Evolving Security Experts Among Teenagers

Designing the next generation of cybersecurity experts

Nahman Khayet & Shlomi Boutnaru

Abstract

By 2020 the estimated shortfall in cybersecurity workforce will reach 1.5 million people. Moreover, in today's world, there are emerging security challenges/threats due to evolving technologies and their increased complexity, thus startups and large companies require talented employees in order to face those challenges. For this reasons, we are lacking not only in quantity but also in quality. Additionally, these people are harder to recruit and maintain. The utopia is finding those that work hard, innovative, are creative and keep on learning. Finding them sounds like a tough mission. So why not create them?

Thus, what if we could only teach teenagers technical computer skills like (but not limited to): networking, operating systems internals, programming languages and the security implications of writing vulnerable code? What if we could afterward let them solve CTFs and then mentor other teenagers about the same things they have just learned? What if based on that, they will think about new ways to protect our systems? Only then, we could really create the next generation of those talented people that the industry is so eager to find.

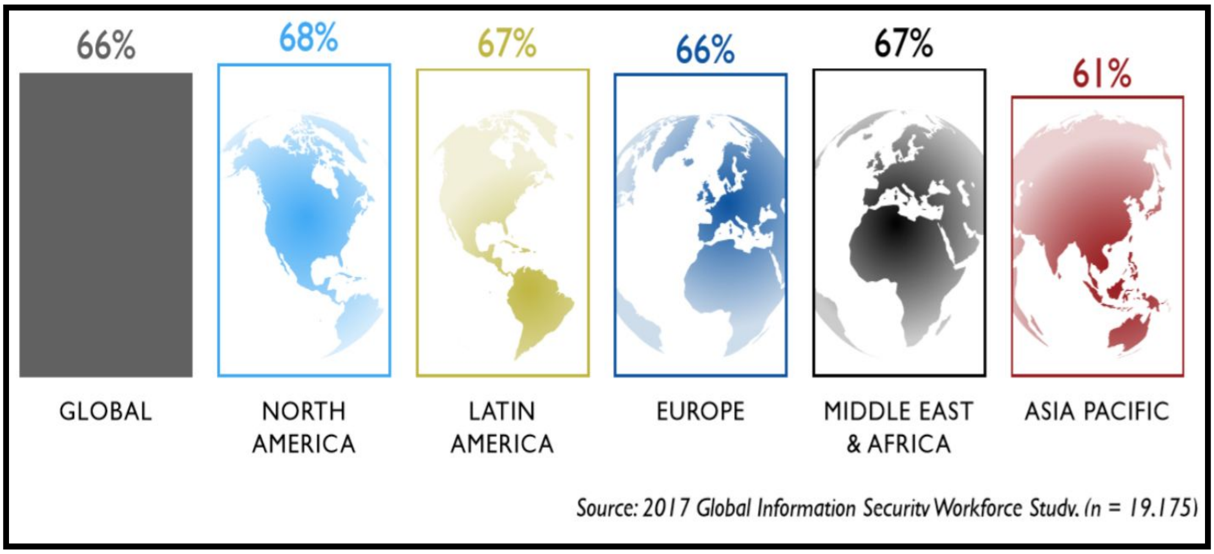
In this paper (and talk), we will present a new approach for education in the field of cybersecurity, which is demonstrated by a use case in Israel. We will explain in detail how to build a framework (leveraging different pedagogical paradigms) of programs and groups, with the support of government, industry, and community, all for the sole purpose of creating a new generation of experts inventing the next big thing.

In summary, the paper is divided to 10 main parts. **"Introduction"**, describes the growing need for cybersecurity experts. **"Overview"**, showcasts the current cybersecurity education landscape. **"Problem Definition"**, focuses on three main angles resulting in the lack of cybersecurity personnel. **"Suggested Solution"**, which details an optional solution demonstrated in Israel. **"What Can Those Kiddies Even Do?"**, showing examples of what technical activities teenagers can perform in the field cybersecurity (despite their young age). **"The Mental Model Problem"**, details how to use conflict based learning to avoid cognitive misconceptions by teenagers while learning advanced cybersecurity topics. **"Europe Case Study"**,

shows examples of cybersecurity educational initiatives in Europe. **“noxale Case Study”**, shows an example of what a local Israeli security group composed of teenagers can achieve (both in the form of knowledge and in promotion of the teenagers community). **“Future Thinking”**, discusses the further improvements and research that can be done in the field of cybersecurity education. **“Blackhat Sound Bytes”**, details the three key takeaways to remember and share with fellow colleagues.

Introduction

In the last few years, there has been an increasing demand for cybersecurity personnel. It is estimated that the worker shortage will be 1.5 million by 2020[1], and 1.8 million by 2022[2]. Moreover, 66% of workers all over the globe have cited that there are too few cybersecurity workers in their departments. Among many reasons found by recent studies, one that is strongly highlighted is the lack of qualified personnel[3].



Source: 2017 Global Information Security Workforce Study. (n = 19,175)

Too Few Information Security Workers in My Department

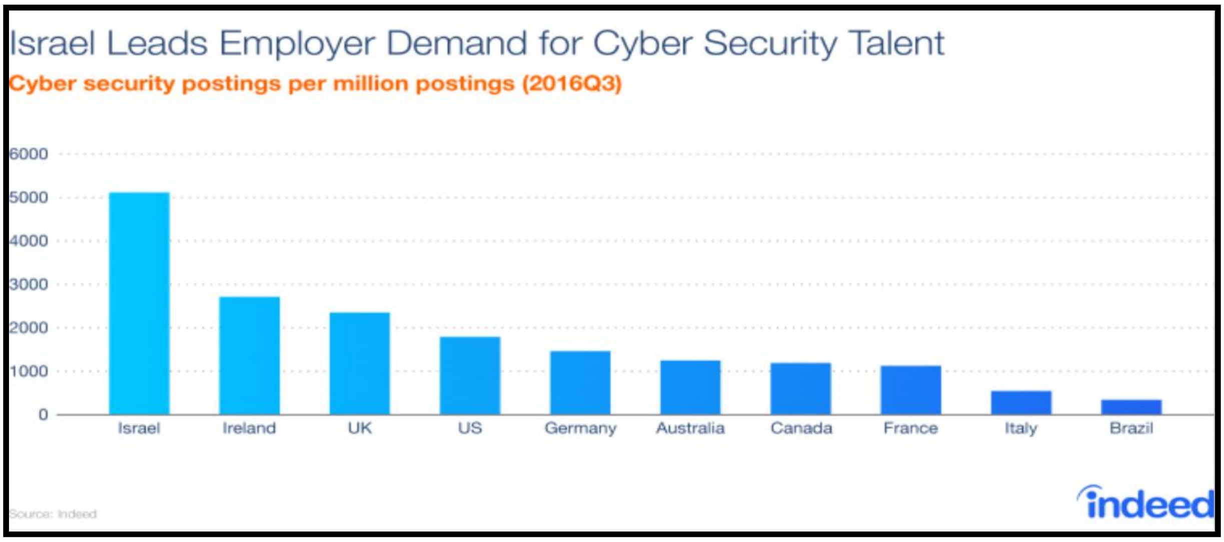
Also, According to a 2016 report by Indeed, Israel, is the second largest exporter of cybersecurity technology behind the US. Furthermore, Israel leads employer demand for cybersecurity talent by a wide margin[4]. A little bit over 5000 (per million positions) cybersecurity positions demanded in Israel, while countries like Ireland and UK which are ranked second and third, stay far behind with roughly 2500 positions open per million positions.

