Course name
Cyber Security Training

Course Stages:

Stage A1
Network Training: Network training for the following certification: MCSE, MCSA, CCNA.

Stage B1A1 (for graduates of stage A1)
Advanced Linux LPI1 & LPI 2

Stage B2A1 (for graduates of stage A1)
Hacking and Networking Defense training

Stage B3A1 (for graduates of stage A1)
Programming (Python, C++, C).

Stage C1B3 (for graduates of stage B3A1)
Secure Development and Programming Training

Stage C2B (for graduates of any of the stage B plans)
Big Data & Data Mining

Stage D1 (for graduates of stages A1, B2A1, B3A1 and C1B3)
Cyber Operations
It is important to note, that at any level's completion, the student will be qualified and trained for several positions in the job market. Should the students choose to advance their skills, and reach for the highest levels of expertise (and highest paying jobs) in the cyber market, they may elect their own path in the program.
**Duration**

Stage A1 – Twelve (12) weeks onsite training.
Stage B1A1 – Twelve (12) weeks onsite training.
Stage B2A1 – Twelve (12) weeks onsite training.
Stage B3A1 – Twelve (12) weeks onsite training.
Stage C1B3 – Nine (9) weeks onsite training.
Stage C2B - Ten (10) weeks onsite training.
Stage D1 -  Ten (10) weeks onsite training.

**Number of participants**

Up to 40 students per class.

**Number of Lecturers**

1-2 Trainers per class.
About HackerU:

HackerU Hi-Tech College is the leading center for computer and information technology training in Israel. HackeruPro is the Business Division of HackerU that specializes in computer and information technology training for hi-tech professionals.

HackeruPro offers professional enrichment courses, on-site custom training, seminars and events on a wide array of relevant technologies. In addition, we also offer tailor made courses suited for the needs of each organization individually.

At HackeruPro, our goal is to lead the professional training market for Hi-Tech industry. Our objective is to provide professionals with innovative up-to-date content to enhance their current position by acquiring new skills.

Participants will expand their knowledge and upgrade their skills with the help of leading industry instructors and gain new tools to enhance their-selves within their organization.

HackeruPro offers the ultimate combinations of quality, leading Hi-Tech instructors, and state of the art facilities. HackeruPro provide personalized courses tailor fit for your employee’s needs and organizational requirements that are mutually beneficial for both parties.

HackeruPro’s goal is to train and develop both new and veteran Hi-Tech professionals via our enrichment courses lead by our dedicated, talented instructors and team.

HackeruPro offers various courses in Software Development, Information Security, Cloud, Mobile Development (Android and iOS), QA & Testing, UX/UI, Databases, Big Data etc.
CERTIFICATION

Our proposal, which was presented to you, which is comprised of stages containing Network training for international certification: MCSE, MCSA, CCNA. Advanced Linux, Secure development, Programming, Big Data, Osint and cyber operation training – is designated specifically for Australia. The following reflects the outlines and the course topics that we are able and willing to provide you as our services, please note that this proposal might change and be modified in accordance with the students learning process.

CYBER SECURITY TRAINING PROGRAM DETAILS

Stage A1

Computer Basics, Networking & Linux Certifications

Duration: 12 Weeks, including exercise
(4 hours each week for practical training, with the tutor on site)

This first level training course will give the knowledge, tools and practical experience in computers, servers and network communications, to provide a complete infrastructure management and computerized business solutions.

This course also brings the theoretical contents needed to gain access to the most desirable international certification exams in the field, pass them successfully and get the ticket to work in a variety of roles of the IT world.

In addition to content based on Microsoft technologies, advanced professional content is taught, such as Microsoft expertise, Linux and Cisco.

