**Киберхавфсизлик департаменти, Мониторинг ва киберхавфсизлик ходисаларини хабар бериш бўлими, Киберхавфсизлик соҳасидаги илмий-техник ва инновацион фаолият бўлими, UZCERT, Киберхавфсизлик соҳасида ишланмалар департаменти ва сунъий интеллект бўлим ходимларининг киберхавфсизлик ва тармоқ технологиялари йўналишларида билим ва кўникмаларини ошириш мақсадида 2025 йил мобайнида амалга оширилиши режалаштирилган ўқув курслари**

**РЎЙХАТИ**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Т/р** | **Тадбир номланиши** | **Тадбир жойи** | **Иштирокчилар сони** | **Тадбир куни** | **Нархи**  **(минг сўмда)** | **Умумий сумма (минг сўмда)** | **Изоҳ** |
|  | Certified Information Systems Security Professional (CISSP) | Сингапур | 13 | 2 - чорак | 31 336 | 407 380 | Koenig Solutions томонидан тақдим этилаётган Certified Information Systems Security Professional (CISSP) курсининг мақсади - талабаларни ахборот хавфсизлиги бўйича кенг қамровли билим ва кўникмалар билан таъминлаш, уларни хавфсизлик сиёсатлари, риск бошқаруви, ва ҳуқуқий-меъёрий талабларни тушуниш ҳамда ахборот хавфсизлиги бўйича мутахассис сифатида юқори малакага эга бўлишларига ёрдам беришдир.   1. Security and Risk Management   Security concepts, governance, ethics, policies, frameworks, legal issues, risk management, and threat modeling.   1. Risk response, controls, and reporting. 2. Asset Security Asset classification, data lifecycle, and domain summary. 3. Security Architecture and Engineering Secure design principles, secure system components, physical security, cryptography, and environmental controls. 4. Communication and Network Security Network protocols, secure network design, monitoring, and network components. 5. Identity and Access Management (IAM) Identity-based access controls, managing identity lifecycle, and IAM domain summary. 6. Security Assessment and Testing Testing strategies, tools, remediation, and domain summary. 7. Security Operations Operation management, managed services, and incident management. 8. Software Development Security Secure coding, software development methodologies, and testing. |
|  | CCNP Enterprise: Core Networking | Тошкент, Ўзбекистон Республикаси | 8 | Сўровга асосан | Шартнома асосида | Шартнома асосида | Ўқув курси шаклида мутахассислар тармоқ қурилмалари, улардаги технологиялар ҳамда протоколлар билан ўзаро ишлаш бўйича ўз малакаларини оширадилар (бошланғич даражада). |
|  | CCNP: Enterprise Networking, Security, and Automation | Тошкент, Ўзбекистон Республикаси | 8 | Сўровга асосан | Шартнома асосида | Шартнома асосида | Ўқув курси шаклида мутахассислар тармоқ қурилмалари, улардаги технологиялар ҳамда протоколлар билан ўзаро ишлаш бўйича ўз малакаларини оширадилар (проффесионал даражада). |
|  | CompTIA Pentest+ Certification and Training | АҚШ | 12 | 3 - чорак | 20 900 | 250 694 | Ўқув курси шаклида мутахассислар ахборот тизимлари ва ресурсларини “pentest” қилиш бўйича улардаги заифликлар ва камчиликларни аниқлаш ва уларни бартараф этиш йўлларини, шунингдек хакерларнинг замонавий “инструмент”лари билан танишиш, уларни амалда қўллаш бўйича ўз малакаларини оширадилар.   