[1] https://www.cybercompex.org/fileSendAction/fcType/0/fcOid/445471828686010375/filePointer/445471828686010530/fodoid/445471828686010527/frostsullivan-ISC2-global-information-security-workforce-2015.pdf

[2] https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf

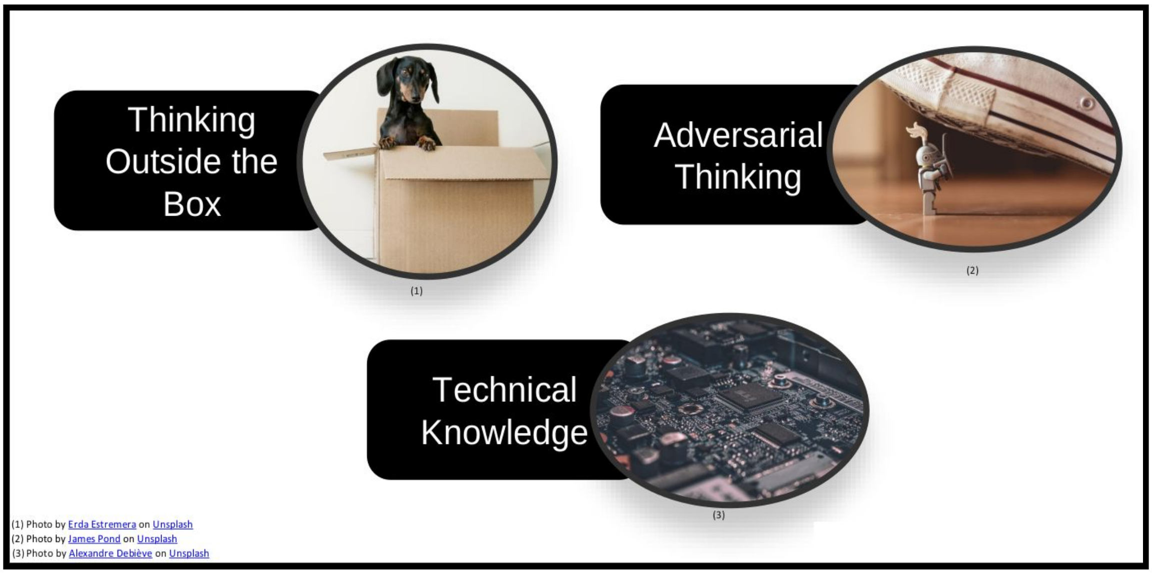
[3] https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf

[4] http://blog.indeed.com/2017/01/17/cybersecurity-skills-gap-report/



http://blog.indeed.com/2017/01/17/cybersecurity-skills-gap-report/

Moreover, while trying to sketch a blueprint for a cybersecurity experts we converge to the top three main characteristics: thinking outside the box (meaning creativity, unconventional ideas, etc), adversarial thinking (understanding the ways in which the enemy will try to attack) and have technical knowledge (networking, programming, operating systems, crypto, etc). Those three key aspects of expertise often lack in the regular educational system, and thus security personnel often comes out unprofessional or unfitted for the job.

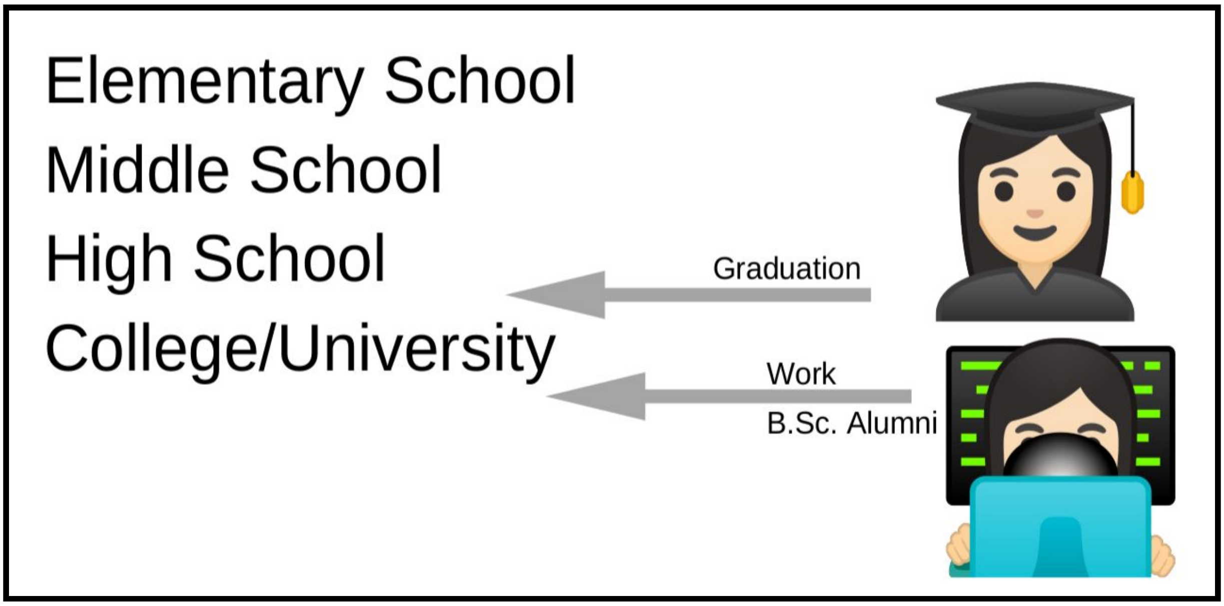


(1) Photo by Erda Estremera on Unsplash
(2) Photo by James Pond on Unsplash
(3) Photo by Alexandre Debiève on Unsplash

Cybersecurity Experts - Main Characteristics

Overview

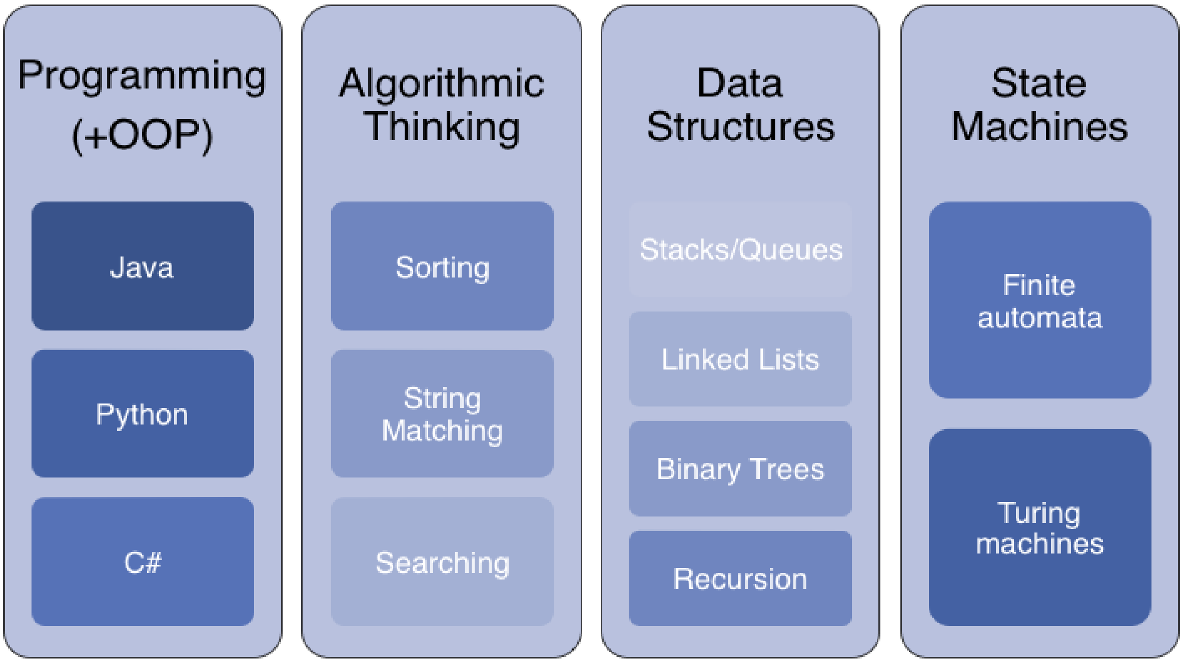
After examining the current conservative educational system we had identified four main phases: “Elementary School”, “Middle School”, “High School” and “College/University”. Also, there are two important events during that time: *graduation* after finishing high school and starting to *work* in the industry somewhere around the end of university/college (see also Working in Industry).



Current Educational System

Moreover, while looking at computer science curriculum for teenagers (mostly during high school), we had found that it is mostly devoted to evolving computational thinking among teenagers, and usually centered around topics such as programming, algorithmic thinking, data structures, and state machines. Although all of those topics are super important, there is no cybersecurity material as part of the curriculum.