This content is an important element in the industry and provides a significant advantage and differentiation from the other contender's track graduates in the labor market and allow them faster readjustment leading professionals

20h  Introduction
180h  MCSA
• **60h** Installing and configuring Windows Server 2012  
• **60h** Administering Windows Server 2012  
• **60h** Configuring Advanced Windows Server 2012 Services  

**100h** **MCSE**  
• **50h** Core Solutions of Microsoft Exchange Server 2013  
• **50h** Advanced Solutions of Microsoft Exchange Server 2013  

**50h** **Linux**  

**100h** **Cisco**  

**Summary: 450 hours**  

**Each Week Contains 40 academic hours**  

**Description:**

**First part – MCSA 1/3: Installing and Configuring Windows Server 2012 (60h)**  
- Module 1: Deploying and Managing Windows Server 2012  
- Module 2: Introduction to Active Directory Domain Services  
- Module 3: Managing Active Directory Domain Services Objects  
- Module 4: Automating Active Directory Domain Services Administration  
- Module 5: Implementing IPv4  
- Module 6: Implementing Dynamic Host Configuration Protocol  
- Module 7: Implementing DNS  
- Module 8: Implementing IPv6  
- Module 9: Implementing Local Storage  
- Module 10: Implementing File and Print Services  
- Module 11: Implementing Group Policy  
- Module 12: Securing Windows Servers Using Group Policy Objects  
- Module 13: Implementing Server Virtualization with Hyper-V  

**Second part – MCSA 2/3: Administering Windows Server 2012 (60h)**  
- Module 1: Configuring and Troubleshooting Domain Name System  
- Module 2: Maintaining Active Directory Domain Services  
- Module 3: Managing User and Service Accounts
- Module 4: Implementing a Group Policy Infrastructure
- Module 5: Managing User Desktops with Group Policy
- Module 6: Installing, Configuring, and Troubleshooting the Network Policy Server Role
- Module 7: Implementing Network Access Protection
- Module 8: Implementing Remote Access
- Module 9: Optimizing File Services
- Module 10: Configuring Encryption and Advanced Auditing
- Module 11: Deploying and Maintaining Server Images
- Module 12: Implementing Update Management
- Module 13: Monitoring Windows Server 2012

Third part – MCSA 3/3: Configuring Advanced Windows Server 2012 Services (60h)

- Module 1: Implementing Advanced Network Services
- Module 2: Implementing Advanced File Services
- Module 3: Implementing Dynamic Access Control
- Module 4: Implementing Distributed Active Directory Domain Services Deployments
- Module 5: Implementing Active Directory Domain Services Sites and Replication
- Module 6: Implementing AD CS
- Module 7: Implementing Active Directory Rights Management Services
- Module 8: Implementing and Administering AD FS
- Module 9: Implementing Network Load Balancing
- Module 10: Implementing Failover Clustering
- Module 11: Implementing Failover Clustering with Hyper-V
- Module 12: Implementing Business Continuity and Disaster Recovery

Forth part – MCSE 1/2: Core Solutions of Microsoft Exchange Server 2013 (50h)

- Module 1: Deploying and Managing Microsoft Exchange Server 2013
- Module 2: Planning and Configuring Mailbox Servers
- Module 3: Managing Recipient Objects
- Module 4: Planning and Deploying Client Access Servers
- Module 5: Planning and Configuring Messaging Client Connectivity
- Module 6: Planning and Implementing High Availability
- Module 7: Planning and Implementing Disaster Recovery
- Module 8: Planning and Configuring Message Transport
- Module 9: Planning and Configuring Message Hygiene
- Module 10: Planning and Configuring Administrative Security and Auditing
- Module 11: Monitoring and Troubleshooting Microsoft Exchange Server 2013
Fifth part – MCSE 2/2: Advanced Solutions of Microsoft Exchange Server 2013
(50h)
- Module 1: Designing and Implementing Site Resilience
- Module 2: Planning Virtualization for Microsoft Exchange Server 2013
- Module 3: Overview of Exchange Server 2013 Unified Messaging
- Module 4: Designing and Implementing Exchange Server 2013 Unified Messaging
- Module 5: Designing and Implementing Message Transport Security
- Module 6: Designing and Implementing Message Retention
- Module 7: Designing and Implementing Messaging Compliance
- Module 8: Designing and Implementing Administrative Security and Auditing
- Module 9: Managing Exchange Server 2013 with Exchange Management Shell
- Module 10: Designing and Implementing Integration with Microsoft Exchange Online
- Module 11: Designing and Implementing Messaging Coexistence
- Module 12: Designing and Implementing Exchange Server Upgrades

