Curriculum

Õppekava Eesti keeles
https://www.ettevotluskeskus.ee/vCYBRen-google-cybersecurity-professional-certificate
https://www.coursera.org/professional-certificates/google-cybersecurity

Training Institution Name	Ettevõtluskeskus OÜ
Curriculum Title	Online Training vCYBRen Google Cybersecurity Professional Certificate (with mentoring session in English/Estonian/Russian) Curriculum Title in Estonian Küberturvalisus (Google spetsialisti sertifikaat)
Curriculum Code	vCYBRen
Curriculum Group	Informatsiooni- ja kommunikatsioonitehnoloogia - Informatsiooni- ja kommunikatsioonitehnoloogia
Target Learners	● Aspiring Cybersecurity Professionals: Individuals interested in starting a career in cybersecurity. This includes those without a degree or prior experience in the field. ● Career Switchers: Professionals from other industries looking to transition into the high-demand field of cybersecurity. ● Continuous Learners: Individuals seeking to expand their knowledge and skills, particularly in Python, Linux, SQL, and other cybersecurity tools and techniques. ● Professionals Aiming for Certifications: Individuals who want to prepare for the CompTIA Security+ exam and other industry-recognized certifications. ● Hands-On Learners: Those who prefer a practical, hands-on approach to learning, with a focus on real-world scenarios and applied learning activities. ● Google Career Aspirants: Individuals interested in applying for jobs with Google and its partner organizations after course completion.
Purpose of Learning	The purpose of the Google Cybersecurity Professional Certificate program is to provide learners with essential skills and knowledge for a career in cybersecurity. We offer practical training in vital tools and techniques, prepares participants for industry certifications, and facilitates connections with top employers, ensuring job readiness in this high-demand field. The program is accessible to a broad range of learners, including those without prior experience or degrees, and focuses on delivering a comprehensive, hands-on educational experience.
Curriculum Development Basis	Based on the Google Cybersecurity course on Coursera, "Google Cybersecurity Professional Certificate ," covering modules 1-8.

Learning Outcomes	A student who has completed the Google Cybersecurity Professional Certificate: 1. Recognizes Core Cybersecurity Skills: Understands the essential skills and knowledge necessary for a cybersecurity analyst role. 2. Identifies Security Attack Impacts: Can pinpoint how security breaches affect business operations and explain the importance of security ethics. 3. Proficient in Cybersecurity Tools: Knows common tools used by cybersecurity analysts and understands the key threats, risks, and vulnerabilities to businesses 4. Understands Security Frameworks and Controls: Has knowledge of how organizations implement security frameworks and controls to protect operations, and can define commonly used SIEM tools 5. Responds to Threats with Playbooks: Capable of using playbooks to address threats, risks, and vulnerabilities effectively 6. Secures Networks and Data: Has the ability to secure networks against intrusion tactics and understands data transmission in networks. 7. Applies System Hardening Techniques: Knows how to harden systems, understands the interplay between operating systems, applications, and hardware, and can navigate Linux using command-line interface. 8. Uses SQL and Linux Effectively: Proficient in managing file systems with Linux commands and retrieving data using SQL. 9. Analyzes Risks and Threats: Skilled in classifying assets, analyzing attack surfaces, identifying threats like social engineering and malware, and understands threat modeling. 10. Handles Security Incidents: Knows how to contain, eradicate, and recover from incidents, analyzes network communications, and understands IDS and NIDS tools. 11. Investigates Events with SIEM Tools: Can perform queries in SIEM tools to investigate cybersecurity events. 12. Utilizes Python in Cybersecurity: Uses Python for cybersecurity tasks, creates custom functions, employs regular expressions, and practices code debugging. 13. Prepared for Cybersecurity Career: Ready to escalate security incidents, engage with the cybersecurity community, seek cybersecurity job opportunities, and prepare for job interviews.
Preconditions for enrollment to the training	Skills required to start studying: ● Basic Computer Literacy: Familiarity with basic computer use, such as using a web browser, installing software, and understanding basic computer terminology. ● Language Proficiency: A good understanding of English is essential, as the course materials, instructions, and interactions are conducted in English. The program is open to all, regardless of previous educational background or professional experience in cybersecurity. Those interested in the training can receive initial feedback on the suitability of this particular training. During this process, it will become clear

