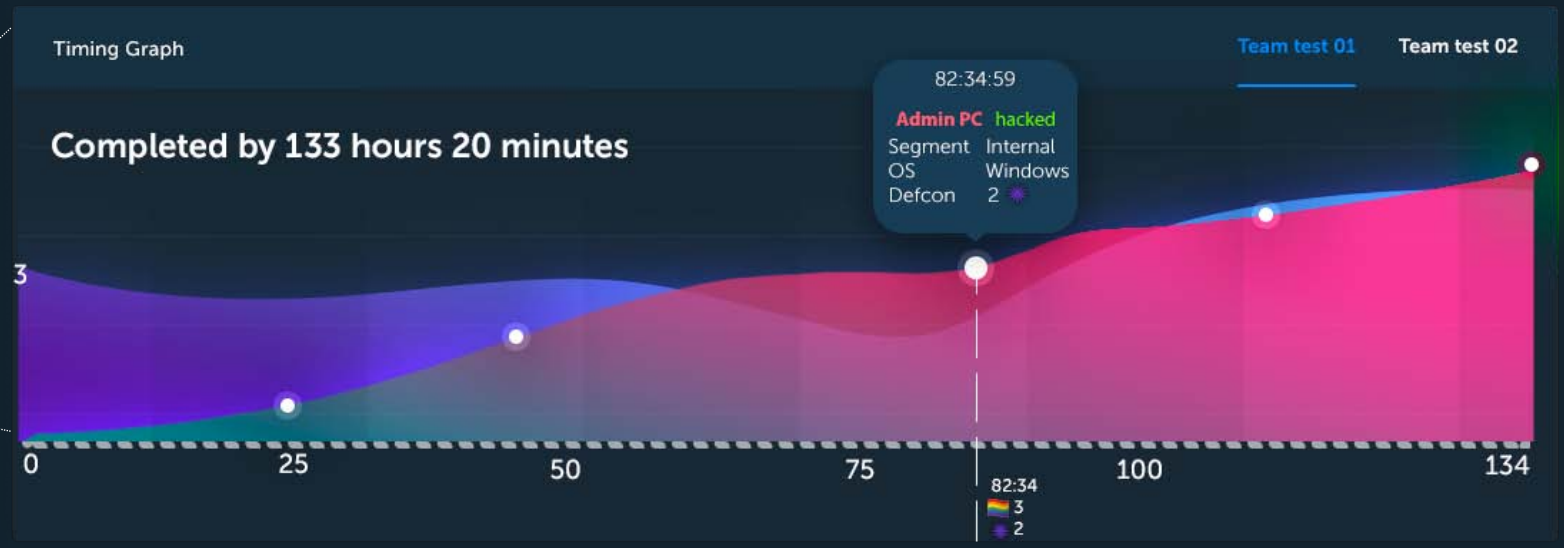




Check out which skills you have to improve or what you are good at

Statistics