Sixth part – Linux: (50h)
- Linux Basics
- Files and Directories
- Monitoring
- Standard IO and Pipes, Text & Strings
- Network management
- Remote Administration

Seventh part – Cisco: (100h)
- Routing and Switching Fundamentals
- Routing
- Protocols and Concepts
- LAN Switching and Wireless
- Accessing the WAN


**Stage B1A1**

**Advanced Linux LPI Certifications**

**Duration:** 12 Weeks, including exercise

(8 hours each week for practical training, with the tutor on site)

In this Linux servers course we will use Debian, a free operating system that uses the Linux kernel (the central core of the computer operating system).

The Debian GNU Project gives us more than a standard operating system. It comes with over 25,000 packages, precompiled software bundled format for installation on servers.

This course will expose the technological capabilities of Linux-based Debian interior features, including networks, servers’ establishment and Linux Administration.

- **20h** Introduction
- **65h** LPI 101
- **10h** Python 101
- **65h** LPI 102
- **10h** Python 102
- **80h** LPI 201
- **15h** Python 201
- **80h** LPI 202
- **10h** Python 202

**Summary: 450 hours**

Each Week Contains 40 academic hours
Description:

First part – LPI 101: (65h)
- System Architecture
- Linux Installation and Package Management
- GNU and Unix Commands
- Devices, Linux Filesystems, Filesystem Hierarchy Standard

Second part – Python 1 – Python Syntax: (10h)
- Code syntax
- Variables and Types
- Lists
- Basic Operators
- String Formatting
- Basic String Operations
- Conditions
- Loops
- Basic script
- Command line manipulation with os.system

Third part – LPI 102: (65h)
- Shells, Scripting and Data Management
- User Interfaces and Desktops
- Administrative Tasks
- Essential System Services
- Networking Fundamentals
- Security

Forth part – Python 2 – Medium level coding: (10h)
- Functions
- Advance syntax
- Connect to mysql
- Manipulate ssh
- Create simple Brute force script
- Try, Except
Fifth part – LPI 201: (80h)
- Capacity Planning
- Linux Kernel
- System Startup
- Filesystem and Devices
- Advanced Storage Device Administration
- Advanced Network configuration and Troubleshooting
- System Maintenance

Sixth part – Python 3 – Advanced level coding: (10h)
- Classes and Objects
- Dictionaries, tuple, sets
- Packages
- Generators

Seventh part – LPI 202: (80h)
- Domain Name Server
- Web Services
- Implementing a proxy server
- Implementing Nginx as a web server and a reverse proxy
- File Sharing
- NFS Server Configuration
- Network Client Management
- E-Mail Services
- System Security
- Secure shell (SSH)
- Security tasks
- OpenVPN
- DevOps

Eighth part – Python 4 – Advanced level coding – Object-oriented: (10h)
- Classes
- Multi-threads
- Multi-processing
Stage B2A1
Networking & Hacking & Defense training

Duration: 10 Weeks + 2 Weeks Exercise

Description:

First week: Hacking
- Introduction
- Cryptography
- Web application security
- Reconnaissance
- Networking security
- Basics (Hackers, White Hats & Penetration tests)
- Common PT Types (White \ Gray \ Black Box)
- Understanding common PT Attacks (Web \ NetworkLevel)
- Common PT Techniques (Web \ Network Level)
- Common Exploiting Techniques

During this part, the students will be familiar with hacking techniques and will immerse the students into an interactive environment where they will be shown how to scan, test, hack and secure their own systems. This session will be very interesting and will be based on the previous session and will upgrade their networking skills.
Second week: Hacking advanced
- Penetration
- Commercial Tools
- Open source tools
- Simulation in tools