1. Scoping Organizational Customer Requirements 2. Defining the Rules of   Engagement   1. Scanning Logical Vulnerabilities 2. Analyzing Scanning Results 3. Testing Wireless Networks 4. Targeting Mobile Devices 5. Performing System Hacking 6. Scripting and Software Development 7. Recommending Remediation 8. Performing PostReport Delivery Activities 9. Footprinting and Gathering Intelligence 10. Evaluating Human and Physical Vulnerabilities 11. Preparing the Vulnerability Scan 12. Avoiding Detection and Covering Tracks 13. Exploiting the LAN and Cloud 14. Attacking Specialized Systems 15. Web Application-Based Attacks 16. Leveraging the Attack 17. Pivot and Penetrate 18. Communicating During the PenTesting Process 19. Summarizing Report Components |
|  | Certified Penetration Testing Professional v1 (CPENT) | Англия | 13 | 3 - чорак | 31 010 | 403 136 | Ўқув курси шаклида мутахассислар қуйидаги модуллар бўйича ўз малакаларини оширадилар.   * + - 1. Introduction to Penetration Testing       2. Penetration Testing Scoping and Engagement       3. Open Source Intelligence (OSINT)       4. Social Engineering Penetration Testing       5. Network Penetration Testing – External       6. Network Penetration Testing – Internal       7. Network Penetration Testing – Perimeter Devices       8. Web Application Penetration Testing       9. Wireless Penetration Testing       10. IoT Penetration Testing       11. OT/SCADA Penetration Testing       12. Cloud Penetration Testing       13. Binary Analysis and Exploitation       14. Report Writing and Post Testing Actions |
|  | Pen 200 (OSCP) | Малайзия | 11 | Сўровга асосан | Шартнома асосида | Шартнома асосида | Ўқув курси шаклида мутахассислар қуйидаги модуллар бўйича ўз малакаларини оширадилар.   1. Penetration Testing with Kali Linux: General Course Information 2. Introduction To Cybersecurity 3. Effective Learning Strategies 4. Report Writing for Penetration Testers 5. Information Gathering 6. Vulnerability Scanning 7. Introduction to Web Application Attacks 8. Common Web Application Attacks 9. SQL Injection Attacks 10. Password Attacks 11. Client-side Attacks 12. Locating Public Exploits 13. Fixing Exploits 14. Antivirus Evasion 15. Windows Privilege Escalation 16. Linux Privilege Escalation 17. Port Redirection and SSH Tunneling 18. Tunneling Through Deep Packet Inspection 19. The Metasploit Framework 20. Active Directory Introduction and Enumeration 21. Attacking Active Directory Authentication 22. Lateral Movement in Active Directory 23. Enumerating AWS Cloud Infrastructure 24. Attacking AWS Cloud Infrastructure |
|  | Mobile Security Training | Mobile Device Security Training | Истанбул, Туркия | 10 | 2 - чорак | 23 502 | 235 026 | Ўқув курси шаклида мутахассислар иловани тескари муҳандислик орқали текшириш ва қуйидаги модуллар бўйича ўз малакаларини оширадилар   1. Android Bug Bounty 2. iOS pentesting 3. Android Game hacking 4. Construction and functions of other spy applications 5. Application hacking tools |
|  | Internet of Things: Connectivity and Networking | Сингапур | 9 | 2 - чорак | 32 642 | 293 783 | Ўқув курси шаклида  мутахассислар қуйидаги модуллар бўйича ўз малакаларини оширадилар.   1. Introduction to IoT and Connectivity 2. IoT Networking Technologies 3. IoT Security Fundamentals 4. IoT Privacy and Data Management 5. Advanced IoT Networking Technologies 6. IoT Security and Privacy Best Practices   IoT Project Development and Deployment |
