Job title: Cybersecurity Analyst (Security Operations Center Analyst (Tier 2) – Security Operations)	Location: Gibraltar & Hyderabad
Function: *Cybersecurity* Reports to: Security Operations Center Manager	No. of direct reports: N/A No. of non-direct reports: N/A
Budgetary responsibility: N/A	NGR/P&L: N/A

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.

This role works closely with teams across the group to identify and handle security incidents, ensuring that relevant security attacks are timely detected, investigated and mitigated. In addition, it reviews the security risks that our organization faces, executing appropriate responses to ensure our security posture remains aligned with the needs of our dynamic organization.

Key responsibilities

- Monitor security events and identify potential incidents across the organization environments (Corporate, Production, Development)
- Review alerts, assess risks and prioritize incident investigation efforts.
- Develop security tools and integrations to automate security operation processes.
- Interface with technical and business units to identify the source of the incidents and the appropriate resolution.
- Identify "lessons learned" together with other organizational teams.
- Investigate security incidents. Produce accurate and timely reports on Information Security incidents so that mitigation measures can be effectively decided and implemented.
- Assist technical teams in gathering incident evidence and remediating issues.
- Operate and Tune security consoles configuration.
- Conduct forensic analysis as required during the investigation of incidents.
- Support the fraud investigation teams on their incident investigations.

Occasional Responsibilities:

- Respond to critical incidents on a 24x7 basis.

Specialist skills and experience

The role requires a team player with strong technical foundations, hands-on information security skills, attention to detail and great problem-solving skills.

Essential

- At least two years' experience in a similar Information Security position
- Experience developing security tools and open-source projects.
- Attention to detail and great problem-solving skills.
- Outstanding 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
- Vulnerability research and exploitation skills
- Autonomous and self-organized
- Good communication skills and customer-facing experience
- Experience in the following areas:
    - Vulnerability management
    - Risk management.
    - Traffic and packet analysis

Desired

- Security Certification (GIAC, OSCP, etc.) or similar qualification
- Experience configuring and maintaining SIEM tools.
- Experience in creation of log correlation and incident detection rules.
- Experience managing security consoles and log correlation solutions.
- Online Gaming security experience
- Experience in forensic analysis.
- Experience in security assessments.
- Experience securing Microsoft protocols.
- 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

- Works well with others, a good collaborator, communicates effectively with a positive impact, a team player and builds effective working relationships.
- Agility: Quickly adapts and remains flexible while managing risks
- Builds capability: Invests in developing oneself (and others)
- Acts with integrity: Takes ownership and does the right thing

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.