Third week: Information Security
- Virtualization
- Windows Monitoring and Auditing
- Information Security Attack Vectors
- Cyber and Infosec
- Cybercrime Forensics
- Information Warfare
- Security Architecture
- Cyber Kill Chain - Demo

Forth week: Information Security
- APT, Security Tools
- Security Open Source Tool – WAF, HoneyPot, Firewall
- Hardening
- Wireless & Mobile Security
- Detection Techniques
- Hacking vs. Ethical Hacking
- Risk analysis & threat Intelligence
- Event management

Fifth week: Network Defense A
- Network security infrastructure
- Impact of compromised routers and switches
- Escalating privileges at Layers 2 and 3
- Weaknesses in Cisco router and switch architecture
- Understanding existing network devices to defend against attacks
- DHCP, ARP snooping, and port security
Giving the fact that the students have studied at the first part of the course the capabilities of programming and development, the student will implement their skills in defending their network. They will be familiar with secured network structure, ways of upgrading main permissions, vulnerabilities and security holes/breaches helping defending from them. They will create network rules/doctrines in favor of defense in several different platforms. In addition, they will learn about popular routing protocols and their weaknesses.

**Sixth week: Network Defense B**
- Architecture design and preparing filters
- Building intrusion detection capability into a network
- Understanding the components currently in place
- Detection techniques and measures
- Traffic
- Packet analysis and more

This week the students will acquire the necessary skills and capabilities for network defense. This will be the continuation of the previous week where students will face different types of traffic and capability of detecting suspicious traffic. They will perform a defense layer that monitors and detects of attack and even preventing them. They will perform deep packet inspection which will enable them to analyze network traffic at the network level. The student will make advanced rules for protecting the network, install and configure IDS tools and other analyzers advanced tools. Students will face Event correlation and analysis, Building advanced snort rules and more. By the end of this session the students will have multiple capabilities of network defense.

**Seventh week: Monitoring the Network**
- Web Application A
- Basic networking terms and concepts
- OSI model: Offensive and Defensive point of view
- Wireshark interface: Deeper look
- Protocol filters
- IP and port filtering
- HTTP packet analysis
- Monitoring on a proxy server
In this part the student will acquire deep knowledge of the OSI model in the aspects of defense and offense. The emphasis will be on sniffing the traffic using Wireshark. The student will study about advanced filters including IP protocols and ports. They will go through HTTP traffic analyzer and identity hijacking within the net. Understanding right and analyzing correct the data will help them to really understand how Firewalls works in the network traffic which will help them find unauthorized traffic. Students will acquire the tools of monitoring the network and the proxy servers.

**Eighth week: Identifying vulnerabilities**

- The Pentest Process
- Footprinting
- Reconnaissance
- Scanning
- Vulnerability analysis
- Key tools and techniques

During this week the students will be focusing on vulnerabilities and security holes in the servers. They will deeply analyze the penetration testing process along with other interesting techniques. The students will gain the necessary tools of understanding the full process of cyber attacker that focuses on finding vulnerabilities and executing penetration testing. This part will help them to prevent such attacks. The students will understand the Focus, requirements, and outputs of a successful test. This part will also deal with Application testing and reporting.

**Ninth week: PenTesting with Metasploit**

- Metasploit Basics and Framework Organization
- Server and Client Side Exploitation
- Meterpreter – Extensions and Scripting
- Database Integration and Automated Exploitation
- Exploring the system
During this week the students will be specializing in Metasploit platform. They will get to know its capabilities and work with its features. This will provide the students with many tools for improvement of the penetration skills learned in session 3. By the end of this session they will be able to do Token stealing and impersonation, Backdoors and Rootkits, Pivoting and Port forwarding, Railgun and Custom Scripting, Backdoor an Executable. By giving them those tools and with the studies they made so far, they will gain the capabilities in all these aspects.