Before we continue, it is important to state that different certifications and academic tracks will be shown as examples. The authors by no means recommend or prefer them in any way, they act only as examples to demonstrate the cybersecurity education landscape.



Computer science curriculum for teenagers

In general, the cybersecurity education landscape is centered around the following areas: Academia, Industry and Kids/Teenagers. In Academia, they are different M.Sc programs focusing at cybersecurity across Europe. Examples for such programs are: the cybersecurity M.Sc program at the Ben-Gurion[5] University (Israel), M.Sc in software and system security at Oxford[6] (UK) and M.Sc in cybersecurity at University of York[7] (UK). We have to remember that those programs are not relevant for most 8th-12th grade students because they had not earned their B.Sc yet.

In addition to that, the researcher Abu-Taieh identified in his paper "Cyber Security Body of Knowledge"[8] (2017) a total of 61 master programs in cybersecurity from 17 countries. These countries are: Australia, Cyprus, Czech Republic, Estonia, Finland, France, Germany, India, Italy, Lithuania, Malaysia, Malta, Netherlands, New Zealand, Spain, UK, and the US. The country with most programs was the US with a total of 25 master programs and second was the UK with a total of 16 master programs.

In parallel, the industry has its own education programs which are expressed in the form of certifications[9]. Examples of such certifications are:

[5] https://en.universities-colleges.org.il/Israel-Degree-Programs-Undergraduate-Degree-Programs/
[6] https://www.cybersecurity.ox.ac.uk/education/msc-courses
[7] https://www.york.ac.uk/study/postgraduate-taught/courses/msc-cyber-security/
[8] https://www.researchgate.net/profile/Evon_Abu-Taieh2/publication/323629371_Cyber_Security_Body_of_Knowledge/links/5aa111ae45851543e639852c/Cyber-Security-Body-of-Knowledge.pdf
[9] https://networkel.com/top-15-cyber-security-certifications-get-ahead-2018/

Certification Provider	Certifications' Examples
ISC2[10]	CISSP, SSCP, CAP, CSLP and HCISPP
Offensive Security[11]	OSCP, OSCE, OSWP, OSEE and OSWE
EC-Council[12]	CEH, CCISO, CES, CHFI, CND and APT
CompTIA[13]	CompTIA Security+
ISACA[14]	CISA, CRISC, CISM and CGEIT

A partial list of security certifications

It is important to remember that those certifications are mostly out-of-reach for teenagers due to two main reasons: the high cost of the certifications and the need of minimal time of experience in security (requested by some of the certifications). Furthermore, the cybersecurity education for teenagers/kids usually consists of topics which don't cover the entire cybersecurity field such as: "Safe internet" training, privacy controls, awareness, password safety and social media safety.

[10] https://www.isc2.org/Certifications
[11] https://www.offensive-security.com/information-security-certifications/
[12] https://cert.eccouncil.org/certifications.html
[13] https://certification.comptia.org/certifications/security#overview
[14] http://www.isaca.org/CERTIFICATION/Pages/default.aspx

Problem Definition

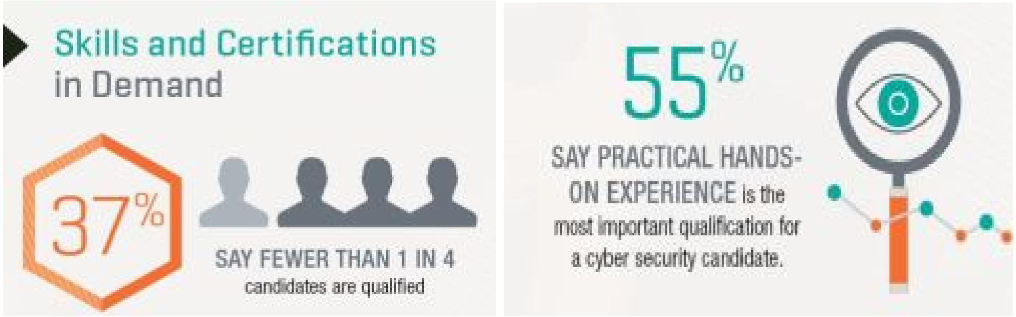
Based on our understanding, the problem can be divided into three main categories (while excluding the lack of personnel) which are:

1. Unskilled workforce
2. Limitations of the educational system
3. Lack of women in cybersecurity and tech in general

Unskilled Workforce

Although there is a high demand for security personnel (as shown before) none of the top 10 U.S. computer science programs require even a single cybersecurity course for graduation. Not only that, three of the top 10 universities' programs don't even offer an elective course in cybersecurity[15].

Moreover, According to an Intel (McAfee) Study[16], only 23% of respondents (decision makers from IT companies from all over the world) say that education programs are preparing students to enter the industry. Also, 82% of the respondents reported a shortage of cybersecurity skills[17]. Also, according to another Study conducted by ISACA[18], 37% of respondents say fewer than 1 in 4 candidates have the qualifications employers need to keep companies secure.



ISACA Surve: Cyber Security Skills Gap Leaves 1 in 4 Organizations Exposed for Six Months or Longer

Limitations of Educational System

While analyzing the current educational system, targeting teenagers in cybersecurity, we have encountered (in our opinion) two main limitations which we are going to

[15] https://www.cloudpassage.com/company/press-releases/cloudpassage-study-finds-u-s-universities-failing-cybersecurity-education/

[16] https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hacking-skills-shortage.pdf

[17] https://www.tripwire.com/state-of-security/security-data-protection/universities-can-help-fill-security-skills-gap/

[18] https://www.businesswire.com/news/home/20170213005553/en/ISACA-Survey-Cyber-Security-Skills-Gap-Leaves

detail. First, the educational system doesn't face the students with complex projects and doesn't require them to deal with real-world technologies (cloud, containers, NoSQL, etc). Thus, how can a graduate, who has a minimal understanding of complex systems/technologies handle their security challenges? How can a cybersecurity "Expert" create practices for the organization while he/she had never experienced those systems/technologies with hands-on experience? Hint: he/she can't.

Second, for some unknown reason, our educational system believes that teaching kids about "Internet Safety" and how to control their privacy on social networks is all they need to know about cybersecurity. As we all know, cybersecurity is not only to prevent your friends from stalking you. Cybersecurity includes a lot more like the protection of Internet-connected systems, including hardware, software, and data, from cyber attacks. How do we protect? What are cyber attacks? What is the technology behind them? These are the questions that should ignite the classes of cybersecurity (and many more).

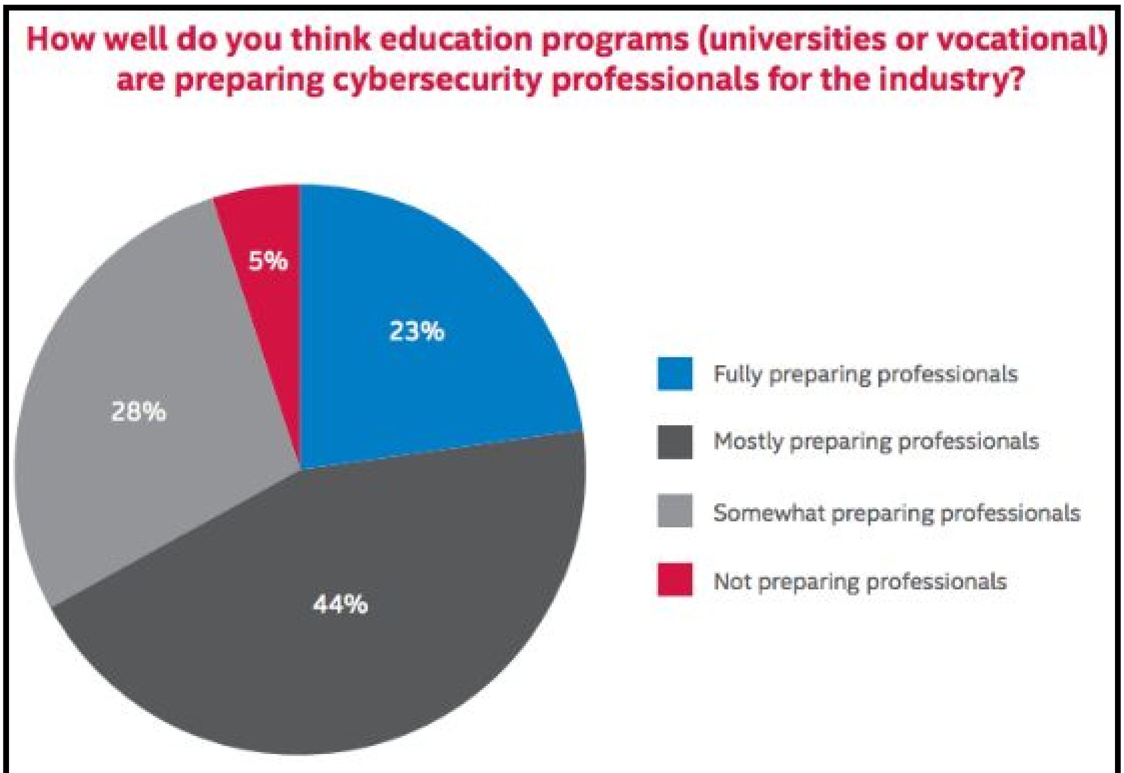

How well do you think education programs (universities or vocational) are preparing cybersecurity professionals for the industry?

