	• Good knowledge of secure coding practices and security testing methodologies and standards like OWASP, OSSTMM, CERT and ISSAF guides and standards. • Ability to consult and proactively enforce building of security in all phases of application development • Knowledge about detective (alerting) and defensive mechanisms that can be built into web applications • Secure configuration of application middleware components • Strong hands-on knowledge on penetration testing and security assessment on Web application and related middleware layers including both manual testing and use of automated tools. • Up to date expertise in testing and remediating OWASP Top 10 and CWE/SANS Top 25 vulnerabilities • General knowledge of IT security including Operating Systems,, containers, Network, Middleware (e.g. Apache, Wildfly, Tomcat) and databases (e.g. Oracle, MSSQL). • Security event / incident analysis and threat hunting • Security incident management, both in collaboration and independent manner
Experience	• Working in an international/multicultural environment. • Minimum 8 years in IT, of which minimum 5 years' experience in technical security of enterprise-scale IT systems, preferably within a high security environment. • Minimum 3 years' experience in hands-on testing of web applications. • Minimum of 3 year experience in one or more of the following: security event analysis, security incident detection, security incident management, threat hunting. • Minimum of 1 year experience in supporting secure software development, for example performing threat analysis, providing support to system and software architecture work, training and supporting secure coding practices, building security defences or building security event logging into web applications • Minimum of 1-year experience in secure configuration of web application middleware components. • Experience in the range of IT security including Operating Systems, Network, Middleware and databases.
Nature of the tasks	• Carrying out security testing of developed bespoke applications, audits and IT processes security assessments. • Technical evaluations of security requirements. • Performing threat analysis and designing security measures to remediate threats. • Reviewing and consulting system and software architecture in security aspects • Training and coaching in secure coding and application development practices, including how to build detective and defensive capabilities into web applications • Organising and performing IT security testing, including penetration testing. • Secure configuration of application middleware components • Security event analysis, incident detection and threat hunting