Tenth week: Wi-Fi (Defense and Offense points of view)
- Bypassing WLAN Authentication
- Cracking WLAN Encryption
- Offensive the WLAN Infrastructure
- MITM, Wi-Fi Protected Setup
- Exploiting the Wireless Client
- Breaking into the Client

This week the students will acquire the necessary skills and capabilities of Wi-Fi. They will be familiar with Wi-Fi in offensive and defensive points of views. They will master varied types of encryption, types of security and the ability to defend from Wi-Fi hacking which include the most advanced technologies. They will study about different attack in the Wi-Fi world including Rogues devices, evil twins MITM and more. Students will face Bypassing Authentication, Shared Key, MAC Filtering, Hidden SSIDs, Cracking Encryption, WEP and WPA/WPA2. They will be able to Exploit WLAN, deal with DoS Attacks, Advanced Attacks e.g. 802.1x, EAP, LEAP, PEAP, EAP-TTLS; the students will implement the Wireless Client, Metasploit, Wi-Fi Worms, WiFishing and Social Engineering. The students will experience honey-pots and their behaviors and gain the right capabilities for their unit’s network
Stage B3A1
Programming (Python, C++, C).

Duration: Ten (10) weeks onsite training + 2 Weeks Exercise (1 DAY a week practical training with the tutor on site).

Description:
Stage B3A1 will consist of Programming, during which, the students will learn different key languages for their programming capabilities enhancement; they will be familiar with the structure of the language and able to run applications necessary for their rolls.

First week: Python 1
- Python Scripting
- System Programming and Security

Second week: Python 2
- System Programming and Security
- Network Security

Programming Third week: Python 3
- Network Security Programming
- Web Application Security

This is the first part of the first session out of the requested course. This part of the course will teach the students Python scripting, System programming and Security and its application to problems in computer and network security. This course is ideal for penetration testers, Cyber security experts. During this part, the students will be introduced to Python and lean about Data Types and variables, Operators and Expressions, Program Structure and Control, Functions and Functional Programming, Classes, Objects and other OOPS concepts, Modules, Packages and Distribution. The students will practice Python in different operating systems (Linux & windows) and in different platforms (Mobiles: iPhone and Androids, Python in Routers). The students
will experience intensive studies of I/O, File and Directory Access, Multithreading and Concurrency, Inter Process Communication, Permissions and Controls. At the end of this module the students will get an overview and training on Python programming necessary for the beginning of every hacker who deals with scripts and this module will implement & enhance their skills on various case studies. The students will also learn Raw Socket basics, Socket Libraries and Functionality. This week will give the students the required skill to program servers, clients, sniffers, arbitrary packet injectors with Python which is very important tool for hackers in programming attacks (Web Services & Automated web attacks), scripts and environments. In addition, the students will analyze HTML and XML and emulate Web Browser. This session will be based on the previous stage and will upgrade their networkingskills.

Fourth week: Malware Analysis & Reverse Engineering
- Malware Analysis in VirtualMachines
- Anti-DisassemblyAnti-Debugging
- Malware Behavior
- Anti-Virtual Machine Techniques
- Packers and Unpacking

During this part the students will learn the basic and advanced techniques of malware analysis including Assembly and advanced debuggers which will allow them to receive in depth understanding of malware behavior. This is a critical stage of both of offensive and defensive.

Fifth week: Python 4
- Exploitation Techniques
- Malware Analysis

During this part the students will learn programming exploitation techniques combined with advanced capabilities that will allow them to develop tools for exploits using Python. In addition, the students will learn how to use the knowledge they gained and implement it into writing, memorizing and analyzing running applications. They will focus on Exploit Development techniques, Immunity Debuggers, Writing plug-ins, Binary data analysis and Exploit analysis Automation. The students will understand malwares’ behaviors and will be to do debugging basics, analyze live applications, In-memory modifications and even breakpoints & memory.
In this part the students will summarize the Python programming by combining all their knowledge from the previous sessions in analyzing malwares and up to understanding their structure as independent malwares. It will involve exploits, injections and understand the offense and defense parts including Language Essentials, System Programming and Security, Exploitation Techniques, Malware Analysis and Reverse Engineering, System Programming and Security and Network Security Programming.

