Masterschool

Become a *Cyber Analyst*

Cybersecurity Syllabus

Table of contents

Career Training

Our 7-month intensive training program will equip you with the essential cybersecurity analyst skill set and get you job-ready. You will learn cybersecurity fundamentals, get hands-on experience, and develop a stellar portfolio with real-world experience sourced from the world's leading cybersecurity companies.

Career Accelerator

After your technical training, you will join the Career Accelerator until you find a job. You will focus on searching for a job in Cybersecurity while participating in extensive career workshops and benefiting from one-on-one mentorship sessions. You will also continue to develop your technical skills and gain more experience.

Endless Career Growth

Our goal is to ensure that you build an inspiring career. This means we're here for you even after being hired for your first role. As our graduate, you will become a part of our vibrant alumni community, gain access to exclusive events and workshops, and get the undivided support of our team whenever you start thinking about the next step in your career journey.

Become a 10x More Efficient Cyber Analyst with AI Based Syllabus

At Masterschool, our comprehensive training program goes beyond traditional cybersecurity education. We understand that in today's rapidly evolving technological landscape, the integration of artificial intelligence (AI) is crucial for staying ahead of emerging threats. That's why our syllabus incorporates cutting-edge AI-related topics, ensuring that our Cybersecurity Program is future-proof, and our students are well-equipped to tackle the challenges of tomorrow.

By learning how to work with AI tools, our students gain a competitive edge, and become 10 times more efficient as cybersecurity analysts. Through hands-on experience, our students develop a stellar portfolio that showcases their ability to leverage AI for advanced threat detection, intelligent data analysis, and proactive defense strategies.

- Students leverage the power of Language Models (LLMs) to scan vast data sets and identify suspicious logs efficiently. As they harness the capabilities of LLMs, our students develop a deep understanding of log analysis, enabling them to detect potential cyber threats with greater accuracy and speed.

- Throughout the program, our experienced School Masters share real-world examples of how AI-based tools are utilized in defending against cyber threats. These practical insights provide students with valuable knowledge and demonstrate the practical applications of AI in the cybersecurity domain.

- While participating in real-time events, students learn how to enhance their skills as cyber analysts by integrating AI models into their incident response workflow. They practice providing incident details to an LLM model, receiving suggested actions, incorporating the results as input, and iterating the process until the incident is successfully resolved. This firsthand experience strengthens their ability to leverage AI for effective incident management.

- Students gain proficiency in efficiently protecting and scanning both Windows and Linux systems by leveraging AI platforms. These platforms provide advanced capabilities such as anomaly detection, behavioral analysis, and predictive modeling, enabling students to proactively identify and mitigate potential vulnerabilities.

- Our curriculum includes training in using AI tools to assist them in writing protective policies. For instance, students learn to utilize AI-powered platforms to generate comprehensive "Do’s and Don'ts" guides for new employees, determine the appropriate threshold for blocking an account after a specific number of password attempts, and cover edge cases that may otherwise be

overlooked. With their newly acquired proficiency in utilizing AI tools, students save time and improve the coverage of their policy development process.

- Students are trained to extract the key insights from incident reports and effectively communicate them to management and other stakeholders. Additionally, they learn how to leverage AI tools to visualize and present reports in a more accessible manner, ensuring that non-cyber personnel can understand as well as make informed decisions based on the information presented.

Incorporating these AI-related topics into our syllabus ensures that students not only develop strong foundational cybersecurity skills, but also become adept at leveraging AI tools to be 10 times more efficient as cybersecurity analysts. Our program equips students with the knowledge and expertise needed to navigate the ever-changing cybersecurity landscape and make a significant impact in the field.

CY-101

Tech Fundamentals

During the first unit of our program, we will lay the groundwork with the tech fundamentals you need to succeed. Learn programming with Python, practice algorithmic thinking, and complete your first coding projects. In addition, this unit will teach you time management skills, touch typing, and how to use keyboard shortcuts to work effectively.

