Maslak Mahallesi, Maslak Meydan Sk. No:5. Spring Giz Plaza. Maslak/İstanbul
+90 212 282 7700 - info@bilginc.com

IT Security Fundamentals

Eğitim Tipi: **Clasroom**

Süre: **5 Day**

Eğitim Hakkında

This 5-day instructor-led course serves as an in depth introduction to the field of Information Security - it is not aligned to a specific examination or vendor accreditation and therefore the content will be updated by QA on a regular basis.

The course allows delegate extensive hands-on experience with a variety of security software and techniques. The content is vendor-agnostic and focuses on general information security.

Target Audience

This course is designed for IT professionals and technical managers who want to understand key IT security issues and how best to address them. The course will also be of benefit to IT systems analysts, designers and software developers.

This course will be suitable for delegates interested in the SANS Institute course SEC401: Security Essentials.

Önkoşullar

- Previous knowledge and use of the Internet is essential, particularly awareness of TCP/IP and standard Internet services such as the World Wide Web, e-mail and DNS. This knowledge can be gained by attending our Introduction to Networking course
- The course requires an understanding of Microsoft Windows operating systems; and familiarity with Linux would be an advantage.

Neler Öğreneceksiniz

At the end of this course you will be able to:

- Understand the IT security threats faced by a modern network
- Understand the techniques used to mitigate these threats
- Respond to IT security incidents
- Understand IT security policies
- Understand cryptography and its uses
- Understand authentication mechanisms
- Understand the importance of physical security
- Understand the compliance and legal requirements of an organisation

Eğitim İçeriği

Introduction to Information Security

- Information Security fundamentals, Information Security models, IS standards, attack overviews.

Risk Management

- Risk management process, risk analysis, risk control.

Operating System Security

- Popular operating systems, OS hardening, vulnerabilities and the patch cycle, OS scanning.

Access Control

- Types of access control, physical access, controlling resource access, Microsoft Windows NTFS, Linux ext3/4, cloud security.

Encryption

- Introduction to cryptography, hashing, encrypting stored data, digital signatures, Public Key Infrastructure (PKI), encrypting network data,

Transport Layer Security, virtual private networks.

Authentication

- Authentication mechanisms, good password strategies, Microsoft Windows Kerberos, attacking Windows authentication, Linux authentication mechanisms, certificate-based authentication, biometric authentication.

Legal Compliance& Security Policies

- UK legal regulations, the role of security policies, writing security policies, ensuring business continuity.

Application Security

- General guidelines for application security, securing web applications, securing mail applications, securing databases.

Malware

- Types of malware, malware detection, malware removal, Trojans, rootkits, botnets, Spam delivery

Perimeter Security

- Network designs, mobile workers, firewalls, proxy servers

Attacking TCP/IP

- Weaknesses in TCP/IP, securing network devices, IPSec, Network Intrusion Detection, SNORT.

Wireless Network Security

- Introduction to wireless networking, problems with WEP, WPA2, mobile IP.