**Sixth week: Python 5**

- Malware with Python

During this part the students will continue to learn programming exploitation techniques combined with advanced capabilities that will allow them to develop tools for exploits using Python. This week is in direct continuity with week seven.

**Seventh week: C - Vulnerabilities, exploits and countermeasures Module 1***

- C - Fundamentals
- Control Flow
- Functions
- Classes

**Eight week: C++: Vulnerabilities, exploits and countermeasures Module 2***

- C++ Fundamentals
- Control Flow
- Advanced Functions
- C++ and code writing

During this part, the students will be familiar with C and C++ fundamentals and understand this super important language for coding. The fundamentals will include built-in types, Integer numbers, floating Point numbers, characters, Booleans and more. The students will face the simple and compound statements, Conditional expression which they will immerse the students into the functions of the language, including navigation & delegation; they will experience its unique classes and practice with functions. During this part the students will continue the course of programming and will drill down into more complex and advanced aspects.

*Depends on students' progress.
Ninth week: C++ Module 3
- Basic and Advanced OOP
- Containers

Tenth week: C++ Module 4
- Polymorphism
- Secure Coding

In this stage some of the subjects learned in the previous week might slip through this week. In addition, the students will work with OOP (Object Oriented Programming) which provide the build of a comprehensive data base program and integration of other programs in the code aspect. They will be familiar with advanced programming including guidelines for system program, Declaring and defining virtual functions, Virtual destructors and Polymorphism through pointers and references. During this part, the students will also be familiar with secure coding and understanding how they can to create and develop better codes. They will study the weaknesses points of C++ allowing them to write clean codes that are protected from hacking and exploits. This stage is very important in the defense part. The students will be familiar with off- by-one errors, Problems with NTBSs, causes of buffer overflows, and Causes of heap overflows, Common memory management errors, Integer promotion standards, Side effects of integer promotions, Common integer errors, Common semaphore issues, File I/O errors and Review process for identifying coding errors.
Stage C1B3
Secure Development and Programming Training

**Duration:** Seven (7) weeks onsite training + 2 Weeks Exercise (1 DAY a week practical training with the tutor on site).

**Description:**
Stage C1B3 will consist of Programming (Assembly), the student will be familiar with the structure of the language and able to run applications necessary for their rolls.

First week: C and C++: Vulnerabilities, exploits and countermeasures Module 1*

- Memory Management in C/C++
- Vulnerabilities
- Countermeasures

During this part, the students will be familiar with C++ fundamentals and understand this super important language for coding. They will master the C language which is very close to the machine language where they will understand how programming with C works in memory. In addition, they will identify security holes and breaches of C++ of code injection and buffer overflow, hence learning how to avoid future security holes. The students will also experience Format string vulnerabilities, Safe languages, Verification countermeasures and more.

* Depends on students' progress

Second week: Assembly Module 1

- 32 Assembly Language

During this part, the students will study the basics and fundamentals of Assembly language. This will allow the students to understand all the processes that are behind the scenes including reading and writing to memory and etc. they will be familiar with the program structure, data type, data movements Instructions, Arithmetic instructions, Conditional instructions, Interrupts, Traps and Exceptions, Procedures, Prologues and Epilogues, Syscall structure and ABI for Linux, Calling standard library functions and FPU instructions.
Third week: Exploits A
- Windows
- Linux

Forth week: Exploits B
- Protection Mechanisms
- Writing Exploits for Win32
- Writing Remote and Local exploits

During this part, the students will study how to work with exploits, how to identify them using advanced tools. They will gain introduction to the Stack, the Stack overflows on Linux, Shellcode, Intro to heap overflows, Intro to 64-Bit Assembler, Windows Overflows, tampering with the Return Address, Buffer Overflow, BC Detection, The art of Fuzzing and be able to write exploits. This part is super important for the development of the students as they will use materials and tools they have studied over the previous sessions.