Sprint 1	Problem Solving and Algorithmic Thinking
Sprint 2	Programming with Python 1
Sprint 3	Programming with Python 2
Sprint 4	Practice Week

Concepts covered:

- Python
- Problem Solving
- Algorithmic Thinking
- Time Management
- Touch Typing
- Keyboard Shortcuts
- Networking
- Internet

CY-102

Cyber, Windows, and Linux

This unit journeys from the dawn of cybercrime to modern threats while emphasizing the importance of cybersecurity and its terminologies. You will understand hackers, cyber-attacks, and the potency of social engineering. We then explore Windows and Linux operating systems. We focus on the desktop, NTFS File System, UAC, and troubleshooting for Windows. For Linux, we delve into file permissions, text editors, utilities, processes, package management, and log files, thus highlighting the importance of securing digital infrastructures.

Sprint 1 Security Foundations

Sprint 2 Windows Foundations

Sprint 3 Linux Navigation and Commands

Sprint 4 Practice Sprint

Concepts covered:

- The World's First Cyber Crime
- What is Cybersecurity?
- Cybersecurity Terminology
- Why Cybersecurity Matters
- Hackers and Cyber Attacks
- The Power of Social Engineering
- Introduction to The Windows Operating System
- Troubleshooting Windows
- Windows Desktop, The NTFS File System, UAC, and the Control Panel
- Introduction To Linux
- Flags, Permissions, and the Filesystem
- Text Editors, Utilities, Processes, Package Management, and Logs

CY-103

Networking and Cryptography

This unit is a comprehensive journey into network fundamentals, protocols, security, and the cornerstones of cryptography. It begins with an overview of basic networking, types of networks, and networking devices, underpinned by a deep dive into the OSI and TCP/IP models. This unit navigates through the world of network security, emphasizing security protocols and network monitoring. Simultaneously, it unravels cryptography, covering encryption types, hashing, digital signatures, and the Public Key Infrastructure. By the conclusion of this module, participants will possess the knowledge and skills to secure computer networks effectively.

Sprint 1	Networking Foundations
Sprint 2	Cryptography
Sprint 3	Network Protocols, Security, and Monitoring
Sprint 4	Practice Sprint

Concepts covered:

- Basics of networking
- OSI and TCP/IP Models
- Networking devices
- Types of Networks
- Network protocols
- Basics of cryptography and encryption
- Encryption Types
- Hashing and Digital signatures
- Public Key Infrastructure
- Network Security
- Security Protocols
- Network Monitoring

CY-104

Security Foundations

Here we will be starting with an introduction to PowerShell; you will learn the basics of scripting and how to apply PowerShell for effective Windows administration. This is complemented by a deep dive into Windows Administration Tools, where you will gain hands-on experience in their practical usage, with a specific emphasis on the integral role of Active Directory. A key element of this unit is the exploration of system logs and the crucial insights they provide into system operations and security incidents. You will learn the best-practice security measures, how to enhance system defense, and effectively troubleshoot potential issues.

Sprint 1	Windows Administration - PowerShell
Sprint 2	Windows Administration Tools
Sprint 3	System Logs
Sprint 4	Practice Sprint

Concepts covered:

- Introduction to PowerShell
- PowerShell Scripting
- Windows Administration with PowerShell
- Introduction to Windows Administration Tools
- Windows Administration Tools Practical Usage
- Active Directory
- System Logs in Windows
- Security Practices
- Troubleshooting and Best Practices

CY-105

CompTIA Security+ Part One

This unit will explore various topics, including types of malware, social engineering attacks, Advanced Persistent Threats, and insider threats. The unit also covers threat intelligence and hunting, vulnerabilities and exploits, penetration testing techniques, and secure application development. Important frameworks and guidelines for physical security, secure network architecture concepts, secure staging deployment concepts, and cloud and virtualization concepts are included. You will learn how to proactively secure networks and systems throughout this unit, using various tools and methodologies to prevent, detect, and mitigate security threats.