Figure 10. Education programs and skill development.

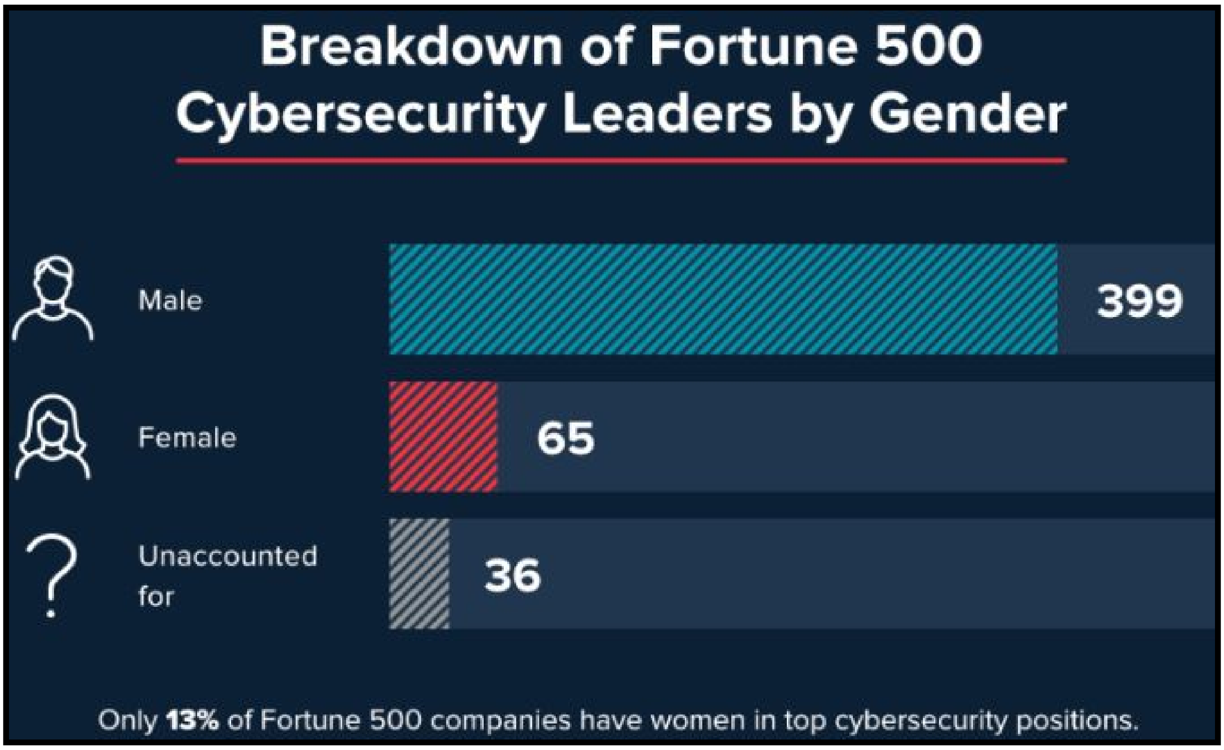
Source: Hacking the Skills Shortage, Intel Security

Lack of Women in Cybersecurity and Tech in General

How does it happen that only 0.4% of high school girls select computer science in their college major, while 74% (!!) of girls express interest in STEM subjects in middle school[19]?

Also, one might think: “Well, at least the gender gap in computing is getting closed” but the fact is that in the last 30 years the number of female computer science graduates narrowed down from 37% in 1984 to 18% in 2014[20]. Further, If we look at the Fortune 500 Cybersecurity Leaders, we find that only 65 are Women.

Now Let’s ask the simple question that connects those two dots: How a young girl can get the “push” she needs to pursue her will to learn cybersecurity if all that she sees is that most of the leader/experts in cybersecurity are men?



https://theundercoverrecruiter.com/women-in-cyberscurity/
Author: Sarah Hospelhorn, Director of Product Marketing @ Varonis

[19] https://techcrunch.com/2016/04/14/women-in-tech-whats-the-real-problem/
[20] https://fairygodboss.com/articles/women-in-tech-facts-figures-and-percentages

Suggested Solution

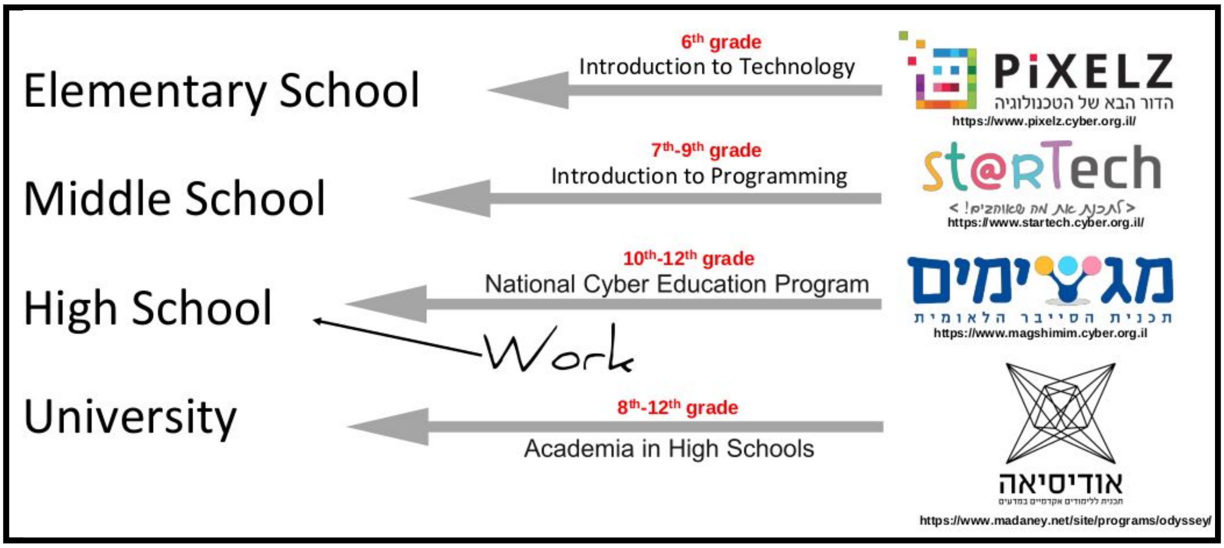
Overall the suggested solution is a combination of educational programs, excellence competitions and working in industry/mentoring. Each of the components shapes and evolves skills/mindset/capabilities which are crucial for a cybersecurity expert. In the next sections we are going to detail each one of them.

Educational Programs

When we examined the Israeli cybersecurity educational system for teenagers we had found that for each stage in the conservative educational system there is a specific education program as followed:

- Elementary School -> Pixelz[21]
- Middle School -> StarTech[22]
- High School -> Magshimim[23]
- University -> Odyssey[24]

Although our goal is not to give a full review of each program, each of them deserves its own paper, we'll give a short explanation about them in order to demonstrate the suggested solution.


