Opleiding
PECB IT Cyber Security Specialist

www.bpmo-academy.nl

Versie 01-08-2018

Wat doet een IT Cyber Security Specialist?

De Cyber Security Specialist is verantwoordelijk voor de beveiliging van de technologische infrastructuur van een bedrijf. De Security Specialist stelt een plan op om ervoor te zorgen dat een computernetwerk of website niet geïnfiltreerd kan worden door niet-geautoriseerde personen. Ook geeft de Security Specialist advies over de beveiliging van informatiesystemen die nog gebouwd moeten worden. Als de Security Specialist bovendien in vast dienstverband werkt verzorgt hij vaak ook het onderhoud van de beveiliging en garandeert zo de voortdurende bewaking van het systeem.

Naast het implementeren van (updates in) beveiligingssoftware is het natuurlijk ook belangrijk voor de Sercurity Specialist om een veiligheidsprotocol op te stellen. Het zijn niet alleen zwakke plekken in het systeem die toegang geven tot een netwerk, maar ook de gebruikers zelf. Deze moeten dus geïnstrueerd worden over hun werkgedrag en computergebruik, om zo te voorkomen dat ze per ongeluk virussen via het Internet binnenhalen of op andere manieren voor veiligheidsproblemen zorgen.

Hoe lang duurt de opleiding?

De opleiding tot IT Cyber Security Specialist duurt 6 maanden. Uw 10-daagse theorie training wordt aangevuld met een 5,5 maanden durende praktijkgerichte stage bij een of meerdere bedrijven.

Kosten van de opleiding

De opleiding kost €5000,00 exclusief 21% btw. Er bestaat de mogelijkheid dat de werkgever de opleidingskosten (deels) voor haar rekening wil nemen. Neem hierover met ons contact op.

Onderdelen van het opleidingstraject

- ISO 27032 Lead Cyber Security Manager (5 dagen)
- Lean Pen Test Professional (5 dagen)

ISO 27032 Lead Cybersecurity Manager

Why should you attend?

ISO/IEC 27032 Lead Cybersecurity Manager training enables you to acquire the expertise and competence needed to support an organization in implementing and managing a Cybersecurity program based on ISO/IEC 27032 and NIST Cybersecurity framework. During this training course, you will gain a comprehensive knowledge of Cybersecurity, the relationship between Cybersecurity and other types of IT security, and stakeholders' role in Cybersecurity.

After mastering all the necessary concepts of Cybersecurity, you can sit for the exam and apply for a "PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager" credential. By holding a PECB Lead Cybersecurity Manager Certificate, you will be able to demonstrate that you have the practical knowledge and professional capabilities to support and lead a team in managing Cybersecurity.

Who should attend?

- Cybersecurity professionals
- Information Security experts
- Professionals seeking to manage a Cybersecurity program
- Individuals responsible to develop a Cybersecurity program
- IT specialists
- Information Technology expert advisors
- IT professionals looking to enhance their technical skills and knowledge

Learning objectives

- Acquire comprehensive knowledge on the elements and operations of a Cybersecurity Program in conformance with ISO/IEC 27032 and NIST Cybersecurity framework
- Acknowledge the correlation between ISO 27032, NIST Cybersecurity framework and other standards and operating frameworks
- Master the concepts, approaches, standards, methods and techniques used to effectively set up, implement, and manage a Cybersecurity program within an organization
- Learn how to interpret the guidelines of ISO/IEC 27032 in the specific context of an organization
- Master the necessary expertise to plan, implement, manage, control and maintain a Cybersecurity Program as specified in ISO/IEC 27032 and NIST Cybersecurity framework
- Acquire the necessary expertise to advise an organization on the best practices for managing Cybersecurity

Educational approach

- This training is based on both theory and best practices used in the implementation and management of a Cybersecurity Program
- Lecture sessions are illustrated with examples based on case studies
- Practical exercises are based on a case study which includes role playing and discussions
- Practical tests are similar to the Certification Exam

Prerequisites

A fundamental understanding of ISO/IEC 27032 and comprehensive knowledge of Cybersecurity.

Lead Pen Test Professional

Why should you attend?

Lead Pen Test Professional training enables you to develop the necessary expertise to lead a professional penetration test by using a mix of practical techniques and management skills.

This course is designed by industry experts with in-depth experience in the Penetration Testing field. Unlike other trainings, this training course is focused specifically on the knowledge and skills needed by professionals looking to lead or take part in a penetration test. It drills down into the latest technical knowledge, tools and techniques in key areas including infrastructure, Web Application security, Mobile security and Social Engineering. In addition, this course concentrates on how to practically apply what is learned on current day-to-day penetration testing and does not expand on unrelated, dated or unnecessary theoretical concepts.

Along with the in-depth hands-on practical skills, this training course equips you with the management skills you need to lead a penetration test, taking into account business risks and key business issues. The individuals who complete the course have the right blend of the real business and technical competencies needed to be a respected, understood and professional penetration tester. On the last day of the training course, you will get to use the skills learned in a comprehensive capture and flag penetration testing exercises.

Who should attend

- IT professionals looking to enhance their technical skills and knowledge
- Auditors looking to understand the Penetration Testing processes
- IT and Risk managers seeking a more detailed understanding of the appropriate and beneficial use of Penetration Tests
- Incident handlers and Business Continuity professionals looking to use testing as part of their testing regimes
- Penetration testers
- Ethical hackers
- Cybersecurity professionals

Learning objectives

- Learn how to interpret and illustrate the main Penetration Testing concepts and principles
- Understand the core technical knowledge needed to organize and carry out an effective set of Pen Tests
- Learn how to effectively plan a Penetration Test and identify a scope which is suitable and appropriate based on risk
- Acquire hands-on practical skills and knowledge on relevant tools and techniques used to efficiently conduct a Penetration Testing

- Learn how to effectively manage the time and resources needed to scale a specific Penetration Test

Educational approach

- This training is based on both theory and best practices used in Pen Testing
- Lecture sessions are illustrated with examples based on case studies
- Practical exercises are based on a case study which includes role playing and discussions
- Practical tests are similar to the Certification Exam

Prerequisites

A fundamental understanding of Penetration Testing and comprehensive knowledge of Cybersecurity.