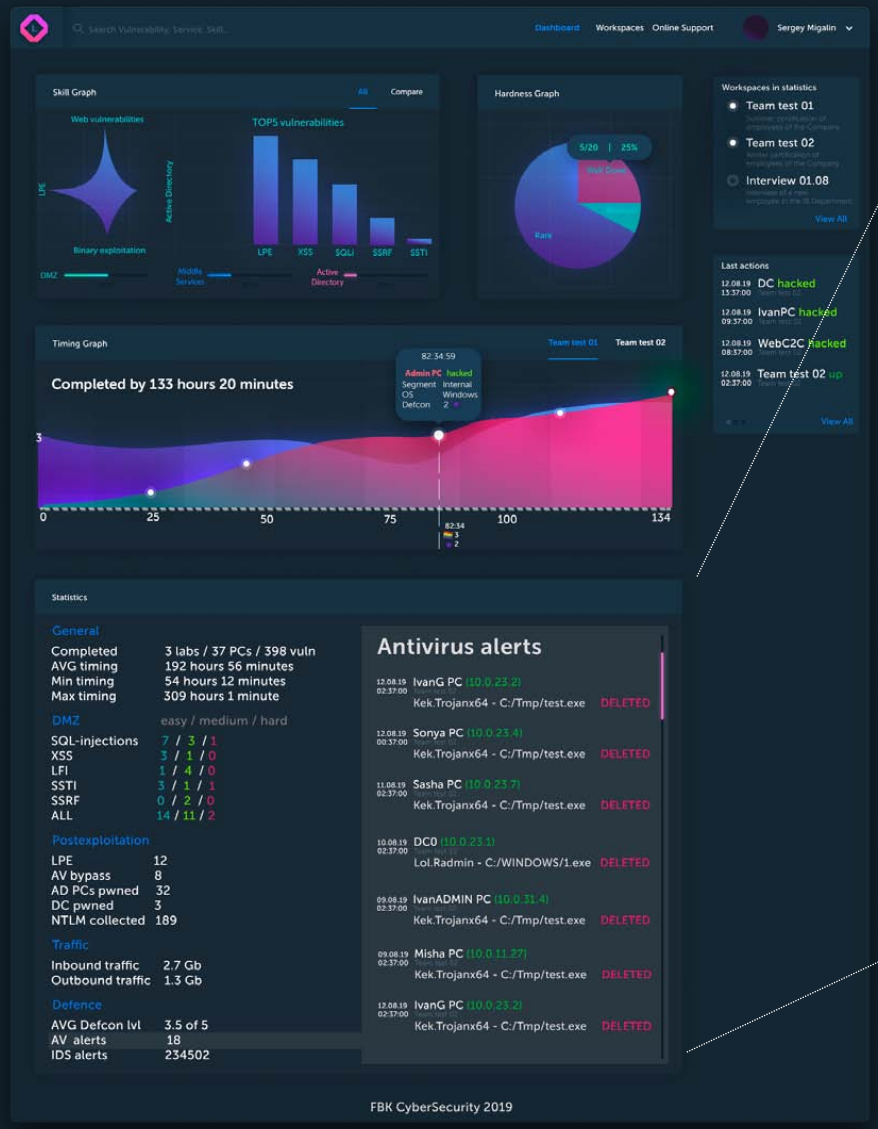


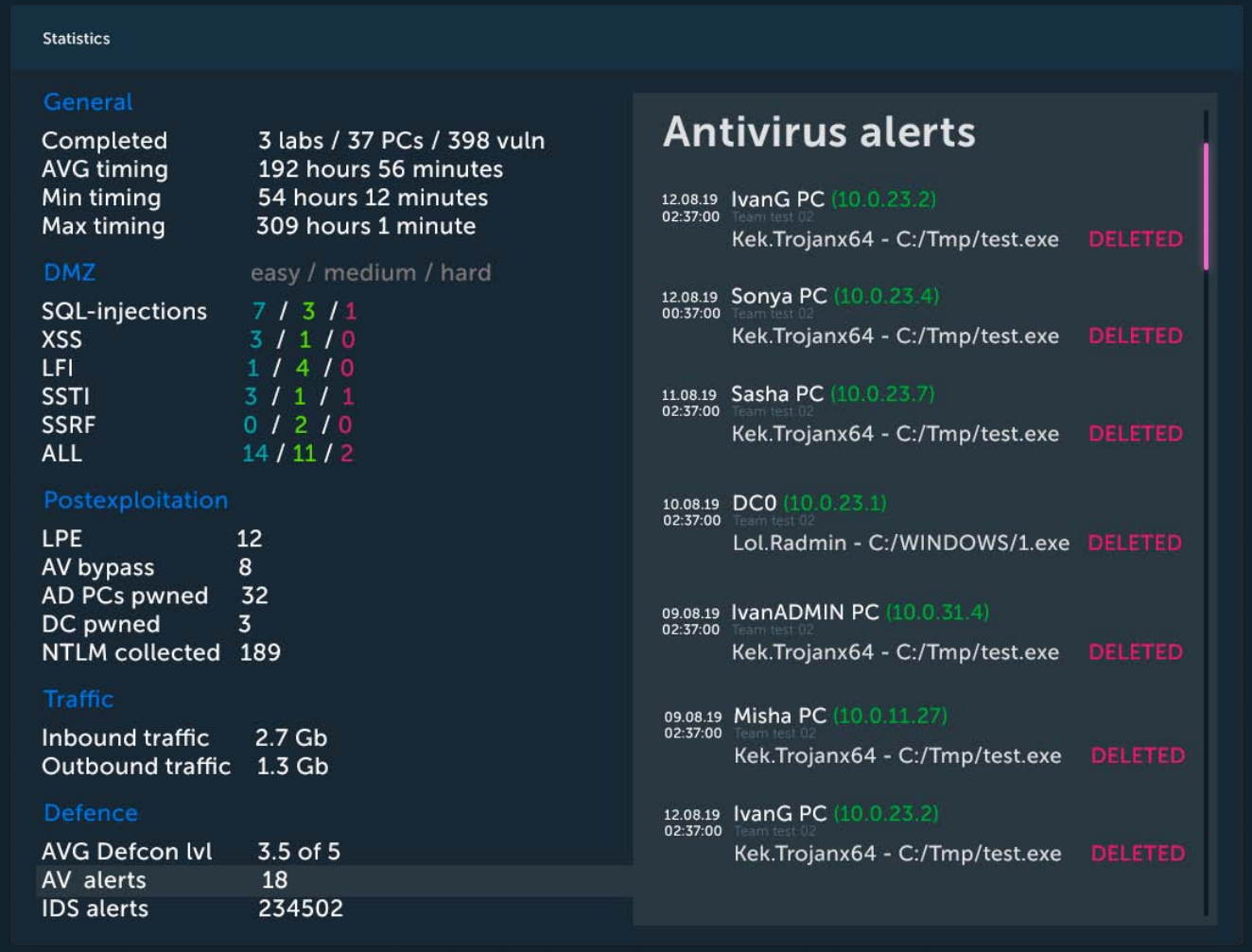
Check out correlation between defcon level and flag submitting