|  | SEC450: Blue Team- Security Operations and Analysis. SANS organization | АҚШ,  Туркия | 10 | 1-чорак | 13 216 | 132 160 | SOC операцияларини тушуниш ва бошқариш. Кибертаҳдидлар ва хакерлик техникаларини аниқлаш. Ҳодисаларга тезкор жавоб бериш усулларини ўрганиш. Логларни тўплаш, таҳлил қилиш ва таҳдидларни аниқлаш. Хавфсизлик мониторинг воситаларидан фойдаланишни ўзлаштириш. GCDA (GIAC Certified Detection Analyst) сертификати берилади. |
|  | GCCD ( Global Cybersecurity Center for Development) seminar. KISA organization | Корея | 10 | 1-чорак | 6 450 | 64 500 | SOC ташкил этиш бўйича амалий маслаҳатлар. SOC операцияларини бошқариш ва таҳдид таҳлили усуллари. Киберхавфсизлик таҳдидларини аниқлаш ва уларга жавоб бериш. Таҳдидларни аниқлашда замонавий технологиялардан фойдаланиш.  Курс якунлангач расмий сертификат берилад |
|  | SOC Analyst and SOC Specialist | Хиндистон | 10 | 1-2-чорак | 400 | 4 000 | SOC таҳлилчиси ва SOC мутахассиси тайёрлаш. |
|  | SOC and AI integration. KAIST university | Корея | 14 | 2-чорак | 6 100 | 85 400 | SOC операцияларини автоматлаштириш. AI ёрдамида реал вақт режимида таҳдидларни аниқлаш. Таҳдидларни таҳлил қилишда Deep Learning ва Machine Learning моделларидан фойдаланиш.  Курсни муваффақиятли тамомлаган ўқувчиларга сертификат берилади. Бу сертификат сизнинг SOC ва AI соҳаларидаги билим ва кўникмаларингизни тасдиқлайди. |
|  | SOC with SIEM, ITSM and a SOC Ticketing System | Нидерландя | 7 | 1-2-чорак | 8 800 | 61 600 | Splunk: Илғор таҳдидларни аниқлаш ва уларга жавоб қайтариш имкониятлари.  QRadar: IBM томонидан ишлаб чиқилган ва хавфсизлик маълумотларини тезкор таҳлил қилиш учун мос келади.  Elastic Stack (ELK): Open-source воситаси бўлиб, маълумотларни йиғиш, таҳлил қилиш ва визуализация қилиш учун қулай. |
|  | Cyber Defence (SOC) Analyst Foundation Training Course | Тайвань | 12 | Сўровга асосан | 13 000 | 130 570 | SOAR (Security Orchestration, Automation and Response) платформаларидан фойдаланиш.  Cortex XSOAR, IBM Resilient. |
|  | Coursera 1 йиллик ваучер | онлайн | 2 | Сўровга асосан | 5 400 | 10 800 | Киберхавфсизлик соҳасидаги ахлоқий хакерлик, тармоқ билимлар, сунъий интелектнинг киберхавфсизлик билан боғлиқлиги каби 1000 дан ортиқ ўқув курсларни ўз ичига олган платформа. Шунингдек, Cоурсера платформасида Cомптиа сертификатларига ҳамда Google, Amazon, IBM каби соҳадаги йетакчи ташкилотларнинг ўқув дастурларига кириш имкониояти мавжуд. Ҳар бир курс тугагандан сўнг сертификат тақдим етилади. |
|  | Hack The Box 1 йиллик ваучер | онлайн | 3 | Сўровга асосан | 17 000 | 51 000 | Aхлоқий хакерликдаги янги хужум турларини ўрганиш ва синаб кўриш учун платформа |
|  | Advanced Web Application Penetration Testing – Advanced Level | Сингапур, Малайзия, Туркия | 13 | Сўровга асосан | 28 350 | 283 500 | Ўқув дастури қуйидагиларни ўз ичига олади: мураккаб заифликларни експлуатация қилиш, API хавфсизлиги (RESTful ва SOAP) ва хавфсизлик стандартлари (PCI DSS, OWASP Тop 10) билан ишлаш каби билимлар янада чуқурроқ ўргатилади. Шунингдек, мазкур билимлар курс давомида асосан амалиёт машқлари орқали ўргатилади. |
|  | Cyber Threat Intelligence | Венгрия | 13 | Сўровга асосан | 32 737 | 425 582 | Кибер таҳдидларни аниқлаш, уларни самарали бошқариш ва бартараф етишга йўналтирилган ўқув дастури, мазкур ўқув дастури бугунги кундаги актуал бўлган кибер таҳдидлар билан ишлаш бўйича янги билим ва кўникмаларни ўргатади |