Fifth week Assembly (Module 2)
- Shell coding on Linux

In this section the students will study how to work with exploits using assembly by creating Shell code, allowing them to understand and write their own sophisticated software tools.

Sixth-Second Week Assembly (Module 3)
- Encoders, Decoders and Crypters on Linux

In this section the students will study how to work with intricate exploits using assembly by creating Shellcode, and understanding the work method of popular Trojans in Assembly perspective. This will give the students full understanding of the exploits world where they will gain the capabilities and skills necessary to detect them and protect against them.
Seventh week Assembly (Module 4)

- Polymorphism

In this section the students will study how to work with intricate exploits using assembly by creating Shellcode, and understanding the work method of popular Trojans in Assembly perspective. This will give the students full understanding of the exploits world where they will gain the capabilities and skills necessary to detect them and protect against them.
Stage C2B
Big Data, Data Mining and Osint

Duration: Eight (8) weeks onsite training+ 2 Weeks Exercise (1 DAY a week practical training with the tutor on site).

Description:
Stage C2B will instruct students in Osint, Big Data and Data Mining basics. During the training, the students will learn different key languages for their building and accessing data storage. They will be familiar with the structure data banks, and able to run applications necessary to mine them for relevant information. They will have basic understanding of what is Osint and how to find and gather information on the web.

First week: Introduction to Big Data
- Big Data Overview
- What is data sciences
- The rising and importance of data sciences
- Big data analytics in industry verticals
- Data Understanding
- Data Preparation

In this week, the students will the basics of Big Data, starting from what is a data base, where to find them and what they are good for. The rampant accumulation of data online, and finding the order in the disorder in which it is stored. They will learn what big data is, and the benefits and dangers of it. The structures and languages typically in use will also be covered.

Second week: Data Analytics 1 - Lifecycle and methodology
- Modeling
- Evaluation
- Communicating results
- Deployment

In this week, the students will attempt accessing data banks. They will understand and use the different forms of data storage, learn to evaluate relevant information forms and develop their own data storage and programs. They will learn the ways a data bank communicates, and how to query and draw information from it.
**Third week: Data exploration & preprocessing**

- Data base location
- Specific data focus
- Measures and evaluation

During this week the students will continue working Data Bases, learning their physical locations and storage, and forms of processing data for storage. They will write their own sub-routines and learn about the problems of indexing data fields and records, and limitless storage capacities, as well as filtering out irrelevant and redundant information present in most data storages, by using Data preparation and filtering steps like: cleaning, normalization, transformation, feature extraction and selection.

**Fourth week: Data Analytics 2 - Theory & Methods**

- Linear/Logistic regression
- Decision trees
- Naïve Bayes
- K-means clustering
- Association rules

Students will learn advanced techniques for constructing classifiers: models that assign class labels to problem instances, represented as vectors of feature values, where the class labels are drawn from some finite set. They will get acquainted with some types of probability models, vector quantization, and initialization methods such as Forgy and Random Partition.
Fifth week: Unstructured Data Analytics

- Technologies & tools
- Text mining, Web mining

Students will learn about information that either does not have a pre-defined data model or is not organized in a pre-defined manner, and how to find and process it. They will cover semi-structured data, structuring input texts and deriving patterns. Students will perform monitoring and analysis of online plain text sources such as internet news and blogs, searching for data with national security importance. Students will also begin to cover the study of text encryption and decryption.

Sixth week: The Endgame

- Operationalizing an Analytics project
- Data Visualization Techniques
- Creating final deliverables

Students will learn and put to use a data location, retrieval and analysis project in real life. They will learn techniques used to communicate data or information by encoding it as visual objects contained in graphics. The students will create a final presentation using the data they retreated, delivering it in a clear, understandable and usable form and fashion to their teacher/supervisor, as a mock-up of an actual intelligence report.

