CompTIA Security+

Kestus: 40 akadeemilist tundi

Äripäev, Vana-Lõuna 39/1, Tallinn

Vaata kõiki toimumiskuupäevi

CompTIA Security+ koolituse eesmärgiks on anda IT-spetsialistidele edasi parimad praktikad tõrkeotsingu teemadel ning tagada seeläbi ulatuslikud teadmised ja oskused turvaprobleemide lahendamisel.

Koolitusel käsitletakse töökeskkonna turvalisuse hindamist ja sobivate turbelahenduste juurutamist ning hübriidkeskkondade (sealhulgas mobiil-, pilve- ja asjade interneti keskkonna) jälgimist ja turvamist. Õppe käigus harjutatakse turbeintsidentide kindlakstegemist, analüüsimist ja nendele vastamist lähtudes seadusandlusest.

Koolitus on mõeldud IT-spetsialistidele, kes omavad teadmisi operatsioonisüsteemidest ja nende administreerimisest ning kasutaja-aspektidest, kuid tahavad end lisaks täiendada küberhügieeni teemades.

CompTIA Security+ on sinu lähtepunktiks karjäärile küberturbe valdkonnas!

Koolitus aitab valmistuda uueks *SY0-601: Security+* eksamiks (jõustus 12. november 2020). **NB! Eksamit saab sooritada meie eksamikeskuses!**

The main purpose of CompTIA Security+ course is *to incorporate best practices in hands-on troubleshooting, ensuring candidates have practical security problem-solving skills required to:*

- ***Assess*** *the security posture of an enterprise environment and recommend and implement appropriate security solutions*
- ***Monitor and secure*** *hybrid environments, including cloud, mobile, and IoT*
- ***Operate*** *with an awareness of applicable laws and policies, including principles of governance, risk, and compliance*
- ***Identify, analyze, and respond*** *to security events and incidents*

In this course, students will gain the core knowledge required of any cybersecurity role and will be provided a springboard to intermediate-level cybersecurity jobs.

Jobs that use Securiy+: *Security Administrator, Helpdesk Manager / Analyst, Security Engineer / Analyst, IT Auditors, Systems Administrator,Network / Cloud Engineer, DevOps / Software Developer, IT Project Manager*

Target audience:

This course is designed for *information technology (IT) professionals who have networking and administrative skills in Windows®-based Transmission Control Protocol/Internet Protocol (TCP/IP) networks; familiarity with other operating systems, such as macOS®, Unix®, or Linux®; and who want to further a career in IT by acquiring foundational knowledge of security topics or using CompTIA Security+ as the foundation for advanced security certifications or career roles.*

After completing this course, students will be able to:

- Compare and contrast attacks.
- Compare and contrast security controls.
- Use security assessment tools.
- Explain basic cryptography concepts.
- Implement a public key infrastructure.
- Implement identity and access management controls.
- Manage access services and accounts.
- Implement a secure network architecture.
- Install and configure security appliances.
- Install and configure wireless and physical access security.
- Deploy secure host, mobile, and embedded systems.
- Implement secure network access protocols.
- Implement secure network applications.
- Explain risk management and disaster recovery concepts.
- Describe secure application development concepts.
- Explain organizational security concepts.

Prerequisites to the course (recommended):

To ensure your success in this course, you should have basic Windows user skills and a fundamental understanding of computer and networking concepts.

CompTIA A+ and Network+ certifications, or equivalent knowledge, and six to nine months' experience in networking, including configuring security parameters, are strongly recommended.

The training topics and description:

In this course, students will use fundamental security principles to install and configure cybersecurity controls and participate in incident response and risk mitigation.

- **Attacks, Threats and Vulnerabilities**

Focusing on more threats, attacks, and vulnerabilities on the Internet from newer custom devices that must be mitigated, such as IoT and embedded devices, newer DDoS attacks, and social engineering attacks based on current events.

- **Operations and Incident Response**

Covering organizational security assessment and incident response procedures, such as basic threat detection, risk mitigation techniques, security controls, and basic digital forensics.

- **Architecture and Design**

Includes coverage of enterprise environments and reliance on the cloud, which is growing quickly as organizations transition to hybrid networks.

- **Governance, Risk and Compliance**

Expanded to support organizational risk management and compliance to regulations, such as PCI-DSS, SOX, HIPAA, GDPR, FISMA, NIST, and CCPA.

- **Implementation**

Expanded to focus on administering identity, access management, PKI, basic cryptography, wireless, and end-to-end security.

Training Principles:

The training is held in Estonian, learning material is in English! Practical exercises run on virtual machines.

The achievement of learning outcomes is checked and assessed through independent practical work.

The prerequisite for issuing the certificate is full participation in training.

Length*:* 40 academic hours

Koolituse läbiviimise põhimõtted:

Koolitus toimub eesti keeles, õppematerjal on inglise keeles.

Praktilised ülesanded tehakse virtuaalmasinatel.

Õpiväljundite saavutamist kontrollitakse ja hinnatakse läbi iseseisva praktilise töö.

Tunnistuse väljastamise eelduseks on koolitusel osalemine terves mahus.

Maht: 40 akadeemilist tundi

Koolitushind sisaldab lisaks:

- õppematerjale;
- koolitaja konsultatsiooni õpitud teemade kohta e-posti teel pärast koolitust;
- tunnistust.

Lisaväärtusena pakume:

- sooje jooke koos küpsiste ja puuviljadega ;
- lõunasööki igal koolituspäeval;
- tasuta parkimist.

Koolitusel saab osaleda Töötukassa koolituskaardiga.

Näeme koolitusel!

LISAINFO

Osalemise tingimused

Registreerudes e-poe, e-kirja või telefoni teel, saadame Teile arve ja täpsema info osalemise kohta.
Üksteist päeva enne koolitust saadame Teile e-kirjaga meenutuse osalemise infoga.

Koolitusel osalemine on nimeline, kuid saate osalejat tasuta muuta kuni koolituse alguseni.

Koolituse eest tasumine toimub arvel viidatud arveldusarvele. Arve saadetakse maksja aadressile e-postiga. Arve tuleb tasuda enne koolituse algust arvel märgitud maksetähtajaks.

Kui Te ei saa mingil põhjusel osaleda, palun andke sellest kindlasti teada e-posti aadressil info@koolitus.ee või telefonil 618 1727 . Kui teatate koolitusel mitteosalemisest kuni 10 tööpäeva enne algust, pakume mõnd muud samaväärset koolitust või tagastame 100% tasutud koolituse maksumusest. Mitteosalemisest vähemalt 5 tööpäeva varem teatades, tagastame 50%. Muul juhul kuulub arve tasumisele. Raha tagastame ette antud summas juhul, kui pole tehtud koolituse korraldamisega seotud kulutusi (ostetud õppematerjale jms). Koolitusele mitteilmumisel, sellest mitteteatamisel või koolituse poolelijätmisel õppetasu ei tagastata.

IT Koolitusel on õigus koolitusgrupi mitte täitumisel koolituse toimumine edasi lükata või koolitus ära jätta. Koolitusele registreerunuid teavitatakse kursuse edasi lükkumisest või ära jätmisest telefoni või e-posti teel. Koolituse ära jäämisel korraldajatest tulenevatel põhjustel makstakse õppetasu tagasi. .

IT Koolitus on Eesti Töötukassa koolituskaardi koostööpartner. Tutvuge koolituskaardi infoga SIIN.
Täpsema info saamiseks võtke meiega ühendust telefonil 618 1727 või info@koolitus.ee.