|  | FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics | Япония, Буюк Британия, AҚШ, Aвстралия, Нидерландия, Қатар | 8 | Сўровга асосан | 130 950 | 1 047 640 | Ҳодисаларни текшириш ва таҳдидларни қидиришнинг ушбу чуқурлаштирилган курси мутахассисларга корпоратив тармоқларда кенг кўламли таҳдидларни, шу жумладан AПТ миллий давлатларининг рақиблари, уюшган жиноятчилик синдикатлари ва дастурий таъминот операторларининг товламачиларини кузатиш, аниқлаш, қарши туриш ва тиклаш учун илғор кўникмаларни беради. Ушбу курсда мутахассислар жиноятчиларнинг ишлаш усулларини тушуниб, компрометацияларни баҳолаш, ҳодиса қандай ва қачон содир бўлганлигини аниқлаш, компрометация ва зарарланган тизимларни тезда аниқлаш, зарарни баҳолаш ҳамда нима ўқилгани, ўғирлангани ёки ўзгартирилганини аниқлашни ўрганадилар.  Шунингдек, барча турдаги ҳодисаларни тўхтатиш ва бартараф етиш, криминалистикага қарши курашиш ва техник субйектлардан маълумотларни яширишга қарши илғор криминалистик кўникмаларни ривожлантириш усулларини ўзлаштирадилар. |
|  | FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques | Британия, AҚШ, Нидерландия | 10 | Сўровга асосан | 130 950 | 1 309 500 | Ушбу курс тизим ва тармоқ мониторинги, дизассемблер, созловчи ва бошқа кўплаб еркин фойдаланиш мумкин бўлган воситалардан фойдаланган ҳолда зарарли дастурий таъминотни қайта лойиҳалаш учун мустаҳкам асос яратади.  Курсда зарарли дастурий таъминотнинг ички ишини ўрганиш учун мослашувчан лабораторияни қандай созлаш ва зарарли дастурларнинг ҳақиқий намуналарининг хусусиятларини аниқлаш учун лабораториядан қандай фойдаланиш кераклиги ўргатилади. |
|  | PC-3000 технологияларидан фойдаланган ҳолда маълумот сақловчи қурилмалардан маълумотларни қайта тиклаш (ўқиш курсига 5 йўналиш киради) | Истанбул, Туркия | 8 | Сўровга асосан | 229 500 | 1 836 000 | Ушбу курсда мутахассислар PC-3000 технологияларидан фойдаланган ҳолда RAID маълумотларини тиклашни илғор даража ўрганадилар |
|  | Advanced APT Threat Hunting & Incident Response | онлайн | 5 | Сўровга асосан | 51 780 | 285 900 | Ушбу курс киберхавфсизлик соҳасида АРТ (Advanced Persistent Threats) гуруҳларининг ҳужум техникаларини аниқлаш, уларга жавоб бериш ва бартараф этиш бўйича амалий билим ва кўникмаларни оширишга қаратилган.  Курс давомида қатнашчиларга Россия, Хитой, Шимолий Корея ва Эрон АРТ гуруҳлари томонидан сўнгги икки йил ичида қўлланилган замонавий ҳужум техникаси ҳақида маълумот берилади. Ушбу техникаларни идентификация қилиш ва таҳлил қилишда амалий лаборатория ишлари таклиф этилади. |
|  | SEC565: Red Team Operations and Adversary Emulation™ | БАА, Недерландия, АҚШ, ФранцияГермания | 5 | Сўровга асосан | 155 340 | 776 701 | SEC565 курси иштирокчиларни рақиб симуляцияси асосида қизил жамоа (Red Team) операцияларини режалаштириш ва амалга ошириш бўйича билим ва кўникмалар билан таъминлайди. Курсда кибер таҳдид разведкасини ўрганиш, MITRE ATT&CK орқали ҳужум тактика ва техникасини хариталаш, корпоратив тармоқларда хавфсиз сизниш ва ҳаракатланиш, Active Directory ни таҳлил қилиш ва заифликларни аниқлаш, ҳамда муваффақиятли ҳисобот тайёрлаш ўргатилади.  Курснинг асосий мақсади ҳимоя стратегияларини яхшилаш учун ҳужум ва мудофаа ўртасидаги тажриба алмашинувини таъминлашдир. |
