Contents

1 Cybersecurity with Python Lyon College Certificate

Proposal for a 23-day summer course on cybersecurity with a certificate for successful completion. To be piloted summer 2024.

1.1 Schedule

The course would meet on 23 days (May 28-June 27) for 2 hours each day. There would be 2 hours homework outside of class - in total, this is the equivalent of 3 credit course (92 hours).

For the first time, the course should take care in the classroom at Lyon, though a hybrid is possible (classroom + online attendees). To attract a diverse group of students, it could take place during lunchtime or evening hours.

No prerequisites except a general affinity to numbers and computers. The programming language (Python) and the necessary maths (graph theory, discrete maths, number theory, combinatorics) are introduced and unpacked during the course.

1.2 Certificate

Successful course completion ($> 60\%$ of available points) would come with a Lyon College Certificate "Cybersecurity with Python" that lists major course components mastered:

1. Securing computer networks with Graph algorithms.
2. Analyzing and monitoring network traffic and packet data.
3. Identifying threats with Social Network Analysis.

4. Tracking people in space with digital information.

5. Cybersecurity capstone project.

1.3 Instructor

- Dr. Marcus Birkenkrahe has been a teacher of computer and data science and business informatics since 2007. Prior to teaching, he was head of competitive intelligence at Shell International, and head of knowledge management at Accenture. At Shell, he supervised globe-wide network penetration testing and participated in global scenario analysis. At Accenture, he helped to build an active threat simulator for professional IT consultants. He is associate editor of the International Journal of Data Science, and editorial board member of the International Journal of Big Data Management.

1.4 Draft syllabus

The draft syllabus can be adapted as per the learning pace of the students:

- Each topic includes practical examples and exercises for better understanding.

- The course provides resources for further learning and exploration.

- The course includes discussions on cybersecurity ethics and responsible conduct throughout the course.

- Regular assessments, quizzes, and feedback are integrated to gauge the understanding and learning progress of the students.

Day 1-3: Introduction to Cybersecurity and Python
Day 1: Introduction to Cybersecurity and Overview

- Cybersecurity fundamentals

- Importance of Cybersecurity

- Python for Cybersecurity

Day 2: Basic Python Programming

- Python data types, variables, and operations

- Control structures (loops, conditionals)

- Functions and modules

Day 3: Working with Libraries in Python

- Introduction to libraries (NumPy, Pandas)
- Installation and basic operations

Day 4-6: Securing Networks with Graph Theory
Day 4: Introduction to Graph Theory

- Basics and terminology
- Real-world application in network security

Day 5: Graph Algorithms

- Dijkstra's, Bellman-Ford algorithms
- Detecting vulnerabilities in networks

Day 6: Python Libraries for Graph Theory

- NetworkX
- Creating and analyzing network graphs

Day 7-9: Building a Network Traffic Analysis Tool
Day 7: Introduction to Network Traffic Analysis

- Understanding network traffic
- Importance and application in Cybersecurity

Day 8: Packet Analysis with Python

- Working with pcap files
- Analyzing packet data

Day 9: Building a Basic Network Traffic Analysis Tool

- Python scripting for traffic analysis
- Real-time traffic monitoring

Day 10-13: Identifying Threats with Social Network Analysis
Day 10: Introduction to Social Network Analysis (SNA)

- Fundamentals and principles of SNA
- Application in cybersecurity

Day 11: SNA Metrics and Algorithms

- Centrality measures, clustering coefficients
- Detecting potential threats using SNA

Day 12-13: Python for Social Network Analysis

- Using Python libraries for SNA (NetworkX)
- Case study: Identifying Threats with SNA

Day 14-17: Tracking People in Physical Space with Digital Information
Day 14: Introduction to Digital Tracking

- Concepts and techniques
- Ethical considerations

Day 15: Geolocation and Tracking with Python

- Working with GPS data
- Analyzing and visualizing location data

Day 16-17: Building a Digital Tracking System

- Python libraries and APIs for tracking
- Case study: tracking people in physical space

Day 18-20: Python and Cybersecurity Tools
Day 18: Working with Cybersecurity Tools in Python

- Popular cybersecurity libraries and tools
- Integrating Python with cybersecurity tools

Day 19-20: Developing a Cybersecurity Project

- Students will start working on a small cybersecurity project integrating the concepts learned

Day 21-23: Project Work and Conclusion
Day 21-22: Continue Project Work

- Working on the project
- Solving problems and doubts

Day 23: Conclusion and Presentation

- Project presentation
- Conclusion and feedback
- Further learning resources and pathways

1.5 References

"Hackers Arise." Occupy the Web. https://www.hackers-arise.com/. Accessed September 30, 2023.

Hernandez-Ramos JL, Matheu SN, Skarmeta A. The Challenges of Software Cybersecurity Certification [Building Security In]. IEEE Secur Priv. 2021;19(1):99-102. https://doi.org/10.1109/MSEC.2020.3037845.

Matheu SN, Hernández-Ramos JL, Skarmeta AF, Baldini G. A Survey of Cybersecurity Certification for the Internet of Things. ACM Comput Surv. 2021;53(6):Article 115. https://doi.org/10.1145/3410160.

1.6 Textbooks

1. Reilly D. Math for Security: From Graphs and Geometry to Spatial Analysis. September 2023:312. ISBN-13: 9781718502567.

2. OccupyTheWeb. Linux for Hackers: Getting Started with Networking, Scripting, and Security in Kali. December 2018:248. ISBN-13: 9781593278557.

3. Stamp M. Introduction to Machine Learning with Applications in Information Security. 2nd ed. Chapman and Hall/CRC; 2022.