



**Telenor Common Operation (TnCO),
recently founded internal Technology Service Provider offering IT and
Network operation services to Telenor business units
is currently looking for candidates for the following position:**

Vulnerability Assessor

Are you our new vulnerability assessor?

We are lifting up our security verification capabilities to the next level and our new colleagues will play a key role in systematic discovery of existence of security vulnerabilities within the Telenor's digital products (DPs) and information assets (IT and telco network infrastructure, applications, etc.) before an adversary does.

Working with us your main responsibility will be to:

- Conduct vulnerability scans for IP and/or telco networks, web applications and infrastructure (OS & DB) to identify security vulnerabilities that cyber attackers could exploit,
- Analyse results and eliminate false positives,
- Deliver and present comprehensive report as a complete and prioritized list of vulnerabilities.

In order to achieve agreed goals in this role you will:

- Use automated tools to pinpoint vulnerabilities and reduce time-consuming tasks
- Use manual testing techniques and methods to gain a better understanding of the environment and reduce false negatives
- Develop, test and modify custom scripts and applications for vulnerability testing

In addition, with your expertise, you will support other teams to mitigate the findings and to validate mitigation results.

Monitoring and research of industry information sources for zero-day threats and emerging security trends and vulnerabilities impacting the organization is needed for your everyday work but also to support the organisation with recommending additional security solutions or enhancements to existing solutions in order to improve overall security of the company.

About you:

We are looking for more people to this role, with slightly different background, so if you like the job description above and if you have majority of the skills, qualifications or experience below, we want to hear from you!

- Desirable to have at least one of the following certifications: CEH, CPT, CEPT, GPEN, OSCP, CISSP, GCIA, CVA
- Security-related experience with practice in vulnerability assessments and/or penetration testing
- Familiar with the following technologies:
 - Computer hardware and software systems
 - Windows, UNIX and Linux operating systems
 - Web-based applications, OWASP
 - C, C++, Java, ASM, PHP, PERL
 - Network scanning tools
 - Security tools and products
 - Telco core network and signalling
 - Vulnerability analysis and reverse engineering
 - Metasploit framework
- Commitment to stay on top of the technology
- Possess an understanding of secure architecture designs
- Curious, creative, attention to details and out-of-the-box thinking
- Excellent communication skills in English – written and verbal
- Ability to present information concisely, to identify key issues clearly and to educate other teams about better security practices
- Live the highest ethical standards