INFORMATION SECURITY INTRODUCTION

HAUTE-ÉCOLE LÉONARD DE VINCI

PRESENTATION

WELCOME
TO AWESOME STUDENTS

$> WHOAMI

Grégoire Grison

CyberLab Manager
Senior Cybersecurity Engineer
CyberSec Teacher
Be.Cyber Community Admin

gregoire.grison@vinci.be

https://discord.gg/4fmHCybcs

POURQUOI J'ENSEIGNE ?

- Pas que des bons souvenirs
- Enorme besoin d'aide en Cybersécurité
- Envie de partager et de susciter cette même passion
- Former des personnes en ligne avec la réalité d'aujourd'hui

CYBERLab

CyberLab Directions

CYBERLab

Training

Developing **human** and **technical skills** to effectively defend systems and organizations against cyber-attacks.

● People ● Processes ◐ Products

Testing

Analyzing and **understanding** the **resilience** of systems when they are subject to a cyber-attack.

○ People ◐ Processes ● Products

Research

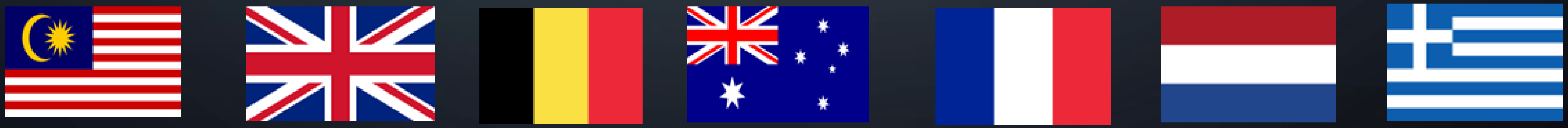
Improving the state-of-the-art **capabilities** by exploring the unknown and propose **innovative approaches.**

○ People ○ Processes ● Products

> *I **hear** and I **forget**.*
> *I **see** and **I remember**.*
> *I **do** and I **understand**.*
>
> *Confucius*

> ***Testing** leads to **failure**,*
> *and **failure** leads to*
> ***understanding**.*
>
> *Burt Rutan*

> ***Research** is creating new*
> ***knowledge.***
>
> *Neil Armstrong*



CyberLab Pillars

Defense & Gov

ATTACK SURFACE
LARGE NUMBER OF COMPLEX SYSTEMS
COMMUNICATIONS & SENSORS
PLATFORM MANAGEMENT SYSTEM
NAVIGATION SYSTEMS & PROPULSION
COMBAT MANAGEMENT SYSTEM
THALES

Research & Commercial Activities

CYBERLab

Region & Europe

LynkEUs project

Multitel INNOVATION CENTRE

ENGIE Laborelec

Critical Infra & Private Sector

héna llux HAUTE ÉCOLE DE NAMUR-LIÈGE-LUXEMBOURG

UMONS Université de Mons

UCL Université catholique de Louvain

ULB CYBERSECURITY RESEARCH CENTER

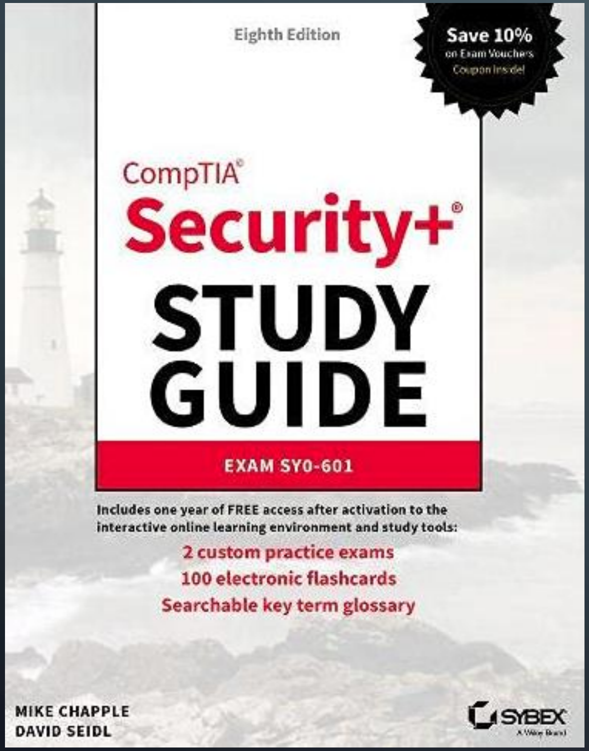
Academia

CyberLab : Proposed trainings

Immersive training platform with realistic and typical IT systems

- CYBERSECURITY AWARENESS
- VULNERABILITY ASSESSMENT & MANAGEMENT
- SECURITY THROUGH SOFTWARE LIFECYCLE
- ICS CYBERSECURITY
- RED TEAM
- BLUE TEAM
- PURPLE TEAM
- PENTESTING
- TABLETOP CYBER CRISIS MANAGEMENT

MATERIAL USED FOR THIS COURSE



Eighth Edition

Save 10% on Exam Vouchers Coupon Inside!