Sprint 1	Threats, Attacks, and Vulnerabilities
Sprint 2	Architecture and Design
Sprint 3	Implementing Secure Network Architecture
Sprint 4	Practice Sprint

Concepts covered:

- Types of Malware
- Social Engineering Attacks
- Advanced Persistent Threats
- Vulnerabilities and Exploits
- Frameworks, Guidelines, and Physical Security
- Secure Network Architecture Concepts
- Secure Systems Design
- Secure Staging Deployment Concepts
- Secure Application Development and Deployment
- Secure Communication Channels
- Network Configuration Management

CY-106

CompTIA Security+ Part Two

This unit delves into critical areas of cybersecurity, starting with Identity Management and Access Controls, exploring how they intertwine with common account practices. We then examine the importance of structured Policies, Plans, and Procedures alongside Business Impact Analysis and Risk Management. This informs our study of Incident Response Procedures, which are essential for effectively tackling breaches. Finally, we demystify Cryptography, discussing key algorithms, Public Key Infrastructure, and Cryptographic Attacks. This comprehensive study equips learners with a robust understanding and practical insight into cybersecurity, empowering them to safeguard digital landscapes confidently and competently.

Sprint 1	Identity and Access Management
Sprint 2	Risk Management
Sprint 3	Cryptography and PKI
Sprint 4	Practice Sprint

Concepts covered:

- Identity Management Concepts
- Identity and Access Management Controls
- Common Account Management Practices
- Business Impact Analysis Concepts
- Risk Management Processes and Concepts
- Incident Response Procedures
- Cryptographic Algorithms
- Public Key Infrastructure
- Cryptographic Attacks

CY-107

CompTIA Security+ Part Three

This unit will navigate the dynamics of Incident Response Management, Digital Forensics, and Disaster Recovery, complemented by a comprehensive understanding of legal and regulatory facets of cybersecurity. Further, we will explore risk management strategies, evolving technologies like IoT, Mobile, and Cloud Virtualization, and cybersecurity trends. This multidisciplinary approach culminates in a complete readiness to handle security challenges, empowering learners to safeguard digital environments effectively and proactively in the face of rapidly evolving threats.

Sprint 1 Operations and Incident Response

Sprint 2 Governance, Risk, and Compliance

Sprint 3 Emerging Technologies and Trends

Sprint 4 Practice Sprint

Concepts covered:

- Incident Response Management
- Disaster Recovery and Business Continuity
- Legal and Regulatory Concepts
- Privacy Concepts
- Risk Management
- Security Awareness and Training
- IoT and Embedded Systems
- Mobile, BYOD, and Small Form Factor Devices
- Cloud and Virtualization

Career acceleration to land your first Cybersecurity role, and beyond.

During the Career Accelerator, you will be actively looking for your first full-time Cybersecurity role. You will be learning everything you need to know about how to get hired for your dream job at a top tech company, while continuing to develop your technical and soft skills. Our goal here is to make you the ideal candidate for the role you are after, and to help you start your career as early as possible.

Career Workshops	Participate in extensive live workshops that are focused on developing your "elevator pitch", activating your personal and professional networks, learning job search and salary negotiation strategies, setting weekly goals, and more.
Squad Sessions	Join a Squad of a small number of your fellow students for weekly group sessions to share advice and drive each other forward. Squad Leaders are industry experts who bring their squad members from being job-ready to getting hired. You will meet your Squad Leader in Squad meetings and 1:1 sessions.
Advanced Learning	Continuous advanced training to keep sharpening your skills and expanding your experience and expertise, with additional challenges and projects to add to your portfolio. Topics include: Cloud Fundamentals, Application Security, Scripting for Security, Attacker Mindset, Purple Team.
Interview Preparation	Master your industry technical proficiency and your personal interviewing skills through taking part in live mock-interview simulations and receiving insightful, personal feedback from industry experts.
Job Search Toolkit	Be a pro candidate by tracking your opportunities, managing your job interview process, building your portfolio, and showcasing your projects with the best tools on the market to organize and accelerate your job search.
Our Career Week	Attend our Career Week, where you'll be able to meet representatives from leading tech companies that are looking to hire our graduates.