CYBERSECURITY TRAINING

UFAR FRENCH UNIVERSITY IN ARMENIA

API Armenia Peace Initiative

THIS CYBERSECURITY TRAINING PROGRAM IS FUNDED BY ARMENIA PEACE INITIATIVE, AN ENDOWMENT FUND ESTABLISHED IN PARIS AND YEREVAN.

GENERAL OBJECTIVE OF THE TRAINING COURSE

These training program goals aim to provide participants with:

- comprehensive understanding of security risks,
- secure development practices,
- forensic investigation,
- network penetration testing techniques.

Practical application, hands-on exercises, and real-world examples should be incorporated throughout the training to enhance participants' skills and knowledge.

Knowing that zero-risk does not exist, companies must constantly monitor the evolution and maintenance of their IT systems or applications.
At the end of this training, which is intended to be an operational training, participants will be able:

- to understand the mechanisms of Cybersecurity,
- to periodically check an IT infrastructure or a computer program by auditing it then to patch the vulnerabilities found,
- to find out if the system has been compromised by investigating the systems and taking countermeasures.

TECHNICAL DETAILS

Number of participants	10-23
Level	Intermediate
Total number of hours	92
Duration	October 5 - October 30
Price	40 000 AMD

Course Prerequisite

- Hardware understanding (Workstation and Server)
- Windows system administration (Workstation and Server)
- Linux system administration (Workstation and Server)
- Networking (IPv4, IPv6, Routing)
- Virtualization (VMware, Proxmox)
- Web development (PHP, JS, ...)

Course Title	Hours	ECTS	Trainer
Cybersecurity: Threats and Needs Analysis	7	1	Sébastien BARGUIRDJIAN
Networking	14	2	Nicolas RENARD
System Administration & Hardening (Windows & Linux)	28	4	Nicolas RENARD
Virtualization	18	2	Sébastien BARGUIRDJIAN
Digital Forensics	11	2	Sébastien BARGUIRDJIAN
Pentest	14	2	Sébastien BARGUIRDJIAN

INFORMATION ABOUT THE TRAINERS

Sébastien Barguirdjian

Sébastien Barguirdjian is an internatinally certified computer science expert with a specialization in Cybersecurity. He has worked on four continents, with experience ranging from small businesses to global corporations and even the armed forces.
Currently, Mr. Barguirdjian holds the position of CEO at EXAGENIUS, a leading Cybersecurity firm.

He also serves as a dedicated Cybersecurity Teacher at the Faculté des Métiers de Bretagne, in addition to his role as an Operational Reserve Officer and Instructor in the French Gendarmerie Nationale.

Nicolas Renard

Nicolas Renard is a VMware vExpert & Microsoft Certified Expert and Trainer.

He is a trainer at SUP de Vinci and Orange Cloud Campus.

Currently, he works at Orange Cloud For Business as VMware Cloud Engineer.

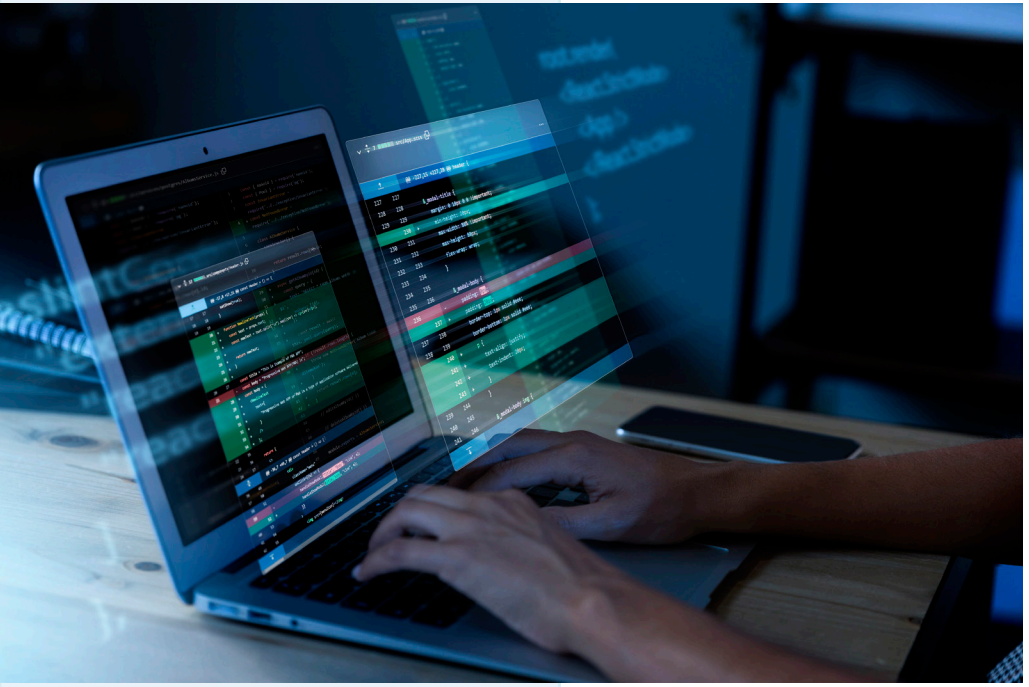
Course title: **Cybersecurity: Threats and Needs Analysis**