Statistics

Check out complexity progress

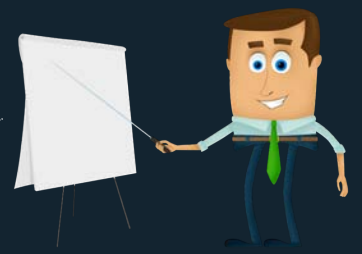
Statistics





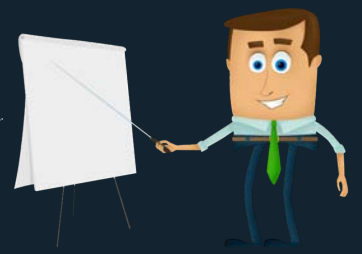
Check out general statistics across all workspaces and detailed AV report info

Workshops | Summary



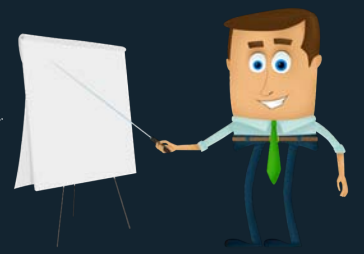
- ✓ Lectures

Workshops | Summary



- ✓ Lectures
- ✓ Practical examples

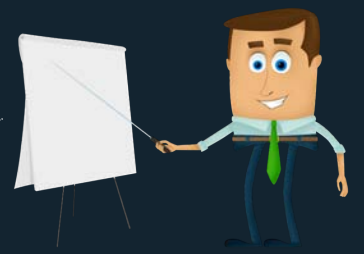
Workshops | Summary

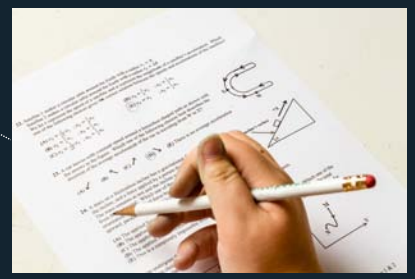


- ✓ Lectures
- ✓ Practical examples
- ✓ Online trainings

Workshops | Summary

- ✓ Lectures
- ✓ Practical examples
- ✓ Online trainings
- ✓ Final exam





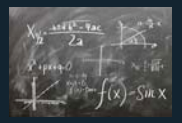
Personal workshops for your team

If you want to teach your interns or improve qualifications of your full-time team, specialist from FBK CyberSecurity can hold a workshop.

Your penetration testing team

Different levels

Choose which workshop level would you like: basic, advanced or custom.



Learn theory

Learn exclusive theoretical material about vulnerabilities, protocols and technics.

Test new knowledge in practice

Solve a series of tasks to consolidate acquired skills.

FBK CyberSecurity team

Summary?

- Focus on real security, not papers
- Think as offensive even if you are defensive
- Upgrade and invest in your Blue Team
- Lab is better than separated tasks for complex training

Questions?

???

mfirstov@fbkcs.ru
info@fbkcs.ru