|  | Rogue Ops - Red Team 1 | онлайн | 5 | Сўровга асосан | 110 320 | 553 400 | ROPS-RT1 курси тингловчиларни ҳақиқий ҳолатга яқинлаштирилган Red Team баҳолашларини бажаришга ўргатади. Курс давомида иштирокчилар замонавий Red Team усуллари, воситалари ва техникаси билан танишадилар. Курснинг якуний қисмида тингловчилар янги реалистик муҳитда амалий сертификатлаш тестини топшириб, ўз билимларини амалий жиҳатдан синаб кўрадилар. Ушбу курс Red Team кўникмаларини такомиллаштириш ва ҳақиқий ҳужум сценарийларига тайёргарликни таъминлашга қаратилган. |
|  | DronSec платформасидаги барча курслар | онлайн | 5 | Сўровга асосан | 51 780 | 258 900 | DroneSec дрон таҳдидларини кузатиш ва таҳлил қилиш учун махсус яратилган платформа бўлиб, дрон таҳдидларига оид разведка хизмати ҳисобланади. У таҳдидларни ва уларга боғлиқ акторлар, тактика, техника ва процедуралар (TTPs) ҳақида маълумотга эга бўлиш имконини беради.  Дрон таҳдидларига қарши курашиш учун махсус яратилган, тўлиқ автоматлаштирилган ечимдир. У дрон таҳдидларини тезкор аниқлаш, кузатиш ва таҳлил қилиш учун ишлаб чиқилган.  Бу платформа дронларга оид таҳдидларни кузатиш ва унинг мураккаб сценарийларига тайёргарликни таъминлашда ёрдам беради. |
|  | MTIA - Certified Threat Intelligence Analyst | онлайн | 4 | Сўровга асосан | 7 767 | 31 068 | Ушбу курс кибер таҳдид разведкаси (CTI) бўйича мутахассисларни ўз таҳдид разведкасини ишлаб чиқариш кўникмалари билан таъминлашга қаратилган. Унда илғор киберхавфсизлик жамоаларига APT таҳдидларини аниқлаш, текшириш ва уларга жавоб бериш учун мураккаб техника ва усуллар ўргатилади.  MCSI сертификатига эга Таҳдид Разведкаси Аналитиги вазиятли таҳлиллар ўтказиш, разведка маълумотларини йиғиш, ишлаб чиқиш ва ҳужумларга қарши чоралар кўриш қобилиятига эга. У шунингдек, "hacking back" каби жавоб ҳужумларини амалга оширишга қодир.  Курс юқори малакали кибероператорларга Defend Forward қобилиятларини ривожлантириш учун махсус мўлжалланган. |
|  | Hex-Rays платформасидаги барча курслар | АҚШ, Франция | 5 | Сўровга асосан | 129 450 | 1 294 502 | Ушбу тренинг курслари IDA Pro ва Hex-Rays Decompiler каби кучли воситалар орқали реверс муҳандислик кўникмаларини такомиллаштиришга қаратилган. Курслар ҳам назарий билимлар, ҳам амалий машғулотларни ўз ичига олади ва соҳанинг тажрибали экспертлари томонидан ўтказилади. Бошланғич даражадаги иштирокчилардан тортиб, тажрибали мутахассисларгача барча учун мослаштирилган даражаларда машғулотлар таклиф этилади. |
|  | Signal Labs: Reverse Engineering | онлайн | 5 | Сўровга асосан | 58 253 | 582 526 | Курс зарарли дастурларни таҳлил қилувчилар, заифликларни тадқиқ қилувчилар ва Windows кодларини дисассемблировка/декомпиляция қилиш орқали унинг ички ишлашини тушуниш ёки патч қўллаш зарурати бўлганлар учун мосдир.  Бошланғич ва ўрта даражадаги Windows реверс муҳандислик тажрибасига эга иштирокчилар учун мос бўлиб, илғор машқлар (масалан, мураккаб код таҳлили) ҳам қамраб олинади. Курсда ёпиқ манбали фойдаланувчи ва ядро мақсадли дастурларига нисбатан ҳақиқий дунё реверс муҳандислиги амалга оширилади ва Rust тилидаги махсус деобфускация усулларини ишлаб чиқиш ҳам ўрганилади. |