Trainer: **Sébastien BARGUIRDJIAN**

Introduction :

Cybersecurity is today a key issue for the future of large countries. According to the World Economic Forum, the probability of a major failure of critical information systems in the next ten years is 10%, with a potential impact of $250 billion.

Cyberattacks are on the rise and target small and medium-sized businesses in 80% of cases. France is ranked 15th among the countries most attacked by cyberattacks, far behind the United States, China and India.



Presentation :

The objective of this cybersecurity training is to discover current threats and the cybersecurity needs of companies by understanding the attack mechanisms and the methods of analyzing the need in correlation with the national policy on security of enterprise systems information.

Acquired skills :

At the end of this module, students will be able to:

- Understand the main threats and their impact
- Know how to analyze a company's needs
- Know the legislative bodies in the field and their role
- Implement good cybersecurity practices to protect against attacks.

Duration: 7 hours

Course program:

- IS security issues
- Security needs
- Concepts of vulnerability, threat, attack
- Overview of some threats
- ICT law and the organization of security in France

Learning methods:

This course indicates what the threats are and what their impact is through concrete examples.
Digital media may be used to illustrate the lessons.

Assessment :

MCQ of 20 questions (20 x 1 point)

Course title: **Networking**

Trainer: **Nicolas RENARD**

Introduction :

A computer network is a set of computers linked together that exchange information. Except that in addition to computers, a network can also contain specialized equipment, such as hubs, routers, and many other equipment that we will cover in this course. Broadly speaking, a network is entirely composed of: IT equipment (computers and network hardware) and point-to-point links which connect two devices together.

Presentation :

Network administration is an essential task in the IT world. There are many ways to organize the connections and computers on a network, thousands of ways to manage the transfer of information on the network.

Acquired skills :

At the end of this module, students will be able to:

- Understand the basics of networking
- Know the network models (OSI, TCP/IP)
- Know network protocols (ICMP, TCP, UDP)
- Use network analysis tools
- Use IPv4 and IPv6

Duration: 14 hours

Course program:

- Introduction to Networks
- Discovery of the OSI model
- Learning standard protocols
- Differences between IPv4 and IPv6
- Using network analysis tools
- Practical work

Learning methods:

This course shows how the secure implementation of a server takes place through concrete examples. Digital media may be used to illustrate the lessons.

Assessment :

MCQ of 40 questions (40 x 0.50 points)

Course title: **System Administration & Hardening (Windows & Linux)**

Trainer: **Nicolas RENARD**

Introduction :

The server operating system provides the central interface for managing users and encompasses various security and administration related services. All of these elements are essential to operating a client-server architecture.

Presentation :

The administration of a system is an important, sensitive and strategic load which determines the integrity, durability, accessibility and confidentiality of the resources (hardware, software, data) of an information system.

Acquired skills :

At the end of this module, students will be able to:

- Deploy a server
- Configure network and remote connection
- Know and configure services
- Secure the server
- Deploy automation tasks
- Monitor server operation

Duration: 28 hours

Course program:

- Windows Server - Installation
- Windows Server - Network Configuration
- Windows Server - Powershell
- Windows Server - Active Directory
- Windows Server - DNS
- Windows Server - WSUS
- Windows Server - Hardening
- Windows Server - Practical work
- Linux Server - Installation
- Linux Server - Network Configuration
- Linux Server - Basic System Commands
- Linux Server - Common Services
- Linux Server - Cron
- Linux Server - Hardening
- Linux Server - Practical work

Learning methods:

This course shows how the secure implementation of a server takes place through concrete examples. Digital media may be used to illustrate the lessons.

