

How to secure your IT infrastructure? Learn how to secure your legacy, cloud and virtualized infrastructure.

According to the Belgian Federal Cyber Emergency Team security incidents 30% more were reported in 2015 than in 2014. What's more: cyber incidents become more and more complex. Securing the use of Internet for communication and business starts with understanding known threats and security techniques, following the C-I-A triad philosophy: confidentiality, integrity and availability. In this three-day course you learn the fundamentals of a secure virtualized enterprise infrastructure. Theory is illustrated with numerous demos of current security technologies and products.

Participants who complete the course will receive a certificate of completion allowing them to gain Continuing Professional Credits (CPEs). Those credits can be submitted for GIAC or ISC2 certification renewal. The most well-known ISC2 certification is the CISSP certification (Certified Information Systems Security Professional).

1. Essential security terminology and basic concepts
2. Crypto, hashing and PKI basics
3. Virtual Private Networks: SSL, TLS, ssh, IPSEC concept and terminology, Site-to-Site configuration
4. Network security: Internet Access Street (IAS) concepts, firewall overview and concepts, NAT, flows, proxy, SSL inspection, UTM, Next generation firewall, web application firewall, IPS/IDP
5. End-point security and malware protection: sandboxing, retrospection, baselining, detection: signature based, exploit based, behavioral
6. Incident response and forensics
7. Identity & access management: authentication, RADIUS basics, SSO, OTP
8. Virtualization concepts:
 - VM concepts, introduction to VMware ESXi 5.x, ...
 - Defining the Data Center (DC): definition, multi-tier, consumerization, Virtualized Multiservice DC (VMDC), layered security, DC multi tenancy, ...
9. Firewall virtualization: concept, advantages, CheckPoint Virtual Edition & VSX, SDN/NSX, micro-segmentation
10. Integrated Virtualization Services: traditional server security vs hypervisor security, example with Trend Micro Deep Security 9.x, VMware vShield, ...
11. Availability: introduction and concepts, high availability, clustering concepts, Distributed Denial of Service (DDoS), business continuity, disaster recovery
12. Monitoring, security and threat intelligence: SIEM

Prerequisites: a basic knowledge of IP networking is desired (Enterprise Networking is an excellent preparation for this course).