CompTIA Security+

კიბერუსაფრთხოების სპეციალისტი

პროგრამა

SY0-701

კურსის ხანგრძლივობა: 3 თვე

სწავლების ენა: ქართული (ინგლისურენოვანი სახელმძღვანელოებით)

კურსზე დაიშვებიან მსმენელები 16 წლის ასაკიდან. ერთ-ერთი აუცილებელი წინაპირობა აიტი აკადემიაში სასწავლებლად არის ინგლისური ენის Elementary დონეზე ფლობა, რაც შემოწმდება მისაღებ გამოცდაზე

თემა 1. შესავალი უსაფრთხოებაში

უსაფრთხოების ფუნდამენტური ცნებები, CIA, Gap ანალიზი, კონფიდენციალურობა, შესაბამისი კრიპტოგრაფიული გადაწყვეტილებების გამოყენება, უსაფრთხოების კონტროლების გამოყენება

თემა 2. საფრთხეები, სისუსტეები და საფრთხეების შერბილება

Threat actors, მათი ატრიბუტები და მოტივაცია, საფრთხეების მიმართულებები და ვექტორები. Zero day. საფრთხეების იდენტიფიკაცია და იდენტიფიკაციის მეთოდები.

თემა 3. მავნე კოდი

Ransomware, Trojan, Worm, Spyware, Bloatware, Virus, Keylogger, Logic bomb, Rootkit

თემა 4. სოციალური ინჟინერია და შეტევა პაროლზე

Phishing, Vishing, Smishing, Watering hole, Brand impersonation, Typosquatting, Spraying, Brute force

თემა 5. უსაფრთხოების ტესტირება

საფრთხეების იდენტიფიკაციის, ანალიზის და მოგვარების მეთოდები, რეპორტინგი. მონიტორინგის ინსტრუმენტები. უსაფრთხოების პროგრამების მენეჯმენტი

თემა 6. აპლიკაციების უსაფრთხოება

Memory injection, Buffer overflow, Race conditions (Time-of-check (TOC), Target of evaluation (TOE), Time-of-use (TOU)), Malicious update, SQLi, XSS, Sandboxing, Software development ifecycle (SDLC))

თემა 7. კრიპტოგრაფია და PKI

Public key, Private key, Key escrow, დაშიფვრა, Hashing, Salting, ციფრული ხელმოწერა, ბლოკჩეინი, კრიპტოგრაფიული შეტევები

თემა 8. ვინაობის და წვდომის მენეჯმენტი

Authentication, Authorization, and Accounting, წვდომის კონტროლი, SSO, LDAP, OAuth, SAML, პაროლები, მულტიფაქტორული ავთენტიფიკაცია.

თემა 9. ფიზიკური უსაფრთხოება და მონაცემთა რეზერვირება

ფიზიკური უსაფრთხოების უზრუნველყოფა, Brute force, Radio frequency identification (RFID) cloning, Backups (Onsite/offsite, Frequency, Encryption, Snapshots, Recovery, Replication, Journaling)

თემა 10. ვირტუალიზაციის და ღრუბლოვანი უსაფრთხოება

ღრუბლოვანი უსაფრთხოების კონცეფცია, ვირტუალიზაციის სუსტი მხარეები.

თემა 11. კომპიუტერების უსაფრთხოება

TPM, HSM, Secure Enclave, Host Firewall, HIPS, პროტოკოლების და პორტების მართვა, DLP, Group Policy, SELinux, EDR, XDR

თემა 12. ქსელის უსაფრთხოება

შეტევები ქსელზე, DDOS, შეტევა DNS-ზე, SDN, Load Balances, IDS, IPS, NGFW, IPsec, TLS, VPN, SASE. სვიტჩების და როუტერების უსაფრთხოების ამაღლება

თემა 13. მობილური უსაფრთხოება

Side loading, Jailbreaking, BYOD, COPE, CYOD, MDM

თემა 14. უსაფრთხოების მონიტორინგი და პასუხი ინციდენტზე

მავნე აქტივობის იდენტიფიკაცია და მისი ინსტრუმენტები, ინციდენტის შემდგომი მოქმედებები, მომხმარებელთა დატრენინგება.

თემა 15. ციფრული სასამართლო ექსპერტიზა

Legal hold, Chain of custody, Acquisition, Reporting, Preservation, E-Discovery

თემა 16. უსაფრთხოების მმართველობა და შესაბამისობა

ბიზნეს პროცესების და უსაფრთხოების მოთხოვნების მორგება, დოკუმენტაცია, ვერსიების კონტროლი, პოლიტიკები, სტანდარტები და პროცედურები, ვენდორების შერჩევა. პროცედურების დარღვევის ან გვერდის ავლის შედეგები

თემა 17. რისკების მართვა და კონფიდენციალურობა

მონაცემთა ტიპები და კლასიფიკაციები, როლები რისკის მართვაში, რისკის მოხსენება, რისკების ზეგავლენა ბიზნესზე.