Assessment :

MCQ of 80 questions (80 x 0.25 points)

Course title: **Virtualization**
Trainer: **Sébastien BARGUIRDJIAN**

Introduction :

Virtualization is a set of techniques that allow multiple operating systems to run on the same physical machine. Before virtualization, 80% of servers in a data center had an average utilization rate of less than 10%. Taking into consideration technological progress as well as Microsoft recommendations or Linux distributions (A single service or a single application on the same operating system), it is essential to use virtualization.

Presentation :

Virtualization will make it possible to use physical resources as much as possible, reduce the number of physical servers, save space in server rooms, reduce hardware maintenance time and costs, reduce electricity consumption and therefore the company's carbon footprint.

Acquired skills :

At the end of this module, students will be able to:

- Differentiate between level 1 and 2 hypervisors.
- Install and configure a type 1 hypervisor.
- Create virtual machines (VMs).
- Manage Failover
- Manage VM backup and recovery.

Duration: 18 hours

Course program:

- Concept of virtualization
- Installing a Type 1 Hypervisor
- Hypervisor configuration
- Creating a cluster
- Storage management
- Virtual machine (VM) management
- Failover management
- Backup and restoration management

Learning methods:

This course shows the procedure for setting up a type 1 hypervisor server in the form of practical work. Digital media may be used to illustrate the lessons.

Assessment :

TP (20 points)

Course title: **Digital Forensics**
Trainer: **Sébastien BARGUIRDJIAN**

Introduction :

Forensic analysis is not a new science: the first analysis dates back to 1284 in China. In 1835, work began on ballistics and the traces left by firearms. In 1901, fingerprints were introduced. We began digital analyzes in 1978 and it was from 1984 that we began to be interested in DNA in the context of forensic analysis. There are therefore several subjects in forensic analysis and when we talk about "computer" forensics, we find the term digital forensics to define the scope and the subject.

In Infosec, we use forensic analysis to find attacks, respond to incidents, uncover espionage, particularly industrial espionage, data exfiltration, document falsification or even data loss.

Presentation :

The DUMP method performs post-mortem analysis of a medium or disk, a method which has the advantage of having little impact on the data. It is considered the most "pure" and neutral method in the sense that data alteration is low.

Acquired skills :

At the end of this module, students will be able to:

- Collect data for an investigation.
- Conduct the analysis on a copy of the disk.
- Scan malicious files.
- Construct an investigation report.

Duration: 11 hours

Course program:

- Identification: find and identify information and image the system as a first step.

- Acquisition: restoring the disk image

- Analysis: analysis of all data recovered, prioritization, restitution of the chronology and actions carried out during the infection / intrusion.

- Presentation: provide a detailed report.

Learning methods:

This course shows the process of a post-mortem analysis through concrete examples. Digital media may be used to illustrate the lessons.

Assessment :

TP (20 points)

Course title: **Pentest**

Trainer: **Sébastien BARGUIRDJIAN**

Introduction :

Pentest, also called intrusion testing in French, is an ethical hacking technique consisting of testing the vulnerability of a computer system, an application or a website by detecting flaws likely to be exploited by a hacker or malware.

Pentesting can be done automatically by using software applications or it can be done manually by a pentester. Regardless of the option chosen, the different stages of this strategy are based on the identification of points of vulnerability and on an attempted intrusion into the heart of the system, allowing key information to be obtained to improve cybersecurity.

Presentation :

The goal of this course is to provide students with an in-depth understanding of cybersecurity principles and techniques. It will allow them to understand the different methods and tools used to protect computer systems and networks against threats and attacks.

Acquired skills :

At the end of this module, students will be able to:

- Identify and exploit an organization's vulnerabilities.
- Apply security principles and protect infrastructure.
- Detect and respond to a cyberattack.

Duration: 14 hours

Course program:

- Collection of information
- Threat Determination
- Vulnerability Analysis
- Operation
- Post exploitation
- Audit report

Learning methods :

This course shows how a Cybersecurity audit will take place through concrete examples. Digital media may be used to illustrate the lessons.

Assessment : TP (20 points)