Elementary School
6th grade
Introduction to Technology
PiXELZ
הדור הבא של הטכנולוגיה
https://www.pixelz.cyber.org.il/
Middle School
7th-9th grade
Introduction to Programming
st@rTech
< לתכנת את מה שאוהבים! >
https://www.startech.cyber.org.il/
High School
10th-12th grade
National Cyber Education Program
מגשימים
תכנית הסייבר הלאומית
https://www.magshimim.cyber.org.il
Work
University
8th-12th grade
Academia in High Schools
אודיסיאה
תכנית ללימודים אקדמיים במדעים
https://www.madaney.net/site/programs/odyssey/

Israel's teenage cybersecurity/technological programs

[21] https://www.pixelz.cyber.org.il/
[22] https://www.startech.cyber.org.il/
[23] https://www.magshimim.cyber.org.il
[24] https://www.madaney.net/site/programs/odyssey/

First, Pixelz is a special program targeting 6th grade students. The program provides a first exposure to technology in various subjects such as (but not limited to): binary numbers, cryptography, how images are represented by a computer, code games, AI and more. The program is operated by the Cyber Education Center[25], which was founded by the Rashi[26] Foundation with the support of the Ministry of Defense and the National Cyber Bureau within the Prime Minister's Office.

Second, StarTech is a program targeting 7th-9th grade students with the goal of providing practical tools in technology and computers to enable the participants to express their capabilities and ideas. As part of the program the students learn by doing projects (developing computer games, graphical interfaces etc), participating in conferences and more. The studies are conducted once a week (3 hours sessions). This program is operated also by the Cyber Education Center.

Third, Magshimim is targeting 10th-12th grade students. Magshimim started as an intensive, three-year, after school hours educational program. Studies take place during the school year based on a curriculum developed by cyber experts. For six hours weekly students are engaged in hands-on learning which includes: programming in various languages (such as C, C++, C#, Python and x86 Assembly), computer and operating systems architecture and structure (Both in Linux and Windows), networking and independent projects. These independent projects are built by 12th graders and professionals from the industry are mentoring them and introducing them to real-world work methodologies. Furthermore, Magshimim includes a community of volunteers and a "big brother"[27] program. In addition to that, Magshimim also hosts the monthly challenge[28] for students, as well as "Peak days"[29]. This program is also operated by the Cyber Education Center with many partners[30].

Forth, The Odyssey Program[31] is targeting 8th-12th grade students. Odyssey was developed to nurture a unique scientific-technological group - a new generation of inventors and scientists in Israel who possess both the ability to lead and a sense of social responsibility. The program is implemented in parallel with academic studies and during vacation, the students participate in workshops and full-day intensive seminars. The program operates through the Maimonides Fund's Future Scientists Center, as a joint initiative with the Ministry of Education's Department for

[25] http://cyber.org.il/

[26] http://www.rahifoundation.org/

[27] In which a Magshimim senior student (12th grade) is mentoring (in addition to the teacher) a whole class of 10th or 11th graders.

[28] In which every grade has its own set of monthly challenges and leaderboards challenging different topics that are teached in class.

[29] In which students are engaged in different teaching activities such as competitions, practical training sessions and classes which extends their skills set.

[30] https://www.magshimim.cyber.org.il/blank-3

[31] The program was inspired and initiated by the late President of the State of Israel, Mr. Shimon Peres.

Gifted and Talented Students and the National Cyber Bureau within the Prime Minister's Office. Other partners in the program include the Rashi Foundation, the Jerusalem Foundation, Check Point Software Technologies Ltd., SanDisk, Mellanox Technologies, and Keter.

More than that, due to the low number of women in cybersecurity there are two specific frameworks in Israel which are trying to cope with that. The first, CyberGirlz[32] which is a community that focuses on technology, computers and cyber. CyberGirlz provides summer camps, contents, cyber challenges, events (such as hackathons), meetings with industry leaders, answering online to any technical question and more. In addition to that, a couple of months ago a new program was founded called Mehamemet. The goal is to encourage girls to select computer science/technology as a course of study.

Moreover, In order to arouse interest and encourage Israeli teenagers to excellent in computer science and cybersecurity a couple of local competitions were created. As our goal is not to explore and detail each contest, we have selected three local Israeli contests (CodeGuru[33][34], CodeGuru Extreme[35], and SkillZ[36]) of which a brief overview is given. Our purpose is to emphasize the value of excellence competitions and demonstrate the educational benefits of them (and not detail each one of them).

First, CodeGuru, a math & computer science personal competition for teenagers. The competition is based mostly on closed questionnaire. CodeGuru was founded on 2000, and until now overall of 19 competitions were held. Second, CodeGuru Extreme, a Team competition based on COREWARS[37]. All "Survivors" are written in assembly 8086. Until now overall of 13 competitions were held. SkillZ, Israel's Cyber's Championship which is running since 2015 and operated by the ministry of education with the support of the Rashi Foundation and IATI[38]. Skillz is a set of competitions for all school grades, including math, code, and robotics competitions. SkillZ Coding is a team competition for 10-12th graders which is based on gamification[39] (code vs code) which hosts 4000 teenagers every year.

[32] http://cyber-girlz.org/

[33] https://codeguru.co.il/classic/

[34] aka CodeGuru classic

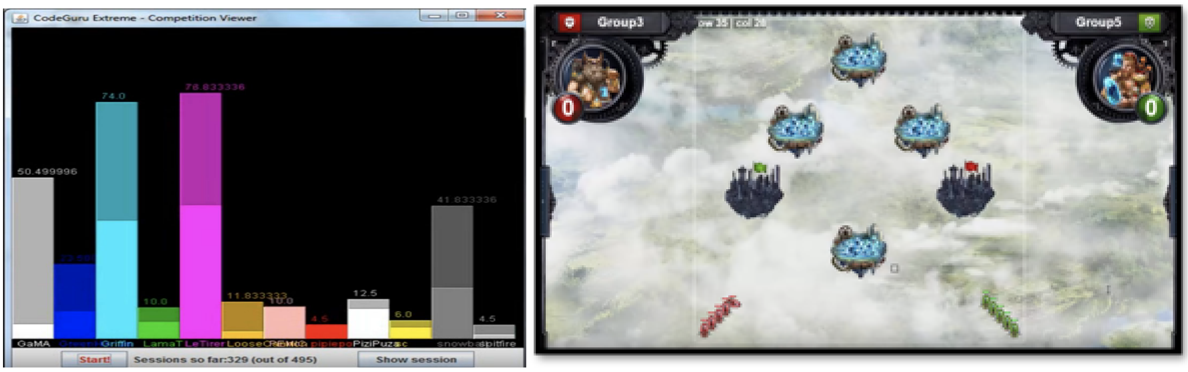
[35] https://codeguru.co.il/Xtreme/

[36] https://pub.skillz-edu.org/portal/

[37]A programming game in which two or more programs run in a simulated computer with the goal of terminating every other program and surviving as long as possible. Known as *Warriors*, these programs are are written in an assembly language called Redcode (https://www.corewars.org/).

[38] Israeli Advanced Technology Industries - http://www.iati.co.il/

[39] In which the goal of each team is to gain greater number of gems, that can be found on a random map while overcoming different obstacles and fighting the opponent. Students write bots in various languages: C#, Java, Javascript and Python.



Codeguru extreme[40] and SkillZ coding[41] scoreboard

Working in Industry

In Israel, it's not uncommon to find teenagers of these cybersecurity education programs working in the industry. Many of them find jobs after graduating high school, while some of them will find themselves working in the industry as early as at 10th grade (16 years old). The roles which these teenagers occupy ranges from QA and programming to security research and reverse engineering. This is made possible because the education programs teach both practical hands-on/material and learning methodologies which result in teenagers learning by themselves after school hours and getting the correct expertise and knowledge required to work in the industry.

In summary, we can conclude that the main characteristics of the new educational approach are:

- We should teach teenagers on various technical topics (and not only “Internet Safety”) such as: networking, python, operating systems, and OOP.
- Mentoring of teenagers while working on real-world projects.
- Encourage excellence in technical areas (by leveraging projects, CTFs, and contests).
- Internship in different cybersecurity/hi-tech companies.

[40] https://www.youtube.com/watch?v=mXv2MgMJ8lA
[41] https://www.youtube.com/watch?v=4WF3LOqg1fc

What Can Those Kiddies Even Do?

