|  |  |
| --- | --- |
| Job title: Vulnerability Analyst | Location: Gibraltar / Hyderabad |
| Function: Product and Tech  Reports to: Vulnerability Management, Red Team Lead | No. of direct reports: None  No. of non-direct reports: None |
| Budgetary responsibility: None | NGR/P&L: |
| Purpose of role | |
| We’re Entain. Powered by our very own technology and building products that push boundaries, Entain is home to a global family of more than 25 well-known brands and over 24,000 people, but we all play for the same team. When we win, we win together.  Our vision is to be the world leader in betting, gaming and interactive entertainment by bringing moments of excitement into people’s lives. We will achieve this through our focus on sustainability and growth, driving change in the fast-paced world of entertainment.  As a Vulnerability Analyst you will work closely with teams across the group to identify and correct security vulnerabilities, ensuring that systems and devices are properly maintained in order to reduce the possibilities of malicious actors to compromise them. In addition, you will keep probing the company’s infrastructure to detect flaws that will affect our security posture.  The role takes a hands-on approach to identify any known flaws on our current infrastructure and applications and develop the technical designs to mitigate them. | |
| Key responsibilities | |
| * Executes robust penetration test scopes that ensure penetration tests meet all certification and compliance requirements. * Identifies gaps and areas of improvement in penetration testing and vulnerability remediation/threat mitigation. Responsible to review, assess, track and mitigate identified vulnerabilities. * Executes threat, vulnerability, and risk analysis, determines mitigating and remediation capabilities, provides guidance, assesses inherent and residual risks and articulate results. * Develop/Adapt/Verify exploits to prove the criticality of disclosed vulnerabilities against the group systems * Develop applications to test security in the group environment and integrate with other internal tools. * Stay up to date with new vulnerabilities being disclosed that affect our state and communicate to teams across the organization. * Champions, continuously develops and shares with the wider team knowledge on emerging trends and changes in security testing. * Contributes to the development of red teaming, penetration testing, code scanning, and vulnerability management policies and procedures. * Operate the vulnerability management infrastructure. * Oversee external security testing providers, including bug bounty platforms. * Follow-up on identified issues until bringing them to closure. * Monitor the patch level of the company servers and devices. * Investigate attack trends that might affect the organization. * Make sure the company is compliant against our regulatory requirements imposed by the industry in which we operate.   **Occasional Responsibilities:**   * Support on Security Incidents investigations. * Respond to critical incidents on a 24x7 basis | |
| Specialist skills and experience | |
| **Knowledge/Expertise/Qualifications:**  The role requires a team player with strong technical foundations, hands-on information security skills, attention to detail and good problem-solving skills.  Essential   * At least two-year experience in a similar Information Security position * Vulnerability research skills * Experience in security assessments, pentesting web applications and infrastructure. * Experience developing security tools and open source projects * Attention to detail and good problem solving skills * Very good knowledge of the technical foundations behind networking, operating systems and applications   + TCP/IP   + Linux   + Windows   + Web technologies   + Other networking protocols * Good understanding of Information Security processes and theory * Good communication skills and customer-facing experience * Experience in the following areas:   + Vulnerability management   + Risk management   Desired   * Security Certification (GIAC, OSCP, etc.) or similar qualification * Experience integrating systems and tools via API’s * Online Gaming security experience * Experience in Application Security * Experience in red teaming * Regulatory and industry standards work: ISO27001, PCI-DSS, etc.   Other relevant professional qualifications will be considered, although not a requirement, e.g. CISA, CISM, CISSP, GIAC, etc. | |
| Competencies / behaviours | |
| This part of the job description summarises the behaviours necessary to succeed in the role.   * Stakeholder engagement: Builds effective working relationships * Collaboration: Communicates effectively with a positive impact * Agility: Quickly adapts and remains flexible while managing risks * Drives performance: Continually raises the bar for oneself (and others) * Delivers results: Plans for success and gets the job done | |
| Diversity and equal opportunities:  As a global employer, Entain is committed to providing a safe, fun, and inclusive culture where our people feel like they truly belong.  We are a multicultural business that values, celebrates and respects individual differences, so whatever your sexuality, gender, gender identity, ability, age, race, religion or belief, you will have a voice here, and the space to do your best work.  Our diverse internal networks provide the support for you to express your views and make a positive difference. | |