	how realistic it is to attend real-time online seminars and whether it is necessary to participate in on-site training sessions with more trainer support. Tripod test VVS, at least 30% average result (mathematical, spatial, and logical). The test is conducted in English because Coursera tests are in English. If there are more applicants than available places, learners will be selected based on the score ranking. There will be a waiting list and an opportunity to participate in the next group if there are more learner candidates than the group capacity.
Estimated time for studies, including online group meetings and independent learning	Total training volume: 250 academic hours. Independent work: 224 hours of independent learning, including independent study and preparation of homework for group meetings. Mentor sessions: 26 hours of online group meetings.
Independent learning	Independent work tasks are: 1. Completing exercises and tests in Coursera, including small-scale practice tests (quizzes) and larger tests (challenges) at the end of each module. 2. Optional case study submitted to Coursera. 3. Tasks provided by the mentor coach, which the learner completes before individual and group mentoring sessions. Mentor coaches and peer learners provide feedback on specific assignments and projects, such as analyzing a simulated cybersecurity threat and suggesting mitigation strategies, evaluating the student's use of cybersecurity tools in a lab environment to detect and respond to intrusions, reviewing the setup and configuration of network security measures in a simulated scenario, assessing the implementation of system hardening techniques on a given operating system or application, critiquing Python scripts written for automating cybersecurity tasks, and providing insights on the development and presentation of a comprehensive cybersecurity project that encapsulates various aspects of the course, including threat analysis, tool usage, incident response, and system security. This feedback is tailored to improve practical skills and theoretical understanding in real-world contexts. The weekly estimated workload of independent learning varies from 4-5 academic hours depending on the learner's previous exposure. The learner will be given access to the Coursera learning environment on the training start date. Those who finish the course in the expected time will be granted additional access for two months to revisit and consolidate what they have learned.
Topics and learning content	Key topics: Python Programming, Security Information and Event Management (SIEM) tools, SQL, Linux, Intrusion Detection Systems (IDS)

	Learner 1. Takes the Tripod VVS test: mathematical, spatial, and logical thinking and discusses the test results with the program manager. 2. Plans their learning with the support of the program manager. 3. Completes the Google Cybersecurity Professional Certificate path: https://www.coursera.org/professional-certificates/google-cybersecurity Attends real-time online meetings with mentor coaches, presentations, and guidance for independent learning. Sample course plan: [vCYBRSen] - Google Cybersecurity Professional Certificate plan
Training methods	Various active learning methods are used in the training, including case studies, practical work, and independent work. Work in small groups and peer to peer feedback is used.
Description of the learning environment	Independent learning takes place in the Coursera learning environment, access is granted to accepted learners. An internet-connected mobile device is required. Meetings with the mentor and group work are online real time activities.
List of learning materials	The learner completes the Coursera "Google Cybersecurity Professional Certificate" learning path. Completes self-tests at https://www.coursera.org/professional-certificates/google-cybersecurity
Completion conditions and issued documents	A certificate of completion of the training is issued if the learner achieves the learning outcomes and has successfully completed all 8 courses on the Coursera learning platform. These courses comprise the comprehensive Google Cybersecurity Professional Certificate learning path. This includes passing tests with at least 80% correct answers in each test (automated assessment on the Coursera learning platform, tests can be retaken until the desired threshold of correct answers is reached). In addition, a Coursera's Google Cybersecurity Professional Certificate is issued to the learner who completes all Coursera assignments (exercises and tests) and submits the optional case study in the Coursera environment. If the learner did not achieve all learning outcomes or did not want to be assessed, a certificate of participation is issued.
Description of the Qualifications, Learning, or Work Experience Required to Conduct the Training	All trainers have higher education, work experience in the field they teach, and experience in training adults. Short introductions of trainers can be read on the specific training page.
Curriculum approval time	