Despite the fact we focus on teenagers which don’t have a lot of experience in the cybersecurity world they perform extremely well in various cybersecurity tasks such as: real-world projects, CTFs, contests organization and more. This part demonstrated and detailed some of those achievements.

Real World Projects

Because we want to evolve the next generation of cybersecurity experts it is important to expose teenagers as soon as possible to real-life challenges. In order to do so teenagers are performing real-world projects (examples of those projects are followed) which force them to do the following things:

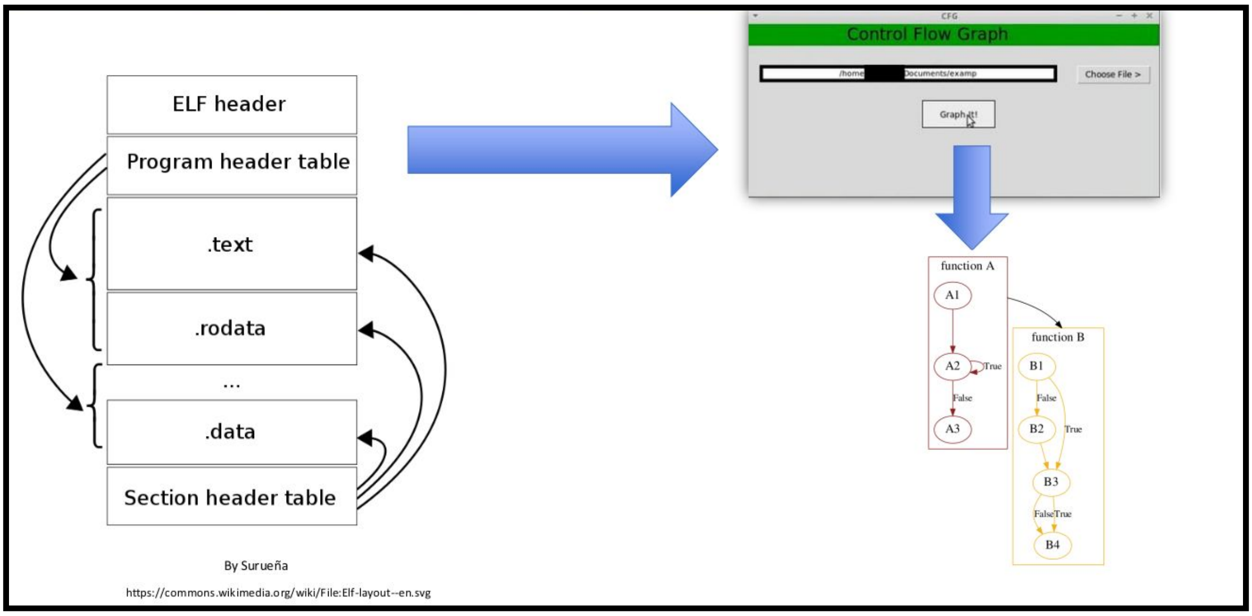
- Identify problems that they can solve
- Define requirements for their solution
- Perform a research (academic/business) to locate existing solutions
- Create a work plan for the project
- Work in teams
- Multi-developer[42] environment
- Testing (QA[43] & UT[44])
- etc

ELF CFG Creator

The goal of the project was creating a CFG[45] (Control Flow Graph) for ELF files (without the need for source files). The project consists of the following steps:

1. Disassembling the ELF file using objdump.
2. Extracting functions and basic blocks based on opcode analysis (such as function prologue identification, function call, unconditional jumps, etc)
3. Creating the CFG based on the block relationships.
4. Creating a visual representation for the user (as shown in the upcoming diagram).

[42] Including the use of source control
[43] Quality Assurance
[44] Unit Testing
[45] https://en.wikipedia.org/wiki/Control_flow_graph



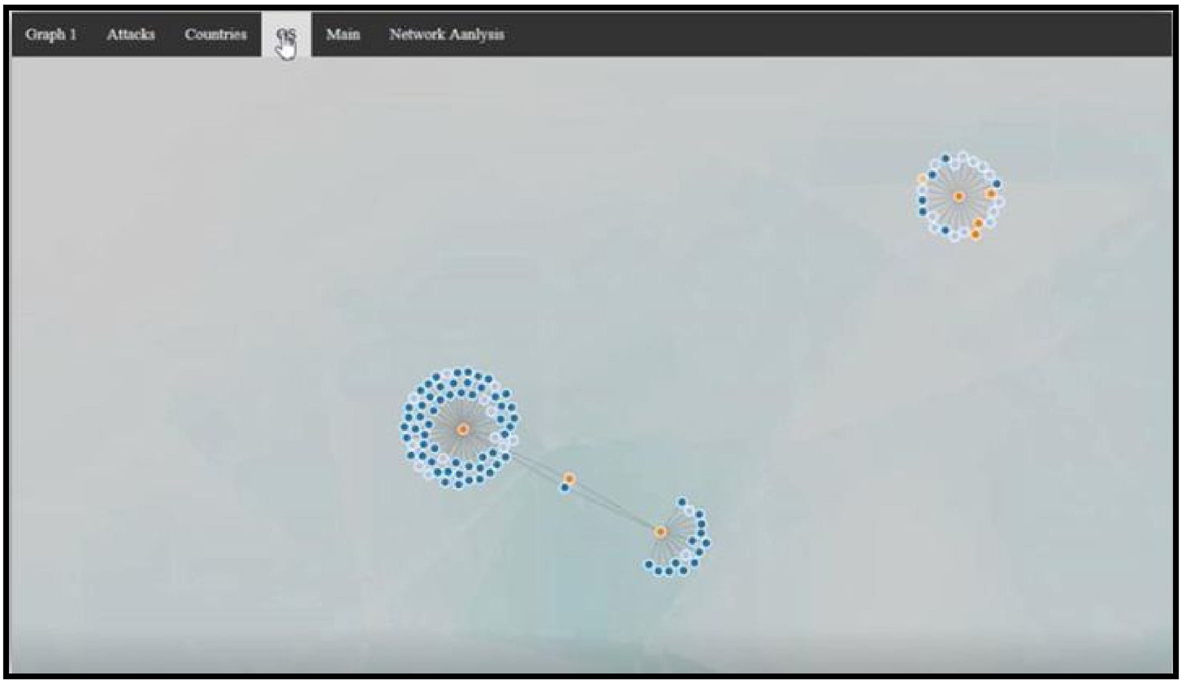
The process of creating the CFG from ELF binaries

After producing it, the CFG can be used for various use cases such as: CFI[46] (Control Flow Integrity), identification of algorithms implemented[47] (can aid with reverse engineering) and identifying code coping[48].

Network Mapping

The goal of the network mapping project was to leverage passive/active fingerprinting techniques in order to identify the different operating systems communicating over the network and to visualize the results. The techniques used were based on prior research, for example: Ofir Arkin's "Remote ICMP Based OS Fingerprinting Techniques"[49], the P0f[50] tool, Nmap[51] OS fingerprinting signatures, DHCP fingerprinting[52] and "Passive OS fingerprinting by DNS traffic analysis" by Matsunaka, Yamada & Kubota. The GUI of the system was built using Flask[53].

[46] https://nebelwelt.net/blog/20160913-ControlFlowIntegrity.html
[47] by matching to known sub graphs
[48] by matching sub graphs between programs
[49] https://www.defcon.org/images/defcon-10/dc-10-presentations/dc10-arkin-xprobe.pdf
[50] http://lcamtuf.coredump.cx/p0f3/
[51] https://nmap.org/book/osdetect-fingerprint-format.html
[52] https://fingerbank.org/
[53] https://github.com/pallets/flask/



Sample screenshot of "Network Mapping" (Orange==Linux, Blue==Win)

More Projects

In addition to the two projects that were detailed above we have also spoken about the following projects:

Project Name	Short Description	Age of Participants
Suspicious Users Detection	Network anomaly detection system which identifies outlier behavior of users (UBA[54]).	15 years old
You Can't See Me	VMI[55] based sandbox implementation for	15 years old
Syntaxipot	Honeypot for web-based applications.	15 years old
hackermen	Identifying key network elements from passive sniffing (DGW, DNS,	15 years old

[54] User Behaviour Analytics

[55] Virtual Machine Introspection - https://publish.illinois.edu/assured-cloudcomputing/files/2015/05/041915-Virtual-Machine-Instrospection-Overview.pdf

	DHCP, etc).	
Cryptonic	Stopping process based on executed syscalls (implementation of a seccomp[56] like solution for non supported OSes).	15 years old
Matlac	Binary analysis based on histograms of library calls.	15 years old

**9th grade ~=15 , 10th grade ~=16*

It is important to remember that these projects are only examples and not a full survey and review of all the projects conducted by teenagers from Israel. The goal was to showcase a span of projects performed by teenagers and give a hunch to the high technical level young students can get (despite their age).