CompTIA® Security+® STUDY GUIDE

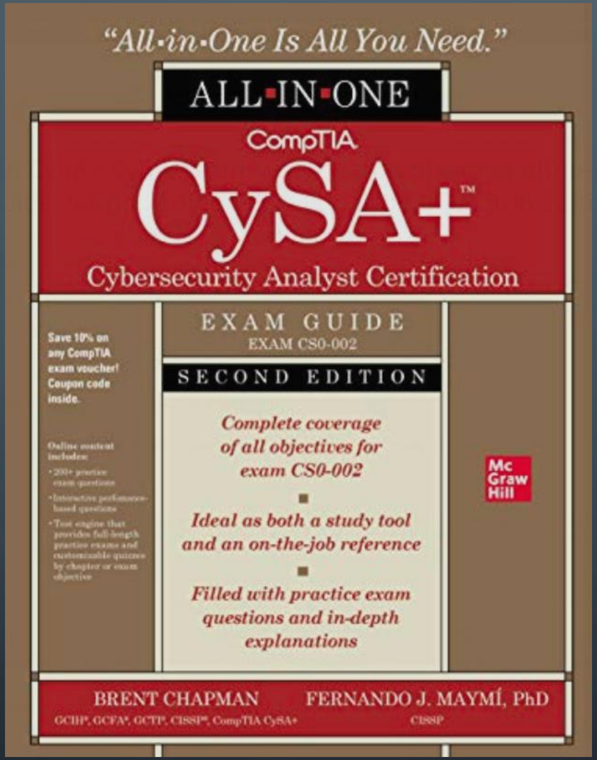
EXAM SY0-601

Includes one year of FREE access after activation to the interactive online learning environment and study tools:

2 custom practice exams
100 electronic flashcards
Searchable key term glossary

MIKE CHAPPLE
DAVID SEIDL

SYBEX A Wiley Brand



"All-in-One Is All You Need."

ALL-IN-ONE

CompTIA CySA+™

Cybersecurity Analyst Certification

EXAM GUIDE
EXAM CS0-002

SECOND EDITION

Save 10% on any CompTIA exam voucher! Coupon code inside.

Online content includes:
- 200+ practice exam questions
- Interactive performance-based questions
- Test engine that provides full-length practice exams and customizable quizzes by chapter or exam objective

Complete coverage of all objectives for exam CS0-002

Ideal as both a study tool and an on-the-job reference

Filled with practice exam questions and in-depth explanations

Mc Graw Hill

BRENT CHAPMAN
GCIH®, GCFA®, GCTP®, CISSP®, CompTIA CySA+

FERNANDO J. MAYMÍ, PhD
CISSP

Internet

Me

COURSE STRUCTURE

Chapter 1 – Generalities

1.1 Cybersecurity Objectives

1.2 Threat Landscape

1.3 Malicious Code

1.4 Breach Impact

1.5 To have fun

COURSE STRUCTURE

Chapter 2 – Cyber Threat Intelligence

2.1 Threat Data Intelligence

2.2 Indicators of Compromise

2.3 The Cyber Kill Chain

2.4 The MITRE ATT&CK

2.5 Vulnerability Management

COURSE STRUCTURE

Chapter 3 – Secure Coding

3.1 Injection Vulnerabilities

3.2 Software Assurance Best Practices

3.3 Designing & Coding for Security

3.4 Software Security Testing

3.5 Application Security Controls

COURSE STRUCTURE

Chapter 4 – Cryptography

4.1 Definition & History

4.2 Cryptography Objectives

4.3 Steganography

4.4 Substitution & Poly Substitution

4.5 Symmetric

4.6 Asymmetric

4.7 Hashing

4.8 Digital Signature

4.9 Public Key Infrastructure

4.10 Post-Quantum

COURSE STRUCTURE

Chapter 5 – Network Security

5.1 D4RK W3B

5.2 Network Design

5.3 Network Appliances and Security Tools

5.4 Network Discovery

5.5 Network Attacks

COURSE STRUCTURE

Chapter 6 – Incident Response

6.1 Definition

6.2 Les incidents 2022

6.3 L'incident Medibank

6.4 Process

6.5 Incident Response Team

6.6 Incident Response Plans

6.7 Data & Tools

6.8 Mitigation and Recovery

6.9 CERT

COURSE STRUCTURE

Chapter 7 – Digital Forensics

7.1 Concepts

7.2 Conducting Digital Forensics

7.3 Acquiring Forensics Data

7.4 Acquisition Tools

7.5 Analysis

7.6 Reporting

7.7 Intelligence