|  | 5 Days Machine Learning Specialization | Малайзия | 5 | 2 - чорак | 14 770 | 73 850 | Дастурда Python асослари, маълумотлар таҳлили ва визуализацияси, машина ўрганиш ва нейрон тармоқлар ўрганилади. Биринчи куни Python'га кириш, маълумот турлари, операторлар, цикллар, функциялар ва модуллар тушунтирилади. Иккинчи куни Python'да маълумотларни тайёрлаш, трансформация қилиш, визуализация ва таҳлил қилиш ўргатилади. Учинчи куни Scikit-Learn ёрдамида машина ўрганиш усуллари, жумладан классификация, регрессия, кластерлаш ва асосий компонентлар таҳлили муҳокама қилинади. Тўртинчи куни TensorFlow билан асосий нейрон тармоқлар, чуқур ўрганиш, регрессия ва классификация ўрганилади. Бешинчи куни эса TensorFlow асосида конволюцион нейрон тармоқлар (CNN), трансфер ўрганиш ва рекуррент нейрон тармоқлар (RNN) билан ишлаш кўникмалари берилган. |
|  | AI and Cybersecurity | Сингапур | 10 | 2 - чорак | 38 185 | 381 850 | Ушбу курсда сунъий интеллект тизимларининг таҳдид моделлари, машина ўрганишга асосланган AI тизимларидаги заифликлар ва уларни ҳимоя қилиш усуллари ўрганилади. Шунингдек, AI ёрдамида киберхавфсизликни мустаҳкамлаш ва AI билан амалга ошириладиган ҳужумларга қарши чоралар кўриш йўллари муҳокама қилинади. |
|  | AI-Powered Cybersecurity: Threat Detection & Response Training Course | Хитой | 10 | 2 - чорак | Шартнома асосида | Шартнома асосида | AI-Powered Cybersecurity — бу сунъий интеллект ва киберхавфсизликни бирлаштириб, таҳдидларни аниқлаш, уларга жавоб бериш ва олдини олишни кучайтиришга йўналтирилган тренинг. Ушбу курс AI технологияларидан фойдаланиб, таҳдидларни аниқлаш ва зарарсизлантириш усулларини ўргатади.  Курс бошланғич даражадаги киберхавфсизлик мутахассислари учун мўлжалланган бўлиб, улар AI ёрдамида таҳдидларни яхшироқ аниқлаш ва жавоб қайтариш имкониятларини ўрганадилар.  Тренинг якунида иштирокчилар AI’нинг киберхавфсизликдаги қўлланилиши, таҳдидларни аниқлаш учун AI алгоритмларидан фойдаланиш, AI ёрдамида ҳодисаларга автоматик жавоб бериш ва мавжуд киберхавфсизлик инфратузилмасига AI’ни интеграция қилиш кўникмаларига эга бўладилар.  Курс интерфаол маърузалар ва муҳокамалар, амалий машғулотлар ва жонли лаборатория муҳитида бажариладиган тажрибаларни ўз ичига олади. |
|  | AI and big data analytics training (AI and data professional) | БАА | 5 | 4 - чорак | 10 775 | 53 875 | Дастур катта ҳажмдаги маълумотлар (Big Data) ва уни таҳлил қилиш усулларига йўналтирилган. Унда технологик-нейтрал моделлар, асосий машиналари ўрганиш (Machine Learning) техникалари, Big Data иловаларини ишлаб чиқиш методологияси ва NOSQL экотизими каби мавзулар қамраб олинади. Шунингдек, тармоқ таҳлили, графлар ва регрессия усуллари, MapReduce билан боғлиқ жараёнлар ва булутли ҳисоблаш технологиялари ҳам ўрганилади. |
|  | AI and big data fundamental course in Huawei | Хитой | 10 | Сўровга асосан | Шартнома асосида | Шартнома асосида | Курсда сунъий интеллектнинг асосий тушунчалари, ривожланиш йўналишлари ва Huawei’нинг AI стратегияси ўрганилади. Иштирокчилар машинавий ўрганиш, маълумотларни қайта ишлаш, модел яратиш ва баҳолаш усулларини ўзлаштирадилар. Тасвир, овоз ва матн ишлаш асослари ҳамда MindSpore фреймворкида AI дастурларини ишлаб чиқишни ўрганадилар. Huawei Ascend ва Cloud EI платформалари, шунингдек, reinforcement learning, generated adversarial network, knowledge graph, automatic smart driving ва quantum computing каби замонавий AI технологиялари билан танишадилар. |