



IT-Security Practitioner

Cursusduur: 5 Dagen **Cursuscode: S-ITSP**

Beschrijving:

IT-Security Practitioner (ITSP) takes you deep into the pragmatics of securing an IT infrastructure. This certification enables you to exhibit your knowledge about all the aspects of IT-security a future security specialist needs to master. You will be tested on the latest technologies, trends, technical aspects and threat mitigation techniques.

Doelgroep:

This level is designed for professionals who are or expect to become responsible for IT-security in their organisations, thus need to have a solid grounding in the subject. For example: IT-Security Managers, IT-auditors, Junior and mid-level application, system and network administrators

Doelstelling:

- As you move along in the course, you will immerse yourself in attack trends and mitigation techniques, and you will perform hands-on assignments that ready you for accomplishing a Security Manager's tasks. You will complete exercises in the technical domain, including security zoning, system hardening, and firewall rule construction. In addition, you will perform traditional management activities, such as developing a company-wide security framework, creating a role-based access model, and determining benchmarks for information classification. Finally, you will try your hand at penetration testing in a simulated environment.
 - The knowledge and skills you develop in this course ready you for the Expert level, where you will develop into a competent Security Operations Centre (SOC) analyst.
 - Benefit from the insights of practicing Security Managers and cybersecurity advisors;
 - Apply IT security management principles to real-life situations;
 - Prepare for your certification assessment with a free sample exam.
-

Vereiste kennis en vaardigheden:

A good understanding of fundamental IT security terms, concepts and principles is required.

SECO IT-Security Foundation certificate (or equivalent) is recommended.

Cursusinhoud:

In particular, an S-ITSP certificate attests to your ability to:

- Translate relevant legal, regulatory and standard requirements and industry-best practices to a company-wide cybersecurity framework;
- Handle security incidents in line with incident management best practices, with special regard to the European Union Agency for Network and Information Security (ENISA) Good Practice Guide for Incident Management;
- Demonstrate an in-depth understanding of switches, routers, gateways, firewalls and intrusion detection systems;
- Design a secure network architecture;
- Apply basic Windows and Linux hardening techniques;
- Develop an implement a patch management policy;
- Demonstrate an in-depth understanding of application vulnerabilities and apply basic application hardening techniques;
- Identify security measures to counter the OWASP Top 10;
- Apply encryption to protect communications, file systems and files;
- Implement role-based access control;
- Use penetration testing tools to access a system and exploit an SQL injection vulnerability

Nadere informatie:

Neem voor nadere informatie of boekingen contact op met onze Customer Service Desk 030 - 60 89 444

info@globalknowledge.nl

www.globalknowledge.com/nl-nl/

Iepenhoeve 5, 3438 MR Nieuwegein