What Did They Learn?

Overall the main objective of the technical project is to expose the teenagers/young students to real-world challenges, dilemmas, technologies and more. Based on 1:1 sessions conducted with the teenagers/young students before/at the time/after the projects we had realized that there are several areas which significantly improved (due to the work performed): improvements in technical knowledge and improvements in working capabilities/habits.

Thus, regarding technical knowledge improvements we can give a couple of examples: a deeper understanding of scapy[57] (packet crafting framework), manipulation of data stored in databases[58], multiprocessing, source control management and more. Moreover, the improvements in working capabilities/habits include: collaboration, planning, going over researches, sticking to schedule and more.

MagTF 2017

MagTF 2017 was a CTF event organized for Magshimim[59] program graduates (18+) by noxale[60] (see also noxale Case Study) members, which are young students (16-17 years old) of the program. The CTF included challenges in various topics

[56] https://www.kernel.org/doc/Documentation/prctl/seccomp_filter.txt

[57] https://github.com/secdev/scapy

[58] Including SQL and stored procedures

[59] Israel National Cyber Education Program, https://www.magshimim.cyber.org.il

[60] A youth security group, https://www.noxale.com

such as: web exploitation, binary exploitation, reverse engineering, forensics, cryptography, and even biological hacking. Around 150 teenagers took part in the event which was held for about 8 hours. For the first time, students who had not graduated from the program yet created challenges which graduates of the same program tried to solve.

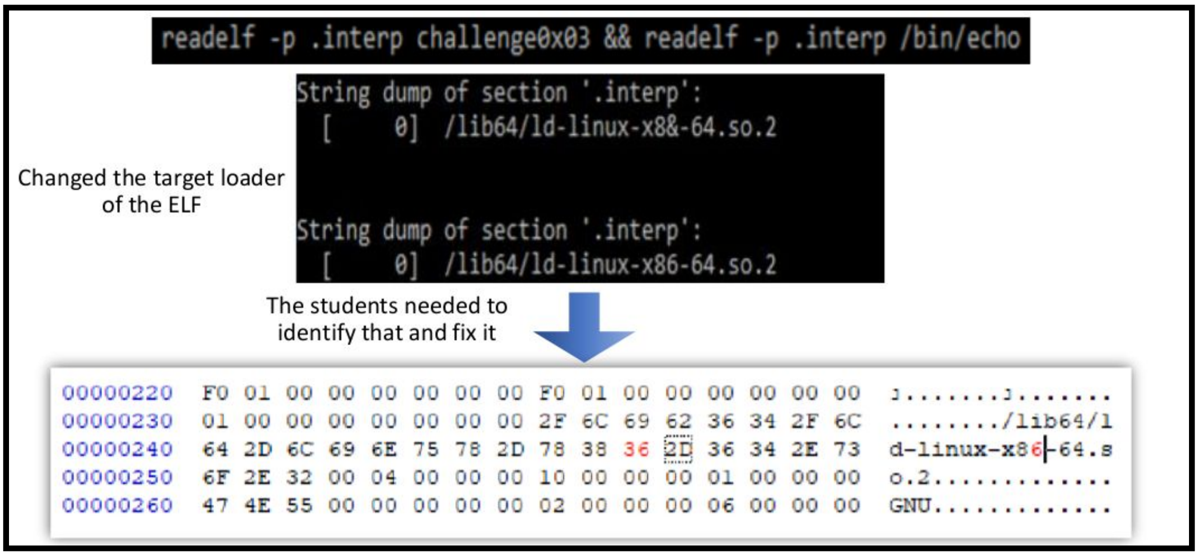
Entrance to the event
https://m.facebook.com/Magshimim/albums/1740624735948663/

Thus, the event had benefited both the participants and the organizers. The participants who weren’t familiar with a specific topic had the opportunity to learn it by solving challenges, which simulated real-world implementations and weaknesses. The organizers had to create the challenges - which required them to be very fluent at the challenges topics and learn various attack and defense techniques on the reflected technologies. The deep knowledge required for creating good challenges helped the teenagers (which organized the event) find jobs in the industry afterward.

The Mental Model Problem

If we think about it, human's decision-making process is composed by the following components: the processing power of our brain[61], the amount of time we have to decide/act[62] and the information we have available[63] (Simon, 1955[64]). Thus, the lack of knowledge in cybersecurity can lead to improper design/implementation decisions which increase the probability of security vulnerabilities.

Moreover, In 1970 Piaget[65] stated that in case of discrepancy between two cognitive entities cognitive development emerges. Thus, to tackle such problems we can leverage conflict based learning[66]. In order to do so, we created a set of challenges that are broken by design and the goal of the student was to fix them. Two examples of these challenges are: modification of the .interp section of an ELF file to point to a nonexisting loader file and an alteration of the syscall opcode to sysret as part of a system call stub.



```
readelf -p .interp challenge0x03 && readelf -p .interp /bin/echo
```

```
String dump of section '.interp':
  [     0]  /lib64/ld-linux-x8&-64.so.2


String dump of section '.interp':
  [     0]  /lib64/ld-linux-x86-64.so.2
```

Changed the target loader of the ELF

The students needed to identify that and fix it

```
00000220  F0 01 00 00 00 00 00 00 F0 01 00 00 00 00 00 00  ð.......ð.......
00000230  01 00 00 00 00 00 00 00 2F 6C 69 62 36 34 2F 6C  ......../lib64/l
00000240  64 2D 6C 69 6E 75 78 2D 78 38 36 2D 36 34 2E 73  d-linux-x86-64.s
00000250  6F 2E 32 00 04 00 00 00 10 00 00 00 01 00 00 00  o.2.............
00000260  47 4E 55 00 00 00 00 00 02 00 00 00 06 00 00 00  GNU.............
```

Alteration of the .interp section

Also, the students that tried to solve the challenges ranged from 9th-10th grade. The results of the conflict based learning approach among that group of teenagers were amazing. The students got a better understanding of the ELF format, they understood in detail how the syscall mechanism in Linux worked, it helped them

[61] Which will always be limited.

[62] Which will always be finite.

[63] Which will always be incomplete.

[64] http://www.dtic.mil/get-tr-doc/pdf?AD=AD0604198

[65] https://www.researchgate.net/publication/222650482_Piaget's_stages_The_unfinished_symphony_of_cognitive_development

[66] Introduce conflicts by design to enable learning (by solving them).

with the use of gdb/objdump/readelf/etc, gave them a deeper understanding of operating system fundamentals and much more.

Europe Case Study

Due to the fact that the conference is held in Europe, we had decided to demonstrate how cybersecurity education among teenagers is being conducted in Europe. We had decided to focus on three examples: TeenTech, DCMS (Department of Culture, Media and Sports) Cyber School Program and The College of National Security.

First, there is TeenTech which help teenagers to see the wide range of career opportunities in STEM (Science, Engineering and Technology)[67]. Also, TeenTech collaborated with companies, universities in UK and Europe to achieve their goal. In the cybersecurity[68] field, TeenTech produced a series of films and events to help students/parents/teachers to be aware of the enormous opportunities at their reach[69].

Second, in order to defend the UK against cyber attacks at least 5,700 teenagers aged 14-18 are going to be taught 'cyber curriculum' by 2021[70]. The program led by DCMS (Department of Culture, Media and Sports). The newer cyber school program aims to teach pupils some of the skills they would need to help defend British businesses and institutions against online threats. The cybersecurity curriculum composed by classroom and online teaching with hands-on experience and real-world challenges. The students are expected to commit to four hours a week, starting at 14 to complete a four-year course.

