Job Title Security Operations Team Lead

Department Information Security

Location Hybrid – Manchester/Home

Reporting Line Head of Information Security

Direct Reports 1

**Job Purpose**

Our Information Security team help maintain the availability, confidentiality, and integrity of BPP’s data and systems. As the **Security Operations Team Lead** you will report to the Head of Information Security and be responsible for developing and managing the day-to-day security operations across the Group.

**Key Responsibilities**

* Manage the day-to-day operations of the Security Operations Centre (SOC) in partnership with our managed service provider.
* Develop the maturity of the Security Operations function across the Group.
* Produce monthly reporting on the on the performance of the unction for the Head of Information Security.
* Defining scope and conducting vulnerability assessments using internal tooling.
* Define penetration testing schedule and tracking remediation action from the tests.
* Detect, investigate, and respond to incidents and events, including leading on root cause analysis.
* Ensuring consistent controls, polices, and procedures are in place across the Group.
* Working with key stakeholders across the Group to ensure that systems are
* Developing and growing a team.

**Skills**

* Experience managing a 24/7 SOC capability using Managed Service Provider and in-house staff.
* Effective verbal and written communication skills, with the ability to collaborate with cross-functional teams with varying technical ability.
* Experience working with security frameworks and compliance standards, including ISO27001, Cyber Essentials Plus, NIST and PCI-DSS.
* Experience leading and developing a team.
* Analytical thinking.
* Strong problem-solving skills.
* Takes ownership of own development by ensuring that skills are kept up to date, in line with industry changes.
* Experience with vulnerability management tools, such as Tenable.io.
* Experience with SIEM and SOAR platforms.