Seventh week OSINT – Open Source Intelligence

In this week the student will learn what is OSINT; How the WWW is built; What are we looking for and where; What is the difference between information and intelligence; central OSINT tools: free databases and paid databases. Google tool box: Google advanced search. Geographic Information – Google maps, Google street view, IP geo-location. a set of tools for gathering information in unconventional ways (but still legal ways), Google images – reverse search. The "Babylon tower" – searches in different languages etc.....
• Introduction to Open Source Intelligence (OSINT)
• Google and other search engines
• Alternative Data and Operative Intelligence.
• The "gold mine" – extracting information from social networks

Eight week OSINT
In this week the student will Local databases, Operative Intelligence guidelines, Smaller social networks, Meta searches in social networks, Tips on finding a person that doesn't want to be found, Identity verification in social networks, How to identify avatars and false virtual identities, How to create an avatar, including cover stories and methods to make the avatars appear real, Etc….

• The "gold mine" – extracting information from social networks
• Creating a subject profile
• Avatars
• The Dark Web
**Stage D1**  
**Cyber Operations**

**Duration:** Eight (8) weeks onsite training + 2 Weeks Exercise (1 DAY a week practical training with the tutor on site).

**Description:**

Stage **D1** is the culmination of the training program. During the training, the students will apply all tools and languages and put them to use, learning the tools of Cyber Operations, data retrieval and Hacking. All classes will prepare students to know and handle list of topics below, first for defense then for offense. Impotent concepts of data security, threats, computers, protocols and other subjects shall be included.

**Week 1 – Methodology**

In this week we will explain the basics of infrastructures, the fundamentals of this class, and general survey of solutions, data management and cyber, course basics, and setting goals for students and teachers alike.

**Week 2 – Honeypots, FW**

The challenges if managing FW, local FW and FW infrastructure, different kinds of honeypots including monitoring, knowing open source FW and FW solutions all the way to the basics, advantages and disadvantages. Goals – Hands on experience with FW integration and Honeypots basic development, monitoring and implementation.
Week 3 – DLD, encryptions

Most common challenges of DLP’s including the business world. Political problems with employees, managers, changing work protocols, implementing new organizational work rules, product implementation, common products, encryption methods (symmetric, a-symmetric), common algorithms. Goals – building an encryption system for data, implementing it, and storing data on web based interface.

Week 4 – SIEM, Antivirus

Basics of Antivirus, common market products, in-depth learning of how antivirus works, imprinting virus-affected files, work process and implementation of antivirus, Basics of SIEM including work routines, Information security protocols, analyzing and writing logical rules, and common market SIEM systems.

Week 5 – 0-days, Darknet, Spider Recon

Students will search information on people and companies to better know the internet and all its layers. Students will write scripts to automate common searches, which were first made manually. Introduction to Darknet, access, and attempts to penetrate closed groups and gather information. Protocol methods and basic 0-days.

Week 6 – Botnet, Trojan horses

Introduction to how botnets and Trojans and how they work. Hands on – students will operate and change existing botnets and creat new ones – undetectable by antivirus software. Demonstrations and black-red team wars will take place as well.
Week 7 – Malware

The workings of malware, differences between malware and other attack methods, and matching attack types to objective and target. We will lean the different kinds of malware, hands on with simple malwares to practice making them and using vulnerabilities. Students will analyze each other's software.

Week 8 – Cyber Lab

Students will be divided into two teams – and play out scenarios. Attack team will analyze and penetrate, and defense team will build and repel attacks. Then teams will switch. This will combine all materials learned, and the teachers will supervise logging and building projects in both attack and defense, until both teams are fully capable.

In the 10 weeks of Stage D1, the students will be using the acquired knowledge from previous stages A1, B2A1, B3A1 & C1B3, and implement it, demonstrating it through practices of cyber operations. They will make work protocols for real events, build firewalls and be divided into teams, where they will be practice offensive and defensive tactics on eachother

This stage will be focusing on providing cyber tools for operations (e.g. knowing where and when the network is being attacked, securing web applications, etc.). Simulations will be conducted, in which one team attacks the other while the second team defends. They will practice monitoring and forensics for each operation. Hence, Stage D1 will provide the students plenty of cyber operation knowledge and experience, making them into professional Hackers and Cyber Expe