Third, The College of National Security[71], a first for the UK, is scheduled to open in 2020 in a specially adapted premises on the Bletchley Park site. It's a sixth-form college of National Security cyber skills for Britain's most gifted teenagers aged 16-19 years old. The sixth-form boarding school will be free to the 500-odd applicants, with a mix of venture capital, corporate sponsorship and very possibly state funding underwriting the multimillion-pound costs. It will select on talent alone, looking in particular for exceptional problem solvers and logic fiends, regardless of wealth or family background. The opening of the college, originally planned for 2016, has been delayed to 2020 as their application to open (as a college in the Department for Education's Free Schools program) is yet to be granted[72].

[67] http://www.teentech.com/about-teentech/

[68] http://www.teentech.com/cybersecurity/

[69] set to offer over 4.5 million more jobs worldwide by 2019.

[70] https://www.independent.co.uk/news/uk/home-news/cyber-attacks-security-uk-russia-china-isis-terrorist-nhs-websites-curriculum-school-teenagers-a7574611.html

[71] https://en.wikipedia.org/wiki/National_College_of_Cyber_Security

[72] https://qufaro.uk/news/christmas-update

Moreover, the college is led by Qufaro[73], a non-profit organization created by a consortium of cybersecurity experts for the purposes of education. The college curriculum balances cybersecurity (approximately 40%) with related subjects including maths, physics, and computer science over a three-year study period. The college will be boarding partly to ensure attendance by those who do not live in the south-east.

[73] https://qufaro.uk/

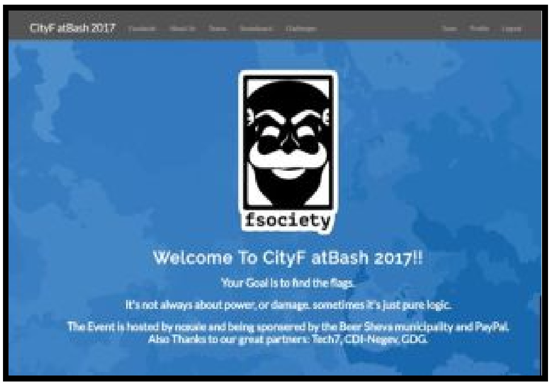
noxale Case Study

noxale[74] is a local Israeli security team which includes passionate teenagers that are engaged in the creation/participation of CTFs and spreading of cybersecurity knowledge among the Israeli community. In order to give a background about noxale following is a table which consists of basic information regarding the group:

Founded	2016
Number of Members	50 - Global group 35 - CTF team
Age Range	17-18
Activities	Blog & Weekly challenges CTF creation & participation Security tools development Community education Conferences
CTF Rating 2018	Overall 74[75] (156.738 points)

Basic information about the noxale group

Also, as part of the contribution to the local Israeli cybersecurity community, noxale group organized the CityF atBash 2017[76] CTF (the first CTF organized by teenagers in Israel). The CTF was created with the support of industry, community, and municipality. The CTF included different challenges in various topics such as: web exploitation, binary exploitation, reverse engineering, cryptography, and forensics.



Welcome To CityF atBash 2017!!

Your Goal is to find the flags.

It's not always about power, or damage. sometimes it's just pure logic.

The Event is hosted by noxale and being sponsered by the Beer Sheva municipality and PayPal.
Also Thanks to our great partners: Tech7, CDI-Negev, GDG.

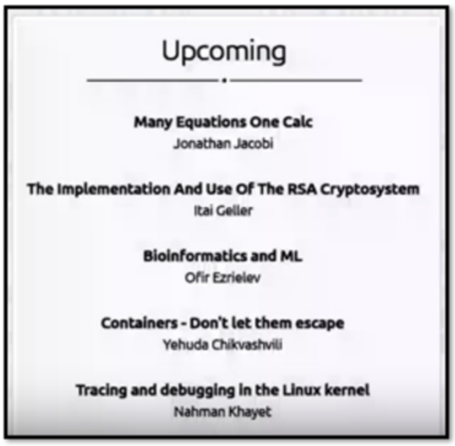
The online portal of the CityF atBash 2017 CTF

[74] www.noxale.com
[75] https://ctftime.org/team/33990
[76] https://ctftime.org/event/419

Furthermore, as part of the ongoing effort to enhance the capabilities of the team members, noxale organized noxCTF 2018[77] which was the first worldwide online CTF an Israeli team has initiated. 40 Challenges were included in the CTF on many topics such as: web and binary exploitation, steganography, reverse engineering, forensics, pwn and cloud exploitation. More than 900 teams and 4000 people took part in the event which was running for 48 hours.

CTF's headquarters

Moreover, to support the community of Israeli teenagers with passion for cybersecurity, noxale group had organized the first security conference for teenagers that was organized by teenagers (noxCon 0x01[78]). The conference included talks from 5 different teenage speakers and included topics such as: implementation of RSA cryptosystem, bioinformatics and machine learning, container technology escaping techniques, tracing and debugging in the Linux kernel and one interesting story of how a team member found a vulnerability in Microsoft word equation feature.



Upcoming

Many Equations One Calc
Jonathan Jacobi

The Implementation And Use Of The RSA Cryptosystem
Itai Geller

Bioinformatics and ML
Ofir Ezrielev

Containers - Don't let them escape
Yehuda Chikvashvili

Tracing and debugging in the Linux kernel
Nahman Khayet

noxcon 0x01 timeline

[77] https://ctftime.org/event/671
[78] https://www.youtube.com/watch?v=RXB-C1Sks8k

Another one of noxale activities is noxale’s blog[79] in which they upload write-ups of the their solutions for CTF challenges (in events the team participated). In this blog they also upload the solutions for the weekly challenges[80] and for some of the challenges in their events (such as noxCTF 2018). The purpose of the blog is both to contribute to the security community by sharing methods of attacks and real-world methodologies and to practice research document writing.

In the area of education of the teenage community, noxale members are volunteering in most of the Israeli educational programs creating teaching material, creating educational challenges, and organization of various teaching events. Some of noxale members also act as teachers in these programs after they graduate.

In addition, noxale members created educational programs of themselves. One example is JuniorsTeachJuniors[81], an educational program created with the help of Tech7Juniors[82] innovation community whose purpose is to give teenagers the stage to teach other teenagers about stuff that they are interested in. One noxale member was the creator and the first speaker of the program, and led a short introduction course (5 hands-on sessions of 3 hours each) to cybersecurity and attacking techniques to 20+ teenagers (aged 11-17).

On top of all of that, noxale members are also taking part in spreading its educational approach among teachers and the community. noxale members find themselves almost on a weekly basis meeting teenagers and speaking to high school crowd all over the country and spreading the sense of innovation which leads them. As part of this effort, they meet teachers from excellence programs in Israel to expose them to different types of self-education of cybersecurity and computer science and the corresponded needs of the students.

[79] https://blog.noxale.com
[80] https://blog.noxale.com/page/weekly/
[81] https://www.t7j.org/juniors-teach-juniors
[82] https://www.t7j.org/

Future Thinking

All of the above is only the tip of the iceberg and there is still a long way to go. There are still things we as a community should do:

- Organize practical learning events (CTFs, trainings, competitions, etc) in order to attract more teenagers to the field of cybersecurity and to challenge them.
- Mentor teenagers and help them learn the ever-evolving realm of cybersecurity.
- Coach them in the creation of real-world projects while evolving their understanding of the different project phases: initiation, planning, execution, and termination.
- Expose the industry to teenagers (by things like internships) and vice versa.

Also, we can think of different ways in which we can upgrade the current approach such as:

- Adding practical cybersecurity training in schools as earlier as possible (maybe starting from 1st grade).
- Exposing girls in middle school to female cybersecurity leaders systematically (to encourage them to be part of the ecosystem).
- Teaching cutting-edge technology with hands-on experience.
- Investing more in pedagogical concepts to improve the education process.

Blackhat Sound Bytes

Overall the three key takeaways that anyone should remember and share with fellow colleagues are:

1. Youth age is most suitable for education in cybersecurity.
2. A full-package education system in cybersecurity for teenagers can aid in solving the workforce shortage.
3. Cooperation, Cooperation, Cooperation. Cooperation between community and industry is the key to achieving the 2nd point.